IntechOpen

Advanced Technologies of Quantum Key Distribution

Edited by Sergiy Gnatyuk

ADVANCED TECHNOLOGIES OF QUANTUM KEY DISTRIBUTION

Edited by **Sergiy Gnatyuk**

Advanced Technologies of Quantum Key Distribution
http://dx.doi.org/10.5772/65232
Edited by Sergiy Gnatyuk

Contributors

Oleg Morozov, Airat Sakhabutdinov, Il'Daris Gabdulkhakov, Gennady Morozov, Mhlambululi Mafu, Makhamisa Senekane, Er'El Granot, Tiago Debarba, Farid Ablayev, Marat Ablayev, Neslihan Nesliye Pelen, Ayşe Feza Güvenilir, Kaymakçalan Billur, Wen Wei, Luis Lizama, Mauricio López, Eduardo De Carlos Lopez, Aghaddin Mamedov

Notice

Statements and opinions expressed in the chapters are these of the individual contributors and not necessarily those of the editors or publisher. No responsibility is accepted for the accuracy of information contained in the published chapters. The publisher assumes no responsibility for any damage or injury to persons or property arising out of the use of any materials, instructions, methods or ideas contained in the book.

First published in London, United Kingdom, 2018 by IntechOpen
eBook (PDF) Published by IntechOpen, 2019
IntechOpen is the global imprint of INTECHOPEN LIMITED, registered in England and Wales, registration number: 11086078, The Shard, 25th floor, 32 London Bridge Street
London, SE19SG – United Kingdom
Printed in Croatia

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Additional hard and PDF copies can be obtained from orders@intechopen.com

Advanced Technologies of Quantum Key Distribution
Edited by Sergiy Gnatyuk

p. cm.

Print ISBN 978-1-78923-196-0

Online ISBN 978-1-78923-197-7

eBook (PDF) ISBN 978-1-83881-243-0

Meet the editor

Dr. Sergiy Gnatyuk obtained his master's degree in Information Security and PhD degree in Cybersecurity (Quantum Cryptography) from the National Aviation University, Kyiv, Ukraine. Currently, he is an associate professor at the Academic Department of IT-Security of the National Aviation University.

He is a reviewer of several international journals and an executive editor of *Ukrainian Scientific Journal of Information Security* (www.infosecurity.nau.edu.ua). His research interests are cryptography, quantum key distribution (QKD), network and internet security, information security incident management, critical information infrastructure protection, and cybersecurity of civil aviation.

Contents

Preface

One of the most effective ways to ensure confidentiality and data integrity during transmission is cryptography. The purpose of the cryptographic system is to provide key distribution, authentication, legitimate user authorization, and encryption. Today, key distribution is one of the most important problems of cryptography. This problem can be solved with the help of the following schemes: classical information-theoretic scheme, classical public-key cryptographic scheme, classical computationally secure symmetric-key cryptographic scheme, trusted courier key distribution, and quantum key distribution (QKD).

QKD includes the number of protocols (such as BB84, SARG04, E91, B92, six-state protocol, Goldenberg-Vaidman protocol, and Koashi-Imoto protocol), and the main task of these is encryption key generation and distribution between the two users connecting through quantum and classical channels. The main advantages of all QKD protocols are as follows: (1) these protocols always allow eavesdropping to be detected because eavesdropper's connection brings much more error level (compared with natural error level) to the quantum channel. The laws of quantum mechanics allow eavesdropping to be detected, and the dependence between error level and intercepted information to be set. This allows to apply the privacy amplification procedure that decreases the quantity of information about the key, which can be intercepted by eavesdropper. Thus, QKD protocols have an unconditional (information-theoretic) security. (2) The information-theoretic security of QKD allows using an absolutely secret key for further encryption using the well-known classical symmetrical algorithms. Thus, the entire information security level increases. It is also possible to synthesize QKD protocols with the Vernam cipher (one-time pad), which, in complex with unconditionally secured authenticated schemes, gives a totally secured system for transferring the information.

Besides, there are also disadvantages of QKD protocols that are as follows: (1) a system based only on QKD protocols cannot serve as a complete solution for key distribution in open networks because additional tools for authentication are needed. (2) The limitation of quantum channel length is caused by the fact that there is no possibility of amplification without quantum properties being lost. However, the technology of quantum repeaters could overcome this limitation in the near future. (3) There is a need for using the weak-coherent pulses instead of single-photon pulses. This decreases the efficiency of protocol in practice. However, this technological limitation might be defeated in the near future. (4) The data-transfer rate decreases rapidly with an increase in the quantum channel length. (5) Photon registration problem leads to a key rate of decrease in practice. (6) Photon depolarization in the quantum channel leads to errors during data transfer. Now, the typical error level equals a few percent, which is much greater than the error level in classical information and communication systems. (7) Difficulty in the practical realization of QKD protocols for d-level (multilevel) quantum systems. (8) The high price of commercial QKD systems (more than $100,000 for two subscriber systems).

The book “Advanced Technologies of Quantum Key Distribution” contains the results of scientific research eliminating the abovementioned disadvantages. In view of this, the book was divided into two sections—the first one “Modern QKD Technologies” is devoted to advanced protocols and systems for key distribution using quantum technologies, and the second part “Quantum Channel Construction” is related to corrective measures for improving the quantum channel efficiency.

There are also other quantum technologies of information security (such as quantum secure direct communication, quantum secret sharing, quantum stream cipher, and quantum digital signature), but in practice, these have not been extended beyond the laboratory experiments. However, practical implementation of these quantum technologies is also faced by some technological difficulties.

QKD and other quantum technologies, therefore, represent an important step toward improving the security of modern (and future) information and communication systems against cyberattacks, but many theoretical and practical problems must be solved for a wide practical use of them.

Professor Sergiy Gnatyuk
National Aviation University
Ukraine

Section 1

Modern QKD Technologies

Chapter 1

Security of Quantum Key Distribution Protocols

Mhlambululi Mafu and Makhamisa Senekane

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.74234

Abstract

Quantum key distribution (QKD), another name for quantum cryptography, is the most advanced subfield of quantum information and communication technology (QICT). The first QKD protocol was proposed in 1984, and since then, more protocols have been proposed. It uses quantum mechanics to enable secure exchange of cryptographic keys. In order to have high confidence in the security of the QKD protocols, such protocols must be proven to be secure against any arbitrary attacks. In this chapter, we discuss and demonstrate security proofs for QKD protocols. Security analysis of QKD protocols can be categorised into two techniques, namely infinite-key and finite-key analyses. Finite-key analysis offers more realistic results than the infinite-key one, while infinite-key analysis provides more simplicity. We briefly provide the background of QKD and also define the basic notion of security in QKD protocols. The cryptographic key is shared between Alice and Bob. Since the key is random and unknown to an eavesdropper, Eve, she is unable to learn anything about the message simply by intercepting the ciphertext. This phenomenon is beyond the ability of classical information processing. We then study some tools that are used in the derivation of security proofs for the infinite- and finite-length key limits.

Keywords: quantum cryptography, QKD, protocols, security, finite-security, entanglement, QKD schemes

1. Introduction

Quantum cryptography, specifically QKD, has been built based on physical concepts associated with quantum mechanics. In contrast to conventional cryptography, whose security is based on the complex computational and mathematical algorithms for security, it is founded on the uncertainty relations, Bell's inequalities, entanglement or non-locality [1]. The implementation of QKD consists of detectors, repeaters, quantum memories and decoy states [2–4]. These concepts form the basis of security proofs [5]. In order for Eve to obtain the secret key, she needs to break the laws of physics, but this is impossible without her presence being detected. Since there is great need for security in a communication system, it is necessary to investigate security proofs for QKD systems.

Regardless of the challenges that come with developing unconditional security proofs, a lot of progress has been realised in the last two decades. An unconditional security proof considers all kinds of attacks that Eve can perform and incorporating this into the security proof is a difficult task. However, a new technique for analysing collective attacks due to an eavesdropper was developed in 1995 by Yao [6]. Later, Bennett et al. realised that if the legitimate parties possess a reliable quantum computer, they can implement an entanglement distillation (ED) protocol to obtain a secure version of an EB key distribution [7]. In 1998, based on this idea, Lo and Chau then developed a formal security proof for the protocol [8]. By using the ideas of Mayers, Lo and Chau then Shor and Preskill developed a simple proof of security for the BB84 protocol in 2000 [9]. This was followed by a proof of Biham who was the second to show an unconditional security proof [10]. In 1991, Biham's proof was then used by Gottesman and Preskill to prove the unconditional security proof of a continuous variable protocol where Alice's signals are sufficiently squeezed [11]. In the same spirit, Inamori et al. showed the unconditional security proof of BB84 protocol where Alice's source emits weak coherent states and Bob's detector remains uncharacterised [12]. However, a complete security proof that is secure against arbitrary attacks by the eavesdropper and full realistic implementation of the QKD protocol remains missing. But this progress depicts that major achievements have been made in this field to prove that protocols used in quantum communication are secure for sending messages. Amongst different approaches to security proofs, a number of publications on composable security [13], de Finetti's theorem [5, 14], post-selection technique [15] and recently the finite-length key analysis [16] are now available.

Regardless of enormous progress that has been made in QKD, there are still some theoretical and experimental problems of communicating in absolute secrecy in the presence of an eavesdropper. In particular, matching the theoretical security proofs to real devices still remains unknown. The security proofs still contain assumptions concerning the behaviour of devices used by the communicating parties [17]. As a result of this mismatch, an eavesdropper can learn part of the key shared by Alice and Bob, thus rendering some schemes insecure over large distances. Moreover, the existing security proofs have been derived in the asymptotic limit which is not very realistic. In fact, the bits which are processed in QKD are necessarily of finite length. Therefore, thanks to Valerio and Renner for introducing the general framework for the security analysis of QKD with finite resources [16]. The security study is mainly based on the framework introduced by Devetak-Winter, Csiszar-Körner and Renner security [5, 18]. For a detailed overview of QKD, we refer the reader to [2, 4].

2. Quantum features

2.1. Detection of measurements

Based on the measurement postulate of quantum mechanics [19], it is impossible to perform a measurement on an unknown quantum state without introducing a disturbance unless the state is an eigenstate to the observable being measured [20]. This means that Eve is unable to perform a measurement on an unknown quantum state without introducing a disturbance that can be discovered by Alice and Bob.

2.2. Uncertainty principle

The uncertainty principle states that a measurement of one quantum observable intrinsically creates an uncertainty in other properties of the system. This means that it is impossible to measure the simultaneous values of non-commuting observables on a single copy of a quantum state [21]. This ensures that an eavesdropper cannot perform measurements that leave the quantum state undisturbed [22]. This automatic detection of an eavesdropper is impossible with classical cryptography.

2.3. No-cloning theorem

In quantum mechanics, it is impossible to make a perfect copy of an unknown state with perfect fidelity. This is called the no-cloning theorem [23]. This prevents an eavesdropper from simply intercepting the communication channel and making copies (so as to make measurements on them later) of the transmitted quantum states, while passing on an undisturbed quantum state to Bob [24, 25]. Therefore, the no-cloning theorem forms an important property in the security of QKD protocols [26].

2.4. Non-orthogonality principle

Suppose, we have quantum states $|\psi_i\rangle$ which are not orthogonal, then it can be proved that there exists no quantum measurement that is able to distinguish states [19]. In this case, a non-zero component of the state $|\psi_1\rangle$ parallel to the state $|\psi_2\rangle$ always gives a non-zero probability of the measurement outcome associated with the state $|\psi_2\rangle$ also occurring when the measurement is applied to the state $|\psi_1\rangle$. This is because $|\psi_2\rangle$ can be decomposed into a non-zero component parallel to $|\psi_1\rangle$ and a component orthogonal to $|\psi_1\rangle$. Then, there is no measurement of any kind that can reliably determine which of the two non-orthogonal quantum states were measured [27]. This feature is very useful for cryptographic applications such as QKD [20].

3. QKD schemes

There are two major types of QKD schemes, namely prepare and measure (P&M) and entanglement-based (EB) schemes [2, 4]. A P&M scheme is based on individual qubits, while an EB scheme is based on entangled qubits. Either of these schemes can be used by two parties in order to end up with a shared secret key. However, a P&M scheme can immediately be translated into an EB scheme [4, 28]. However, there exists another family of protocols called continuous-variable protocols and distributed-phase-reference (DPR) protocols [4], which consist of the coherent-one-way protocol [29, 30] and the distributed-phase-reference protocols [31, 32]. In the following sections, we briefly describe the processes for each scheme.

3.1. Prepare and measure (P&M) scheme

In a P&M scheme, Alice encodes some classical information into a set of quantum states and sends them via an insecure quantum channel to Bob. Bob then performs measurements on the quantum states he receives. This results in classical data generated by quantum means being shared between Alice and Bob. Examples of protocols that use this scheme are BB84 [33], B92 [27], six-state [34] and SARG04 [35] protocols.

3.2. Entanglement-based (EB) scheme

In an EB scheme, a source prepares and distributes a maximally entangled quantum state where one system is sent to Alice and another to Bob. Alice and Bob then perform measurements in two mutually unbiased bases on their system, respectively. Upon measurement, they obtain perfectly correlated outcomes which are completely random. Since the source prepares a pure state, it means that this state cannot be correlated with an eavesdropper. This implies secrecy of the key. An example of a protocol which uses this scheme is the E91 protocol [36].

4. QKD procedure

In this section, we describe what happens in a P&M scheme, specifically in the BB84 protocol [33]. In this protocol, Alice and Bob are connected by two communication channels, namely an insecure quantum channel and an authenticated classical channel [2]. The quantum channel is used for the transmission of qubits and is controlled by the eavesdropper. The classical channel is authenticated so that the eavesdropper can only listen to the communication but cannot alter the messages being transmitted. This ensures that Alice and Bob can prove that they are communicating between each other. Otherwise, an eavesdropper could simply block all quantum and classical communication between Alice and Bob and perform QKD with Alice while taking on Bob's role and vice versa. Therefore, Alice and Bob have to identify each message they send as originating from themselves before any post-processing can begin.

4.1. Quantum phase

In the quantum phase, Alice and Bob make use of the quantum channel. They employ the quantum mechanical signals (i.e. qubits) and they also perform measurements. Three subprotocols take place which are as follows:

a. Signal preparation: Alice prepares a random sequence of strings which are drawn from a set of four signal states and encodes each bit value in the state of a quantum system. The basis states are horizontal, vertical, diagonal and anti-diagonal.

b. Transmission: The encoded quantum system is sent to Bob via the quantum channel.

c. Measurement: Bob applies a quantum measurement on the quantum system to decode a bit value. The signals are measured in a random sequence of polarisation bases, either in the horizontal/vertical or diagonal/anti-diagonal bases.

Afterwards, Alice keeps the record of signal choices; Bob keeps the record of his basic choices and the corresponding measurement results.

4.2. Classical phase

In this phase, Alice and Bob use some classical communication protocol in order to distil a secret key from their correlated data. They achieve this by means of a discussion over the authenticated classical channel. The key extraction procedure is described as follows:

a. Parameter estimation: Alice randomly chooses some fraction of her signal slots and announces for these slots to Bob which signal she sent. Bob announces the measurement he performed and the outcome which he obtains. Depending on the amount of errors which they obtain from their comparisons, they may also decide whether to continue or abort the protocol.

b. Sifting: In the sifting protocol, Alice and Bob announce the polarisation bases they used for the preparation of the signals and which bits are discarded. In order to prevent Eve from modifying the transmitted messages, Alice and Bob use the authentication scheme. The remaining data are called sifted data. Alice and Bob proceed to the reconciliation phase or error correction phase.

c. Key map: Alice and Bob discard the basis which they were using so that Eve may not learn any information about the encoding. During key map, Alice and Bob map their event records of the sifted data into a raw key. This step applies to prepare and measure protocol.

d. Error correction: The sifted data may still contain some errors; therefore, Alice and Bob execute a classical error correction protocol in order to reconcile their data. They need to exchange additional information about their respective data over the public channel. In addition, they need to authenticate this phase because Eve is still able to modify the messages in this step. As a result of this protocol, Alice and Bob agree now on a key which is identical with very high probability but Eve might still have some small additional information about the key. After this stage, privacy amplification takes place.

e. Privacy amplification: After Alice and Bob have reconciled their key, they can cut the correlations between their key and Eve by using the so-called privacy amplification. In this stage, Alice and Bob map their string via a special family of functions called universal hash functions to a shorter final key [5].

5. Security in QKD

5.1. Security definition

A good definition of security would allow the key generated by a QKD protocol to deviate by a small parameter ε, from a perfect key [2]. This definition should be able to bound Eve's knowledge about the final key. A perfect key refers to a uniformly distributed bit string whose value is completely independent and remains unknown to an eavesdropper [16]. The main requirement that the definition of security must fulfil is composability [5]. The composable definition characterises the security of a protocol with respect to the ideal functionality. This means that the security of the key generated could be used in any subsequent cryptographic task such as the one-time pad for message encryption, where an ideal key is expected. However, there always exist some challenges in constructing security proofs without making any assumptions either about the devices or the parties. For example, attacks against practical schemes exist, such as photon-number-splitting attacks (PNS) [37], time-shift attacks [38], large pulse attacks [17, 39], blinding attacks [40] and high-power damage attack [41]. Some of the assumptions made in the definition of QKD security are as follows:

a. there should be no side channels. Side channels are basically discrepancies between the theoretical model and a practical implementation. They always exist if some information about the raw key is encoded in degrees of freedom not considered in the theoretical model. Therefore, this leads to a wrong assessment of the dimension of the Hilbert space which describes the protocol,

b. there should be access to perfect or almost perfect randomness (locally) and

c. quantum theory is correct and complete.

If there is randomness and quantum theory is correct, then this leads to completion of the security proofs. However, in classical cryptography, the security is based on the difficulty or complication of a certain mathematical algorithm to afford security of the protocol. Therefore, the security is mainly based on the failure to solve the algorithm. This can fail in four ways that are as follows:

a. conjecture of hardness/difficulty in this case is wrong,

b. underlying computation model could be wrong or could be unphysical,

c. the algorithm is easy for many instances and.

d. the computation could be small.

5.2. Security requirements

In this section, we follow closely the definitions in [5, 42]. A QKD protocol outputs a key SA on Alice's side and also a key SB on Bob's side. The length of the key is $l > 0$, otherwise no key is extracted. The length of the key depends on the noise level of the communication channel as well as security and on the correctness requirements of the protocol. Depending on the deviation of the output key from the ideal one, the protocol aborts in which case $S_A = S_B = \perp$ [42].

1. Correctness: A QKD protocol is called "correct", if, for any strategy by the eavesdropper $S_A = S_B$. This occurs whenever Alice and Bob output the classical keys S_A and S_B, respectively, such that $\Pr[S_A \neq S_B] \leq \varepsilon_{cor}$. The term ε_{cor} is the maximum probability that the protocol deviates from the behaviour of the correct protocol. In order for correctness to be achieved, the QKD devices must perform what they are supposed to do according to a specified model. The devices generate the correct correlations which they are supposed to output, otherwise the protocol aborts. In other terms, the devices should not send any

other information to the outside world, in which it is not supposed to do (i.e. devices work according to their specification),

2. Secrecy: A random variable S drawn from the set S is said to be ε-secure with respect to an eavesdropper holding a quantum system E, if.

$$\min_{\in \sigma E} \frac{1}{2} \mathrm{tr}|\rho_{SE} - \rho_U \otimes \sigma_E| \leq \varepsilon, \tag{1}$$

where $\rho_{SE} = \sum_{s\in S} P_s(s)|s\rangle\langle s| \otimes \rho_E \,|S = s$ is the actual state that contains some correlations between the final key and Eve and ε gives the maximum failure probability of the key extraction process. The state $\rho_U = \sum_{s\in S} |s\rangle\langle s|\,|S|$ is the completely mixed state on S and $|S|$ is the size of S. Since the trace distance, that is, $\frac{1}{2}\mathrm{tr}|\rho_0 - \rho_1|$ refers to the maximum probability of distinguishing between the two quantum states (ρ_0,ρ_1), this composable security definition naturally gives rise to the operational meaning that the protocol is ε-secure, that is, S is identical to an ideal key U except with probability ε [5]. Again, according to Helstrom's Theorem, the probability of distinguishing between the two quantum states ρ_0 and ρ_1 is bounded by $\frac{1}{2} + \frac{1}{4}\mathrm{tr}|\rho_0 - \rho_1|$ [43].

3. Robustness: A QKD protocol is said to be "not robust" if the protocol aborts even though the eavesdropper is inactive. While correctness and secrecy are difficult to prove, robustness can simply be proven by running the protocol.

5.3. Infinite-length key security in QKD

Over the last decade, a lot of work in QKD has been devoted to the derivation of unconditional security proofs [8, 16, 44–47]. One of the main problems is that Eve has the power to perform any type of eavesdropping strategy. In particular, she can evade detection by attributing noise caused by her eavesdropping attack to normal noise in the channel. Therefore, it remains difficult to accurately bound the amount of information that Eve may obtain from the communication channel. The most important resource which should be determined when constructing security proofs for QKD protocols is the secret key rate. Therefore, all QKD protocols must be able to provide a clear expression for the secret key rate. In the asymptotic limit, the secret key rate is expressed as

$$r = \lim_{n\to\infty} \frac{l}{n}, \tag{2}$$

where l is the length of the final secret key and n is a list of symbols called r raw keys [2]. This rate was established by Devetak and Winter [18]. The secret key rate against collective attacks was derived by Kraus, Gisin and Renner [48] and is expressed as

$$\mathrm{r} = \mathrm{I(X : Y)} - \chi(\mathrm{X : E}) \tag{3}$$

where I(X: Y) = H(X) − (X|Y) quantifies the amount of bits need to be satisfied for error correction. The term χ(X: E) = H(X) + S(E) − S(X, E) refers to the Holevo quantity, where H is the Shannon entropy and S is the von Neumann entropy [49, 50]. The Holevo quantity refers to the amount of privacy amplification required in order to eliminate Eve's information.

The upper bound on the secret key rate r, can be expressed as.

$$r \leq I(A : B{\downarrow}E), \tag{4}$$

where I(A: B ↓ E) is the intrinsic conditional mutual information (intrinsic information for short) between two information sources held by Alice and Bob after Eve has performed an optimal individual attack [51]. The intrinsic information between two information sources A and B given $\bar{E}$ is defined as, $I(A : B \downarrow E) = \inf_{\bar{E}} I(A : B|\bar{E})$, where the infimum is taken over all discrete random variables E such that $AB \rightarrow E \rightarrow \bar{E}$ is a Markov chain [52]. It has been shown that I(A: B ↓ E) is an upper bound on the rate S = S(A;B||E) at which such a key can be extracted [51].

5.4. Finite-length key security

Many efforts have been made to improve the bounds on the secret key rates for a finite amount of resources [5, 16, 53–58]. Since the tools for analysing the security under non-asymptotic regime have become available, there is need to provide new security definitions. In this section, we follow closely the techniques demonstrated in [16] to discuss some of the parameters used in the security of QKD for finite-length key limit. The main goal of finite-length key security is to obtain a secret key rate r, based on a certain number of signals, a security parameter ε, and certain losses from the error correction without making any assumptions about the post processing (sifting, error correction and privacy amplification). For example, one can recognise that the limit in this expression of Eq. (2) is unrealistic because in all implementations of QKD protocols finite resources are used. This is because in this scenario, N is assumed to be large, that is, it approaches infinity, while in practice Alice and Bob exchange a limited number of symbols or signals. In the non-asymptotic limit, the secret key rate can be expressed as.

$$r = n/N[S_{\xi}(X|E) - \triangle - \text{leak}_{EC}/n]. \tag{5}$$

This shows that only a fraction of n out of N signals exchanged contributes to the key. This is because of the fact that m = N − n is used for parameter estimation thus leading the presence of a pre-factor of n/N. The expression S_{ξ} (X |E) takes into account the finite precision of the parameter estimation. Eve's information is calculated by using measured parameters, for example, error rates. In the finite-key scenario, these parameters are estimated on samples of finite length. The parameter △ is related to the security of privacy amplification. Its value is given by.

$$\triangle \equiv (2\log d + 3)\surd[\log 2(2/\varepsilon)/n] + 2/n\log_2 1/\varepsilon_{PA}, \tag{6}$$

where d is the dimension of the Hilbert space, $\bar{\varepsilon}$ is a smoothing parameter and ε_{PA} is the failure probability of the privacy amplification procedure. Eve's uncertainty is quantified by a generalised conditional entropy called the smooth min-entropy and is denoted as $H_{min}^{\bar{\varepsilon}}$ $(X^{(n)}|E^{(N)})$ [5]. The smoothing parameters, $\bar{\varepsilon}$ and ε_{PA}, are parameters which should be optimised numerically. The square-root term corresponds to the speed of convergence of the smooth-min entropy, which is used to measure the key length of an identical and independently distributed (i.i.d) state toward the von Neumann entropy. In the asymptotic limit, the smooth-min entropy of an i.i.d state is equal to the von Neumann entropy. The second term ε_{PA} is directly linked to the failure probability of the privacy amplification procedure. Finally, leak_{EC}/n corresponds to the amount of information which needs to be exchanged by Alice and Bob during the reconciliation phase. This quantity may not reach the Shannon limit, so $\text{leak}_{EC} \geq nH(X \mid Y)$. Typically,

$$\text{leak}_{EC} \approx f_{EC} H(X|Y) + 1/n \ \log_2(2/\varepsilon_{EC}), \tag{7}$$

where $f_{EC} > 1$ depends on the code and ε_{EC} refers to the failure probability of the error correction procedure.

Unlike in the asymptotic scenario, one needs to fix an overall security parameter ε for the QKD protocol. The parameter ε corresponds to the maximum probability failure that is tolerated on the key extraction protocol. This can be expressed as $\varepsilon = \varepsilon_{PE} + \varepsilon_{EC} + \varepsilon^{\bar{}} + \varepsilon_{PA}$, where ε_{PE} is the error in the parameter estimation step and the other terms are as previously defined. All the parameters, ε_{PE}, ε_{EC}, $\varepsilon^{\bar{}}$, ε_{PA}, can be independently fixed at arbitrarily low values.

As a result, the overall security parameter ε can be chosen arbitrarily small, to a value corresponding to Alice and Bob's wishes, but this comes at a cost of decreasing the final secret key rate. If m signals have been used to estimate the parameter λ, then the deviation of measurement outcomes λ_m obtained from measuring the m samples from the ideal estimate λ_∞ can be quantified by using the law of large numbers resulting [5, 59].

$$|\lambda_m - \lambda_\infty| \leq \xi(m, d) = \sqrt{}[\ln(1/\varepsilon_{PE}) + d\ln(m+1)/2\,m] \tag{8}$$

The objective of the privacy amplification step is to minimise the quantity of correct information which the eavesdropper may have obtained about Alice and Bob's reference raw key. After privacy amplification, the length of the raw key that remains will be.

$$l \leq H_{min}{}^{\varepsilon}\ (X|E) - 2\log_2\ (1/\varepsilon_{PA}), \tag{9}$$

where $H_{min}\ (X \mid E)$ expresses Eve's uncertainty and ε_{PA} is the error in the privacy amplification step.

6. Conclusion

In the general philosophy of proving the security of QKD protocols, standard methods are known to exist. However, these seem to fail for other classes of protocols, for example, the distributed phase reference protocols. In this chapter, we discussed that QKD is a technique, which uses the power of quantum mechanics to establish a string of random bits called a key. We also showed how the secret key is generated and shared between Alice and Bob. Since the key is random and unknown to an eavesdropper, Eve, she is unable to learn anything about the message simply by intercepting the ciphertext. This phenomenon is beyond the ability of classical information processing.

In this chapter, we provided a background study of QKD and also defined the basic notion of security in QKD protocols. In particular, the tools for analysing the security proofs for both infinite- and finite-key QKD protocols were discussed and demonstrated. Further, we discussed that the finite-key analysis offers more realistic results than the infinite-key one, while the infinite-key analysis provides more simplicity.

Author details

Mhlambululi Mafu[1]* and Makhamisa Senekane[2]

*Address all correspondence to: mhlambululi.mafu@gmail.com

1 Department of Physics and Astronomy, Botswana International University of Science and Technology, Palapye, Botswana

2 Department of Physics and Electronics, National University of Lesotho, Roma, Lesotho

References

[1] Nielsen M, Chuang I. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press; 2002

[2] Gisin N, Ribordy G, Tittel W, Zbinden H. Reviews of Modern Physics. 2002;**74**:145-195

[3] Lo HK, Ma X, Chen K. Physical Review Letters. 2005;**94**:230504

[4] Scarani V, Bechmann-Pasquinucci H, Cerf N, Dušek M, Lütkenhaus N, Peev M. Reviews of Modern Physics. 2009;**81**:1301-1350. ISSN 1539-0756

[5] Renner R. International Journal of Quantum Information. 2008;**6**:1-127

[6] Yao ACC. Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing; 1995. pp. 67-75

[7] Bennett CH, Brassard G, Popescu S, Schumacher B, Smolin JA, Wootters WK. Physical Review Letters. 1996;**76**:722

[8] Lo HK, Chau HF. Science. 1999;**283**:2050-2056

[9] Shor PW, Preskill J. Physical Review Letters. 2000;**85**:441-444

[10] Biham E, Boyer M, Boykin PO, Mor T, Roychowdhury V. Journal of Cryptology. 2006;**19**: 381-439

[11] Gottesman D, Preskill J. Quantum Information with Continuous Variables. Amsterdam: Springer; 2003. pp. 317-356

[12] Inamori H, Lütkenhaus N, Mayers D. The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics. 2007;**41**:599-627

[13] Ben-Or M, Horodecki M, Leung D, Mayers D, Oppenheim J. In: Kilian J, editor. Theory of Cryptography: Second Theory of Cryptography Conference TCC 2005; vol. 3378 of Lecture Notes in Computer Science. Springer Verlag; 2005. pp. 386-406

[14] Renner R, Cirac J. Physical Review Letters. 2009;**102**:110504

[15] Christandl M, König R, Renner R. Physical Review Letters. 2009;**102**:20504

[16] Scarani V, Renner R. Physical Review Letters. 2008;**100**:200501

[17] Makarov V, teknisk-naturvitenskapelige universitet Institutt for elektronikk og telekommunikasjon N. Quantum Cryptography and Quantum Cryptanalysis. Department of Electronics and Telecommunications, Faculty of Information Technology, Mathematics and Electrical Engineering, Norwegian University of Science and Technology; 2007. ISBN 824711478X

[18] Devetak I, Winter A. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science. 2005;**461**:207-235

[19] Nielsen M, Chuang I, Grover L. American Journal of Physics. 2002;**70**:558

[20] Audretsch J. Entangled Systems: New Directions in Quantum Physics. New York: Wiley-VCH; 2007

[21] Deutsch D. Physical Review Letters. 1983;**50**(9):631-633. DOI: 10.1103/PhysRevLett.50.631

[22] Fuchs CA, Peres A. Physical Review A. 1996;**53**:2038-2045

[23] Wooters W, Zurek W. A single quantum cannot be cloned. Nature. 1982;**299**:802

[24] Bruss D, Leuchs G. Lectures on Quantum Information. New York: Wiley; 2007

[25] Peres A, Wootters W. Physical Review Letters. 1991;**66**:1119-1122

[26] Dieks D. Physics Letters A. 1982;**92**:271-272

[27] Bennett CH. Physical Review Letters. 1992;**68**(21):3121-3124. DOI: 10.1103/PhysRevLett.68.3121

[28] Meyer T. Finite key analysis in quantum cryptography [PhD Thesis]. Heinrich Heine University, Dsseldorf; 2007. http://d-nb.info/987330772. URL: http://docserv.uni-duesseldorf.de/servlets/DerivateServlet/Derivate-6444/thesis_noextras.pdf

[29] Stucki D, Fasel S, Gisin N, Thoma Y, Zbinden H. Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, vol. 6583; 2007. p. 18

[30] Mafu M, Marais A, Petruccione F. Applied Mathematics & Information Sciences. 2014;**8**: 2769

[31] Inoue K, Waks E, Yamamoto Y. Physical Review Letters. 2002;**89**:037902

[32] Marais A, Konrad T, Petruccione F. Journal of Physics A: Mathematical and Theoretical. 2010;**43**:305302

[33] Bennett C, Brassard G. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, vol. 175; Bangalore, India. 1984

[34] Bruß D. Physical Review Letters. 1998;**81**:3018-3021

[35] Scarani V, Acín A, Ribordy G, Gisin N. Physical Review Letters. 2004;**92**:057901

[36] Ekert A. Physical Review Letters. 1991;**67**:661-663

[37] Lütkenhaus N. Physical Reviews A. 2000;**61**(5):052304

[38] Qi B, Fung C, Lo H, Ma X. Quantum Information and Computation. 2007;**7**:073-082

[39] Vakhitov A, Makarov V, Hjelme D. Journal of Modern Optics. 2001;**48**:2023-2038

[40] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V. Nature Photonics. 2010;**4**:801-801

[41] Bugge AN, Sauge S, Ghazali AMM, Skaar J, Lyderseb L, Makarov V. Physical Review Letters. 2014;**112**:070503

[42] Tomamichel M, Lim CCW, Gisin N, Renner R. Nature Communications. 2012;**3**:634

[43] Helstrom CW. Journal of Statistical Physics. 1969;**1**:231-252

[44] Wolf S. Lectures on Data Security. Amsterdam: Springer; 1999. pp. 217-250

[45] Mayers D. Journal of the ACM (JACM). 2001;**48**:351-406

[46] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S, Sanpera A. Physical Review Letters. 1996;**77**:2818

[47] Tamaki K, Lo H. International Symposium on Information Theory, IEEE 2005. ISIT 2005. Proceedings. 2005. pp. 1603-1606. ISBN 0780391519

[48] Kraus B, Gisin N, Renner R. Physical Review Letters. 2005;**95**:80501

[49] Holevo A. Proceedings of the Second Japan-USSR Symposium on Probability Theory. Springer; 1973. pp. 104-119

[50] Holevo A. Probabilistic and Statistical Aspects of Quantum Theory. Amsterdam: Springer; 1982

[51] Christandl M, Renner R, Wolf S. IEEE International Symposium on Information Theory. 2003. pp. 258-258

[52] Maurer U, Wolf S. IEEE Transactions on Information Theory. 1999;**45**:499-514

[53] Hayashi M. Physical Review A. 2007;**76**:012329

[54] Cai R, Scarani V. New Journal of Physics. 2009;**11**:045024

[55] Sheridan L, Le TP, Scarani V. New Journal of Physics. 2010;**12**:123019

[56] Abruzzo S, Kampermann H, Mertz M, Bruß D. Physical Review A. 2011;**84**:032321

[57] Mafu M, Garapo K, Petruccione F. Finite-size key in the Bennett 1992 quantum key distribution for Renyi entropies. Physical Review A. 2013;**88**(6):1-4

[58] Mafu M, Garapo K, Petruccione F. Physical Review A. 2014;**90**:032308

[59] Cover TM, Thomas JA. Elements of Information Theory. New York: John Wiley; 1991

Chapter 2

On Quantum Fingerprinting and Quantum Cryptographic Hashing

Farid Ablayev and Marat Ablayev

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.70692

Abstract

Fingerprinting and cryptographic hashing have quite different usages in computer science, but have similar properties. Interpretation of their properties is determined by the area of their usage: fingerprinting methods are methods for constructing efficient randomized and quantum algorithms for computational problems, whereas hashing methods are one of the central cryptographical primitives. Fingerprinting and hashing methods are being developed from the mid of the previous century, whereas quantum fingerprinting and quantum hashing have a short history. In this chapter, we investigate quantum fingerprinting and quantum hashing. We present computational aspects of quantum fingerprinting and quantum hashing and discuss cryptographical properties of quantum hashing.

Keywords: quantum computations, quantum cryptography, fingerprinting, hashing

1. Introduction

Fingerprinting and hashing are well-known techniques. Fingerprinting is widely used in various meanings in different areas of computer science. We restrict ourselves to the area of computational complexity theory where the notion of fingerprinting is more or less formalized. Cryptographic hashing allows to securely present objects and mathematically is more formalized. Fingerprinting and cryptographic hashing have quite different usages in computer science, but have similar properties. Interpretation of their properties is determined by the area of their usage: fingerprinting methods are methods for constructing efficient randomized and quantum algorithms for computational problems, whereas hashing methods are one of the central cryptographical primitives.

Fingerprinting and hashing methods are being developed from the mid of the previous century, whereas quantum fingerprinting and quantum hashing have a short history.

In this chapter, we present computational aspects of quantum fingerprinting, discuss cryptographical properties of quantum hashing, and present the possible use of quantum hashing for quantum hash-based message authentication codes (QMAC).

1.1. Classical and quantum fingerprinting

Fingerprinting in complexity theory is a procedure that maps a large data item to a much shorter string, its fingerprint, that identifies the original data (with high probability). The key properties of classical fingerprinting methods are (i) they allow to build efficient randomized computational algorithms and (ii) the resulting algorithms have bounded error [1].

Rusins Freivalds was one of the first researchers who introduced methods (later called fingerprinting) for constructing efficient randomized algorithms (which are more efficient than any deterministic algorithm) [2, 3].

In quantum case, fingerprinting is a procedure that maps classical data to a quantum state that identifies the original data (with high probability). One of the first applications of the quantum fingerprinting method is due to Ambainis and Freivalds [4]: for a specific language, they have constructed a quantum finite automaton with an exponentially smaller size than any classical randomized automaton. An explicit definition of the quantum fingerprinting was introduced by Buhrman et al. [5] in (2001) for constructing efficient quantum communication protocol for equality testing. It is worth noting that the fingerprinting by Buhrman et al. has been used as a cryptographic hash function in [6, 7].

1.2. Cryptographic quantum hashing

Cryptographic hashing has a lot of fruitful applications in cryptography. Note that in cryptography functions satisfying (i) one-way property and (ii) collision resistance property (in different specific meanings) are called hash functions, and we propose to do so when we are considering cryptographical aspects of quantum functions with the above properties. So, we suggest to call a quantum function that satisfies properties (i) and (ii) (in the quantum setting), a cryptographic quantum hash function or just quantum hash function. Note, however, that there is only a thin line between the notions of quantum fingerprinting and quantum hashing. One of the first considerations of a quantum function (that maps classical words into quantum states) as a cryptographic primitive, having one-way property and collision resistance property is due to [6], where the quantum fingerprinting function from [5] was used. Another approach to constructing quantum hash functions from quantum walks was considered in [8, 9, 10], and it resulted in privacy amplification in quantum key distribution and other useful applications.

1.3. The chapter organization

In Section 3, we consider quantum fingerprinting as a mapping of classical inputs to quantum states, which allows to construct efficient quantum algorithms for computing Boolean functions. We consider the quantum fingerprinting function from [5] as well as the quantum fingerprinting technique from [11]. The latter was motivated by the paper [4] and its generalization [12].

We define a notion of quantum (δ, ε)-hash function that is quantumly one-way δ-resistant and quantumly collision ε-resistant.

We show that one-way property and collision resistance property are correlated for a quantum hash function. The more the function is one-way, the less it is collision resistant and vice versa. We show that such a correlation can be balanced.

We present an approach for quantum hash function constructions by establishing a connection with small-biased sets [13] and quantum hash function constructions: we prove that each ε-biased set allows to generate quantum collision ε-resistant function. Note that one-way property of this function depends on the size of such ε-biased set: the smaller ε-biased set allows to generate a quantum function with the better one-way characteristics. Such a connection adds to the long list of small-biased sets' applications.

In particular, it was observed in [13, 14] that the ε-bias property is closely related to the error-correcting properties of linear codes. In particular, for the binary case, a set S is ε-biased iff every pair of distinct code words of corresponding error correcting code C_S has relative Hamming distance $(1 \pm \varepsilon)/2$.

Note that the quantum fingerprinting function from [5] is based on a binary error-correcting code, and so it solves the problem of constructing quantum hash functions for the binary case. For the general (nonbinary) case, ε-bias does not correspond to Hamming distance. Thus, in contrast to the binary case, an arbitrary linear error correcting code cannot be used directly for quantum hash functions.

Note that one-way property of function means computational effectiveness of this function. We show that considered construction of quantum (δ, ε)-hash function is computed effectively in the model of quantum branching programs. We consider two complexity measures: a number $width(Q)$ of qubits that QBP Q uses for computation and a number time(Q) of computational steps of QBP Q. Such QBP Q is of $width(Q) = O(\log\log q)$ and $time(Q) = \log\ q$.

We prove that such QBP construction is optimal. That is, we prove lower bounds $\Omega(\log\log q)$ for QBP width and $\Omega(\log\ q)$ for QBP time for quantum (δ, ε)-hash function presentation.

2. Preliminaries

We recall that mathematically a qubit is described as a unit vector in the two-dimensional Hilbert complex space $\mathcal{H}^2$. Let $s \geq 1$. Let $\mathcal{H}^d$ be the $d = 2^s$-dimensional Hilbert space, describing the states of s qubits. Another notation for $\mathcal{H}^d$ is $(\mathcal{H}^2)^{\otimes s}$, i.e., $\mathcal{H}^d$ is made up of s copies of a single qubit space $\mathcal{H}^2$.

$$\left(\mathcal{H}^2\right)^{\otimes s} = \mathcal{H}^2 \otimes, \ldots, \otimes \mathcal{H}^2 = \mathcal{H}^{2^s}. \tag{1}$$

Conventionally, we use notation $|i\rangle$ for the vector from H^d, which has a 1 on the i-th position and 0 elsewhere. An orthonormal basis $|1\rangle, \ldots, |d\rangle$ is usually referred to as the *standard computational basis*.

We let $\mathbb{Z}_q$ to be a finite additive group of Z/qZ, the integers modulo q. Let Σ^k be a set of words of length k over a finite alphabet Σ. Let $\mathbb{X}$ be a finite set. In this paper, we let $\mathbb{X} = \Sigma^k$ or $\mathbb{X} = \mathbb{Z}_q$. For $K = |\mathbb{X}|$ and integer $s \geq 1$, we define a $(K; s)$ classical-quantum function (or just quantum function) to be mapping

$$\psi : \mathbb{X} \to \left(\mathcal{H}^2\right)^{\otimes s} \qquad \text{or} \qquad \psi : w \mapsto |\psi(w)\rangle. \tag{2}$$

In order to outline a computational aspect and present a procedure for quantum function ψ, we define ψ to be a unitary transformation (determined by an element $w \in \mathbb{X}$) of the initial state $|\psi_0\rangle \in (\mathcal{H}^2)^{\otimes s}$ to a quantum state $|\psi(w)\rangle \in (\mathcal{H}^2)^{\otimes s}$

$$\psi : \{\left|\psi_0\right\rangle\} \times \mathbb{X} \to \left(\mathcal{H}^2\right)^{\otimes s} \qquad |\psi(w)\rangle = U(w)\left|\psi_0\right\rangle, \tag{3}$$

where $U(w)$ is a unitary matrix.

Extracting information on w from $|\psi(w)\rangle$ is a result of measurements of quantum state $|\psi(w)\rangle$. In this chapter, we consider quantum transformations and measurements of quantum states with respect to computational basis.

3. Quantum fingerprinting

The ideas of the fingerprinting technique in the quantum setting for the first time appeared in [4]. The authors used a succinct presentation of the classical input by a quantum automata state, which resulted in an exponential improvement over classical algorithm. Later in the works of [12] the ideas were developed further to give an arbitrarily small probability of error. This was the basis for the general quantum fingerprinting framework proposed in [11].

However, the term "quantum fingerprinting" is mostly used in scientific literature to address a seminal paper [5], where this notion first appeared explicitly. To distinguish between different versions of the quantum fingerprinting techniques, the fingerprinting function from [5] is called as "binary" (since it uses some binary error-correcting code in its construction), whereas the fingerprinting from [11] is called "q-ary" for it uses presentation of the input in $\mathbb{Z}_q$.

3.1. Binary quantum fingerprinting

The quantum fingerprinting function was formally defined in [5], where it was used for quantum equality testing in a quantum communication model. It is based on the notion of a binary error-correcting code.

An (n, k, d) *error-correcting code* is a map $C : \Sigma^k \rightarrow \Sigma^n$ such that, for any two distinct words w, $w^{'} \in \Sigma^k$, the Hamming distance $d(C(w), C(w^{'}))$ between code words $C(w)$ and $C(w^{'})$ is at least d. The code is binary if $\Sigma = \{0, 1\}$.

The construction of the quantum fingerprinting function is as follows.

- Let $c > 2$ and $\varepsilon < 1$. Let k be a positive integer and $n = ck$. Let $E : \{0, 1\}^k \rightarrow \{0, 1\}^n$ be a (n, k, d) binary error-correcting code with Hamming distance $d \geq (1 - \varepsilon)n$.
- Define a family of functions $F_E = \{E_1, \ldots, E_n\}$, where $E_i : \{0, 1\}^k \rightarrow \mathbb{F}_2$ is defined by the rule: $E_i(w)$ is the i-th bit of the codeword $E(w)$.
- Let $s = \log\ n + 1$. Define the quantum function $\psi_{F_E} : \{0, 1\}^k \rightarrow (\mathcal{H}^2)^{\otimes s}$, determined by a word w as

$$|\psi_{F_E}(w)\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle |E_i(w)\rangle. \tag{4}$$

Original paper of [5] used this function to construct a quantum communication protocol that tests equality in the simultaneous message passing (SMP) model with no shared resources. This protocol requires $O(\log\ n)$ qubits to compare n-bit binary strings, which is exponentially smaller than any classical deterministic or even randomized protocol in the SMP setting with no shared randomness. The proposed quantum protocol has one-sided error of $1/2(1 + \langle \psi_{F_E}(x) |\ \psi_{F_E}(y)\rangle^2)$, where $|\psi_{F_E}(x)\rangle$ and $|\psi_{F_E}(y)\rangle$ are two different quantum fingerprints. Their inner product $|\langle \psi_{F_E}(x) |\ \psi_{F_E}(y)\rangle|$ is bounded by ε, if the Hamming distance of the underlying code is $(1 - \varepsilon)n$. Thus, ε is determined by the chosen error-correcting code. For instance, Justesen codes mentioned in the paper give $\varepsilon < 9/10 + 1/(15c)$ for any chosen $c > 2$.

In the same paper, it was shown that this result can be improved by choosing an error-correcting code with Hamming distance between any two distinct code words $(1 - \varepsilon)n/2$ and $(1 + \varepsilon)n/2$ for any $\varepsilon > 0$ (however, the existence of such codes can only be proved nonconstructively via probabilistic argument).

Further research on this topic mostly used the following phase presentation version of quantum fingerprinting. We define the quantum fingerprinting function $\psi : \{0, 1\}^k \rightarrow (\mathcal{H}^2)^{\otimes s}$ determined by a word w as

$$\psi_{F_E}(w) = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{E_i(w)} |i\rangle \tag{5}$$

This function gives the following bound for the fingerprints of distinct inputs

$$\left| \left\langle \psi_{F_E}(x) | \psi_{F_E}(y) \right\rangle \right| = \frac{1}{n} \sum_{i=1}^{n} (-1)^{E_i(w) \oplus E_i(w')} = \frac{n - d(E(w), E(w'))}{n} \leq \varepsilon \tag{6}$$

3.2. *q*-ary quantum fingerprinting

In this section, we demonstrate the generalization of binary fingerprinting function to the q-ary case. General technique is presented in [11, 15]. Here, we present the idea using specific Boolean function $g:\{0,1\}^n \to \{0,1\}$ where $g(\sigma)=1$ iff $\sigma = 0 \bmod sq$. We treat σ also as an integer encoded by binary string σ.

To test g, we rotate the initial state $|0\rangle$ of a single qubit by an angle $\theta = \pi\sigma/q$:

$$|0\rangle \to |\psi(\sigma)\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle \tag{7}$$

Then, this state $|\psi(\sigma)\rangle$ is measured and the input σ is accepted iff the result of the measurement is $|0\rangle$.

Obviously, this quantum state is $\pm|0\rangle$ iff $\sigma = 0 \bmod q$. In the worst case, this algorithm gives the one-sided error of $\cos^2\pi(q-1)/q$, which can be arbitrarily close to 1.

The above description can be presented as follows using $\log t + 1 = (\log\log q) + 1$ qubits:

$$\underbrace{|0\rangle \otimes \cdots \otimes |0\rangle}_{\log t} \otimes |0\rangle \to \frac{1}{\sqrt{t}}\sum_{i=1}^{t} |i\rangle(\cos\theta_i|0\rangle + \sin\theta_i|1\rangle), \tag{8}$$

where $\theta_i = \frac{2\pi s_i \sigma}{q}$ and the set $S = \{s_1, \ldots, s_t\} \subseteq \mathbb{Z}_q$ is chosen in order to guarantee the small probability of error [11, 15]. That is, the last qubit is simultaneously rotated in t different subspaces by corresponding angles θ_i.

The above q-ary quantum fingerprinting method can be presented in the following procedure:

1. The initial state of the quantum register is $|0\rangle^{\otimes \log t}|0\rangle$.
2. The Hadamard transform creates the uniform superposition $\frac{1}{\sqrt{t}}\sum\limits_{j=1}^{t} |j\rangle|0\rangle$of the basis states $\{|j\rangle|0\rangle : j \in \{1, \ldots, t\}\}$.
3. Based on the input σ, its fingerprint is created: $\frac{1}{\sqrt{t}}\sum_{j=1}^{t} |j\rangle\Big(\cos\frac{2\pi s_j\sigma}{q}|0\rangle + \sin\frac{2\pi s_j\sigma}{q}|1\rangle\Big)$.
4. The Hadamard transform turns the fingerprint into the state $|\psi\rangle = \big(\frac{1}{t}\sum_{l=1}^{t} \cos\frac{2\pi s_l\sigma}{q}\big)|0\rangle^{\otimes \log t}|0\rangle + \ldots$
5. The quantum state $|\psi\rangle$ is measured and the input is accepted iff the result is $|0\rangle^{\otimes \log t}|0\rangle$.

In [11, 15, 16], we have applied this technique to construct efficient quantum algorithms for a certain class of Boolean functions in the model of read-once quantum branching programs [17].

3.2.1. Quantum branching programs

Branching program is a well-known computational model in computer science, also known as a binary decision diagram in Applied Computer Science. Informally speaking, branching program is a circuit with ability to test in each of its computational step a needed bit of an input. Such circuit is a realization of a program that uses only "if then else" and "go to" primitives. We use the definition from [18]

Definition 1 ([18]) *A Quantum Branching Program Q over the Hilbert space $\mathcal{H}^d$ is defined as*

$$Q = \langle T, |\psi_0\rangle\rangle, \tag{9}$$

where T is a sequence of l instructions: $T_j = (x_{i_j}, U_j(0), U_j(1))$ *is determined by variable x_{i_j} tested on the step j, and* $U_j(0)$ and $U_j(1)$ *are unitary transformations in $\mathcal{H}^d$.*

Vectors $|\psi\rangle \in \mathcal{H}^d$ *are called states (state vectors) of Q,* $|\psi_0\rangle \in \mathcal{H}^d$ *is the initial state of Q.*

We define a computation of Q on an input $\sigma = \sigma_1, \dots, \sigma_n \in \{0, 1\}^n$ as follows:

1. *A computation of Q starts from the initial state $|\psi_0\rangle$.*
2. *The j-th instruction* of *Q reads the input symbol σ_{i_j} (the value of x_{i_j}) and applies the transition matrix $U_j = U_j(\sigma_{i_j})$ to the current state $|\psi\rangle$ to obtain the state $|\psi'\rangle = U_j(\sigma_{i_j})|\psi\rangle$.*
3. *The final state is*

$$|\psi(\sigma)\rangle = \left(\prod_{j=l}^{1} U_j\left(\sigma_{i_j}\right)\right)|\psi_0\rangle. \tag{10}$$

Accepting of an input sequence is a result of measuring of final state $|\psi(\sigma)\rangle$ in computational basis and is formalized as follows. Let A*ccept* $\subseteq \{1, 2, \dots d\}$ be the set of indices of accepting basis states. After the l-th (last) step of quantum transformation, Q measures its configuration $|\psi_\sigma\rangle = (\alpha_1, \dots, \alpha_d)^T$ and the input σ is accepted with probability

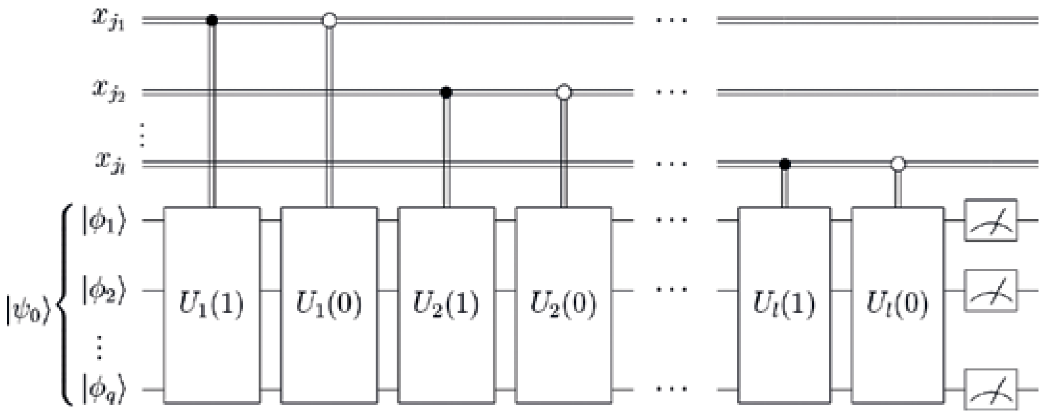


Figure 1. Branching program in the form of circuit. Variables $x_{i_1}, \dots, x_{i_l}$ denoting classical control (input) bits. Single wires carry quantum information, and double wires denote classical information and control.

$$Pr_{\text{accept}}(\sigma) = \sum_{i \in \text{Accept}} |\alpha_i|^2. \tag{11}$$

3.2.2. Circuit representation

Quantum circuits are good formalism for quantum algorithms representation [19, 20]. A quantum branching programs can be viewed as a quantum circuit aided with an ability to read classical bits as control variables for unitary operations (see **Figure 1**).

4. Quantum hashing

In this section, we present notion of quantum (δ, ε)-resistant hash function based on [21].

4.1. One-way δ resistance

We present the following definition of a quantum δ-resistant one-way function. Let "information extracting" mechanism M be a function $M : \left(\mathcal{H}^2\right)^{\otimes s} \to \mathbb{X}$. Informally speaking, mechanism M makes some measurements to state $|\psi\rangle \in (\mathcal{H}^2)^{\otimes s}$ and decodes the result of measurement to $\mathbb{X}$.

Definition 2 ([21]) *Let X be a random variable distributed over $\mathbb{X}$ $\{\Pr[X = w] : w \in \mathbb{X}\}$. Let $\psi : \mathbb{X} \to \left(\mathcal{H}^2\right)^{\otimes s}$ be a quantum function. Let Y be any random variable over $\mathbb{X}$ obtained by some mechanism* **M** *making measurement to the encoding ψ of X and decoding the result of the measurement to $\mathbb{X}$. Let $\delta > 0$. We call a quantum function ψ a one-way δ-resistant function if*

1. *it is easy to compute, i.e., a quantum state $|\psi(w)\rangle$ for a particular $w \in \mathbb{X}$ can be determined using a polynomial-time algorithm.*
2. *for any mechanism* **M**, *the probability* $\Pr[Y = X]$ *that* **M** *successfully decodes Y is bounded by δ*

$$\Pr[Y = X] \le \delta. \tag{12}$$

For the cryptographic purposes, it is natural to expect (and we do this in the rest of the paper) that random variable X is uniformly distributed.

A quantum state of $s \ge 1$ qubits can theoretically record an infinite amount of information. On the other hand, the Holevo's theorem [22] states that by a quantum measurement, one can extract $O(s)$ bits of information about the state. Here, we use the result of [23] motivated by the Holevo's theorem.

Property 1 ([23]) *Let X be a random variable uniformly distributed over $\{0, 1\}^k$. Let $\psi : \{0, 1\}^k \to (\mathcal{H}^2)^{\otimes s}$ be a quantum function. Let Y be a random variable over $\{0, 1\}^k$ obtained by some mechanism* **M** *making some measurement of the encoding ψ of X and decoding the result of measurement to $\{0, 1\}^k$. Then, the probability of correct decoding is given by*

$$\Pr[Y = X] \le \frac{2^s}{2^k}. \tag{13}$$

So, extracting an information on input σ from state $|\psi(\sigma)\rangle$ in conditions of Property 1 is "hard." The effectiveness of computation $|\psi(\sigma)\rangle$ depends on construction of quantum hash function ψ. In Section 4.4, we consider quantum hash function construction based on small-biased sets and prove effectiveness of this construction.

4.2. Collision ε resistance

The following definition was presented in [24].

Definition 3 *Let $\varepsilon > 0$. We call a quantum function $\psi : \mathbb{X} \to \left(\mathcal{H}^2\right)^{\otimes s}$ a collision ε-resistant function if for any pair w, w' of different inputs, $|\langle\psi(w)|\,\psi(w')\rangle| \le \varepsilon$.*

Informally speaking, we need two states $|\psi(w)\rangle$ and $|\psi(w')\rangle$ that is almost orthogonal in order to get small probability of collision, that is, if one tests states $|\psi(w)\rangle$ and $|\psi(w')\rangle$ for equality, then a testing procedure should give positive result with a small probability. We start with quantum testing procedures.

4.2.1. Testing equality

The crucial procedure for quantum hashing is an equality test for $|\psi(v)\rangle$ and $|\psi(w)\rangle$ that can be used to compare encoded classical messages v and w. This procedure can be a well-known SWAP test [5] or something that is adapted for specific hashing function, like REVERSE test, see for example [6].

The SWAP test is the known quantum test for the equality of two unknown quantum states $|\psi\rangle$ and $|\psi'\rangle$ (see [6, 25] for more information).

We denote $Pr_{\text{SWAP}}[v = w]$ a probability that the SWAP test having quantum hashes $|\psi(v)\rangle$ and $|\psi(w)\rangle$ outputs the result "$v = w$" (outputs the result "$|\psi(v)\rangle = |\psi(w)\rangle$").

Property 2 ([6]) *Let function $\psi : w \mapsto |\psi(w)\rangle$ satisfy the following condition. For any two different elements $v, w \in \mathbb{X}$, it is true that $|\langle\psi(v)|\,\psi(w)\rangle| \le \varepsilon$. Then,*

$$Pr_{\text{swap}}[v = w] \le \frac{1}{2}\left(1 + \varepsilon^2\right). \tag{14}$$

Proof. From the description of SWAP test, it follows that

$$Pr_{\text{swap}}[v = w] = \frac{1}{2}\left(1 + |\langle\psi(v)|\psi(w)\rangle|^2\right). \tag{15}$$

4.2.1.1. REVERSE test

The test for equality, which we are presenting here, was first mentioned in [6]. In our paper [25], we call this test a REVERSE test. This test checks if a quantum state $|\psi\rangle$ is a hash of an element v by applying the procedure that inverts the creation of a quantum quantum hash. That is, the REVERSE test procedure transforms the quantum hash to the initial quantum state.

Formally, let the procedure of quantum hashing, given initial state $|0\rangle$, maps the input w by unitary transformation $U(w)$: i.e., quantum hashing produces quantum state $|\psi(w)\rangle = U(w)|0\rangle$. Then, the REVERSE test, given v and $|\psi(w)\rangle$, applies $U^{-1}(v)$ to the state $|\psi(w)\rangle$ and measures the resulting state with respect to initial state $|0\rangle$. The output of REVERSE *test* is "$v = w$" iff the measurement outcome is $|0\rangle$. The output of REVERSE test is "$v \not= w$" iff the measurement outcome is different from $|0\rangle$. The probability that the *REVERSE test* having quantum state $|\psi(w)\rangle$ and an element v outputs the result $v = w$ are denoted by $Pr_{\text{REVERSE}}[v = w]$.

Property 3 ([23]) *Let hash function $\psi : w \mapsto |\psi(w)\rangle$ satisfies the following condition. For any two different elements, v and $w \in \mathbb{X}$, it is true that $|\langle\psi(v)|\psi(w)\rangle| \le \varepsilon$. Then,*

$$Pr_{\text{REVERSE}}[v = w] \le \varepsilon^2. \tag{16}$$

$$Pr_{\text{REVERSE}}[v = w] = |\langle 0|U^{-1}(v)\psi(w)\rangle|^2 = |\langle U^{-1}(v)\psi(v)|U^{-1}(v)\psi(w)\rangle|^2$$
$$= \left|\left\langle \psi(v)|\psi(w)\right\rangle\right|^2 \le \varepsilon^2. \tag{17}$$

4.3. Balanced quantum (δ, ε) resistance

The combination of one-way and collision-resistant function definitions gives the definition of quantum cryptographic function.

Definition 4 ([21]) *Let $K = |\mathbb{X}|$ and $s \ge 1$. Let $\delta > 0$ and $\varepsilon > 0$. We call a function $\psi : \mathbb{X} \to \left(\mathcal{H}^2\right)^{\otimes s}$ a quantum (δ, ε)-hash function iff ψ is one-way δ-resistant and is collision ε-resistant function.*

We present below the following two examples to demonstrate how one-way δ resistance and collision ε resistance are correlated. The first example was presented in [4] in terms of quantum automata.

Example 1 *Let $v \in \{0, \ldots, 2^k - 1\}$. Number v is encoded by a single qubit as follows:*

$$\psi : v \mapsto \cos\left(\frac{2\pi v}{2^k}\right)|0\rangle + \sin\left(\frac{2\pi v}{2^k}\right)|1\rangle. \tag{18}$$

Extracting information from $|\psi\rangle$ by measuring $|\psi\rangle$ with respect to the basis $\{|0\rangle, |1\rangle\}$ gives the following result. The function ψ is one-way $\frac{2}{2^k}$ resistant (see Property 1) and collision $\cos(\pi/2^{k-1})$ resistant. Thus, the function ψ has a good one-way property but has a bad collision resistance property for large k.

Clearly, that one can store (*to hash*) in this way an arbitrary large amount of classical information, that is, for arbitrary large k one can store all numbers from $\{0, \ldots, 2^k - 1\}$ in a single qubit. Holevo bound [22] proves that given $s \ge 1$ qubits, the amount of classical information that can be retrieved, i.e., accessed, can be only up to s classical bits. This is a quantum mechanical approach for the one-way property.

The map ψ is one to one. So, there is no collision in a "quantum level." But extracting the result from quantum state is a probabilistic procedure. This means that one can get the situation when some procedure that tests the equality of different quantum hashes $|\psi(v)\rangle$, $|\psi(w)\rangle$ outputs "the hashes are the same" (equivalently "the numbers v, w are the same"), while the numbers v and w are different. For example, two numbers 0 and 2^{k-2} generate orthogonal states $|\psi(0)\rangle = |1\rangle$ and $|\psi(2^{k-2})\rangle = |0\rangle$. So, numbers 0 and 2^{k-2} are distinguishably reliable in respect of the above encoding. But two numbers 0 and 1 cannot be reliably distinguished by encoding ψ.

Example 2 *Binary word* $v = \sigma_1, \ldots, \sigma_k \in \{0,1\}^k$ *encoded by k qubits (each bit encoded by a qubit):* $\psi : v \mapsto |v\rangle = |\sigma_1\rangle, \cdots, |\sigma_k\rangle$.

Clearly, we have that such encoding is collision one-way, 1-resistant, and 0-resistant. So, in contrast to Example 1, the encoding ψ from Example 2 for different words v and w, their images (quantum states) $|\psi(v)\rangle$ and $|\psi(v)\rangle$ are orthogonal and therefore reliably distinguished; but ψ is easily invertible: the function ψ is not one-way resistant.

The following result [24] proves that a quantum collision ε-resistant function needs at least $\log\log K - c(\varepsilon)$ qubits.

Property 4 ([24]) *Let* $s \geq 1$ *and* $K = |\mathbb{X}| \geq 4$. *Let* $\psi : \mathbb{X} \to \left(\mathcal{H}^2\right)^{\otimes s}$ *be a collision ε-resistant quantum hash function. Then,*

$$s \geq \log\ \log\ K - \ \log\ \log\left(1 + \sqrt{2/(1-\varepsilon)}\right) - 1. \tag{19}$$

Proof. First, we observe that from the definition $\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle}$ of the norm, it follows that

$$\||\psi\rangle - |\psi'\rangle\|^2 = \||\psi\rangle\|^2 + \||\psi'\rangle\|^2 - 2\langle\psi|\psi'\rangle. \tag{20}$$

Hence, for an arbitrary pair w, w' of different elements from $\mathbb{X}$, we have that

$$\||\psi(w)\rangle - |\psi(w')\rangle\| \geq \sqrt{2(1-\varepsilon)}. \tag{21}$$

We let $\Delta = \sqrt{2(1-\varepsilon)}$. For short, we let $(\mathcal{H}^2)^{\otimes s} = V$ in this proof. Consider a set $\Phi = \{|\psi(w)\rangle : w \in \mathbb{X}\}$. If we draw spheres of radius $\Delta/2$ with centers $|\psi\rangle \in \Phi$, then spheres do not pairwise intersect. All these K spheres are in a large sphere of radius $1 + \Delta/2$. The volume of a sphere of radius r in V is $cr^{2^{s+1}}$ for the complex space V. The constant c depends on the metric of V. From this, we have that the number K is bonded by the number of "small spheres" in the "large sphere"

$$K \leq \frac{c(1+\Delta/2)^{2^{s+1}}}{c(\Delta/2)^{2^{s+1}}}. \tag{22}$$

Hence,

$$s \geq \log\ \log K - \log\ \log\left(1 + \sqrt{2/(1-\varepsilon)}\right) - 1. \tag{23}$$

Properties 1 and 4 provide a basis for building a "balanced" one-way δ-resistance and collision ε-resistance properties. That is, roughly speaking, if we need to hash elements w from the domain $\mathbb{X}$ with $|\mathbb{X}| = K$ and if one can build for an $\varepsilon > 0$ a collision ε-resistant $(K; s)$ hash function ψ with $s \approx \log\log K - c(\varepsilon)$ qubits, then the function f is one-way δ resistant with $\delta \approx (\log K/K)$. Such a function is balanced with respect to Property 4.

To summarize the above considerations, we can state the following. A quantum (δ, ε)-hash function is a function that satisfies all of the properties that a "classical" hash function should satisfy. Preimage resistance follows from Property 1. Second preimage resistance and collision resistance follow, because all inputs are mapped to states that are nearly orthogonal. Therefore, we see that quantum hash functions can satisfy the three properties of a classical cryptographic hash function.

4.4. Quantum hash functions construction via small-biased sets

This section is based on the paper [26]. We first present a brief background on ε-biased sets. For more information, see [27]. Note that ε-biased sets are generally defined for arbitrary finite groups, but here we restrict ourselves to $\mathbb{Z}_q$.

For an $a \in \mathbb{Z}_q$, a character χ_a of $\mathbb{Z}_q$ is a homomorphism $\chi_a : \mathbb{Z}_q \rightarrow \mu_q$, where μ_q is the (multiplicative) group of complex q-th roots of unity. That is, $\chi_a(x) = \omega^{ax}$, where $\omega = e^{\frac{2\pi i}{q}}$ is a primitive q-th root of unity. The character $\chi_0 \equiv 1$ is called a trivial character.

Definition 5 *A set $S \subseteq \mathbb{Z}_q$ is called ε biased, if for any nontrivial character $\chi \in \{\chi_a : a \in \mathbb{Z}_q\}$*

$$\frac{1}{|S|} \left| \sum_{x \in S} \chi(x) \right| \leq \varepsilon. \tag{24}$$

These sets are interesting when $|S| \ll |\mathbb{Z}_q|$ (as $S = \mathbb{Z}_q$ is 0 biased). In their seminal paper, Naor and Naor [13] defined these small-biased sets, gave the first explicit constructions of such sets, and demonstrated the power of small-biased sets for several applications.

Remark 1 *Note that a set S of $O(\log q/\varepsilon^2)$ elements selected uniformly at random from $\mathbb{Z}_q$ is ε biased with positive probability* [28].

Many other constructions of small-biased sets followed during the last decades.

Vasiliev [26] showed that ε-biased sets generate (δ,ε)-resistant hash functions. We present the result of [26] in the following form.

Theorem 1 *Let $S \subseteq \mathbb{Z}_q$ be an ε-biased set. Let $H_S = \{h_a(x) = ax (\mathrm{mod}\ q),\quad a \in S, h_a : \mathbb{Z}_q \rightarrow \mathbb{Z}_q\}$ be a set of functions determined by S. Then, a quantum function $\psi_{H_S} : \mathbb{Z}_q \rightarrow (\mathcal{H}^2)^{\otimes \log|S|}$*

$$|\psi_{H_S}(x)\rangle = \frac{1}{\sqrt{|S|}} \sum_{a \in S} \omega^{h_a(x)} |a\rangle \tag{25}$$

is a (δ, ε)-resistant quantum hash function, where $\delta \leq |S|/q$.

Proof. One-way δ-resistance property of ψ_{H_S} follows from Property 1: a probability of correct decoding an x from a quantum state $|\psi_{H_S}(x)\rangle$ is bounded by $|S|/q$.

Collision ε-resistance property of ψ_{H_S} follows directly from the corresponding property of [26]. Note that

$$|\psi_{H_S}(x)\rangle = \frac{1}{\sqrt{|S|}}\sum_{a\in S}\omega^{h_a(x)}|a\rangle = \frac{1}{\sqrt{|S|}}\sum_{a\in S}\chi_x(a)|a\rangle. \tag{26}$$

We will prove that for arbitrary different elements $v, v^{'} \in \mathbb{Z}_q$, it is true that

$$\left|\left\langle \psi_{H_S}(v)|\psi_{H_S}(v')\right\rangle\right| = \frac{1}{|S|}\left|\sum_{a\in S}\chi_v^*(a)\chi_{v'}(a)\right| \leq \varepsilon. \tag{27}$$

Let $\chi_v(x)$ and $\chi_{v'}(x)$ be characters of group $\mathbb{Z}_q$. Then, $\chi_v^*(x)$ is also a character of $\mathbb{Z}_q$ and so the following function is $\chi(x) = \chi_v^*(x)\chi_{v'}(x)$. $\chi(x)$ is nontrivial character of $\mathbb{Z}_q$, since $\chi_v(x) \not\equiv \chi_{v'}(x)$ and $\chi(x) = \chi_v^*(x)\chi_{v'}(x) \not\equiv \chi_v^*(x)\chi_v(x) \equiv 1$, where 1 is a trivial character of $\mathbb{Z}_q$. Thus, the statement of Theorem 1 follows from the definition of an ε-biased set.

$$|\langle\psi_{H_S}(v)|\psi_{H_S}(v')\rangle| = \frac{1}{|S|}\left|\sum_{a\in S}\chi_v^*(a)\chi_{v'}(a)\right| = \frac{1}{|S|}\left|\sum_{a\in S}\chi(a)\right| \leq \varepsilon. \tag{28}$$

4.5. Quantum fingerprinting functions as hash functions

In this section, we give two explicit examples of the quantum hashing for specific finite abelian groups, which turn out to be the known quantum fingerprinting schemas.

4.5.1. Hashing the elements of the Boolean cube

For $G = \mathbb{Z}_2^n$, its characters can be written in the form $\chi_a(x) = (-1)^{(a,x)}$, and the corresponding quantum hash function is the following

$$|\psi_S(a)\rangle = \frac{1}{\sqrt{|S|}}\sum_{j=1}^{|S|}(-1)^{(a,s_j)}|j\rangle. \tag{29}$$

The resulting hash function is exactly the quantum fingerprinting by Buhrman et al. [5], once we consider an error-correcting code, whose matrix is built from the elements of S. Indeed, as stated in [29] an ε-balanced error-correcting code can be constructed out of an ε-biased set. Thus, the inner product (a, x) in the exponent is equivalent to the corresponding bit of the code word, and altogether, this gives the quantum fingerprinting function that stores information in the phase of quantum states de Wolf [30].

4.5.2. Hashing the elements of the cyclic group

For group $G = \mathbb{Z}_q$, the corresponding quantum hash function is given by

$$|\psi_S(a)\rangle = \frac{1}{\sqrt{|S|}} \sum_{j=1}^{|S|} \omega^{as_j} |j\rangle. \tag{30}$$

The above quantum hash function is essentially equivalent to the one we have defined earlier in [25], which is in turn based on the quantum fingerprinting function from [11].

- In the content of the definition of quantum hash generator [24] and the above consideration, it is natural to call the set H_S of functions (formed from ε-biased set S) a *uniform quantum* (δ, ε)*-hash generator* for $\delta = O(\mid S \mid /(q \log q))$.

As a corollary from Theorem 1 and the above consideration, we can state the following.

Property 5 *For an* ε*-biased set* $S = \{a_1, \ldots, a_T\} \subset \mathbb{F}_q$ *with* $T = O(logq/\varepsilon^2)$*, for* $s = logT$*, for* $\delta = O(1/(q\varepsilon^2))$*, a quantum uniform* (δ, ε)*-hash generator* H_S *generates quantum* (δ, ε)*-hash function*

$$\psi_{H_S} : \mathbb{F}_q \to \left(\mathcal{H}^2\right)^{\otimes s} \tag{31}$$

$$|\psi_{H_S}(x)\rangle = \frac{1}{\sqrt{T}} \sum_{j=0}^{T-1} \omega^{a_j x}, \tag{32}$$

5. Computing a quantum hash $\mid \psi_{H_S}(x)\rangle$ by QBP

Theorem 2 *Quantum* (δ, ε)*-hash function (6)*

$$\psi_{H_S} : \mathbb{F}_q \to \left(\mathcal{H}^2\right)^{\otimes s} \tag{33}$$

can be computed by quantum branching program Q composed from $s = O(\log \log q)$ *qubits in* $\log q$ *steps.*

Proof. Quantum function ψ_{H_S} (6) for an input $x \in \mathbb{F}_q$ determines quantum states (7)

$$|\psi_{H_S}(x)\rangle = \frac{1}{\sqrt{T}} \sum_{j=0}^{T-1} \omega^{a_j x} |j\rangle, \tag{34}$$

which is a result of quantum Fourier transformation (QFT) of the initial state

$$|\psi_0\rangle = \frac{1}{\sqrt{T}} \sum_{j=0}^{T-1} |j\rangle. \tag{35}$$

Such a QFT is controlled by the input x. QBP Q for computing quantum hash $\mid \psi_{H_S}(x)\rangle$ determined as follows. We represent an integer $x \in \{0, \ldots, q-1\}$ as the bit-string $x = x_0 \ldots x_{\log q - 1}$ that is, $x = x_0 + 2^1 x_1 + \ldots + 2^{\log q - 1} x_{\log q - 1}$. For a binary string $x = x_0 \ldots x_{\log q - 1}$ a quantum branching program Q over the space $(\mathcal{H}^2)^{\otimes s}$ for computing $\mid \psi_{H_S}(x)\rangle$ (composed of $s = \log T$ qubits) is defined as

$$Q = \langle \mathbb{T}, |\psi_0\rangle \rangle, \tag{36}$$

where $|\psi_0\rangle$ is the initial state and $\mathbb{T}$ is a sequence of log q instructions:

$$\mathbb{T}_j = (x_j, U_j(0), U_j(1)) \tag{37}$$

is determined by the variable x_j tested on the step j, and $U_j(0)$ and $U_j(1)$ are unitary transformations in $(\mathcal{H}^2)^{\otimes s}$. More precise $U_j(0)$ is $T \times T$ identity matrix. $U_j(1)$ is the $T \times T$ diagonal matrix whose diagonal entries are $\omega^{a_0 2j}, \omega^{a_1 2j}, \ldots, \omega^{a_{T-1} 2j}$ and the off-diagonal elements are all zero. That is,

$$U_j(1) = \begin{bmatrix} \omega^{a_0 2^j} & & & \\ & \omega^{a_1 2^j} & & \\ & & \ddots & \\ & & & \omega^{a_{T-1} 2^j} \\ & & & \end{bmatrix}. \tag{38}$$

We define a computation of Q on an input $x = x_0, \ldots, x_{\log q - 1} \in \{0, 1\}^{\log q}$ as follows:

1. A computation of Q starts from the initial state $|\psi_0\rangle$.

2. The j-th instruction of Q reads the input symbol x_j (the value of x) and applies the transition matrix $U_j(x_j)$ to the current state $|\psi\rangle$ to obtain the state $|\psi'\rangle = U_j(x_j)|\psi\rangle$.

3. The final state is

$$|\psi_{H_S}(x)\rangle = \left(\prod_{j=0}^{\log q - 1} U_j(x_j) \right) |\psi_0\rangle. \tag{39}$$

5.1. Complexity measures

We consider the following notations. For the QBP Q from Theorem 2, we let $width(Q) = s$ and $time(Q) = |\mathbb{T}|$. Next for quantum hash function ψ_{H_S} (6), we let

$$width(\psi_{H_S}) = \min width(Q), \qquad time(\psi_{H_S}) = \min time(Q) \tag{40}$$

where minimum is taken over all QBPs that compute ψ_{H_S}.

5.1.1. Upper bounds

Then from Theorem 2, we have the following corollary

Theorem 3

$$width(\psi_{H_S}) = O(\log\ \log q), \tag{41}$$

$$time(\psi_{H_S}) = O(\log\ q). \tag{42}$$

5.1.2. Lower bounds

Here, we show that the quantum branching program from Theorem 2 is optimal for function ψ_{H_S}

Theorem 4

$$width(\psi_{H_S}) = \Omega(\log\ \log q), \tag{43}$$

$$time(\psi_{H_S}) = \Omega(\log\ q). \tag{44}$$

Proof. Let Q be a QBP for the function ψ_{H_S} computation. ψ_{H_S} presented by Q as follows:

$$\psi_{H_S} : \{|\psi_0\rangle\} \times \{0,1\}^{\log q} \to \left(\mathcal{H}^2\right)^{\otimes s}. \tag{45}$$

The lower bound (10) for $width(\psi_{H_S})$ follows immediately from Property 4

$$s \geq \log\ \log q - \log\ \log\left(1 + \sqrt{2/(1-\varepsilon)}\right). \tag{46}$$

The lower bound (11) for $time(\psi_{H_S})$ follows from the fact that ψ_{H_S} is collision ε-resistant function. Indeed, the assumption that QBP Q for ψ_{H_S} can test less than log$q$ (that is, not all log$q$) variables of inputs $x \in \mathbb{F}_q$ means existence of (at least) two different inputs $w, w' \in \mathbb{F}_q$ such that Q produces the same quantum hashes $|\psi(w)\rangle$ and $|\psi(w^{'})\rangle$ for w and $w^{'}$, that is, $|\psi(w)\rangle = |\psi(w^{'})\rangle = |\psi\rangle$. The last contradicts to the fact that states $|\psi(w)\rangle$ and $|\psi(w^{'})\rangle$ are ε orthogonal.

$$|\langle\psi(w)|\psi(w')\rangle| \leq \varepsilon. \tag{47}$$

6. Concluding remarks

To conclude, we first like to mention the results of the paper [31], which presents further development of quantum hash functions construction.

Recall that any ε-biased set gives rise to a Cayley expander graph [28]. We show how such graphs generate balanced quantum hash functions. Every expander graph can be converted to a bipartite expander graph. The generalization of these bipartite expander graphs is the notion of extractor graphs. Such point of view gives a method for constructing quantum hash functions based on extractors. This construction of quantum hash functions is applied to define the notion of keyed quantum hash functions. The latter is used for constructing quantum hash-based message authentication codes (QMAC). The security proof of QMAC is based on using strong extractors against quantum storage developed by Ta-Shma [32].

Secondly, in [24], we offered a design that allows to build a large amount of different quantum hash functions. The construction is based on composition of classical δ-universal hash family and a given family $H_{\delta,q}$, a quantum hash generator. A resulting family of functions is a new quantum hash generator. In particular, we present a quantum hash generator G_{RS} based on Reed-Solomon code.

Author details

Farid Ablayev* and Marat Ablayev

*Address all correspondence to: fablayev@gmail.com

Kazan Federal University, Kazan, Russia

References

[1] Motwani R, Raghavan P. Randomized Algorithms. New York, USA: Cambridge University Press; 1995

[2] Rusins Freivalds. Probabilistic machines can use less running time. In: IFIP Congress. Vol. 839; 1977. pp. 842

[3] Freivalds R. Fast probabilistic algorithms. In: Becvar J, editor. Mathematical Foundations of Computer Science — Lecture Notes in Computer Science. Vol. 74. Heidelberg: Springer Berlin; 1979. p. 57-69

[4] Andris Ambainis, Rusins Freivalds. 1-way quantum finite automata: Strengths, weaknesses and generalizations. In: Proceeding of the 39th IEEE Conference on Foundation of Computer Science, FOCS '98, Washington DC USA: IEEE Computer Society; 1998. pp. 332-342

[5] Buhrman H, Cleve R, Watrous J, Wolf R d. Quantum fingerprinting. Physical Review Letters. 2001;**87**(16):167902

[6] Gottesman D, IC. Quantum digital signatures technical report arXiv:Quant-ph/0105032

[7] Gavinsky D, Ito T. Quantum fingerprints that keep secrets. Quantum Information & Computation. 2013;**13**(7–8):583-606

[8] Li D, Zhang J, Guo F-Z, Huang W, Wen Q-Y, Chen H. Discrete-time interacting quantum walks and quantum hash schemes. Quantum Information Processing. 2013;**12**(3):1501-1513

[9] Li D, Zhang J, Ma X-W, Zhang W-W, Wen Q-Y. Analysis of the two-particle controlled interacting quantum walks. Quantum Information Processing. 2013;**12**(6):2167-2176

[10] Yang Y-G, Peng X, Yang R, Zhou Y-H, Shi W-M. Quantum hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption. Scientific Reports. 2016;**6**:19788

[11] Ablayev F, Vasiliev A. Algorithms for quantum branching programs based on fingerprinting. Electronic Proceedings in Theoretical Computer Science. 2009;**9**:1-11

[12] Ambainis A, Nahimovs N. Improved constructions of quantum automata. In: Kawano Y, Mosca M, editors. Theory of Quantum Computation, Communication, and Cryptography — Lecture Notes in Computer Science. Vol. 5106. Berlin/Heidelberg: Springer; 2008. p. 47-56

[13] Joseph Naor, Moni Naor. Small-bias probability spaces: Efficient constructions and applications. In: Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing, STOC '90, NY, USA, New York: ACM; 1990. 213-223

[14] Eli Ben-Sasson, Madhu Sudan, Salil Vadhan, Avi Wigderson. Randomness-efficient low degree tests and short pcps via epsilon-biased sets. In: Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing, STOC '03, NY, USA, New York: ACM; 2003. pp. 612-621

[15] Ablayev F, Vasiliev A. On computational power of quantum read-once branching programs. Electronic Proceedings in Theoretical Computer Science. 2011;**52**:1-12

[16] Farid Ablayev, Alexander Vasiliev. Classical and quantum parallelism in the quantum fingerprinting method. In: Victor Malyshkin, editor. 11th International Conference PaCT 2011 Proceedings — Lecture Notes in Computer Science. Vol. 6873. Springer; 2011. pp. 1-13

[17] Ablayev F, Gainutdinova A, Karpinski M. On computational power of quantum branching programs. FCT. 2001;59-70

[18] Ablayev F, Gainutdinova A, Karpinski M, Moore C, Pollett C. On the computational power of probabilistic and quantum branching programs of constant width. Information and Computation. 2005;**203**:145-162

[19] Deutsch D. Quantum computational networks. Royal Society of London Proceedings Series A. 1989;**425**:73-90

[20] Andrew Chi-Chih Yao. Quantum circuit complexity. In: Proceedings of Thirty-fourth IEEE Symposium on Foundations of Computer Science. Palo Alto California USA: IEEE Computer Society; 1993. pp. 352-361

[21] Ablayev F, Ablayev M. On the concept of cryptographic quantum hashing. Laser Physics Letters. 2015;**12**(12):125204

[22] Alexander SH. Some estimates of the information transmitted by quantum communication channel (Russian). Probl. Pered. Inform Problems of Information Transmission. 1973;**9**(3):3-11

[23] Ashwin Nayak. Optimal lower bounds for quantum automata and random access codes. In: Foundations of Computer Science. 40th Annual Symposium on; 1999. pp. 369-376

[24] Ablayev F, Ablayev M. Quantum hashing via ε-universal hashing constructions and classical fingerprinting. Lobachevskii Journal of Mathematics. 2015;**36**(2):89-96

[25] Ablayev FM, Vasiliev AV. Cryptographic quantum hashing. Laser Physics Letters. 2014;**11**(2):025202

[26] Vasiliev A. Quantum hashing for finite abelian groups. Lobachevskii Journal of Mathematics. 2016;**37**(6):751-754

[27] Chen S, Moore C, Russell A. Small-bias sets for nonabelian groups. In: Raghavendra P, Raskhodnikova S, Jansen K, Rolim JDP, editors. Approximation, Randomization, and

Combinatorial Optimization. Algorithms and Techniques — Lecture Notes in Computer Science. Vol. 8096. Berlin Heidelberg: Springer; 2013. p. 436-451

[28] Alon N, Roichman Y. Random cayley graphs and expanders. Random Structures & Algorithms. 1994;**5**(2):271-284

[29] Ben-Aroya A., Ta-Shma A. Constructing small-bias sets from algebraic-geometric codes. In: Foundations of Computer Science, FOCS '09. 50th Annual IEEE Symposium on; 2009. pp. 191-197

[30] R d W. Quantum Computing Communication Complexity [Ph.D. Thesis]. Amsterdam: University of Amsterdam; 2001

[31] Ziatdinov M. From graphs to keyed quantum hash functions. Lobachevskii Journal of Mathematics. 2016;**37**(6):704-711

[32] Ta-Shma A. Short seed extractors against quantum storage. Proceedings of the ACM STOC. 2009;401-408

Quantum Flows for Secret Key Distribution

Luis A. Lizama-Pérez, J. Mauricio López and
Eduardo de Carlos Lopez

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.75964

Abstract

Despite the unconditionally secure theory of quantum key distribution (QKD), several attacks have been successfully implemented against commercial QKD systems. Those systems have exhibited some flaws, as the secret key rate of corresponding protocols remains unaltered, while the eavesdropper obtains the entire secret key. We propose a new theoretical approach called quantum flows to be able to detect the eavesdropping activity in the channel without requiring additional optical components different from the BB84 protocol because the system can be implemented as a high software module. In this approach, the transmitter interleaves pairs of quantum states, referred to here as parallel and orthogonal (non-orthogonal) states, while the receiver uses active basis selection.

Keywords: quantum key distribution, photon number splitting attack, intercept resend faked states attack

1. Introduction

Quantum key distribution (QKD) is a technique to distribute securely a cryptographic key between two remote users, usually called Alice and Bob. The first *QKD* method was conceived by Charles Bennett and Gilles Brassard in 1984, usually referred to in literature as *BB84* [1]. **Figure 1** shows a simplified representation of the two-dimensional Bloch sphere, the quantum states, and the measurement bases of *BB84*.

QKD systems are designed to serve the purpose of generating secret bits, usable to encrypt plain-text messages based on a simple $X - Or$ logical function between the message and a secret key. The use of this system provides the availability to detect any eavesdropper, commonly called Eve, trying to intercept the quantum channel to get the key. In this case, the

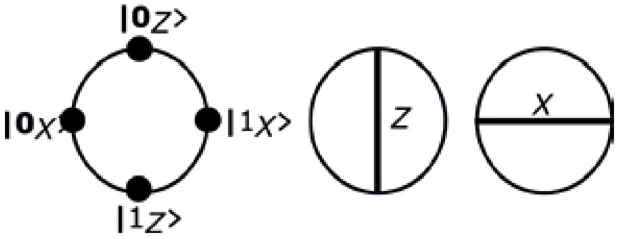


Figure 1. The *BB84* qubits are the *non-orthogonal* states: the measurement bases, Z and X, are shown as vertical and horizontal lines, correspondingly. When basis X (Z) is used by Bob, to measure Alice's state $|i_X\rangle$ ($|i_Z\rangle$), the result gotten by Bob is bit $i\,(i = 0, 1)$; otherwise, if basis X (Z) is applied to measure $|i_Z\rangle$ ($|i_X\rangle$) the probability to get i reduces to $\frac{1}{2}$. So, if Bob measures the $|0_X\rangle$ state with Z basis, he has the same probability to obtain $|0_Z\rangle$ or $|1_Z\rangle$.

whole process will be discarded before a key can be established [2]. On the other hand, if no eavesdropping activity is detected, the quantum measurements are used to derive the secret key. When the transmission is finished, Alice and Bob compare a fraction of the exchanged key in order to detect any transmission errors caused by eavesdropping. Experimentally, *QKD* systems have been proved using dedicated optical fibers, across free space, weak laser pulses or single photons, entangled photon pairs, or continuous variables [3].

We propose a new approach for *QKD* protocols called quantum flows where the transmitter interleaves pairs of quantum states, referred to here as *parallel* and *orthogonal* (*non-orthogonal*) states, while the receiver applies active basis selection to perform state measurement. In a study by Lizama et al. [4], a brand new *QKD* protocol, called *ack-state* and referred to also as *ack-QKD*, is introduced. This protocol uses weak coherent states and active basis measurement and has the capability to detect photon number splitting *(PNS)* eavesdropping activity, and its strengths against the *PNS* attack are discussed by Lizama-Pérez et al. [5]. The *ack-state* protocol was extended by Lizama-Pérez et al. [6] to the dual protocol known as *nack state* protocol in order to have an analysis of its security when facing an intercept and resend with faked states *(IRFS)* attack.

One of the main advantages of these protocols is that they protect against the *PNS* and the *IRFS* attacks without requiring any changes in the hardware; only software changes are required.

2. Quantum hacking in *QKD* systems

In ideal conditions, QKD protocols' security is based on the attributes of quantum mechanics, as it makes eavesdropping activities detectable in the middle of the quantum channel [1, 7]. But the technological implementation brings serious concerns as most of the *QKD* systems have vulnerabilities to quantum hacking due to loopholes in the optical detection system [8–18]. Given this condition, it is necessary to develop new *QKD* protocols that are able to resist different attacks due to such vulnerabilities as the photon number splitting (*PNS*) and the intercept and resend with faked states (*IRFS*) attacks [19, 20].

A variety of attacks have been conceived of as exploiting the security of *BB84*-based systems, either theoretically or technologically. The photon number splitting (*PNS*) attack belongs to the first category. In the second class, commonly referred to as quantum hacking, the intercept resend with faked states (*IRFS*) attack can be included, which exploits loopholes in the avalanche photo diodes (*APD*s) of the electronic detection system. We will briefly describe each of them.

1. In the *PNS* attack the eavesdropper blocks the 1-photon states but she stores the multi-photon states allowing at least one photon to reach Bob's detection system. Ideally, in the *BB84* protocol [1], the quantum states sent by Alice to Bob contain single photons. Nevertheless, perfect single photon sources are not technologically available nowadays [21], so, to get the implementation of *QKD*, laser pulses attenuated to very low levels have been used. Such laser pulses contain very short numbers of photons, in average typically around 0.2 photons per pulse in a Poissonian distribution; that means that most pulses contain no photons, a few pulses contain just one photon, and a really short amount of pulse contains two or more photons. If a pulse contains more than one photon, Eve can get from it the extra photons and transmit a single photon to Bob. Eve can store the photons she obtained from the multi-photonic pulses and wait until Bob reveals the measurement basis he has applied. Then Eve can measure the photons she stored by using the same measurement basis as Bob did. In this way she obtains information about the key without being noticed by Alice and Bob. This is called the photon number splitting (*PNS*) attack, and some related references with security proofs of the *PNS* attack can be found in [1, 7, 22–24].

   To overcome the PNS attack a few protocols have been developed: Decoy QKD [18], SARG04 [25], the differential phase shift (DPSK) [26], and coherent one way (COW) [27]. One of the most promissory alternatives is the decoy QKD. In this protocol Alice prepares a set of quantum states in addition to the typical states of the BB84 protocol. These extra states are called decoy states. Decoy states are used only with the purpose to detect the eavesdropping activity, rather than establishing the key. In order to produce the decoy states, Alice randomly uses different mean photon numbers on the photonic source. For example, she could send the first pulse with a mean photonic pulse of $\mu = 0.1$, the second pulse with $\mu = 0.4$, the third pulse with $\mu = 0.05$, and so on. To each mean photon number a different probability of producing more than one photon in the correlated pulse corresponds. The difference between the standards BB84 states and the decoy states is the mean photon numbers. Given this, Eve is not able to distinguish a decoy state from a quantum key related state and the only information she gets is the number of photons in a pulse. Thus, decoy states can be introduced to secure the BB84 protocol from PNS attacks, allowing at the same time high key rates. In both, BB84 and decoy QKD protocols, a single photonic gain in the quantum channel is established. Lamentably, Eve can set successful attacks to the decoy QKD if it is able to set the QBER to zero by adjusting the gain of the quantum channel.

2. Intercept Resend (*IR*) attack: In this attack, Eve measures each photon pulse sent by Alice and replaces it with a different pulse prepared in the quantum state that she has

previously measured. In 50% of the measurements, Eve successfully chooses the correct measurement basis, while Bob chooses the same basis as her half of the time. Given that, she generates a quantum bit error rate (*QBER*) of 50% $\times$ 50% $=$ 25% (see **Figure 2** and a study by Bennett et al. [7]).

3. Intercept resend with faked states (*IRFS*) attack.

In the intercept resend with faked states (IRFS) attack, the eavesdropper does not want to reconstruct the original states. Instead, it produces pulses of light controlled by her that are detectable by Bob as she stays unnoticed in the quantum channel. Due to imperfections in their optical system, Alice and Bob assume that the quantum states they are detecting are the original ones while they are actually detecting light pulses generated by the eavesdropper. Those light pulses are known as faked states [10]. There are several weaknesses in Bob's detector than can be exploited to perform this attack such as time shift [11–13] or quantum blinding [10–12]. When using quantum blinding (quantum blinding attack), the QKD system is controlled by an eavesdropper who uses bright photon pulses during the linear mode operation of the APDs. Using this attack, Eve can eavesdrop on the full secret key but it will not increase the QBER of the protocol. To do this, Eve sends bright pulses to Bob and those are detected by the APD. It will then operate like a classical photo diode instead of operating in Geiger mode and allowing Eve to obtain the key [14, 15].

Resulting from this, as shown in **Figure 3a**, when Bob selects the same measurement basis Eve has chosen, a detection event occurs in the corresponding APD detector. On the other hand, if Bob measures using the opposite basis, as in **Figure 3b**, the two detectors get a part of the optical power and no event is detected. In this way, the eavesdropper blinds Bob's APD detectors and makes them work as classical photo diodes. In the final stage of the protocol, Eve uses the announcements made by Bob on the public channel to execute the classical post-processing, getting the same secret bit as Alice and Bob.

A watchdog detector that can detect bright faked states can be used as a very simple countermeasure and it can be applied in the electronic detection system [16]. In the University of Singapore an intercept resend attack with faked states and quantum blinding over a commercial QKD system was for the first time implemented [15].

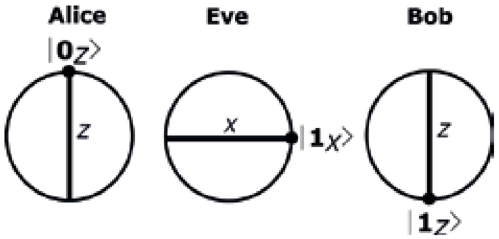


Figure 2. An intercept resend (*IR*) attack toward the *BB84* protocol causes a quantum bit error rate (*QBER*) of 25% that can be detected. The figure shows Alice sending a $|0_Z\rangle$ state to Bob. In the middle of the quantum channel is Eve applying an X basis measurement and she gets $|1_X\rangle$. Consequently, she makes a copy of that state and sends it to Bob who gets $|1_Z\rangle$ as he used the Z basis measurement. The process introduces an error in the secret bit given that Alice expects Bob to get $|0_Z\rangle$.

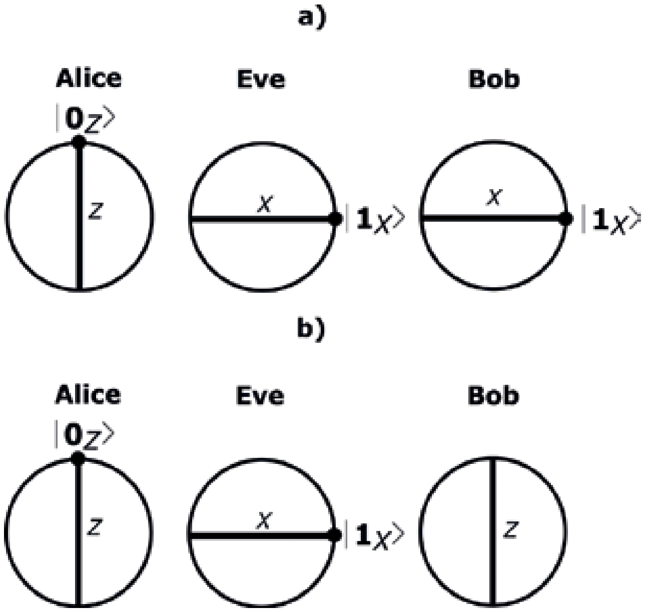


Figure 3. In the intercept resend with faked states (*IRFS*) and quantum blinding attack, Eve and Bob use the same optical receiver unit so that she can detect Alice's states in a random basis. Then, Eve prepares the quantum states but sends them to Bob as bright light pulses instead of quantum pulses. (a) Bob and Eve are using the same basis; (b) the basis Bob is using is the opposite to ve.

It is important to note that the *IRFS* attack works dangerously well on widely used QKD protocols, namely *SARG04*, *BB84*, coherent one way (*COW*), differential phase shift (*DPSK*), Ekert [12], and the *decoy state* method, as described by Wiechers et al. [16] and Sun et al. [28]. The attack shows an extra 3 dB loss due to the basis of mismatch between Eve and Bob. In the practice, Eve compensates it easily as she can use better detector efficiencies and surpass the loss in the channel. Demonstrations of blinding attacks on detectors have been implemented in two commercially available *QKD* systems [14]. Reports show that Eve obtains the entire secret key for the time she remains unnoticed by the legitimate parties [15]. We should finally remark that due to control detector attacks with active basis selection, the gain from Eve to Bob is reduced by a half compared to the gain from Alice to Bob.

i. *For Bob's basis choice matching Eve's, the detector clicks deterministically and.*

ii. *For Bob's basis choice not matching Eve's, the faked state is not detected.*

3. The *ack-state* protocol

Consider a *BB84*-based protocol encoding a classical bit that uses one of the four *non-orthogonal* quantum states $|+_X\rangle, |-_X\rangle, |+_Z\rangle$, and $|-_Z\rangle$ (see **Figure 1**). When using the *SARG04* protocol [25], Alice produces one of the four *BB84* quantum states she will send to Bob, it means, she produces a state associated with two conjugate basis (*X* and *Z*). Classical bits on *SARG04* protocol are encoded as follows: 0 is coded with$|+_Z\rangle$ and $|-_Z\rangle$ and 1 is coded with $|+_X\rangle$ and $|-_X\rangle$ (see **Figure 4**) where black dots in the bidimensional Bloch sphere represent the qubits (the *non-orthogonal* states are right angled and the *orthogonal* states are represented as diametrically opposed and the *parallel* states have the same position in the sphere). The basis measurement X and Z appear as horizontal and vertical lines, respectively. In contraposition, the *BB84* protocol encodes the bit 0 as $|+_Z\rangle$ and $|-_X\rangle$ and the bit 1 with $|-_Z\rangle$ and $|+_X\rangle$.

In the sifting phase of the *SARG04* protocol, the basis used by Alice is not revealed as this would reveal the bit. As a substitute, she declares to which sifting set the state belongs in accordance with the following four sifting sets: $S_{(+,+)} = \{|+_X\rangle, |+_Z\rangle\}$, $S_{(+,-)} = \{|+_X\rangle, |-_Z\rangle\}$, $S_{(-,+)} = \{|-_X\rangle, |+_Z\rangle\}$, and $S_{(-,-)} = \{|-_X\rangle, |-_Z\rangle\}$. For instance, consider that Alice sends $|+_X\rangle$ and she announces the set $S_{(+,+)}$. Bob makes his measurements on the X basis and he gets the

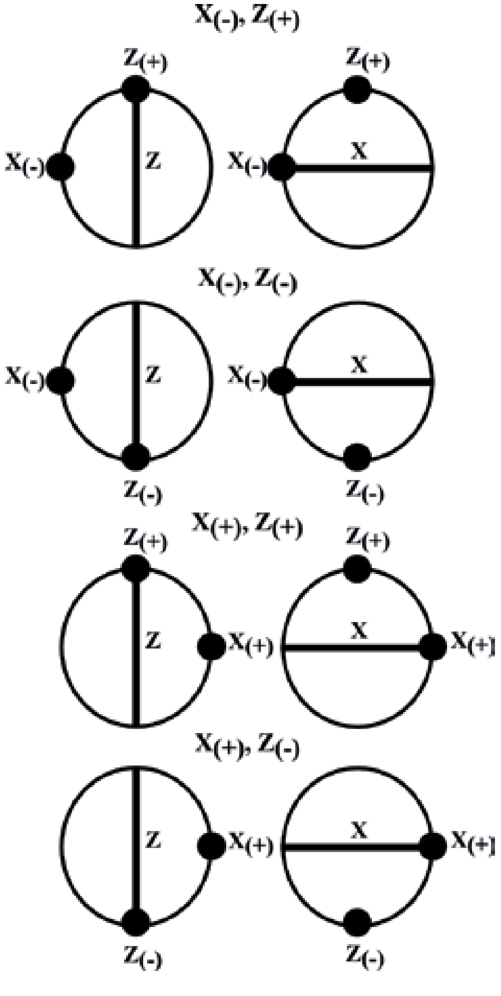


Figure 4. The *non-orthogonal* states used in the *SARG04* protocol encodes the bit 0 with the states $|+_Z\rangle$ and $|-_Z\rangle$ and the bit 1 is encoded with $|+_X\rangle$ and $|-_X\rangle$.

result $|+_X\rangle$; and as this result can be obtained for both states in the set $S_{(+,+)}$; he needs to dispose of the bit 1 from $|+_X\rangle$. In case Bob measures using the Z basis measurement and obtains $|+_Z\rangle$, once more, he is not able to distinguish the state sent by Alice. In the opposite way, if he measures in the Z basis and gets $|-_Z\rangle$, he is sure Alice sent $|+_X\rangle$ and adds a 0 to his key. On her side, Eve needs to perform a measurement using the conjugate basis X and Z to obtain the same secret bit as Bob, demanding multi-photonic pulses with at least three photons.

Similar to the *BB84*, in the *ack-state* protocol, Alice encodes a classical bit as: 0 is encoded with $|+_Z\rangle$ and $|-_X\rangle$ and 1 is encoded with $|-_Z\rangle$ and $|+_X\rangle$. And also, in the same manner as the *SARG04* protocol, the *ack-state* uses the four sets of *non-orthogonal* states $S_{(+,+)} = \{|+_X\rangle, |+_Z\rangle\}$, $S_{(+,-)} = \{|+_X\rangle, |-_Z\rangle\}$, $S_{(-,+)} = \{|-_X\rangle, |+_Z\rangle\}$, and $S_{(-,-)} = \{|-_X\rangle, |-_Z\rangle\}$. But in the *ack-state* protocol the set Alice used, $S_{(+,+)}, S_{(+,-)}, S_{(-,+)}$ or $S_{(-,-)}$, is never revealed. As an illustration, suppose Alice chooses the set $S_{(+,+)} = \{|+_X\rangle, |+_Z\rangle\}$ rather than transmitting one of the two states, say $|+_X\rangle$, and publishing the sifting instance, $S_{(+,+)}$, she transmits the two states $|+_X\rangle$ and $|+_Z\rangle$. At that point, Bob measures the states using the same basis, X or Z, one by one, as the two states reach successively. If Bob measures with the X basis, he surely will obtain $|+_X\rangle$ (after he measures the first state) but he can obtain $|+_X\rangle$ or $|-_X\rangle$ on the second measurement, with a probability of 0.5 for each event. If Bob obtains $\{|+_X\rangle, |-_X\rangle\}$ after the second measurement, the result is unclear to him and he has to discard it. On the other hand, if he gets $\{|+_X\rangle, |+_X\rangle\}$ the result is unambiguous and he should add a bit 1 to his key. With the purpose of allowing Alice to recover the same bit, Bob makes the announcement of the basis measurement X and the matching condition in accordance with the following criterion: $(2M)$ if the two detection events make clicks on the same detector; it includes the cases $\{|+_X\rangle, |+_X\rangle\}, \{|-_X\rangle, |-_X\rangle\}, \{|+_Z\rangle, |+_Z\rangle\}, \{|-_Z\rangle, |-_Z\rangle\}$ and $(2nM)$ if the detection event makes clicks on the opposite detectors, for example, $\{|+_X\rangle, |-_X\rangle\}, \{|-_X\rangle, |+_X\rangle\}, \{|+_Z\rangle, |-_Z\rangle\}, \{|-_Z\rangle, |+_Z\rangle\}$. Alice obtains the secret bit given that the $\{|+_X\rangle, |+_Z\rangle\}$ states she sent, the X basis, and the $(2M)$ measurement result permit her to conclude that Bob definitely got $\{+_X, +_X\}$ (consider the cases depicted in **Table 1**).

Contrarily, in the case Bob measured the two states $|+_X\rangle$ and $|+_Z\rangle$ with the Z basis, he would acquire one of the two possible results: $(2M) = \{|+_Z\rangle, |+_Z\rangle\}$ or $(2nM) = \{|-_Z\rangle, |+_Z\rangle\}$. In the first case, he publishes the Z basis and the $(2M)$ result; then Alice and Bob add a 0 to the key. In the second case, Bob makes the announcement of the Z basis and the $(2nM)$ result but in this case, they discard the result. When using the *ack-state* protocol the $(2M)$ results can be used to

Alice sends	**Bob obtains a $(2M)$**	**Secret bit**
$\{|+_X\rangle, |+_Z\rangle\}$	$\{|+_X\rangle, |+_X\rangle\}$	1
$\{|+_X\rangle, |-_Z\rangle\}$	$\{|+_X\rangle, |+_X\rangle\}$	1
$\{|-_X\rangle, |+_Z\rangle\}$	$\{|-_X\rangle, |-_X\rangle\}$	0
$\{|-_X\rangle, |-_Z\rangle\}$	$\{|-_X\rangle, |-_X\rangle\}$	0

Table 1. Using the X basis, Bob measures the two states sent by Alice and he obtains a $(2M)$ result.

distill secret bits but $(2nM)$ is unclear causing those measurement outcomes to be useless and so they have to be discarded.

The *ack-state* protocol was introduced in [4]. In such a reference, the *non-orthogonal* states are called *protocol* states while *parallel* states are named *decoy* states. The *ack-state* protocol encodes one classical bit using two quantum states. Such encoding is done by means of *non-orthogonal* or *parallel* states. In quantum physics, if $X = \{|0_X\rangle, |1_X\rangle\}$ and $Z = \{|0_Z\rangle, |1_Z\rangle\}$ are orthonormal bases, then the magnitude of each basis vector is the unity and any vector in such a space can be written as a linear combination of such basis. For instance, $|0_X\rangle$ can be rewritten as $\frac{1}{\sqrt{2}}|0_Z\rangle + \frac{1}{\sqrt{2}}|1_Z\rangle$. Two qubits $|0_X\rangle$ and $|0_Z\rangle$ are *non-orthogonal* if the inner product between them is different from zero, symbolically $0_X|0_Z \neq 0$. In consequence, $0_X|0_Z = \frac{1}{\sqrt{2}}(1) + \frac{1}{\sqrt{2}}(0)$ and $0_X|0_Z = \frac{1}{\sqrt{2}}$. The inner product of *orthogonal* qubits is zero, for example, $0_X|1_X = 0$ and identical (or *parallel*) qubits produce the unity under the inner product; thus, $0_X|0_X = 1$.

Using this protocol, Alice chooses at random between sending a pair of *parallel* or *non-orthogonal* states. At the opposite side, Bob makes the measurement of the two successive pulses he receives with the same basis measurement, X or Z (see **Figure 5**). In this context, the pair of quantum states sent by Alice is called biqubit. *Parallel* biqubits define the *parallel* quantum flow and *non-orthogonal* biqubits define the *non-orthogonal* quantum flow. Summarizing the *ack-state* protocol with *non-orthogonal* and *parallel* states, we have the following:

1. Alice randomly selects between a *non-orthogonal* biqubit and a *parallel* bi-qubit. In case she selects a *non-orthogonal* biqubit, she has to select at random one of the following states: $\{(|0_X\rangle, |0_Z\rangle), (|0_X\rangle, |1_Z\rangle), (|1_X\rangle, |0_Z\rangle), (|1_X\rangle, |1_Z\rangle)\}$, where the order between states X or Z is as well picked at random. In case she selects a *parallel* biqubit, she should randomly choose a biqubit from the set: $\{(|0_X\rangle, |0_X\rangle), (|1_X\rangle, |1_X\rangle), (|0_Z\rangle, |0_Z\rangle), (|1_Z\rangle, |1_Z\rangle)\}$. and then she gets it ready and transmits it to Bob.

2. At random, Bob chooses the basis X or Z to measure the received biqubit.

3. Bob's basis of measurement is announced by him over the public channel and he also declares if the result obtained is either a double-detected event ($2M$ or $2nM$), a single-detected event (S-1 or S-2), or a lost biqubit $(2L)$ (see the discussion below).

4. After analyzing those results, Alice tells Bob which cases to discard.

Table 2 shows the results after Bob measures two consecutive states. Thus, one of the following detection events can be obtained:

i. *The states generate a double-detection event:* The symbol $(+, +)$ is used to designate the photonic gain in a double-detection event. When both events are registered in a same detector, we call it a double-matching $(2M)$ detection event. If the results of the measurements of the states are opposite, then we face a double non-matching $(2M)$ detection event. Whereas $(2M)$ *non-orthogonal* outcomes are useful to distill secret bits, the $(2M)$ results cannot be used and are disposed. When we have a $(2M)$ detection event, we may say that the second measurement is the acknowledgment (the *ack*) of the first measurement. In **Figure 5** (top-right) the qubit $|0_X\rangle$ is the first one sent by Alice and then she sends

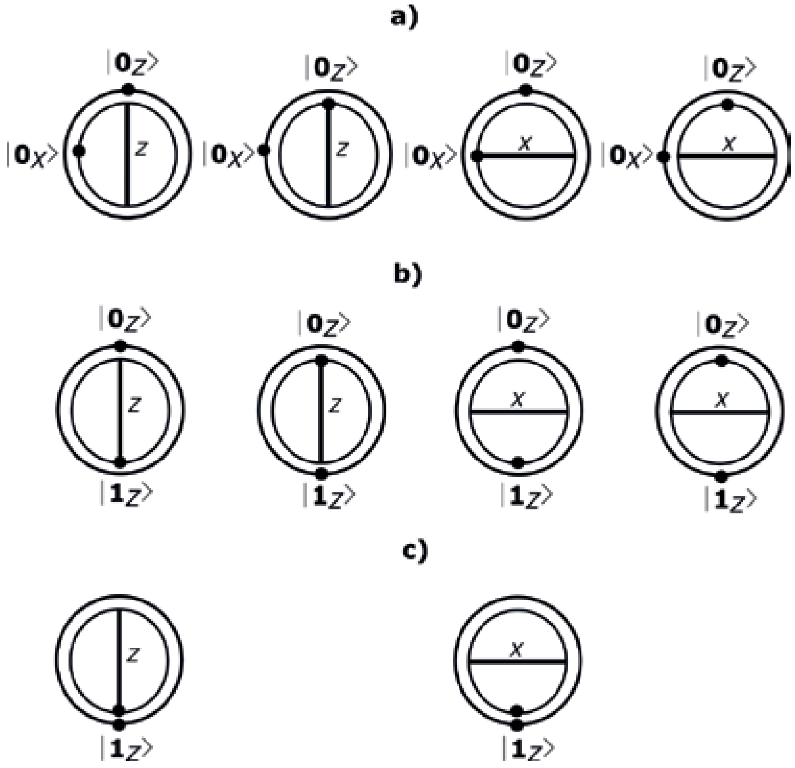


Figure 5. In this representation, two concentric circles define the order in which the states are prepared and sent. Therefore, the state that is first sent is contained in the inner circle state, and the outer circle state is prepared and transmitted. Alice at random interleaves *orthogonal* (*non-orthogonal*) and *parallel* states, given that she can verify the matching cases after Bob measurements. In the *ack-state* protocol, Bob uses the basis $X(Z)$ to measure the two Alice's *non-orthogonal* states $\{|i_X\rangle, |j_Z\rangle\}$. He effectively gets the bit $i(j)$ provided he measures $\{|i_X\rangle, |i_X\rangle\}$ or $\{|j_Z\rangle, |j_Z\rangle\}$ which occurs with $\frac{1}{2}$ probability. For instance, if Bob uses the Z basis to measure the incoming states $\{|0_X\rangle, |1_Z\rangle\}$ he can obtain $\{|0_Z\rangle, |1_Z\rangle\}$ or $\{|1_Z\rangle, |1_Z\rangle\}$ with the same probability. Alice decides to send at random two consecutive *non-orthogonal* states from the set: $\{(|0_X\rangle, |0_Z\rangle), (|0_X\rangle, |1_Z\rangle), (|0_Z\rangle, |1_X\rangle), (|1_Z\rangle, |1_X\rangle)\}$. Bob will measure those states using the same measurement basis (X or Z). The *parallel* biqubits involve the following states: $\{(|0_X\rangle, |0_X\rangle), (|1_X\rangle, |1_X\rangle), (|0_Z\rangle, |0_Z\rangle), (|1_Z\rangle, |1_Z\rangle)\}$. In the *nack-state* protocol Alice chooses randomly two consecutive *parallel* states as the case depicted in (c) $(|1_Z\rangle, |1_Z\rangle)$. They produce a compatible measurement if Bob chooses, X for $|i_X\rangle$ or Z for $|i_Z\rangle$ where $i = 0, 1$. We represent in (b) the case of quantum *orthogonal* states. Two cases are possible here: $\{(|0_X\rangle, |1_X\rangle), (|0_Z\rangle, |1_Z\rangle)\}$.

the qubit $|0_Z\rangle$. As the X basis is used by Bob to measure both qubits, the qubit $|0_X\rangle$ is measured as $|0_X\rangle$ but the qubit $|0_Z\rangle$ is measured as $|0_X\rangle$ or $|1_X\rangle$ with an equal probability of 50%. When Bob's measurement generates $|0_X\rangle$, we say that this measurement is the *ack* of the first $|0_X\rangle$ state. Vice versa, if Bob gets $|1_X\rangle$, we say that $|1_X\rangle$ is the negative acknowledgment (the *nack*) of $|0_X\rangle$.

In a *channel* with losses, we have two more possible results.

ii. *The single-detection event* occurs when one state is lost and Bob obtains only one detection event. The symbol ($\pm$, $\mp$) is used to designate the single-detection event. More specifically, Bob uses the symbol (S-i) to represent the single-detection event, where i can be 1 or

Alice's bi-qubit	Bob's side			
	basis used	Detection event	Public disclosure	Result
$\|0_X\rangle, \|0_Z\rangle$	X	$\|0_X\rangle, \|0_X\rangle$	X, $(2M)$	Useful
	X	$\|0_X\rangle, \|1_X\rangle$	X, $(2nM)$	Discard
	X	$\|0_X\rangle, -$	X, $(S\text{-}1)$	Useful
	X	$-, \|0_X\rangle$	X, $(S\text{-}2)$	Discard
	X	$-, \|1_X\rangle$	X, $(S\text{-}2)$	Discard
	X	$-, -$	X, $(2L)$	Discard
	Z	$\|0_Z\rangle, \|0_Z\rangle$	X, $(2M)$	Useful
	Z	$\|1_Z\rangle, \|0_Z\rangle$	X, $(2nM)$	Discard
	Z	$-, \|0_Z\rangle$	Z, $(S\text{-}2)$	Useful
	Z	$\|0_Z\rangle, -$	Z, $(S\text{-}1)$	Discard
	Z	$\|1_Z\rangle, -$	Z, $(S\text{-}1)$	Discard
	Z	$-, -$	Z, $(2L)$	Discard

Table 2. Alice sends to Bob the *non-orthogonal* states $(|0_X\rangle, |0_Z\rangle)$ and it shows all the possible measurement results at Bob's side.

2, depending on the state number that makes clicks after the basis measurement X or Z is applied to the two consecutive incoming states. This way, the number i will be published by Bob.

iii. *The two pulses are lost.* This case is denoted as $(-,-)$ or alternatively as $2L$.

When applying the *ack-state* protocol, two consecutive *non-orthogonal* states are used by Alice and Bob to distill one secret bit. The basis measurement X or Z is declared publicly by Bob along with the sifting instances; he obtained $(2M)$, $(2M)$, $(S\text{-}1)$, $(S\text{-}2)$, and $(2L)$. Furthermore, the bits acquired from the single-detection events $(S\text{-}1)$ and $(S\text{-}2)$ are used by Alice to confirm the single photonic gain of the quantum channel.

4. The *nack-state* protocol

The *nack-state* protocol is the dual version of the *ack state* protocol discussed in [5]. Both protocols constitute a generalization of the well-known *BB84*. The *nack state* protocol uses couples of *parallel* and *orthogonal* states rather than just single *non-orthogonal* states utilized as a part of *BB84*. This straightforward distinction makes the *nack state* strong when facing the *IRFS* attack, as we will demonstrate later on. We selected the *nack* prefix to indicate that, provided Alice transmits two quantum states to Bob, the second measurement behaves as the negative acknowledgment (*nack*) of the one before, since it yields the opposite bit result.

The pair of quantum states is denoted as a biqubit. More specifically, the following biqubits are defined in the *nack state* protocol: four *parallel* biqubits $(|0_X\rangle, |0_X\rangle)$, $(|0_Z\rangle, |0_Z\rangle)$, $(|1_X\rangle, |1_X\rangle)$,

$(|1_Z\rangle, |1_Z\rangle)$ and two *orthogonal* biqubits $(|0_X\rangle, |1_X\rangle), (|0_Z\rangle, |1_Z\rangle)$. The *parallel* and *orthogonal* biqubits are interleaved at random by Alice. The performance of the protocol is not altered by order of the quantum states within the biqubit (see **Figure 5**). On the opposite side of the

Alice's	**Bob's**	**Detection**	**Public**	**Description**
Biqubit	Basis	Event	Disclosure	
$\|0_X\rangle, \|1_X\rangle$	X	$\|0_X\rangle, \|1_X\rangle$	$X, 2nM$	Compatible double non-matching, useful
				As two compatible single-detection events
	X	$\|0_X\rangle, -$	X, S_1	Compatible single matching, useful
	X	$-, \|1_X\rangle$	X, S_2	Compatible single matching, useful
	X	$-, -$	X, Lost	Biqubit lost
	Z	$\|0_Z\rangle, \|0_Z\rangle$	$Z, 2M$	Non-compatible double matching, useless
	Z	$\|1_Z\rangle, \|1_Z\rangle$	$Z, 2M$	Non-compatible double matching, useless
	Z	$\|0_Z\rangle, \|1_Z\rangle$	$Z, 2M$	Non-compatible double non-matching, useless
	Z	$\|1_Z\rangle, \|0_Z\rangle$	$Z, 2M$	Non-compatible double non-matching, useless
	Z	$\|0_Z\rangle, -$	Z, S_1	Non-compatible single matching, useless
	Z	$\|1_Z\rangle, -$	Z, S_1	Non-compatible single matching, useless
	Z	$-, \|0_Z\rangle$	Z, S_2	Non-compatible single matching, useless
	Z	$-, \|1_Z\rangle$	Z, S_2	Non-compatible single matching, useless
	Z	$-, -$	Z, Lost	Biqubit lost
$\|1_Z\rangle, \|1_Z\rangle$	Z	$\|1_Z\rangle, \|1_Z\rangle$	$Z, 2M$	Compatible double matching, useful
	Z	$\|1_Z\rangle, -$	Z, S_1	Compatible single matching, useful
	Z	$-, \|1_Z\rangle$	Z, S_2	Compatible single matching, useful
	Z	$-, -$	Z, Lost	Biqubit lost
	X	$\|0_X\rangle, \|0_X\rangle$	$Z, 2M$	Non-compatible double matching, useless
	X	$\|1_X\rangle, \|1_X\rangle$	$Z, 2M$	Non-compatible double matching, useless
	X	$\|0_X\rangle, \|1_X\rangle$	$Z, 2nM$	Non-compatible double non-matching, useless
	X	$\|1_X\rangle, \|0_X\rangle$	$Z, 2nM$	Non-compatible double non-matching, useless
	X	$\|0_X\rangle, -$	X, S_1	Non-compatible single matching, useless
	X	$\|1_X\rangle, -$	X, S_1	Non-compatible single matching, useless
	X	$-, \|0_X\rangle$	X, S_2	Non-compatible single matching, useless
	X	$-, \|1_X\rangle$	X, S_2	Non-compatible single matching, useless
	X	$-, -$	X, Lost	Biqubit lost

We expect Alice to send the biqubits $|0_X\rangle, |1_X\rangle$ and $|1_Z\rangle, |1_Z\rangle$; at that point, every conceivable measurement result at Bob's detector is written. We exhibit the detection event and Bob's corresponding advertisement over the public channel according to Bob's basis selection. Notice that the number of the single detections inside the biqubit, first or second, is openly declared by Bob.

Table 3. The *nack-state* protocol running without blunders in the quantum channel is shown with each of the possible measurement results at Bob's detectors.

quantum channel, Bob measures two incoming states of a biqubit utilizing the same measurement basis (X or Z). The following steps depict the *nack state* protocol:

1. Alice is equipped with a photon source with an expected photon number μ showing Poisson distribution. A *parallel* or an *orthogonal* biqubit is selected at random by Alice, and she arranges the biqubit to be sent to Bob through the quantum channel.

2. The biqubit (two incoming pulses) is measured by Bob using the same measurement basis X (or Z) that he selects haphazardly (in a further section, we discuss the convenience of avoiding consecutiveness of states and how it can be prevented if Alice forwards a burst of the first states of each pair, followed by a burst of the second states of each pair).

3. Bob declares publicly his measurement basis decisions.

4. Alice and Bob perform sifting utilizing single compatible events and double compatible matching detection events (from *parallel* states) in order to share secret bits. Likewise, sifting is applied to the double-detection events that contain a single compatible detection event. With this aim, Bob indicates if the single detection is the first or the second inside the biqubit.

Table 3 exhibits a case of the *nack state* protocol. Here, two biqubits are transmitted to Bob from Alice. The first biqubit is the *orthogonal* pair $(|0_X\rangle, |1_X\rangle)$, and the second biqubit is the *parallel* pair $(|1_Z\rangle, |1_Z\rangle)$. In case the two states sent by Alice reach Bob's detection system with no failure, a double-detection event is generated. In the situation that just one of the two states of the biqubit reaches Bob's station, he gets a single-detection event.

The *nack-state* protocol has been conceived of to use the same optical hardware of the *BB84* protocol; thus, it can be configured in most *QKD* systems as a software module application. However, two additional tasks must be implemented: the random computation of biqubits before preparing and sending the quantum states and the sifting stage of the protocol, which must include (1) sifting of single matching (compatible or non-compatible), where Bob announces the number of the single-detections inside the biqubit and (2) sifting of double detection, matching or non-matching, from *parallel* or *orthogonal* states. The error correction and privacy amplification stages of the *QKD* protocol do not require changes.

5. The photon number splitting attack

In the *PNS* attack, the eavesdropper captures no less than one photon from each of the multi-photon states with the purpose of storing them in quantum memory, at the same time that she hinders the single photon states in the quantum channel. When Bob has uncovered over public channels the measurement basis he has used, the eavesdropper executes the same measurements on the quantum states she has stored [25].

When the *PNS* attack is applied to the *ack-state* protocol, the eavesdropper captures no less than one photon of the multi-photon states (*parallel* and *non-orthogonal*), and she stands by Bob's declarations about the measurement bases he has utilized with the aim of applying the same measurements on her stored states. In Bob's side, a distribution over the following sifting events is achieved $(2M)$, $(2nM)$, $(S\text{-}1)$, $(S\text{-}2)$ and $(2L)$, where every one may originate in *parallel* or *non-orthogonal* states; however, just Alice knows those outcomes.

After Bob declares both the measurement bases (X or Z) and the sifting occurrences, Eve executes the measurements utilizing the same measurement bases and she gets the same bits from the multi-photonic single sifting instances: $(S\text{-}1)$ and $(S\text{-}2)$, *parallel* and *non-orthogonal*. Moreover, the same outcomes from the $(2M)$ measurements of the *parallel* and (a half of the) *non-orthogonal* multi-photonic states are acquired by the eavesdropper. However, she cannot acquire the secret bits from the 1-state $(S\text{-}i)$ and $(2M)$ sifting occurrences, given that the eavesdropped cannot discriminate *parallel* and *non-orthogonal* states.

In order to get the secret bits, Eve obstructs the 1-photon states which incorporate single and double-detection events from *parallel* and *non-orthogonal* states. In doing that, an error gain in the photonic gain of the single and double-detection events is introduced by Eve. At that point, Eve executes a channel substitution expanding the transmittance of the channel. The fiber channel transmittance among Alice and Bob is written as $T_{AB} = 10^{-\frac{\alpha l}{10}}$ where α is the loss coefficient measured in dB/km and the length l is measured in km. Moreover, the local transmittance at Bob's side, η_B, is defined as $t_B\eta_D$ where t_B is the internal transmittance of optical components and η_D is the quantum efficiency of Bob's detectors. Then, the general transmission and detection efficiency at Bob's side η_{BT} is computed as $\eta_{BT} = t_B\eta_D T_{AB}$ [18]. A mathematical description of the gain of detection events will be presented in the following section.

5.1. The gain of detection events

In **Table 4** (upper part), the gain of the single-detection events is depicted with the $Q_{(+)}$ symbol. According to Ma et al. [18], the gain of detection events is acquired from two origins: the photon source and the quantum channel. The photon source presents an expected photon number μ, and it adopts Poisson distribution. Contrastively, the quantum channel exhibits a distribution that is computed for every i photons' state (where i is the quantity of photons in each pulse) that is named yield. The gain Q_i of i photons' state is the product of the probability of Alice sending an i photons' state (that adopts Poisson distribution) and the yield of i photons' state (and background states). It will generate a gain at Bob's side provoked by the detection of events corresponding to the relation $Q_i = Y_i \frac{\mu^i}{i!} e^{-\mu}$ where Y_i is the yield of i photons' state.

The yield Y_i is computed across the following steps:

1. The fiber channel transmittance among Alice and Bob is denoted as $T_{AB} = 10^{-\frac{\alpha l}{10}}$ where α is the loss coefficient measured in dB/km, and the length l is measured in km. Moreover, the local transmittance at Bob's side, η_B, is written as $t_B \cdot \eta_D$ where t_B is the internal transmittance of optical components and η_D is the quantum efficiency of Bob's detectors. Then, the overall transmission and detection efficiency at Bob's side, η_{BT}, is computed as $\eta_{BT} = t_B \cdot \eta_D \cdot T_{AB}$ and typically η_{BT} ranges to 10^{-3} [18];

Photonic-Gain	**Alice**	**Alice − Bob**	**Eve − Bob**
$Q_{(-)}$	$e^{-\mu}$	$e^{-\mu\eta_{BT}} - Y_0$	—
$Q_{(+)}$	$1 - e^{-\mu}$	$Y_0 + 1 - e^{-\mu\eta_{BT}}$	$\frac{1}{2}(Y_0 + 1 - e^{-\mu\eta_{ET}})$
$Q_{(-,-)}$	$e^{-2\mu}$	$(e^{-\mu\eta_{BT}} - Y_0)^2$	—
$Q_{(\pm,\mp)}$	$2e^{-\mu}\cdot$	$2(e^{-\mu\eta_{BT}} - Y_0)\cdot$	$(e^{-\mu\eta_{ET}} - Y_0)\cdot$
	$(1 - e^{-\mu})$	$(Y_0 + 1 - e^{-\mu\eta_{BT}})$	$(Y_0 + 1 - e^{-\mu\eta_{ET}})$
$Q_{(+,+)}$	$(1 - e^{-\mu})^2$	$(Y_0 + 1 - e^{-\mu\eta_{BT}})^2$	$\frac{1}{2}(Y_0 + 1 - e^{-\mu\eta_{ET}})^2$

Here, η_{BT} and η_{ET} are the overall efficiency of Bob and Eve, respectively. In the *IRFS* attack, Eve remains undetected given that she meets the condition $\eta_{ET} \geq \frac{\ln(2e^{-\mu\eta_{BT}} - Y_0 - 1)}{-\mu}$. At the lower part of the table, the gain of the double $(+,+)$-detection events is shown, which is denoted as $Q_{(+,+)}$, and the gain of single $(\pm, \mp)$ detection events is represented as $Q_{(\pm,\mp)}$. In the *IRFS* attack, Eve can effectively forward half of her biqubits to Bob's detectors. The "·" symbol denotes multiplication inside the $Q_{(\pm,\mp)}$ relation. The factor of 1/2 is a result of Bob using an active basis choice, compelling Eve to blind his detector when his basis differs from her own (half the time), and considering that each pair of pulses is detected in the same basis, Bob will always be blinded by Eve for both pulses or neither pulses, resulting in the same factor 1/2 for both single and double-detection events

Table 4. The background noise is defined as the gain of the single (non-empty) and empty pulses, $Q_{(+)}$ and $Q_{(-)}$, respectively, where μ is the expected photon number of the source and Y_0.

2. The transmittance η_i of i photons' state at Bob's, that is, $\eta_{BTi} = 1 - (1 - \eta_{BT})^i$ for $i = 0, 1, \ldots$, assuming independence among the i photons of the i photons' state;
3. The yield Y_i of the i photons' state is acquired from two sources, the background noise (Y_0) and the true signal. Presuming that the background counts are independent from the signal photon detection, Y_i is given by $Y_i = Y_0 + \eta_{BTi} - Y_0\eta_{BTi}$. However, assuming Y_0 is small (around 10^{-5}) and $\eta_{BT} \sim 10^{-3}$, the above equation can be reduced to $Y_i \sim Y_0 + \eta_{BTi}$.

The overall gain $Q_{(+)}$ is the summation of each Q_i contribution, thus: $Q_{(+)} = \sum_{i=1}^{\infty} Q_i = \sum_{i=1}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu}$, which leads to the relation $Y_0 + 1 - e^{-\mu\eta_{BT}}$. Finally, the quantum bit error rate (*QBER*) between Alice and Bob has been derived by Ma et al. [18] through the relation $QBER_{AB} = \frac{0.5Y_0 + e_d(1 - e^{-\mu\eta_{BT}})}{Y_0 + 1 - e^{-\mu\eta_{BT}}}$, where e_d is the error probability of the detector $(e_d \sim 10^{-2})$.

With the aim to obtain the gain of double-detection events $Q_{(-,-)}$, $Q_{(\pm,\mp)}$, and $Q_{(+,+)}$, we consider that each gain has independence of any other, that is, $Q_{(-,-)} = Q_{(-)} \times Q_{(-)}$, $Q_{(+,-)} = Q_{(+)} \times Q_{(-)}$, $Q_{(+,-)} \sim Q_{(-,+)}$, and $Q_{(+,+)} = Q_{(+)} \times Q_{(+)}$. From the previous discussion, we know that the gain of the double-detection events decreases quadratically: $Q_{(+,+)} \sim Q_{(+)}^2$. In practical implementations of *QKD*, the single-matching events have the order of 10^{-5}, while the double-matching events reach the order of 10^{-10}.

5.2. Detecting the photon number splitting attack

In replacing T_{AB}, the photonic gain of the single-detection events or the double-detection events can be adjusted by Eve but not both at the same time. In contrast, Alice utilizes the double-matching detection events ($2M$) and the (S-i) sifting instances which are consistent with the states she fixed, to verify corresponding photonic gains, *parallel* and *non-orthogonal*.

As mentioned before, the one-photon states are blocked by eavesdropper and she performs a channel substitution to adjust the transmittance of the channel, T_{AB}. Nevertheless, this activity produces error gains in the single- and double-detection events that Alice can verify.

The *QPEG* after Eve blocks the one-photon states and can be written as $\Delta Q = Q_1$ where Q_1 is the gain of the one-photon states and it must be computed for the single- and the double-detection events. The error gain is $\Delta Q_{(+,+)} = Q^2_{1_{(+)}} = Q_1^2$ and $\Delta Q_{(\pm,\mp)} = Q_1 \cdot Q_{(-)}$ for double-detection events and single-detection events, respectively, where $Q_{1_{(+)}} = (Y_0 + \eta - Y_0\eta)\mu e^{-\mu}$, $Q_{(-)} = e^{-\mu\eta} - Y_0$, η is the transmittance of the channel, and the detectors at Bob's side of the one-photon states and Y_0 is the background noise according to Ma et al. [18].

The eavesdropper must adjust the transmittance, T_{AB}, in order to remain hidden in the channel to achieve the two reference photonic gains, $Q_{(+,+)}$ and $Q_{(\pm,\mp)}$, for the double-detection events and single-detection events, respectively. Given $Q_{(+,+)} \neq Q_{(\pm,\mp)}$ Eve can adjust T_{AB} to Q_1^2 or $Q_1 \cdot Q_{(-)}$ but not both simultaneously. In other words, she is not able to fulfill the conditions $\Delta Q_{(+,+)} = 0$ and $\Delta Q_{(\pm,\mp)} = 0$; in this manner, the attack becomes detectable. If the eavesdropper adjusts T_{AB} to make it produce a photonic deviation in one or in both gains, she will introduce a detectable *QBER* to the system.

Consequently, Eve knows that she must be careful and makes no changes in T_{AB}; otherwise, she will be detected. Now, the *QBER* that Eve produces is $\frac{0.5Q_0+0.5^2Q_1+0.5^3Q_2+\dots}{Q_0+Q_1+Q_2+\dots}$ because the *QBER* of single-detection events is 0.5^2 as in *BB84*. In contrast, when no attack is produced the *QBER* of the system is given by $\frac{0.5Q_0+e_d(Q_1+Q_2+Q_3+\dots)}{Q_0+Q_1+Q_2+\dots}$ where e_d is the detection error according to Ma et al. [18].

Given that the probability of obtaining a (compatible) matching measurement from the *non-orthogonal* double-detection events is 0.5^2, we derived the error rate of the *non-orthogonal* double-detection events as $\frac{0.5(Q_0+Q_1)+0.5^2Q_2+0.5^3Q_3+\dots}{Q_0+Q_1+Q_2+\dots}$. The *QBER* from the multi-photonic *non-orthogonal* states decreases one-half for each copy of quantum states in Eve's memory. In contrast, no contribution is made by the multi-photonic *parallel* states to increase the *QBER* because Bob makes public the basis measurements used by him.

6. The *IRFS* attack

What should Alice and Bob expect from the nonappearance of the *IRFS* attack? For illustrative purposes, consider the situation where $\mu = 0.2$, $\eta_{BT} = 0.8$, which is the general efficiency among Alice and Bob and zero dark counts ($Y_0 = 0$). In such a case, the great majority of the total biqubits sent by Alice to Bob ends up in Bob's station as lost biqubits ($\sim 72.61\%$); single-detection events are $\sim 25.2\%$, and just $\sim 0.0219\%$ of the measurement cases are double-detection events. Despite the double-detection gain being very low, it ought not be viewed as insignificant given that the amount of pulses sent by Alice is high ($10^{11} - 10^{13}$ [29]), and the transmission interim can be legitimately upgraded. However, for practical purposes, we will presume that the secret bits in the *nack state* protocol are delivered by single-detection events, and the key rate is at most the *BB84* key rate. Nevertheless, we assert that double-detection events can be utilized to identify the *IRFS* attack, so in this section, we defend the security of the protocol, in spite of Eve's endeavors to enhance her attack.

6.1. Detecting the *IRFS* attack with blinding pulses and quantum channel substitution

Within the sight of the *IRFS* attack with blinding pulses, Eve is amid the quantum channel utilizing an optical detection system comparable to Bob's station. Eve is challenged to reproduce gains of single- and double-detection events at Bob's side to pass unnoticed in the quantum channel. However, the gain of the single-detection events decreases directly with the channel efficiency, but the double-detection gain drops quadratically. In the next section we demonstrate that, for practical parameters of the quantum channel, the two gains cannot be adjusted by the eavesdropper at the same time. Eve cannot control the two gains because of the fact that:

1. the transmittance of the channel can be adjusted to a unique value by the eavesdropper either to adjust the single or the double-detection gain and

2. Eve's station receives Alice's optical pulses sequentially. In this manner, once a pulse is detected in the eavesdropper station, she is not able to know whether the next pulse will be likewise detected or lost. That is, Eve has no form to know when a single or a double-detection event will occur.

Eve still has the possibility to adjust the efficiency of the quantum channel to the gain of the double-detection events. Therefore, with the purpose of removing the excess of the single-detection gain, Eve could eliminate pulses in proportion to some probability (e.g., 0.5). However, in accordance with the second statement given previously in this section, the eavesdropper would lose double-detection pulses (a quarter in this example). Eve could be more selective discarding only single-detection events on which the detection occurred in the second pulse. By using this scheme, the double-detection gain is unaltered for Eve. However, given that the number of single detections inside the biqubit, first or second (see **Table 3**), is announced by Bob publicly, the presence of Eve becomes evident.

Both strategies could be combined by Eve to increase the efficiency of the channel to produce an overabundance of the double-detection gain, but it would also increase the single-detection gain. The issue for Eve is that once a strategy to remove pulses is chosen, it affects equally the single- and the double-detection gains. Such gains obey diverse rates: while the first decreases linearly, the second fluctuates quadratically with the transmittance of the channel. Moreover, at the receiver station, the single- and double-detection events are registered as haphazard interleaved events.

In the following sections, a convenient method to compute the photon gain deviation caused by the *IRFS* attack at a practical level is discussed.

6.2. Detecting the *IRFS* attack with quantum channel substitution

It is expected that the eavesdropper would endeavor to adjust both gains, from single- and double-detection events, applying a quantum channel substitution and tuning it to a specific transmittance. We define the quantum photon error gain (*QPEG* or simply ΔQ) as the deviation from the reference gain that is caused by Eve's apparatus at Bob's receiver station when she performs the *IRFS* attack. In ordinary conditions, it is ideally expected that $\Delta Q \sim 0$, for the single- and the double-detection events.

QPEG of double $(+,+)$-detection events is written as $\Delta Q_{(+,+)}$, while we denote the *QPEG* of single $(\pm,\mp)$-detection events as $\Delta Q_{(\pm,\mp)}$. $\Delta Q_{(+,+)}$ is computed as the difference $Q_{(+,+)_{AB}} - Q_{(+,+)_{EB}}$ where the symbol $(+,+)_{AB}$ defines the reference gain of the double-detection events and $(+,+)_{EB}$ denotes the gain of the double-detection events at Bob's side but in the presence of Eve. Similarly, $\Delta Q_{(\pm,\mp)}$ is computed as $Q_{(\pm,\mp)_{AB}} - Q_{(\pm,\mp)_{EB}}$, where we apply the sub-index of $(\pm,\mp)_{AB}$ and $(\pm,\mp)_{EB}$ with the same intention.

Using the relations of **Table 4**, the possibility of the eavesdropper to fulfill simultaneously the conditions $\Delta Q_{(+,+)} = 0$ and $\Delta Q_{(\pm,\mp)} = 0$ can be established. Allow Eve to adjust freely η_{BT} and η_{ET}. Thus, the eavesdropper's goal is to make $\Delta Q_{(+,+)_{AB}} = \Delta Q_{(+,+)_{EB}}$ and $\Delta Q_{(\pm,\mp)_{AB}} = \Delta Q_{(\pm,\mp)_{EB}}$. The following equation system is obtained:

$$2(e^{-\mu\eta_{BT}} - Y_0)(Y_0 + 1 - e^{-\mu\eta_{BT}}) = (e^{-\mu\eta_{ET}} - Y_0)(Y_0 + 1 - e^{-\mu\eta_{ET}}) \tag{1}$$

$$(Y_0 + 1 - e^{-\mu\eta_{BT}})^2 = \frac{1}{2}(Y_0 + 1 - e^{-\mu\eta_{ET}})^2 \tag{2}$$

Solving the system for η_{ET}, we get $\frac{\ln Y_0}{-\mu}$ and $\frac{\ln(1+Y_0)}{-\mu}$, which, in the practice, cannot be satisfied, given that the second relation yields η_{ET} as negative and the first relation cannot be fulfilled for typical parameters, for example, $Y_0 = 10^{-5}$, $\mu = 0.1$ produces $\eta_{ET} = 1.15$. Consider also the cases depicted in **Figure 6**.

6.3. The photon and the vacuum ratios

We will introduce a convenient method to detect the presence of the eavesdropper without requiring one to compute deviations from the reference gain, that is, $\Delta Q(+,+) = 0$ or $\Delta Q(\pm,\mp) = 0$. For this purpose, let us define the photon ratio R as the relation between the gains $\frac{Q_{EB}}{Q_{AB}}$ where the subscript EB denotes the presence of the eavesdropper and AB indicates its absence. For double-detection events, we represent R as $\frac{Q(+,+)_{EB}}{Q(+,+)_{AB}}$, while $\frac{Q(\pm,\mp)_{EB}}{Q(\pm,\mp)_{AB}}$ for single-detection events. In addition, we will define the vacuum ratio r as $\frac{e^{-\mu\eta_{ET}} - Y_0}{e^{-\mu\eta_{BT}} - Y_0}$.If the eavesdropper adjusts the channel to achieve $Q(+,+)_{AB} = Q(+,+)_{EB}$, then Eq. (2) is satisfied. We get that $R_{(\pm,\mp)} = \frac{r}{\sqrt{2}}$, but $r = \frac{e^{-\mu\eta_{ET}} - Y_0}{e^{-\mu\eta_{BT}} - Y_0}$ and $\eta_{ET} \geq \eta_{BT}$; thus, $r \leq 1$ and $R_{(\pm,\mp)} \leq \frac{1}{\sqrt{2}}$. To discard Eve's presence, it is not necessary to verify that $\Delta Q(\pm,\mp) = 0$, but it must be confirmed that $R_{(\pm,\mp)} > \frac{1}{\sqrt{2}}$.

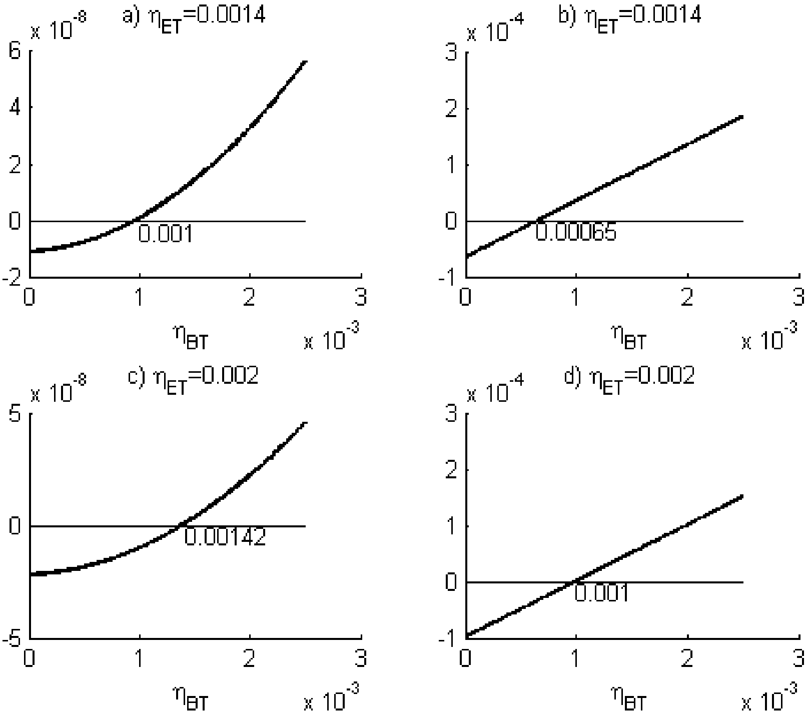


Figure 6. The deviation from the reference gain is shown on the y-axis. The upper and bottom left graphs represent double detections, while the right graphs correspond to single detections. Considering that $\eta_{BT} = 0.001$ and Eve uses $\eta_{ET} = 0.0014$, she accomplishes in (a), $\Delta Q_{(+,+)} = 0$, however, in (b), $\Delta Q_{(\pm,\mp)} \neq 0$. Conversely, if Eve adjusts $\eta_{ET} = 0.002$, she gets in (d)) $\Delta Q_{(\pm,\mp)} = 0$, but in (c), she provokes simultaneously that $\Delta Q_{(+,+)} \neq 0$.

Contrarily, if Eve modifies the channel to achieve $Q(\pm, \mp)_{AB} = Q(\pm, \mp)_{EB}$, we get that $R_{(+,+)} = \frac{2}{r^2}$. Since $r \leq 1$, we obtain that the *IRFS* attack causes $R_{(+,+)} \geq 2$. To make sure that the system is protected against the *IRFS* attack, it is not necessary to check $\Delta Q(+,+) = 0$ but it is enough verifying its equivalent $R_{(+,+)} < 2$.

6.4. The *QBER* of one-photon states

As quoted previously, in the *nack state* protocol, the great majority of the pulses sent by Alice to Bob behave as *BB84* signal pulses. Each time a compatible basis measurement is applied by Bob, the result, either from single detection or double detection, is useful as in *BB84*. Thus, for practical purposes, the *nack state* protocol has an efficiency comparable to the *BB84*. However, a partial reduction of the bit rate can be expected, as Alice reduces the optical pulse rate to avoid the eavesdropper to record double-detection events. In this way, Eve is detected if she stays waiting for double-detection events before she can forward them.

Given that it decreases quadratically, the rate of the double-detection event is small. Nevertheless, at the same time, it is extraordinary that the *QBER* of the double-matching detection events from *parallel* and *orthogonal* states also decreases quadratically. To see this, let us recall that in the *BB84* protocol, the probability to get the correct bit is $pc = (1 + V)/2$, and the probability to obtain an erroneous bit is $pe = (1 - V)/2$, where V is the visibility of the optical system. To calculate the *QBER* of the one-photon states, the relation $QBER = pe/(pe + pc)$ is applied [31].

Now, suppose that the two *parallel* states are sent by Alice $(|1_Z\rangle, |1_Z\rangle)$ to Bob who measures them using the Z basis. Those states are depicted in **Figure 7a**. The probability to get the two states $(|1_Z\rangle, |1_Z\rangle)$ is p_c^2, and the probability to get the opposite values $(|0_Z\rangle, |0_Z\rangle)$ is p_e^2, case II of **Figure 7a**. Since the measurement cases $(|0_Z\rangle, |1_Z\rangle)$ and $(|1_Z\rangle, |0_Z\rangle)$, Cases III and IV of **Figure 7a**, are always disposed because they are non-matching cases, the final probabilities are $pc_{parallel} = \frac{p_c^2}{p_c^2+p_e^2}$ and $pe_{parallel} = \frac{p_e^2}{p_c^2+p_e^2}$. The same reasoning can be applied to the *orthogonal* biqubits case as depicted in **Figure 7b**.

Those relations forward us to the *QBER* of the *parallel* and *orthogonal* states $QBER = \frac{(1-V)^2}{(1-V)^2+(1+V)^2}$. **Figure 8** gives an illustration of the *QBER* of one-photon states of such protocols. Considering the *QBER* of the *nack state* is lower than *BB84*, it is interesting to acknowledge that the double-

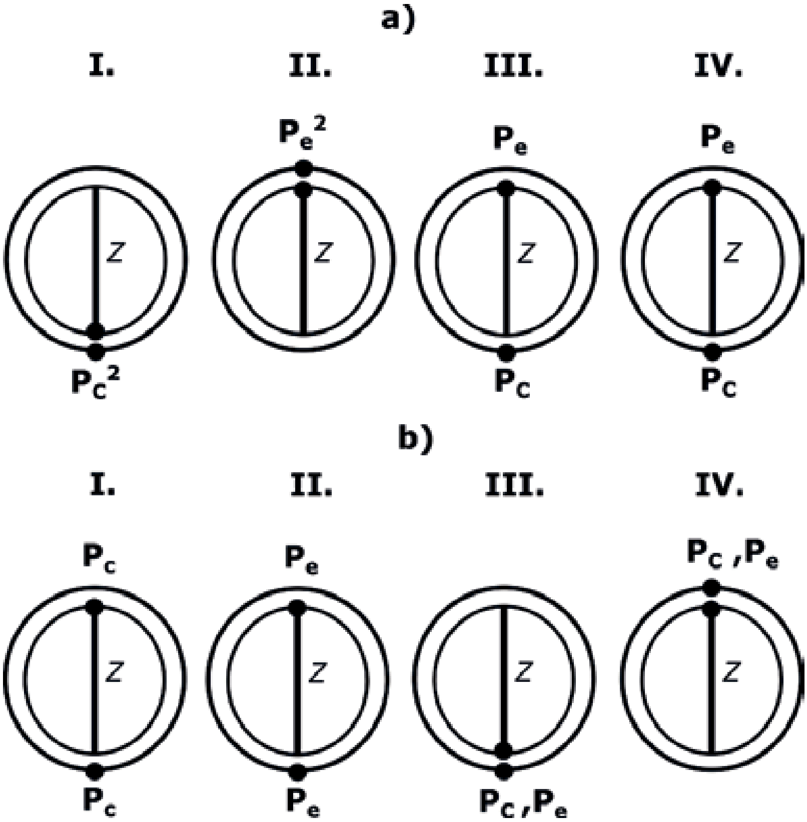


Figure 7. The *QBER* of *parallel* and *orthogonal* states: Cases III and IV of (a) and (b) can be discarded by Alice, so they do not produce errors.

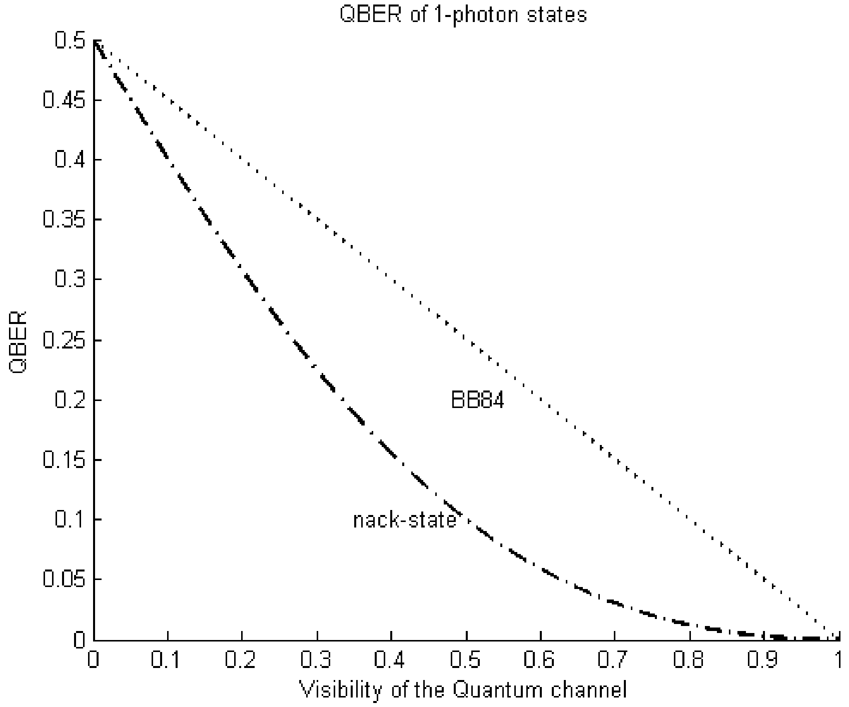


Figure 8. The *nack state* protocol uses pairs of *parallel* and *orthogonal* states. The *QBER* of *parallel* and *orthogonal* states is derived using the probabilities of two consecutive *BB84* measurements.

detection gain could be increased by future technologies. Even though there is not yet a formal derivation of the secret key rate for double-detection events, we can expect that the small *QBER* would lead to reaching longer *QKD* distances.

6.5. The non-structured *nack-state* protocol

In the argument of Point 2 of Section 6.1, it is implicit that Eve uses only a single station, but this is not a practical restriction. Eve could use two stations, one near to Alice to detect and one near to Bob to generate fake pulses. In the event that quantum channel utilizes optical fibers (the most widely recognized useful channel for ground-based *QKD*), everything required by Eve is a radio connection between her two stations to "catch up" with the quantum link. Even assuming a low source rate of 1 MHz, the time delay between pulses is only 1 microsecond, which can be easily compensated using a 600 m link (traveling in free space takes 2 microseconds; traveling in fiber takes 3 microseconds). Any practical *QKD* system will operate over distances greater than 600 m, making it entirely achievable for Eve to detect both pulses of a pair before transmitting her fake state to Bob using a second station.

A 100 km link in optical fiber would limit the source rate to 6 kHz, and much less if the fiber is not straight, which is almost always the case. To truly be secure the period between two pulses would have to be the full travel time of the pulse over the quantum channel. For 100 km, it would be 500 microseconds, forcing a source rate of 2 kHz. Given the conservative fiber link loss of 0.2 dB/km the detection rate after 100 km (20 dB) would be less than 20/s, not counting detection efficiency. Shorter distances would be more favorable, but this implies the protocol is limited to short distances. There also is not any point in randomly adding delays as Eve would still be able to perfectly replicate the gains when the delay is insufficient and could choose to simply not intercept when the delay is too long, giving her partial information without any hint of her presence.

Unfortunately for Eve, Alice can apply a reduction in the optical pulse rate forcing Eve to introduce a delay in the arrival time of the pulses at Bob's station. As a matter of fact, Alice could adjust such delay sending slow pulses as a random burst. Furthermore, slowing pulses can enhance the double-detection rate at Bob's side by reducing after-pulsing errors.

However, there is no reason why each pair must be sent in sequence. We call this protocol the non-structured *nack-state*. If Alice were to transmit a burst of the first states of each pair, followed by a burst of the second states of each pair, she would create a separation between the pairs equal to the length of the bursts and she would not reduce the pulse rate. Consider a 100 km fiber optic link; it would be able to send the first states of each pair for 500 microseconds, followed by the second state of each pair for the next 500 microseconds, with Bob rechoosing the same basis for both 500 microsecond bursts. Since the 500 microsecond delay is at least the full travel time in the quantum channel, Eve would always be compelled to fake the first state of each pair before receiving the second. If there is no issue with this approach, the authors can use it to justify Point 2 of Section 6.1, which in turn justifies Point 1 of the same section.

6.6. Faking double-detection events

Another possibility for the eavesdropper is to fake double-detection events. After all, we may inquire why Eve cannot fake double-detection events as she stays covered up in the channel. First of all, let us recall that Alice knows which biqubits contain *parallel* or *orthogonal* states. Second, consider the cases portrayed in **Table 5**. Assume the $(|0_Z\rangle, |0_Z\rangle)$ biqubit has been sent to Bob by Alice. The first pulse reaches Eve's station, who measures it with the X (or Z) basis, but the second pulse arrives as a vacuum state either by the effect of the quantum channel, the detection system, or the photon source. Thus, Eve gets a single-detection event. In this moment, Eve determines to fake the second state, but she realizes that there are six potential outcomes to fake the $(|0_Z\rangle, |0_Z\rangle)$ biqubit; such cases are listed in **Table 5**. Additionally, one of those cases is erroneous because no *orthogonal* measurement can be derived from *parallel* states. In this example, $(|1_Z\rangle, |0_Z\rangle)$ cannot be obtained from $(|0_Z\rangle, |0_Z\rangle)$. Likewise, $(|0_Z\rangle, |0_Z\rangle)$ cannot be derived from $(|1_Z\rangle, |0_Z\rangle)$. Consequently, if Eve tries to fake a double-detection event, she will produce a bit error of $\frac{1}{6}$. In this situation, a bit error is produced when Alice expects a double non-matching event but Bob announces a double-matching event or vice versa.

According to Collins et al. [30], Bob's visibility of Alice's quantum state is computed as $V_{AB} = \frac{P(signal)}{P(total)}$ where $P(signal) = T_{AB} \times \eta \times V_{opt}$ and $P(total) = T_{AB} \times \eta + (1 - T_{AB} \times \eta) \times 2 \times Y_0$. Here, V_{opt} is the optical visibility with a perfect source and detectors; η is the probability

Alice's Biqubit	Eve's Basis	Eve's Detection	Forwarded States	Eve's Result
$(\lvert 0_Z\rangle, \lvert 0_Z\rangle)$	Z	$(-, \lvert 0_Z\rangle)$	$(\lvert 0_Z\rangle, \lvert 0_Z\rangle)$	Hidden
			$(\lvert 1_Z\rangle, \lvert 0_Z\rangle)$	Detected
	X	$(-, \lvert 0_X\rangle)$	$(\lvert 0_X\rangle, \lvert 0_X\rangle)$	Hidden
			$(\lvert 1_X\rangle, \lvert 0_X\rangle)$	Hidden
		$(-, \lvert 1_X\rangle)$	$(\lvert 0_X\rangle, \lvert 1_X\rangle)$	Hidden
			$(\lvert 1_X\rangle, \lvert 1_X\rangle)$	Hidden
$(\lvert 1_Z\rangle, \lvert 0_Z\rangle)$	Z	$(-, \lvert 0_Z\rangle)$	$(\lvert 0_Z\rangle, \lvert 0_Z\rangle)$	Detected
			$(\lvert 1_Z\rangle, \lvert 0_Z\rangle)$	Hidden
	X	$(-, \lvert 0_X\rangle)$	$(\lvert 0_X\rangle, \lvert 0_X\rangle)$	Hidden
			$(\lvert 1_X\rangle, \lvert 0_X\rangle)$	Hidden
		$(-, \lvert 1_X\rangle)$	$(\lvert 0_X\rangle, \lvert 1_X\rangle)$	Hidden
			$(\lvert 1_X\rangle, \lvert 1_X\rangle)$	Hidden

However, she can use six possible states, but one of them is erroneous, so she introduces an error probability of $\frac{1}{6}$. Here, the six choices for $(\lvert 0_Z\rangle, \lvert 0_Z\rangle)$ and $(\lvert 1_Z\rangle, \lvert 0_Z\rangle)$ biqubits are shown

Table 5. As soon as Eve detects the first state of a biqubit, she tries to fake the second state.

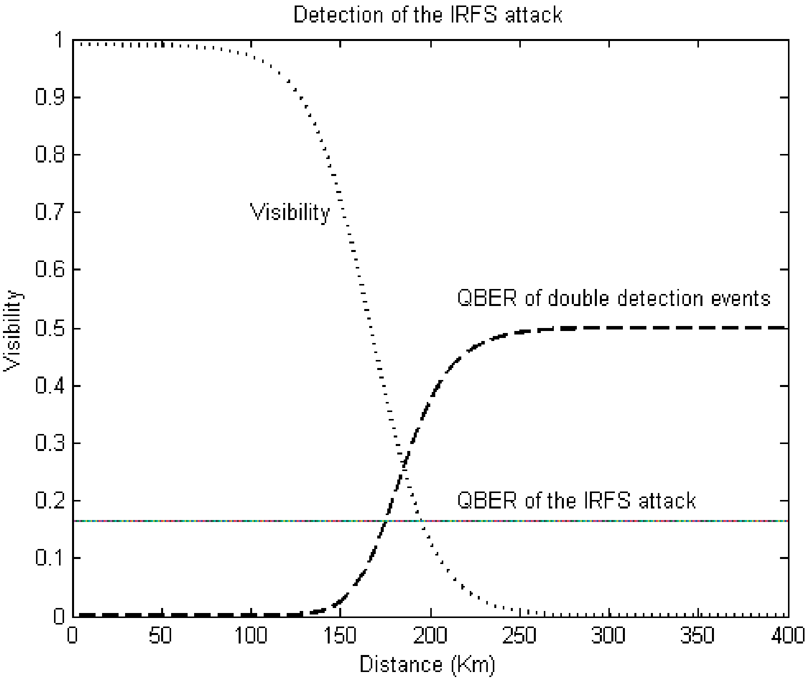


Figure 9. The error rate of double-detection events caused by the *IRFS* attack is $\frac{1}{6}$. When it is compared to the *QBER* of the quantum channel, the maximum secure distance to detect the *IRFS* attack is 176 km. In the presence of the *IRFS* attack, perfect visibility and zero dark counts are assumed in the link between Alice and Eve and from her to Bob.

of detecting the photon when it arrives; T_{AB} is the transmittance between Alice and Bob; and Y_0 is the background noise. On practical experimental parameters: $\alpha = 0.25$ dB· km^{-1}, $\eta = 0.3$, $Y_0 = 10^{-4}$, and $V_{opt} = 0.99$. **Figure 9** shows the visibility as a function of the distance.

On the other hand, the *QBER* in *BB84* can be computed as $QBER = \frac{pe}{pe+pc}$, where pc (pe) is the probability to get, correctly or erroneously, the quantum bit sent by Alice, respectively. If we write such probabilities as a function of the optical visibility V, we have $pc = (1 + V)/2$ and $pe = (1 - V)/2$.

Therefore, $pc = \frac{p_c^2}{p_c^2+p_e^2}$ and $pe = \frac{p_e^2}{p_c^2+p_e^2}$, and we derived the *QBER* of the *parallel* and *orthogonal* states as $QBER = \frac{(1-V)^2}{(1-V)^2+(1+V)^2}$.

If *QBER* of double-detection events produced by the quantum channel is compared against the $\frac{1}{6}$ error rate caused by the eavesdropper, we can find that the maximum secure distance for detecting the *IRFS* attack when the eavesdropper fakes double-detection events is 176 km, which is within the range of the *BB84* key rate, as it appears in **Figure 9**.

7. Conclusions

In the quantum flows approach, the transmitter interleaves pairs of quantum states, *parallel* and *orthogonal* (*non-orthogonal*), while the receiver applies active basis selection to perform state measurement. The *QKD* protocols based on quantum flows uses the same optical hardware of the *BB84* protocol, and they can be implemented in most *QKD* systems as a software module application.

The *ack-QKD* protocol can be useful to detect the *PNS* attack. If the eavesdropper adjusts the transmittance T_{AB} of the channel it produces a deviation in one or in both photonic gains; thus, she will introduce a detectable *QBER* to the system.

On the other side the intercept resend with faked (blinding) states (*IRFS*) attack is detected by the *nack-state* protocol using the gain of single- and double-detection events where the *QBER* of double-detection events of the quantum channel is compared against the $\frac{1}{6}$ error rate caused by the eavesdropper, so the maximum secure distance results in 176 km.

Although double-detection events represent a small fraction of the total detection events, they are useful to detect the *IRFS* attack. In addition, the smaller *QBER* can be useful in future implementations to distill secret bits at longer distances.

Acknowledgements

We would like to mention that a major portion of this chapter has been borrowed from our previous publications: “Quantum Flows for Secret Key Distribution in the Presence of the

Photon Number Splitting Attack" [5] and "Quantum Key Distribution in the Presence of the Intercept-Resend with Faked States Attack" [6].

Author details

Luis A. Lizama-Pérez[1]*, J. Mauricio López[2] and Eduardo de Carlos Lopez[3]

*Address all correspondence to: luislizama@upp.edu.mx

1 Universidad Politécnica de Pachuca, Ex-Hacienda de Santa Bárbara, Municipio de Zempoala, Hidalgo, México

2 Cinvestav Querétaro, Santiago de Querétaro, Querétaro, México

3 Time and Frequency Laboratory, Centro Nacional De Metrología, Santiago de Querétaro, Querétaro, México

References

[1] Bennett CH. Quantum cryptography public key distribution and coin tossing. In: Proceedings of the 1984 International Conference on Computer System and Signal Processing; 1984; Bangalore. pp. 10–19

[2] Van Assche G. Quantum Cryptography and Secret-Key Distillation. Cambridge: Cambridge University Press; 2006

[3] Hughes R, Nordholt J, Rarity J. Summary of implementation schemes for quantum key distribution and quantum cryptography quantum information science and technology roadmap. Available online: http://qist.lanl.gov/pdfs/6.5-continuous.pdf [Accessed on 19 December, 2016]

[4] Lizama L, López JM, De Carlos E, Venegas-Andraca SE. Enhancing quantum key distribution (QKD) to address quantum hacking. Procedia Technology. 2012;**3**:80-88

[5] Lizama-Pérez LA, López JM, De Carlos-López E, Venegas-Andraca SE. Quantum flows for secret key distribution in the presence of the photon number splitting attack. Entropy. 2014;**16**:3121-3135

[6] Lizama-Pérez LA, López JM, De Carlos-López E. Quantum key distribution in the presence of the intercept-resend with faked states attack. Entropy. 2016;**19**

[7] Bennett CH, Bessette F, Brassard G, Salvail L, Smolin J. Experimental quantum cryptography. Journal of Cryptology. 1992;**5**:3-28

[8] Fung CF, Qi B, Tamaki K, Lo H. Phase-remapping attack in practical quantum-key-distribution systems. Physical Review A. 2007;**75**:032314

[9] Xu F, Qi B, Lo H. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. New Journal of Physics. 2010;**12**:113026

[10] Makarov V, Hjelme DR. Faked states attack on quantum cryptosystems. Journal of Modern Optics. 2005;**52**:691-705

[11] Makarov V, Anisimov A, Skaar J. Effects of detector efficiency mismatch on security of quantum cryptosystems. Physical Review A. 2006;**74**:022313

[12] Makarov V, Skaar J. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols. Quantum Information and Computation. 2008;**8**: 622-635

[13] Qi B, Fung CF, Lo H, Ma X. Time-shift attack in practical quantum cryptosystems; 2005. arXiv:quant-ph/0512080

[14] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V. Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photonics. 2010;**4**: 686-689

[15] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kurtsiefer C, Makarov V. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nature Communications. 2011;**2**:349

[16] Wiechers C, Lydersen L, Wittmann C, Elser D, Skaar J, Marquardt C, Makarov V, Leuchs G. After-gate attack on a quantum cryptosystem. New Journal of Physics. 2011;**13**:013043

[17] Weier H, Krauss H, Rau M, Fuerst M, Nauerth S, Weinfurter H. Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors. New Journal of Physics. 2011;**13**:073024

[18] Ma X, Qi B, Zhao Y, Lo H. Practical decoy state for quantum key distribution. Physical Review A. 2005;**72**:012326

[19] Hughes R, Nordholt J. Refining quantum cryptography. Science. 2011;**333**:1584-1586

[20] Lo H, Curty M, Qi B. Measurement-device-independent quantum key distribution. Physical Review Letters. 2012;**108**:130503

[21] Lunghi et al. Free-running single-photon detection based on a negative feedback InGaAs APD. Journal of Modern Optics. 2012;**59**:1481-1488

[22] Gottesman D et al. Proof of security of quantum key distribution with two-way classical communication. IEEE Transactions on Information Theory. 2003;**49**:457-475

[23] Shor P et al. Simple proof of security of the BB84 quantum key distribution protocol. Physical Review Letters. 2000;**85**:441

[24] Scarani V et al. The security of practical quantum key distribution. Reviews of Modern Physics. 2009;**81**:1301

[25] Scarani V et al. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations. Physical Review Letters. 2004;**92**:057901

[26] Takesue H et al. Differential phase shift quantum key distribution experiment over 105 km fiber. New Journal of Physics. 2005;**7**:232

[27] Stucki D et al. Coherent one-way quantum key distribution. Proceedings of SPIE. 2007; **6583**

[28] Sun S, Jiang M, Ma X, Li C, Liang L. Hacking on decoy-state quantum key distribution system with partial phase randomization. Scientific Reports. 2014;**4**:013043

[29] Song T, Qin S, Wen Q, Wang Y, Jia H. Finite-key security analyses on passive decoy-state QKD protocols with different unstable sources. Scientific Reports. 2015;**5**:735-753

[30] Collins D, Gisin N, De Riedmatten H. Quantum relays for long distance quantum cryptography. Journal of Modern Optics. 2005;**52**:735-753

[31] Jeong Y, Kim Y-S, Kim Y-H. Effects of depolarizing quantum channels on BB84 and SARG04 quantum cryptography protocols. Laser Physics. 2011;**21**:1438-1442

Chapter 4

The Role of Quantumness of Correlations in Entanglement Resource Theory

Tiago Debarba

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.70396

Abstract

Quantum correlations: entanglement and quantumness of correlations are main resource for quantum information theory. In this chapter, the scenarios which quantumness of correlations plays an interesting role in entanglement distillation protocol are presented. By means of Koashi-Winter relation, it is discussed that quantumness of correlations are related to the irreversibility of the entanglement distillation protocol. The activation protocol is introduced, and it is proved that quantumness of correlations can create distillable entanglement between the system and the measurement apparatus during a local measurement process.

Keywords: quantumness of correlations, entanglement, quantum information

1. Introduction

Quantum entanglement plays the fundamental role in quantum information and computation [1, 2]. The resource theory of quantum entanglement, entanglement distillation [3] and entanglement cost [4] revealed one of the most fundamental aspects of quantum mechanics. Entanglement distillation protocol consists in converting a number of copies of an entangled state into few copies of maximally entangled states, by means of local operations and classical communication (LOCC) [5]. As maximally entangled states are the main resource of the quantum information, entanglement distillation protocol has many applications in this scenario, as quantum teleport [6], quantum error correction [7] and quantum cryptography [8]. A family of quantum information protocol arises from distillation of quantum entanglement and secret keys [3, 9]

However independently Ollivier and Zurek [10], and Henderson and Vedral [11] found a new quantum property, without counterpart in classical systems. They named it as the *quantumness of correlations*. This new kind of correlation reveals the amount of information destroyed during the local measurement process and goes beyond the quantum entanglement. There are many equivalent formulations for characterization and quantification of quantumness of correlations: quantum discord [10, 11], minimum local disturbance [12–14] and geometrical approach [15–17].

This chapter presents in detail two different ways to relate quantum entanglement and quantumness of correlations. The main purpose of this chapter is to discuss that quantumness of correlations plays an interesting role in entanglement distillation protocol. Entanglement and quantumness of correlations connect each other in two different pictures. The relation derived by Koashi and Winter [18] demonstrates the balance between quantumness of correlations and entanglement in the purification process [19]. This balance leads to a formal proof for the irreversibility of the entanglement distillation protocol, in terms of quantumness of correlations [20]. In the named *activation protocol*, the quantumness of correlations of a given composed system can be converted into distillable entanglement with a measurement apparatus during the local measurement process [21, 22].

The chapter is organized as follow. In Section 2, a mathematical overview is presented, and the notation is defined. Section 3 introduces some important concepts about the notion of quantum correlations: entanglement and quantumness of correlations. Section 4 presents the Koashi-Winter relation and its role in the irreversibility of quantum distillation process. Section 5 is intended to the description of the activation protocol, and the demonstration that quantumness of correlation can be activated into distillable entanglement.

2. Mathematical overview

This section introduces some quantum information concepts and defines the notation used in the chapter.

2.1. Density matrix and quantum channels

As the convex combination of positive matrices is also positive, then the space of positive operators forms a convex cone in Hilbert-Schmidt $\mathcal{L}\left(\mathbb{C}^N\right)$ [23]. If we restrict the matrices in the positive cone to be trace = 1, we arrive to another set of matrices, that is named the set of density matrices. This set of operators also originates a vector space, this space is denoted as $\mathcal{D}\left(\mathbb{C}^N\right)$. Therefore, the matrices that belong to this set, or the vectors in this vector space, are named *density matrices*.

Definition 1. *A linear positive operator $\rho \in \mathcal{D}\left(\mathbb{C}^N\right)$ is a density matrix and represents the state of a quantum system, if it satisfies the following properties:*

- *Hermitian:* $\rho = \rho^\dagger$
- *Positive semi-definite:* $\rho \geq 0$;
- *Trace one:* $\mathrm{Tr}(\rho) = 1$

As the convex combination of density matrices is a density matrix, the vector space $\mathcal{D}$ is a convex set whose pure states are projectors onto the real numbers. A given density matrix $\rho \in \mathcal{D}\left(\mathbb{C}^N\right)$ is a pure state if it satisfies:

$$\rho = \rho^2, \tag{1}$$

then the state ρ is a rank-1 matrix and it can be written as:

$$\rho = |\psi\rangle\langle\psi|. \tag{2}$$

The set of pure states is a $2(N-1)$-dimensional subset of the (N^2-2)-dimensional boundary of $\mathcal{D}(\mathbb{C}^N)$. Every state with at least one eigenvalue equal to zero belongs to the boundary [23]. For two-dimensional systems (it is also named qubit [24]), the boundary is just composed of pure states.

Consider a linear transformation $\Phi : \mathcal{L}(\mathbb{C}^N) \to \mathcal{L}(\mathbb{C}^M)$. This map represents a physical process, if it satisfies some conditions, determined by the mathematical properties of the density matrices. Indeed, to represent a physical process, the transformation must map a quantum state into another quantum state, $\Phi : \mathcal{D}(\mathbb{C}^N) \to \mathcal{D}(\mathbb{C}^M)$. It holds if Φ satisfy the following properties:

- **Linearity:** As a quantum state can be a convex combination of other quantum states, the map must be linear. For two arbitrary operators $\rho, \sigma \in \mathcal{D}(\mathbb{C}^N)$

$$\Phi(\rho + \sigma) = \Phi(\rho) + \Phi(\sigma); \tag{3}$$

- **Trace preserving:** The eigenvalues of the density matrix represent probabilities, and it sum must be one, then a quantum channel must to keep the trace of the density matrix:

$$\mathrm{Tr}[\Phi(\rho)] = 1. \tag{4}$$

- **Completely positive:** Consider a channel $\Phi : \mathcal{D}(\mathbb{C}_A) \to \mathcal{D}(\mathbb{C}_A)$ and a quantum state $\rho, \sigma \in \mathcal{D}(\mathbb{C}_A \otimes \mathbb{C}_B)$, then

$$\mathbb{I} \otimes \Phi(\rho) \geq 0. \tag{5}$$

The map that satisfies this property is named *completely positive map*. The linear transformations mapping quantum states into quantum states are named completely positive and trace preserve (CPTP) *quantum channels*. The space of quantum channels that maps $N \times N$ density matrices onto $M \times M$ density matrices is denoted as $\mathcal{C}(\mathbb{C}^N, \mathbb{C}^M)$.

2.2. Measurement

Measurement is a classical statistical inference of quantum systems. The measurement process maps a quantum state into a classical probability distribution.

We can define a measurement as a function $\Pi : \Sigma \to \mathcal{P}(\mathbb{C}_\Gamma)$[1], associating an alphabet Σ to positive operators $\{\Pi_x\}_x \subset \mathcal{P}(\mathbb{C}_\Gamma)$. For a given density matrix $\rho \in \mathcal{D}(\mathbb{C}_\Gamma)$, the measurement process consists in to chose an element of Σ randomly. This random choice is represented by a

[1] Just to clarify the notation, when we write a subscript in the complex euclidean vector space, as $\mathbb{C}_\Gamma$, it represents a label to the space, it shall be very useful when we study composed systems. When we write a superscript on it, it represents the dimension of the complex vector space. For example, if $\dim(\mathbb{C}_\Gamma) = N$, we can also represent this space as $\mathbb{C}^N$, the usage of the notation will depend on the context.

probability vector $\vec{p} \in \mathbb{R}_{+}^{N}$, with N being the cardinality of the random variable described by $\vec{p}$. The elements of the probability vector $\vec{p}$ are given by:

$$p_x = \mathrm{Tr}(\Pi_x \rho), \tag{6}$$

where Π_x is the *measurement operator* associated to $x \in \Sigma$. The alphabet Σ is the set of measurement outcomes, and the vector $\vec{p}$ is the classical probability vector associated to the measurement process Π of a given density matrix ρ. As the outcomes are elements of a probability vector, these elements must be positive and sum to one. Which implies that the measurement operators must sum to identity:

$$\sum_x \Pi_x = \mathbb{I}_\Gamma, \tag{7}$$

where $\mathbb{I}_\Gamma$ is the identity matrix in $\mathbb{C}_\Gamma$. It is easy to check that this condition implies $\sum_x p_x = 1$:

$$\sum_x p_x = \sum_x \mathrm{Tr}(\Pi_x \rho) = \mathrm{Tr}\left(\sum_x \Pi_x \rho\right) = \mathrm{Tr}(\rho) = 1. \tag{8}$$

For instance, we shall restrict the measurements to a subclass of measurement operators named *projective measurements*. As it is shown later, its generalization can be performed via the Naimark's theorem. For projective measurements, the cardinality of $\vec{p}$ is at least the dimension of ρ, and the measurement operators are projectors:

$$\Pi_x^2 = \Pi_x, \tag{9}$$

for any $x \in \Sigma$. If we consider an orthonormal basis $\{|e_x\rangle\}$, where the vectors $|e_x\rangle$ span $\mathbb{C}_\Gamma$, this set represents a projective measurement for $\Pi_x = |e_x\rangle\langle e_x|$. The output state is described by the expression:

$$\rho_x = \frac{\Pi_x \rho \Pi_x}{\mathrm{Tr}(\Pi_x \rho)}. \tag{10}$$

The set of operators defines a convex hull in $\mathcal{P}(\mathbb{C}_\Gamma)$, then a measured state represents a pure state in this convex hull. In this way, the post-measurement state can be reconstructed by the convex combination of the output states $\rho = \sum_x p_x \rho_x$.

As physical processes are described by quantum channels, it is possible to describe the classical statistical inference of the quantum measurements as a CPTP channel. A channel that maps a quantum state into a probability vector is the dephasing channel. Therefore, the post-measurement state is the state under the action of the dephasing channel.

Theorem 2. *A given map $\Phi \in \mathcal{C}(\mathbb{C}_\Gamma, \mathbb{C}_{\Gamma'})$ is a measurement if and only if:*

$$\Phi(\rho) = \sum_x \mathrm{Tr}(M_x \rho)|e_x\rangle\langle e_x|, \tag{11}$$

where $\rho \in \mathcal{D}(\mathbb{C}_\Gamma)$, $M_x \in \mathcal{P}(\mathbb{C}_\Gamma)$ and $|e_x\rangle \in \mathbb{C}_{\Gamma'}$.

In order to differ the set of measurement channels from a general CPTP channel, this set is represented as $\mathcal{P}$. A given measurement map $\mathcal{M}\in\mathcal{P}(\mathbb{C}_{\Gamma},\mathbb{C}_{\Gamma'})$ is a quantum channel that maps a density matrix in a probability vector, $\mathcal{M}:\mathcal{D}(\mathbb{C}_{\Gamma})\to\mathbb{R}^{+}_{\Gamma'}$. This probability vector is described by a diagonal density matrix as in Eq. (11). The dimension of $\mathbb{C}_{\Gamma'}$ is the number of outcomes of the measurement.

For general measurements, described by positive operators valued measure (POVM), the measurement process can be described by a measurement channel $\Phi\in\mathcal{P}(\mathbb{C}_{\Gamma},\mathbb{C}_{\Gamma})$. The description performed above can be followed to describe these general measurements, indeed projective measurements are a restriction for a POVM composed by orthogonal operators. Consider a set of positive operators $\{M_x\}_x$, representing a POVM, then $\mathrm{Tr}[M_x\rho]=p_x$ are the elements of a probability vector $\vec{p}\in\mathbb{R}^{+}_{\Gamma}$, then the post-measurement state is:

$$\Phi(\rho)=\sum_{x}p_x|e_x\rangle\langle e_x|. \tag{12}$$

Where $\{|e_x\rangle\}_x$ is an orthonormal basis in $\mathbb{C}_{\Gamma}$.

Using the Naimark's theorem, the measurement channel is described as a dephasing channel on a state in a enlarged space. In other words, for POVMs whose elements are rank-1 and linearly independent, it is possible to associate a projective measurement on an enlarged space.

Theorem 3 (Naimark's theorem). *Given a quantum measurement $\mathcal{M}\in\mathcal{P}(\mathbb{C}_{\Gamma},\mathbb{C}_{\Gamma'})$, with POVM elements $\{M_x\}_{x=0}^{M}$, there exists a projective measurement $\Pi\in\mathcal{P}(\mathbb{C}_{\Gamma'})$, with elements $\{\Pi_y\}_{y=0}^{M}$ such that:*

$$\mathrm{Tr}(M_x\rho)=\mathrm{Tr}(\Pi_x V\rho V^{\dagger}), \tag{13}$$

where $V\in\mathcal{U}(\mathbb{C}_{\Gamma},\mathbb{C}_{\Gamma'})$ is an isometry.

The action of the isometry on the state ρ, in the Naimark's theorem, is named as embedding operation. In this way, the isometry will be $V=\mathbb{I}_{\Gamma}\otimes|0\rangle_E$ and the enlarged space $\mathbb{C}_{\Gamma'}=\mathbb{C}_{\Gamma}\otimes\mathbb{C}_{E}$. For this simple case, the relation between the POVM elements $\{M_x\}_x$ and the projective measurement on the enlarged space $\{\Pi_x\}_x$:

$$M_x=\left(\mathbb{I}_{\Gamma}\otimes\langle 0|_E\right)\Pi_x\left(\mathbb{I}_{\Gamma}\otimes|0\rangle_E\right). \tag{14}$$

As the measurement can be described by a quantum channel, we can study how quantum measurements can be performed locally.

Definition 4. *Given a N-partite composed system, represented by the state $\rho_{A_1,\dots,A_N}\in\mathcal{D}(\mathbb{C}_{A_1}\otimes\cdots\otimes\mathbb{C}_{A_N})$, we define the measurement on each subsystem applied locally:*

$$\Phi_{A_1}\otimes\cdots\otimes\Phi_{A_N}\left(\rho_{A_1,\dots,A_N}\right)=\sum_{\vec{k}}\mathrm{Tr}\left[M_{k_1}^{A_1}\otimes\cdots\otimes M_{k_N}^{A_N}\rho_{A_1,\dots,A_N}\right]\left|\vec{k}\right\rangle\left\langle\vec{k}\right|, \tag{15}$$

where $\left|\vec{k}\right\rangle=|k_1\rangle\otimes\cdots\otimes|k_N\rangle$ and the label $\vec{k}$ in the sum represents the set of indexes $k_1,\dots,k_N$. $\left\{M_{k_x}^{A_x}\right\}_{k_x}$ are the measurement operators on each subsystem.

Suppose the measurement is performed on some subsystems, the remaining other subsystems are unmeasured. Consider a bipartite system $\rho_{AB} \in \mathcal{D}(\mathbb{C}_A \otimes \mathbb{C}_B)$ and a measurement acting on the system B, then the measurement map will be written as:

$$\mathbb{I}_A \otimes \Phi_B(\rho_{AB}) = \sum_x \mathrm{Tr}_B\left[\mathbb{I}_A \otimes M_x^B \rho_{AB}\right] \otimes |b_x\rangle\langle b_x|. \tag{16}$$

As the measurement is not acting on A, the post-measured state on A will remain the same. If we write $p_x = \mathrm{Tr}_{AB}\left[\mathbb{I}_A \otimes M_x^B \rho_{AB}\right]$ and $\rho_x^A = \frac{\mathrm{Tr}_B\left[\mathbb{I}_A \otimes M_x^B \rho_{AB}\right]}{\mathrm{Tr}_{AB}\left[\mathbb{I}_A \otimes M_x^B \rho_{AB}\right]}$, the post-measured state will be:

$$\mathbb{I}_A \otimes \Phi_B(\rho_{AB}) = \sum_x p_x \rho_x^A \otimes |b_x\rangle\langle b_x|. \tag{17}$$

As the measurement is a classical statistical inference process, the local measurement process destroys the quantum correlations between the systems. Indeed the post-measured state is not a classical probability distribution, although it only has classical correlations.

2.3. Quantum entropy

Consider that one can prepare an ensemble of quantum states $\xi = \{p_x, \rho_x\}_x$, accordingly to some random variable X. Classical information can be extracted from the ensemble of quantum states, in the form of a variable Y, performing measurements on the quantum system. The conditional probability distribution to obtain a value y, given as input the state ρ_x is:

$$p(y|x) = \mathrm{Tr}(M_y \rho_x), \tag{18}$$

where $\{M_y\}_y$ is a POVM. The joint probability distribution X and Y is given by:

$$p(x, y) = p_x \mathrm{Tr}(M_y \rho_x). \tag{19}$$

The probability distribution of Y is obtained from the marginal probability distribution:

$$p(y) = \sum_x p(x, y) = \sum_x p_x \mathrm{Tr}(M_y \rho_x) = \mathrm{Tr}\left(M_y \sum_x p_x \rho_x\right). \tag{20}$$

Considering the Bayes rule:

$$p(x, y) = p_x p(y|x) = p(y) P(x|y), \tag{21}$$

it is possible to obtain the conditional probability distribution with elements:

$$P(x|y) = \frac{p_x p(y|x)}{p(y)}. \tag{22}$$

Even in the case the system is always prepared in the same state, there exists an uncertainty about the measured of an observable. The probability distributions presented above are evidencing this uncertainty, for the measurement observables of a POVM. These probability distributions are classical probability distributions extracted from the quantum systems, and the Shannon entropy quantifies the degree of surprise related to a given result.

It is also possible to define a quantum analogous to the Shannon entropy. This quantum entropy is named as von Neumann entropy, and in analogy with Shannon entropy, it is defined as the expectation value of the operator $\log_2(\rho)$.

Definition 5 (von Neumann entropy). *Given a density operator $\rho \in \mathcal{D}(\mathbb{C}^N)$, the quantum version of the Shannon entropy is defined as the function:*

$$S(\rho) = -\mathrm{Tr}[\rho \log_2 \rho]. \tag{23}$$

The von Neumann entropy can be rewritten as:

$$S(\rho) = -\sum_k \lambda_k \log_2(\lambda_k), \tag{24}$$

where $\{\lambda_k\}_k$ are the eigenvalues of $\rho = \sum_k \lambda_k |k\rangle\langle k|$. The von Neumann entropy has the same interpretation of the Shannon entropy for the probability distribution composed by the eigenvalues of the density matrix. The von Neumann entropy is zero of pure states, and it is maximum for the maximally mixed state $\mathbb{I}/N$, where it is $S(\mathbb{I}/N) = \log_2 N$.

For composed systems, the von Neumann entropy is analogous to the Shannon entropy of the joint probability. For a bipartite state ρ_{AB}, the joint von Neumann entropy is:

$$S(\rho_{AB}) = -\mathrm{Tr}(\rho_{AB} \log_2 \rho_{AB}). \tag{25}$$

Follow some interesting, and useful, properties about von Neumann entropy:

1. **(Pure states)** For a bipartite pure state $|\phi\rangle_{AB} \in \mathbb{C}_A \otimes \mathbb{C}_B$, the partitions have the same von Neumann entropy:

$$S(\rho_A) = S(\rho_B), \tag{26}$$

   where $\rho_A = \mathrm{Tr}_B(|\phi\rangle\langle\phi|_{AB})$.

2. (**Additivity**) von Neumann entropy is additive:

$$S(\rho \otimes \sigma) = S(\rho) + S(\sigma), \tag{27}$$

   where ρ and σ are density matrices.

3. (**Concavity**) von Neumann entropy is a concave function:

$$S\left(\sum_i p_i \rho_i\right) \geq \sum_i p_i S(\rho_i), \tag{28}$$

   for a convex combination $\rho = \sum_i p_i \rho_i$.

4. **(Classical-quantum states)** For bipartite state in the form $\rho_{AB} = \sum_x p_x |x\rangle\langle x| \otimes \rho_x$, the von Neumann entropy will be:

$$S\left(\sum_x p_x |x\rangle\langle x| \otimes \rho_x\right) = H(X) + \sum_x p_x S(\rho_x), \tag{29}$$

where $H(X) = -\sum_x p_x \log_2 p_x$

For composed system, it is possible to define a quantum analogous to the mutual information for bipartite states.

Definition 6 (Mutual information). *Given a bipartite state $\rho_{AB} \in \mathcal{D}(\mathbb{C}_A \otimes \mathbb{C}_B)$, the quantum mutual information is defined as:*

$$I(A:B)_{\rho_{AB}} = S(\rho_A) + S(\rho_B) - S(\rho_{AB}). \tag{30}$$

The quantum mutual information of ρ_{AB} quantifies the correlations in quantum systems. It can be interpreted as the number of qubits that one part must send to another to destroy the correlations between the entire system. As the amount of correlations in a quantum state must be positive, it is possible to conclude that:

$$S(\rho_A) + S(\rho_B) \geq S(\rho_{AB}). \tag{31}$$

From property 2, it is easy to see that mutual information is zero for product state $\rho_{AB} = \rho_A \otimes \rho_B$. The mutual information of pure states will be equal to:

$$I(A:B)_{\psi_{AB}} = 2S(\rho_A) = 2S(\rho_B), \tag{32}$$

where $\psi_{AB} = |\psi\rangle\langle\psi|_{AB}$ is pure state.

The quantum version of the relative entropy quantifies the distinguishability between quantum states.

Definition 7 (Quantum relative entropy). *Given two density matrices $\rho, \sigma \in \mathcal{D}(\mathbb{C}^N)$, the distinguishability between them can be quantified using the quantum relative entropy:*

$$S(\rho||\sigma) = \mathrm{Tr}[\rho \log_2 \rho - \rho \log_2 \sigma]. \tag{33}$$

It will be zero if $\rho = \sigma$.

The quantum relative entropy is a positive function for $\mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma)$, otherwise it diverges to infinity. The quantum mutual information can also be written as a quantum relative entropy.

Proposition 8. *Consider a bipartite state ρ_{AB}, the following expression holds:*

$$I(A:B)_{\rho_{AB}} = S(\rho_{AB}||\rho_A \otimes \rho_B), \tag{34}$$

where ρ_A and ρ_B are the reduced states of ρ_{AB}.

In contrast with the von Neumman entropy, the relative entropy always decreases under the action of a quantum channel. This property has an operational meaning: two states are always less distinguishable under the action of noise.

Theorem 9. *Given two density matrices* $\rho, \sigma \in \mathcal{D}(\mathbb{C}_A)$ *and a quantum channel* $\Gamma \in \mathcal{C}(\mathbb{C}_A, \mathbb{C}_B)$, *the following inequality holds:*

$$S(\rho||\sigma) \geq S(\Gamma(\rho)||\Gamma(\sigma)) \tag{35}$$

This theorem implies into another property of the quantum mutual information: it decreases monotonically under local CPTP channels. As mutual information quantifies correlations, this means that the amount of correlations reduce under local noise.

Corollary 10. *Given a bipartite state* $\rho_{AB} \in \mathcal{D}(\mathbb{C}_A \otimes \mathbb{C}_B)$ *and quantum channel* $\Phi_B \in \mathcal{C}(\mathbb{C}_B, \mathbb{C}_{B'})$, *the mutual information satisfies:*

$$I(A:B)_{\rho_{AB}} \geq I(A:B')_{\mathbb{I} \otimes \Phi(\rho_{AB})}. \tag{36}$$

Proof. Given the mutual information:

$$I(A:B)_{\rho_{AB}} = S(\rho_{AB}||\rho_A \otimes \rho_B) \tag{37}$$

using the theorem above:

$$I(A:B)_{\rho_{AB}} \geq S(\mathbb{I}_A \otimes \Phi_B(\rho_{AB})||\rho_A \otimes \Phi_B(\rho_B)) = I(A:B')_{\mathbb{I} \otimes \Phi(\rho_{AB})}. \tag{38}$$

Analogous to the classical conditional entropy, it is possible to define a quantum version of it. For a bipartite system ρ_{AB}, the quantum conditional entropy quantifies the amount of information of A that is available when B is known.

Definition 11 (Conditional entropy). *Consider a bipartite system* ρ_{AB}, *the quantum conditional entropy is defined as the function:*

$$S(A|B)_{\rho_{AB}} = S(\rho_{AB}) - S(\rho_B). \tag{39}$$

One interesting property of the quantum conditional entropy is that it can be negative. For example, if we consider a bipartite pure state $|\phi\rangle_{AB} = (|00\rangle + |11\rangle)/\sqrt{2}$, von Neumann entropy of the pure state is zero: $S(|\phi\rangle\langle\phi|_{AB}) = 0$. Nonetheless the reduced state is the maximally mixed state: $\rho_B = \mathbb{I}/2$, whose von Neumann entropy is $S(\mathbb{I}/2) = 1$. Therefore, the conditional entropy of this state is negative $S(A|B)_{|\phi\rangle\langle\phi|_{AB}}) = -1$. The negative value of the quantum conditional entropy is defined as the *coherent information*:

$$I(A\rangle B) = -S(A|B). \tag{40}$$

The conditional entropy has an operational meaning in the state merging protocol, where a tripartite pure state is shared by two experimentalists, one will send part of its state through a quantum channel to the other. The coherent information quantifies the amount of entanglement required to the sender be able to perform the protocol. If it is positive, they cannot use entanglement to perform the state merging, and in the end the amount of entanglement grows [25–27]. The coherent information also quantifies the capacity of a quantum channel, optimizing over all input states ρ_A, the output state is known to be ρ_B. This result is named as *LSD theorem* [28–31].

3. Quantum correlations

3.1. Entanglement

This section introduces the concept of quantum entanglement, presenting its characterization and quantification.

3.1.1. Separable states

Consider two systems A and B, often named the experimentalists responsible by the systems as Alice and Bob, respectively. The state of the systems A and B is described by a density matrix on a Hilbert space. In this way considering two finite Hilbert spaces $\mathbb{C}_A$ and $\mathbb{C}_B$, and a basis in each one:

$$\{|a_i\rangle\}_{i=0}^{|A|-1} \in \mathbb{C}_A; \tag{41}$$

$$\{|b_k\rangle\}_{k=0}^{|B|-1} \in \mathbb{C}_B, \tag{42}$$

where $|A|$ = dim($\mathbb{C}_A$) and $|B|$ = dim($\mathbb{C}_B$). The global system, composed of A and B, can be obtained through the tensor product between the basis in the Hilbert space of each system:

$$\{|a_i, b_k\rangle\}_{i,j=0}^{|AB|-1} = \{|a_i\rangle \otimes |b_k\rangle\}_{i,k=0}^{|A|-1,\,|B|-1}, \tag{43}$$

hence the dimension of the composed system is the product of the dimension: $|AB|$ = dim ($\mathbb{C}_{AB}$) = dim($\mathbb{C}_A$) · dim($\mathbb{C}_B$). The Hilbert space of the composed system is denoted as $\mathbb{C}_{AB} = \mathbb{C}_A \otimes \mathbb{C}_B$. A pure state of the composed system can be decomposed in the basis in Eq. (43):

$$|\psi\rangle_{AB} = \sum_{i,k} c_{i,k} |a_i\rangle \otimes |b_k\rangle. \tag{44}$$

From this expression, one can realize that: in general a pure state, which describes a composed system, cannot be written as the product of the state of each system. In other words, suppose the system A and B described by the states $|\alpha\rangle_A = \sum_i a_i |a_i\rangle \in \mathbb{C}_A$ and $|\beta\rangle_B = \sum_k b_k |b_k\rangle \in \mathbb{C}_B$, the composed system is described by the state:

$$|\alpha\rangle \otimes |\beta\rangle = \sum_{i,k} a_i b_k |a_i\rangle \otimes |b_k\rangle. \tag{45}$$

It is the particular case where the coefficients in Eq. (44) are $c_{i,k} = a_i \cdot b_k$. If a composed system can be written as Eq. (45), it is called a *product state*, and there is no correlations between A and

B. It can be checked easily via the mutual information of the state, which is clearly zero once that the von Neumman entropy of the pure state is zero [32–34].

The concept of product state can be generalized for mixed state. Considering a composed system represented by the state $\rho_{AB} \in \mathcal{D}(\mathbb{C}_A \otimes \mathbb{C}_B)$, it is called a *product state* if can be written as:

$$\rho_{AB} = \rho_A \otimes \rho_B, \tag{46}$$

where $\rho_A \in \mathcal{D}(\mathbb{C}_A)$ and $\rho_B \in \mathcal{D}(\mathbb{C}_B)$ are the states of the systems *A* and *B*, respectively. The product state for mixed states is also no correlated, as its mutual information is zero. As the space of quantum states is a convex set, the convex combination of states will also be a quantum state. The convex combination of product states generalizes the notion of product states, that is named as *separable state* [35].

Definition 12 (Separable states). *Considering a composed system described by the state $\sigma \in \mathcal{D}(\mathbb{C}_A \otimes \mathbb{C}_B)$, it is a separable state if and only if can be written as:*

$$\sigma = \sum_{i,j} p_{i,j} \sigma_i^A \otimes \sigma_j^B, \tag{47}$$

where $\sigma_i^A \in \mathcal{D}(\mathbb{C}_A)$ and $\sigma_j^B \in \mathcal{D}(\mathbb{C}_B)$.

The set of quantum channels that let separable states invariant is named *local operations and classical communication* (LOCC). The set of separable states form a subspace in the space of density matrices, it can be denoted as *Sep*($\mathbb{C}_{AB}$). The separable state can be easily extended to multipartite systems. Considering a *n*-partite system, it is named *m*-separable if it can be decomposed in a convex combination of product states composed by *m* parties.

3.1.2. Entanglement quantification

A measure of entanglement for mixed state can be obtained from the quantification of entanglement for pure states. It is possible to construct a measure of entanglement in this sense calculating the average of entanglement taken on pure states needed to form the state. The most famous measure which follow this idea is named as *entanglement of formation*. The entanglement of formation is interpreted as the minimal pure state entanglement required to build the mixed state [7].

Definition 13. *Considering a quantum state $\rho \in \mathcal{D}(\mathbb{C}_A \otimes \mathbb{C}_B)$, the entanglement of formation is defined as:*

$$E_f(\rho) = \min_{\xi_\rho} \sum_i p_i E(|\psi_i\rangle), \tag{48}$$

where the optimization is performed over all ensembles $\xi_\rho = \{p_i, |\psi_i\rangle\langle\psi_i|\}_{i=1}^M$, such that $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, $\sum_i p_i = 1$ and $p_i \geq 0$.

The entanglement entropy $E(|\psi_i\rangle)$ is defined as:

$$E(|\psi_i\rangle) = S(\mathrm{Tr}_B[|\psi_i\rangle\langle\psi_i|]), \tag{49}$$

where $S(\mathrm{Tr}_B[|\psi_i\rangle\langle\psi_i|])$ is the von Neumann entropy of the reduced state of $|\psi_i\rangle$. The entanglement of formation is not easy to evaluate. Indeed the minimization process implies in to find an optimal convex hull, in function of a nonlinear function. For two qubits systems, it can be calculated analytically [36].

Quantum entanglement also enables an operational interpretation. This interpretation has two different ways: the resource required to construct a given quantum state and the resource extracted from a quantum system. The resource here refers to the amount of copies of maximally mixed state. Then, one can define the measure of this resource as a measure of entanglement in the limit of many copies.

The number of copies m of maximally entangled states required to construct n copies of a given state ρ, by means of LOCC protocols, is named *entanglement cost* [7]. The entanglement cost can be written as the regularized version of the entanglement of formation [4].

Definition 14 (Entanglement cost). *The number of copies of the maximally entangled states required to build the state ρ is given by:*

$$E_C(\rho) = \lim_{n\to\infty} \frac{E_f(\rho^{\otimes n})}{n}, \tag{50}$$

where $E_f(\rho^{\otimes n})$ is the entanglement of formation of the n copies of ρ.

The number of copies m of the maximally entangled state which can be extracted from n copies of a given state ρ, by LOCC, is named as *distillable entanglement* [7].

Definition 15 (Distillable entanglement). *The distillable entanglement of a given state ρ is defined as:*

$$E_D(\rho) = \lim_{n\to\infty} \frac{m}{n}, \tag{51}$$

where m is the number of maximally entangled states that can be extracted from ρ in the limit of many copies.

The distillable entanglement is a very important operational measure of entanglement, because it quantifies how useful is a given quantum state, for the quantum information purpose.

The operational meaning of the entanglement cost and the distillable entanglement compose the research theory of quantum entanglement. The entanglement cost and the distillable entanglement of a given state are not the same. Indeed the cost of entanglement is greater than the distillable entanglement. The point is: it is more expensive to create a state ρ with copies of maximally entangled state than is possible to extract entanglement from ρ. One example is the bound entangled state, even it is entangled it is not possible to extract any maximally entangled state, although it requires an amount of maximally entangled states to build it.

3.2. Quantumness of correlations

This section presents a revision about some basic concepts of quantumness of correlations for distinguishable systems. The notion of classically correlated states and quantum discord is presented.

3.2.1. Classically correlated states

Consider a flip coin game with two distinct events described by the states $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, each with the same probability 1/2. It is known that it is possible to distinguish the faces of the coin, with a null probability of error. The probability of error to distinguish two events, or two probability distributions, depends on the trace distance of the probability vectors of the events:

$$P_E(|0\rangle\langle 0|, |1\rangle\langle 1|) = \frac{1}{2} - \frac{1}{4}\||0\rangle\langle 0| - |1\rangle\langle 1|\|_1, \tag{52}$$

as the states are orthogonal $\||0\rangle\langle 0| - |1\rangle\langle 1|\|_1 = 2$, therefore the probability of error $P_E(|0\rangle\langle 0|, |1\rangle\langle 1|) = 0$, as one expected. Now suppose a quantum coin flip, which coherent superposition between the two faces of the coin, described by the events: $\{|\phi\rangle\langle\phi|, |\psi\rangle\langle\psi|\}$, with equal probability 1/2, where $|\phi\rangle, |\psi\rangle \in \mathbb{C}^2$. As an example, consider the states $|\phi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|\psi\rangle = |1\rangle$. For this case, the overlap is $\langle\phi|\psi\rangle = 1/\sqrt{2}$. The trace distance of these states is simply:

$$\||\phi\rangle\langle\phi| - |\psi\rangle\langle\psi|\|_1 = \sqrt{2},$$

then the probability of error to distinguish the events is not zero. Superposition of states in quantum mechanics creates events that cannot be perfectly distinguished. The distinguishability of quantum or classical events can be quantifier by the Jensen-Shannon divergence. For two probability distributions (or events), it is defined as the symmetric and smoothed version of the Shannon relative entropy, or in the quantum case the von Neumman relative entropy [37, 38].

Definition 16. *The Jensen-Shannon divergence for two arbitrary events* $|\psi\rangle, |\phi\rangle$ *is defined as:*

$$J(|\psi\rangle, |\phi\rangle) = \frac{1}{2}S\left(\frac{|\phi\rangle\langle\phi| + |\psi\rangle\langle\psi|}{2}\||\phi\rangle\langle\phi|\right) + \frac{1}{2}S\left(\frac{|\phi\rangle\langle\phi| + |\psi\rangle\langle\psi|}{2}\||\psi\rangle\langle\psi|\right). \tag{53}$$

For the classical coin flip game, the Jensen-Shannon divergence will be just $J(|0\rangle, |1\rangle) = 1$. On the other hand, for the quantum coin flip with states $|\phi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|\psi\rangle = |1\rangle$, it will be $J(|\phi\rangle, |\psi\rangle) = \sqrt{2}$. The Jensen-Shannon divergence is related to the Bures distance and induces a metric for pure quantum states related to the Fisher-Rao metric [39], it is lager for more distinguishable events, and the largest distance characterizes complete distinguishable events. The Jensen-Shannon divergence for two arbitrary events $|\psi\rangle, |\phi\rangle$ is related to the mutual information [37]:

$$J(|\psi\rangle, |\phi\rangle) = I(R:E)_{\rho_{RE}}, \tag{54}$$

where R represents a register, E represents the events and $\rho_{RE} \in \mathcal{D}(\mathbb{C}_R \otimes \mathbb{C}_E)$ characterizes the existence of two distinct events:

$$\rho_{RE} = \frac{1}{2}|0\rangle\langle 0|_R \otimes |\phi\rangle\langle\phi|_E + \frac{1}{2}|1\rangle\langle 1|_R \otimes |\psi\rangle\langle\psi|_E. \tag{55}$$

For the classical coin flip game, it is $\rho^c_{RE} = \frac{1}{2}|0\rangle\langle 0| \otimes |0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \otimes |1\rangle\langle 1|$, with mutual information $I(R:E)_{\rho^c_{RE}} = 1$. For the quantum coin, the state will be $\rho^q_{RE} = \frac{1}{2}|0\rangle\langle 0| \otimes |\phi\rangle\langle\phi|$ $+\frac{1}{2}|1\rangle\langle 1| \otimes |\psi\rangle\langle\psi|$, where for $|\phi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|\psi\rangle = |1\rangle$, and the mutual information is $I(R:E)_{\rho^q_{RE}} = \sqrt{2}$. As the mutual information is a measure of correlations between two probability distributions, one realizes that there are more correlations between the register and the events for not completely distinguishable registers, in comparison with orthogonal registers. However, two binary classical distributions cannot share more than one bit of information; in other words, their mutual information cannot be greater than one [31]. As the correlations between the quantum coin events and the register are bigger than one, it means that there are correlations beyond the classical case. A quantum state is classically correlated if there exists a local projective measurement such that the state remains the same [10–12]. The state ρ^c_{RE} is an example of *classical-classical state*. In general, these states are defined as:

Definition 17 (classical-classical states). *Given a bipartite state $\rho_{AB} \in \mathcal{D}(\mathbb{C}_A \otimes \mathbb{C}_B)$, it is strictly classically correlated (or classical-classical state) if there exists a local projective measurement Π_{AB} with elements $\{\Pi^A_l \otimes \Pi^B_k\}_{k,l}$ such that the post-measured state is equal to the input state:*

$$\Pi(\rho_{AB}) = \sum_{k,l} \Pi^A_l \otimes \Pi^B_k \rho_{AB} \Pi^A_l \otimes \Pi^B_k = \rho_{AB}, \tag{56}$$

therefore $\rho_{AB} = \sum_{k,l} p_{k,l} \Pi^A_l \otimes \Pi^B_k$, and $\Pi^Y_x = |e_x\rangle\langle e_x|_Y$ is a projetor in the orthonormal basis $\{|e_x\rangle_Y\}_x \in \mathcal{H}_Y$.

The state ρ^q_{ER} is an example of a *classical-quantum state*, because there exists a projective measurement, with elements $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, over partition E that keep the state unchanged. On the other hand, there is not a projective measurement over partition R with this property. In general, a state ρ_{AB} is classical-quantum if there exists a projective measurement Π_A with elements $\{\Pi_k\}_k$ such that:

$$\Pi_A \otimes \mathbb{I}_B(\rho_{AB}) = \rho_{AB} = \sum_k p_k \Pi_k \otimes \rho_k. \tag{57}$$

The set o classically correlated states is not convex, once that combination of block diagonal matrices cannot be block diagonal. As the identity matrix is block diagonal, or just diagonal, this set is connected by the maximally mixed state, and it is a *thin set* [40].

3.2.2. Quantum discord

The amount of classical correlations in a quantum state is measured by the capacity to extract information locally [41]. As the measurement process is a classical statistical inference, classical correlations can be quantified by the amount of correlations that are not destroyed by the local measurement.

Definition 18. *For a bipartite density matrix $\rho_{AB} \in \mathcal{D}(\mathbb{C}_A \otimes \mathbb{C}_B)$, the classical correlations between A and B can be quantified by the amount of correlations that can be extracted via local measurements:*

$$J(A:B)_{\rho_{AB}} = \max_{\mathbb{I}\otimes\mathcal{B}\in\mathcal{P}} I(A:X)_{\mathbb{I}\otimes\mathcal{B}(\rho_{AB})} = \max_{\mathbb{I}\otimes\mathcal{B}\in\mathcal{P}} \left\{ S(\rho_A) - \sum_x p_x S(\rho_x^A) \right\}, \tag{58}$$

where the optimization is taken over the set of local measurement maps $\mathbb{I}\otimes\mathcal{B}\in\mathcal{P}(\mathcal{H}_{AB},\mathcal{H}_{AX})$, and $\mathbb{I}\otimes\mathcal{B}(\rho_{AB}) = \sum_x p_x \rho_x^A \otimes |b_x\rangle\langle b_x|$ is a quantum-classical state in the space $\mathcal{B}(\mathcal{H}_A\otimes\mathcal{H}_X)$.

Originally, Ollivier and Zurek [10] have defined this expression restricting the optimization to projective measurements. Independently, Henderson and Vedral [11] have defined the optimization of the classical correlations over general POVMs. As the mutual information quantifies the total amount of correlations in the state, it is possible to define a quantifier of quantum correlations as the difference between the total correlations in the system, quantified by mutual information, and the classical correlations, measured by Eq. (58). This measure of quantumness of correlations is named as *quantum discord*:

Definition 19. *The quantum discord $D(A:B)_{\rho_{AB}}$ of a state ρ_{AB} is defined as:*

$$D(A:B)_{\rho_{AB}} = I(A:B)_{\rho_{AB}} - J(A:B)_{\rho_{AB}}, \tag{59}$$

where $I(A:B)_{\rho_{AB}}$ is the von Neumann mutual information.

Quantum discord quantifies the amount of information, that cannot be accessed via local measurements. Therefore, it measures the quantumness shared between *A* and *B* that cannot be recovered via a classical statistical inference process. The optimization of quantum discord is a NP-hard problem [42]. A general analytical solution for quantum discord is not known or a criterion for a giving POVM to be optimal. Nonetheless, there are some analytic expressions for some specific states [43–45]. It is a natural generalization of quantum discord for the case the measurement is performed locally on both subsystems.

Definition 20. *Given a bipartite state $\rho_{AB} \in \mathcal{D}(\mathbb{C}_A\otimes\mathbb{C}_B)$ the quantum discord over measurements on both systems is:*

$$D(A:B)_{\rho_{AB}} = \min_{\mathcal{A}\otimes\mathcal{B}\in\mathcal{P}} \left\{ I(A:B)_{\rho_{AB}} - I(A:B)_{\mathcal{A}\otimes\mathcal{B}(\rho_{AB})} \right\}, \tag{60}$$

where $\mathcal{A}\in\mathcal{P}(\mathbb{C}_A,\mathbb{C}_Y)$ and $\mathcal{B}\in\mathcal{P}(\mathbb{C}_B,\mathbb{C}_X)$.

This generalization of quantum discord was first discussed in [46] in the context of the non-local-broadcast theorem. This definition is often named WPM-discord, because it was also studied by Wu et al. [47]. It was also studied restricting to projective measurements by some authors [48, 49].

3.2.3. Relative entropy of quantumness and work deficit

For a given dephasing channel $\Pi \in \mathcal{P}\left(\mathbb{C}^N\right)$, acting on any state $\rho \in \mathcal{D}\left(\mathbb{C}^N\right)$, the support of the dephased state contains the support of the input state: supp(ρ) ⊆ supp($\Pi[\rho]$); therefore, the measure of quantumness of correlations based on the relative entropy remains finite for every composed state [23, 31].

Suppose Alice and Bob have a common composed system described by the state $\rho_{AB} \in \mathcal{D}(\mathbb{C}_A \otimes \mathbb{C}_B)$, they would like to extract work from this system. To accomplish their task, they can perform the *closed set of local operations and classical communication* (CLOCC). This class of operations is composed of: (i) addition of pure ancillas, (ii) local unitary operations and (iii) local dephasing channels. Classical communication is represented by a local dephasing channel. If Alice and Bob are together in the same laboratory, they can extract work globally from the total system, then the total amount of information that Alice and Bob can extract from ρ_{AB} together is defined as the *total work* [12].

Definition 21. *The work that can be extracted from a quantum system, described by the state $\rho \in \mathcal{D}\left(\mathbb{C}^N\right)$, is defined as the change in the entropy:*

$$W_t(\rho) = \log_2 N - S(\rho), \tag{61}$$

$\log_2 N$ *is the entropy of the maximally mixed state, and $S(\rho)$ is the von Neumann entropy of the state.*

This function can be interpreted as a quantifier of information, such that if the state is a maximally mixed state no information can be extracted from it. Therefore, if the state is a pure state, we have the maximum amount of information [12, 50]. The entropy function represents the amount of information that one *can get to know* about the system; therefore, the function Eq. (61) represents the amount of information that one *already knows*. On the other hand, if Alice and Bob cannot be in the same laboratory, the information that can be extracted from the total state is restricted to be locally accessed. In the same way, it is possible to define the total information, named *local work*. Then, Alice and Bob should perform CLOCC operation in order to obtain the maximal amount of local information [50]:

$$W_l(\rho_{AB}) = \log_2 N - \sup_{\Gamma \in CLOCC} S(\Gamma[\rho_{AB}]), \tag{62}$$

where the state $\Gamma(\rho_{AB})$ is the state after the protocol. As CLOCC consist in sending one part of the state in a dephasing channel, at the end of the protocol, the whole state is with the receiver: $\Gamma(\rho_{AB}) = \rho_{AA}$.

One can be interested in the amount of information that cannot be extracted locally by Alice and Bob. This function is named *work deficit* and it quantifies the amount of work that is not possible to extract locally [12].

Definition 22. *Given a bipartite state ρ_{AB}, the information which two parts Alice and Bob cannot access, via CLOCC, is the work deficit:*

$$\Delta(\rho_{AB}) = W_t(\rho_{AB}) - W_l(\rho_{AB}). \tag{63}$$

From the definition of the total work and the local work, we can define the work deficit as the diference of them:

$$\Delta(\rho_{AB}) = \inf_{\Gamma \in CLOCC} \{S(\Gamma[\rho_{AB}]) - S(\rho_{AB})\}. \tag{64}$$

Even though the total and the local work depend explicitly on the dimension of the system, the work deficit should not depend on the dimension of $\Gamma[\rho_{AB}]$. Adding local pure ancillas belongs to the CLOCC cannot change the amount of work deficit. The work deficit can quantify quantum correlations, then it must not change by the simple addition of a uncorrelated system [16, 50].

In the asymptotic limit (the limit of many copies), the work deficit quantifies the amount of pure states that can be extracted locally [51, 52]. However, as a resource cannot be created freely, the addition of pure local ancillas is not allowed, then it is replaced by the addition of maximally mixed states. The set of operations that contains: (i) addition of maximally mixture states, (ii) local unitary operations and (iii) local dephasing channels, is named *noise local operations and classical communication* (NLOCC) [51]. The extraction of local pure states is a protocol, whose goal is to extract resource (coherence). The set of available operations are NLOCC operations, and the set of free resource states is composed only by the maximally mixture state. It is the only state without local purity [53]. It remains an open question if the CLOCC class and the NLOCC class are equivalent classes [50].

In the limit of one copy, the work deficit can quantify quantum correlations present in a given composed system [54]. The scenario where Alice and Bob can perform many steps of classical communication one each other is named *two way*, and the work deficit is named *two-way work deficit*. In this case, they can perform measurements and communicate in each step of the protocol. Mathematically, the two-way work deficit does not have a closed expression [50]. As discussed above, it is possible to activate quantum correlations performing operations on the measured system. Therefore, this many step scenario cannot quantify quantum correlations. Because if Alice and Bob can implement a sequence of non-commuting dephasing channels, the only invariante state is the maximally mixed state. In this way, it is necessary a one round description, where Alice and Bob can communicate at the end of the protocol. Following this idea, it is possible to define the *one-way work deficit*, which just one side can communicate. If Bob communicates to Alice, the state created at the end of the protocol is a quantum-classical state (or a classical-quantum state if Alice communicates at the end of the protocol).

Definition 23 (one-way work deficit). *Given a bipartite state ρ_{AB}, the work deficit with just one side communication is named one-way work deficit* [12]:

$$\Delta^{\rightarrow}(\rho_{AB}) = \min_{\Pi_B \in \mathcal{P}} \{S(\mathbb{I}_A \otimes \Pi_B[\rho_{AB}]) - S(\rho_{AB})\}, \tag{65}$$

where $\Pi_B \in \mathcal{P}(\mathbb{C}_B)$ is a local dephasing on subsystem B. The notation $\Delta^{\rightarrow}(\rho_{AB})$ means that the communication is from A to B and $\Delta^{\leftarrow}(\rho_{AB})$ in the opposite direction.

Another definition for the work deficit is defined when both Alice and Bob communicate at the end of the protocol, this is named *zero-way work deficit*. The state created at the end of the protocol is a classical-classical state.

Definition 24 (zero-way work deficit). *Given a bipartite state ρ_{AB}, the work deficit with no communication until the end of the protocol is named zero work deficit* [12]:

$$\Delta^{\varnothing}(\rho_{AB}) = \min_{\Pi_A \otimes \Pi_B \in \mathcal{P}} \{S(\Pi_A \otimes \Pi_B[\rho_{AB}]) - S(\rho_{AB})\}, \tag{66}$$

where $\Pi_A \otimes \Pi_B \in \mathcal{P}(\mathbb{C}_A \otimes \mathbb{C}_B)$ is a local dephasing on subsystems A and B.

In analogy with the work deficit, Modi et al. proposed a measure of quantumness of correlation defined as the relative entropy of the state and the set of classical correlated states [16]. This measure is named *relative entropy of quantumness*.

Definition 25 (relative entropy of quantumness). *The relative entropy of quantumness $D(\rho_{AB})_{QC}$ for a given state ρ_{AB} is defined as the minimum relative entropy over the set of quantum-classical states* [16]:

$$D(\rho_{AB})_{QC} = \min_{\xi_{AB} \in \Omega_{QC}} S(\rho_{AB} \| \xi_{AB}), \tag{67}$$

where Ω_{QC} is the set of quantum-classical states.

The relative entropy of quantumness for classical-classical states is denoted as $D(\rho_{AB})_{CC}$. It is analogous to Eq. (67) when the optimization is taken over the set of classical-classical states Ω_{CC}:

$$D(\rho_{AB})_{CC} = \min_{\xi_{AB} \in \Omega_{CC}} S(\rho_{AB} \| \xi_{AB}). \tag{68}$$

As discussed previously, in the limit of one copy, the one-way and the zero-way work deficits quantify quantumness of correlations of the system. It is possible to obtain the equivalence between one-way work deficit and relative entropy of quantumness.

Theorem 26. *The one-way work deficit is equal to the relative entropy of quantumness for quantum-classical states* [16, 50]:

$$D(\rho_{AB})_{QC} = \Delta^{\rightarrow}(\rho_{AB}), \tag{69}$$

The same equivalence holds for zero-way work deficit and the relative entropy of quantumness of classical-classical states:

$$D(\rho_{AB})_{CC} = \Delta^{\varnothing}(\rho_{AB}). \tag{70}$$

The one-way and zero-way work deficits quantify quantumness correlations beyond the quantum entanglement; therefore, we should be able to compare these two classes of quantum correlations. For the relative entropy, this comparison is natural of the fact that CLOCC is a subclass of LOCC operations, which naturally implies that [12]:

$$\Delta(\rho) \geq E_r(\rho), \tag{71}$$

where $\Delta(\rho)$ is the work deficit and $E_r(\rho)$ is the relative entropy of entanglement. The equality is attached for bipartite pure states: $|\psi\rangle_{AB} \in \mathbb{C}_A \otimes \mathbb{C}_B$:

$$\Delta(\Psi_{AB}) = E_r(\Psi_{AB}) = S(\rho_A), \tag{72}$$

where $\Psi_{AB} = |\psi\rangle\langle\psi|_{AB}$. An interesting corollary of this proposition is that the quantum discord is equal to the work deficit for pure states, because it is also equal to the entropy of entanglement for pure states.

In this section, the concept of local disturbance was introduced by the definition of the work deficit. That is the smallest relative entropy between the state and its local disturbed version (obtained performing a local dephasing channel on the state). Indeed there are many other local disturbance quantumness of correlation quantifiers, which can be obtained defining a quantum state discrimination measure, for example, Bures distance [55], Schatten p-norm [17], trace distance [56] and Hilbert-Schmidt distance [15, 57].

4. Monogamy relation: entanglement, classical correlations and quantumness of correlations

Given a bipartite system $\rho_{AB} \in \mathcal{D}(\mathbb{C}_A \otimes \mathbb{C}_B)$, then it is possible to purify the state in a larger space $\mathbb{C}_{ABE}$ of the dimension: $\dim(\mathbb{C}_{ABE}) = \dim(A) \cdot \dim(B) \cdot \mathrm{rank}(\rho_{AB})$. The purification process creates quantum correlations between the system AB and the purification system E, unless the state is already pure. Intrinsically, there is a restriction in the amount of correlations that can be shared by the systems. This balance between the correlations for tripartite states can be understood by the Koashi-Winter relation.

Given the definition of the classical correlations for a bipartite state ρ_{AB}:

$$J(A:B)_{\rho_{AB}} = \max_{\mathbb{I}\otimes\ \in \mathcal{P}} I(A:X)_{\mathbb{I}\otimes\boxplus\rho_{AB})}, \tag{73}$$

where $I(A:X)_{\mathbb{I}\otimes\boxplus\rho_{AB}})$ is the mutual information of the post-measured state $\mathbb{I}\otimes\boxplus\rho_{AB})$, and the optimization is taken over all local POVM measurement maps $\in \mathcal{P}(\mathbb{C}_B, BC_X)$.

Given also the definition of the entanglement of formation of a bipartite state ρ_{AB}:

$$E_f(\rho_{AB}) = \min_{\xi_\rho = \{p_i, |\psi_i\rangle\langle\psi_i|\}_i} \sum_i p_i E(|\psi_i\rangle), \tag{74}$$

where the optimization is taken over all possible convex hull defined by the ensemble $\xi = \{p_i, |\psi_i\rangle\langle\psi_i|\}_i$, such that $\rho_{AB} = \sum_i p_i, |\psi_i\rangle\langle\psi_i|$, and $E(|\psi_i\rangle)$ is the entropy of entanglement of $|\psi_i\rangle$.

Theorem 27 (Koashi-Winter relation). *Considering* $\rho_{ABE} \in \mathcal{D}(\mathbb{C}_A \otimes \mathbb{C}_B \otimes \mathbb{C}_E)$ *a pure state then:*

$$J(A:E)_{\rho_{AE}} = S(\rho_A) - E_f(\rho_{AB}), \tag{75}$$

where $\rho_X = Tr_Y[\rho_{YX}]$.

Proof. Suppose $\rho_{AB} = \sum_i p_i | \psi_i\rangle\langle\psi_i |$ is the optimum convex combination, such that $E_f(\rho_{AB}) = \sum_i p_i S(Tr_B[|\psi_i\rangle\langle\psi_i|])$. The classical correlations in system AE relates this decomposition with a measurement on the subsystem E. Therefore, there exists a measurement $\left\{M_j^E\right\}$ on system E such that $\rho'_{ABE} = \sum_j Tr_E\left[\rho_{ABE}\left(\mathbb{I}_{AB} \otimes M_j^E\right)\right] \otimes |e_j\rangle\langle e_j|_E$ and $Tr_E\left[\rho'_{ABE}\right] = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. Tracing over subsystem B, then the post-measurement state will be:

$$\rho'_{AE} = \sum_j p_j Tr_B\left[\left|\psi_j\right\rangle\left\langle\psi_j\right|\right] \otimes |e_j\rangle\langle e_j|, \tag{76}$$

In this way, the mutual information of the post-measurement state:

$$I(A:E)_{\rho'_{AE}} = S(\rho_A) + S(\rho'_E) - S(\rho'_{AE}), \tag{77}$$

$$= S(\rho_A) + H(E) - H(E) - \sum_i p_i S\left(Tr_A\left[\left|\psi_j\right\rangle\left\langle\psi_j\right|\right]\right), \tag{78}$$

$$= S(\rho_A) - \sum_i p_i S\left(Tr_A\left[\left|\psi_j\right\rangle\left\langle\psi_j\right|\right]\right), \tag{79}$$

$$= S(\rho_A) - E_f(\rho_{AB}), \tag{80}$$

It was used as the property of the Shannon entropy for a block diagonal state, where

$Tr_B[|\psi_j\rangle\langle\psi_j|] = Tr_A[|\psi_j\rangle\langle\psi_j|]$ and $E_f(\rho_{AB}) = \sum_i p_i S(Tr_B[|\psi_i\rangle\langle\psi_i|])$. By definition $J(A:E)_{\rho_{AE}} \geq I$ $_{(A:E)\rho'_{AE}}$, then

$$J(A:E)_{\rho_{AE}} \geq S(\rho_A) - E_f(\rho_{AB}). \tag{81}$$

Now, it is proved the converse inequality. Given ρ_{AE}, there exists a POVM $\mathcal{M} \in \mathcal{P}(\mathbb{C}_E, \mathbb{C}_{E'})$ with rank-1 elements $\{M_l\}$, such that $Tr_E\left[M_l\rho_{AE}\right] = q_l\rho_l^A$ that optimizes the classical correlations $J(\rho_{AE}) = S(\rho_A) - \sum_l q_l S(\rho_l^A)$. As the elements of the POVM are rank-1, $M_l = |\mu_l\rangle\langle\mu_l|$, and the state ρ_{ABE} is pure, the state after local measurement on E will be described by an ensemble of pure states:

$$\rho'_{ABE} = \sum_l Tr_E\left[\rho_{ABE}\left(\mathbb{I}_{AB} \otimes |\mu_l\rangle\langle\mu_l|\right)\right] \otimes |e_l\rangle\langle e_l| = \sum q_l |\phi_l\rangle\langle\phi_l| \otimes |e_l\rangle\langle e_l|. \tag{82}$$

Once that $\rho_{ABE} = |\kappa\rangle\langle\kappa|_{ABE}$, and the pure state can be written in the bipartite Schmidt decomposition $|\kappa\rangle = \sum_n c_n |n\rangle_{AB} \otimes |n\rangle_E$, if $\langle\mu_l|n\rangle = r_{ln}$, it is easy to see that:

$$Tr_E\left[\rho_{ABE}(\mathbb{I}_{AB}\otimes|\mu_l\rangle\langle\mu_l|)\right]=\sum_{ij}c_i r_{li} c_j r_{lj}^*|i\rangle\langle j|_{AB}=\left(\sum_i c_i r_{li}|i\rangle_{AB}\right)\left(\sum_j c_j r_{lj}^*\langle j|_{AB}\right)=q_l|\phi_l\rangle\langle\phi_l|. \tag{83}$$

Calculating the mutual information of $\rho'_{AE}=Tr_B\left[\rho'_{ABE}\right]$:

$$I(A:E)_{\rho'_{AE}}=S(\rho_A)-\sum_l q_l S\left(Tr_B\left[|\phi_l\rangle\langle\phi_l|\right]\right), \tag{84}$$

As the POVM $\mathcal{M}$ is the optimal measurement in the calculation of the classical correlations, it implies $I(A:E)_{\rho'_{AE}}=J(A:E)_{\rho_{AE}}$. By definition, the entanglement of formation satisfies: $E_f(\rho_{AB})\le\sum_l q_l S(Tr_B[|\phi_l\rangle\langle\phi_l|])$ for any decomposition $\{p_l,|\phi_l\rangle\langle\phi_l|\}$. Substituting the mutual information in Eq. (84):

$$J(A:E)_{\rho_{AE}}\le S(\rho_A)-E_f(\rho_{AB}). \tag{85}$$

Given Eqs. (81) and (85), it proves the theorem.

The Koashi-Winter equation quantifies the amount of entanglement among A and B, considering that the former is classically correlated with another system C. This property is interesting once that it is related to the monogamy of entanglement [58], where the amount of entanglement shared by three parts is limited, and this limitation is given by the amount of classical correlations among the parties. This limitation holds for any tripartite state as stated in the following corollary:

Corollary 28. *For any tripartite state $\rho_{ABC}\in\mathcal{D}(\mathbb{C}_A\otimes\mathbb{C}_B\otimes\mathbb{C}_C)$, it follows:*

$$E_f(\rho_{AB})+J(A:C)_{\rho_{AC}}\le S(\rho_A). \tag{86}$$

The equality holds for ρ_{ABC} pure.

Proof. If ρ_{ABC} is not a pure state, there exists a purification ρ_{ABCE}, then $\mathbb{C}_A\otimes\mathbb{C}_B\otimes\mathbb{C}_{CE}$, followed by the last theorem:

$$J(A:CE)_{\rho_{ACE}}+E_f(\rho_{AB})=S(\rho_A), \tag{87}$$

Therefore, as the classical correlations are monotonic under local maps, then taking the trace over the system E we have $J(A:CE)_{\rho_{ACE}}\ge J(A:C)_{\rho_{AC}}$.

As the Shannon entropy of ρ_A represents the effective size of A in qubits [24], this size can be approached as the capacity of the system A makes correlations with other systems B and C [18]. In other words, this means that the existence of the quantum or classical correlations between A and another system B is enough to restrict the amount of quantum or classical correlations which A can make with a third system C.

Summing the mutual information $I(A:E)_{\rho_{AE}}$ on both sides of the Koashi-Winter relation, Eq. (75), it is possible to obtain a monogamy expression for the entanglement of formation of the state ρ_{AB} in function of the quantum discord [19]:

$$D(A:E)_{\rho_{AE}} = E_f(\rho_{AB}) - S(A|E)_{\rho_{AE}}, \tag{88}$$

where $D(A:E)_{\rho_{AE}}$ is the quantum discord of the state ρ_{AE} with local measurement on the subsystem E and $S(A|E)_{\rho_{AE}} = S(AE) - S(E)$ is the conditional entropy. As the label in the states is arbitrary, we can rewrite this expression changing the labels $E \rightarrow B$ and vice versa to obtain $D(A:B)_{\rho_{AB}} = S(A|B)_{\rho_{AB}} - E_f(\rho_{AE})$, taking the sum between this and Eq. (88):

$$D(A:E)_{\rho_{AE}} + D(A:B)_{\rho_{AB}} = E_f(\rho_{AE}) + E_f(\rho_{AB}), \tag{89}$$

as the total state is pure $S(A|E)_{\rho_{AE}} = -S(A|B)_{\rho_{AB}}$. This expression means that the sum of total amount of entanglement that A shares with B and E is equal to the sum of the amount of quantum discord shared with B and E [19].

From Eq. 88, it is possible to calculate an interesting expression, which relates the irreversibility of the entanglement distillation protocol and quantum discord [20]. As discussed, the entanglement cost is larger than the distillable entanglement. Given the entanglement cost defined as the regularization of the entanglement of formation [4]:

Definition 29. *For a mixed state $\rho_{AB} \in \mathcal{D}(\mathbb{C}_A \otimes \mathbb{C}_B)$, the regularization of the entanglement of formation $E_f(\rho_{AB})$ results in the entanglement cost:*

$$E_C(\rho_{AB}) = \lim_{n\to\infty} \frac{1}{n} E_f(\rho_{AB}^{\otimes n}). \tag{90}$$

The Hashing inequality says that the distillable entanglement of ρ_{AB} is lower bounded by the coherent information $I(A\rangle B)_{\rho_{AB}} = -S(A|B)$ [3]. As the coherent information can increase under LOCC, it is possible to optimize it under LOCC attaining the distillable entanglement [3].

Definition 30. *The regularized coherent information after optimization over LOCC for a mixed state ρ_{AB} gives the distillable entanglement:*

$$E_D(\rho_{AB}) = \lim_{n\to\infty} \frac{1}{n} I(A\rangle B)_{(V_n \otimes \mathbb{I})\rho_{AB}^{\otimes n}}, \tag{91}$$

where $V_n \otimes \mathbb{I}$ acts locally on the n copies of ρ_{AB}.

It is also possible to define the regularized quantum discord:

Definition 31. *The regularized quantum discord can be defined as the quantum discord of a state ρ_{AB} in the limit of many copies:*

$$D^{\infty}(A:B)_{\rho_{AB}} = \lim_{n\to\infty}\frac{1}{n}D(A:B)_{\rho_{AB}^{\otimes n}}. \tag{92}$$

Therefore, similarly to Eq. (88) in the limit of many copies:

$$D(A:E)_{\rho_{AE}^{\otimes n}} = E_f\left(\rho_{AB}^{\otimes n}\right) - S(A|E)_{\rho_{AE}^{\otimes n}}, \tag{93}$$

taking the regularization we have:

$$D^{\infty}(A:E)_{\rho_{AE}} = E_C\left(\rho_{AB}\right) - S(A|E)_{\rho_{AE}}, \tag{94}$$

as the conditional entropy is additive $S(A|E)_{\rho_{AE}^{\otimes n}} = nS(A|E)_{\rho_{AE}}$. Therefore, the following theorem comes from Eq. (88).

Theorem 32 (Cornelio et al. [20]). *For every mixed entangled state ρ_{AB}, if*

$$E_D\left(\rho_{AB}\right) = \frac{1}{n}I(A\rangle B)_{(V_n\otimes\mathbb{I})\rho_{AB}^{\otimes n}} \tag{95}$$

$$E_C\left(\rho_{AB}\right) = \frac{1}{k}E_F\left(\rho_{AB}^{\otimes n}\right), \tag{96}$$

for a finite number of n and k, the entanglement is irreversible $E_C(\rho_{AB}) > E_D(\rho_{AB})$.

Taking the limit of many copies, the equation can be rewritten as:

$$D^{\infty}(A:E)_{\sigma_{AE}} = E_C(\sigma_{AB}) - E_D(\sigma_{AB}), \tag{97}$$

where $\sigma_{AB} = (V_k\otimes\mathbb{I})\rho_{AB}$ and $E_D(\sigma_{AB}) = kE_D(\rho_{AB})$. The quantum discord $D^{\infty}(A:E)_{\sigma_{AE}}$ in this context can be viewed as the minimal amount of entanglement lost in the distillation protocol, for states belonging to the class described in the theorem [20]. This expression has an operational interpretation for quantum discord, where the quantum discord between the system and the purification system restricts the amount of e-bits lost in the distillation process. A consequence of this result is expressed by the state merging protocol [27], Alice (A), Bob (B) and the Environment (E) share a pure tripartite state ρ_{ABE}, she would like to send her state to Bob, keeping the coherence with the system E. They can perform this protocol consuming an amount of entanglement in the process; the amount of entanglement is the regularized quantum discord $D^{\infty}(A:E)_{\rho_{AE}}$ [25, 26].

In addition to the above relations, some upper and lower bounds between quantum discord and entanglement of formation have been calculated via the Koashi-Winter relation and the properties of entropy [59–62]. Equation (88) was also used to calculate the quantum discord and the entanglement of formation analytically for systems with rank-2 and dimension 2 ⊗ n [41, 63, 64]. Experimental investigations of Eq. (88) were performed in the characterization of the information flow between system and environment of a non-Markovian process [65].

5. Activation protocol

Physically, a measurement process can be described as an interaction between the measurement apparatus and the system, followed by a projective measurement on the apparatus. Consider a state $\rho_{\mathcal{S}} = \sum_k \lambda_k |k\rangle\langle k| \in \mathcal{D}(\mathbb{C}_{\mathcal{S}})$. The input state is described as $\rho_{\mathcal{S}:\mathcal{M}} = \rho_{\mathcal{S}} \otimes |0\rangle\langle 0|_{\mathcal{M}}$, by coupling a pure ancilla, that represents the measurement apparatus. The interaction between the system and the ancillary state is performed by a unitary evolution: $U_{\mathcal{S}:\mathcal{M}} \in \mathcal{U}(\mathbb{C}_{\mathcal{S}} \otimes \mathbb{C}_{\mathcal{M}})$, such that $Tr_{\mathcal{M}}\left[U_{\mathcal{S}:\mathcal{M}}\rho_{\mathcal{S}:\mathcal{M}}U^{\dagger}_{\mathcal{S}:\mathcal{M}}\right] = \sum_l \Pi_l \rho_{\mathcal{S}} \Pi_l^{\dagger}$. A unitary operation satisfying this condition is given by:

$$U_{\mathcal{S}:\mathcal{M}}|k\rangle_{\mathcal{S}}|0\rangle_{\mathcal{M}} = |k\rangle_{\mathcal{S}}|k\rangle_{\mathcal{M}}, \tag{98}$$

where $\{|k\rangle\}$ is an orthonormal basis in $\mathbb{C}_{\mathcal{S}}$. If the orthogonal basis $\{|k\rangle\langle k|\}$ is the canonical basis, this interaction is a Cnot gate [1]. Therefore, after the interaction, the state will be:

$$\tilde{\rho}_{\mathcal{S}:\mathcal{M}} = U_{\mathcal{S}:\mathcal{M}}(\rho_{\mathcal{S}:\mathcal{M}})U^{\dagger}_{\mathcal{S}:\mathcal{M}} = \sum_k \lambda_k |k\rangle\langle k|_{\mathcal{S}} \otimes |k\rangle\langle k|_{\mathcal{M}}. \tag{99}$$

The interaction between the system and the measurement apparatus results in a classically correlated state between the system and the apparatus. Hence performing a projective measurement on the state of the apparatus, the state of the system can be recovered.

Suppose now that the state of the system is composed, for example a bipartite system $\mathbb{C}_{\mathcal{S}} = \mathbb{C}_A \otimes \mathbb{C}_B$. The measurements are performed locally in each system; therefore, the ancilla is also a bipartite system $\mathbb{C}_{\mathcal{M}} = \mathbb{C}_{\mathcal{M}_A} \otimes \mathbb{C}_{\mathcal{M}_B}$. The unitary operator representing the interaction between the system and the measurement apparatus is $U_{\mathcal{S}:\mathcal{M}} = U_{A:\mathcal{M}_A} \otimes U_{B:\mathcal{M}_B}$. Then, the post-measured state is:

$$\tilde{\rho}_{\mathcal{S}} = Tr_{\mathcal{M}}\left[U_{\mathcal{S}:\mathcal{M}}(\rho_{\mathcal{S}} \otimes |0\rangle\langle 0|)U^{\dagger}_{\mathcal{S}:\mathcal{M}}\right] = \sum_{k,l} \Pi_k^A \otimes \Pi_l^B \rho_{AB} \Pi_k^{\dagger A} \otimes \Pi_l^{\dagger B}. \tag{100}$$

As aforementioned, the measurement process consists in interacting the system with an ancilla, which represents the measurement apparatus, and then perform a projective measurement over the ancilla. However, as the dimension of the ancilla is arbitrary, to represent a general measurement (POVM), it is necessary to couple another ancilla with the same size of the state: $\rho_{\mathcal{S}':\mathcal{M}} = \rho_{\mathcal{S}} \otimes |0\rangle\langle 0|_{\mathcal{E}} \otimes |0\rangle\langle 0|_{\mathcal{M}}$, where $|0\rangle\langle 0|_{\mathcal{E}}$ is an ancillary state on space $\mathbb{C}_{\mathcal{E}}$. Then, the interaction with the apparatus, given by a unitary evolution $U_{\mathcal{S}':\mathcal{M}}$, results in the post-measured state

$$\tilde{\rho}_{\mathcal{S}} = Tr_{\mathcal{M}}\left[U_{\mathcal{S}':\mathcal{M}}\rho_{\mathcal{S}':\mathcal{M}}U^{\dagger}_{\mathcal{S}':\mathcal{M}}\right] = \sum_l \Pi_l(\rho_{\mathcal{S}} \otimes |0\rangle\langle 0|_{\mathcal{E}})\Pi_l. \tag{101}$$

By the Naimark's theorem $Tr\left[\Pi_l(\rho_{\mathcal{S}} \otimes |0\rangle\langle 0|_{\mathcal{E}})\right] = Tr\left[E_l \rho_{\mathcal{S}}\right]$, where $E_l = (\mathbb{I} \otimes \langle 0|)\Pi_l(\mathbb{I} \otimes |0\rangle)$ is a element of a POVM.

A general bipartite state can be written as $\rho = \sum_{i,j}|i\rangle\langle j| \otimes O_{i,j}$, where $O_{i,j}$ is an Hermitian operator with trace different from zero. Then if the measurement is performed only on the subsystem A, the state $\tilde{\rho}_{\mathcal{S}:\mathcal{M}}$ after the interaction with the measurement apparatus will be:

$$\tilde{\rho}_{\mathcal{S}:\mathcal{M}} = U_{\mathcal{S}:\mathcal{M}}(\rho_{\mathcal{S}:\mathcal{M}})U^{\dagger}_{\mathcal{S}:\mathcal{M}} \tag{102}$$

$$= U_{A:\mathcal{M}_A} \otimes \mathbb{I}_B \left(\sum_{i,j}|i\rangle\langle j|_A \otimes |0\rangle\langle 0|_{\mathcal{M}_A} \otimes O^B_{i,j}\right) U^{\dagger}_{A:\mathcal{M}_A} \otimes \mathbb{I}_B \tag{103}$$

$$= \sum_{i,j}|i\rangle\langle j|_A \otimes |i\rangle\langle j|_{\mathcal{M}_A} \otimes O^B_{i,j}. \tag{104}$$

Differently of the global measurement process, for local measurements, entanglement can be created during the measurement process. For example, if $O_{ij} = \frac{1}{2}|i\rangle\langle j|$, the interaction with the measurement apparatus creates a maximally entangle state. different from the case where the measurement is performed on the A quantum state cannot create quantum entanglement with the measurement apparatus, if it is classically correlated. As proved in the following theorem.

Theorem 33 ([21, 22]). *A state is classically correlated (has no quantumness of correlations), if and only if there exists an unitary operation such that the post interaction state is separable with respect to system and measurement apparatus.*

Proof. The proof is performed for the general case, for measurements on both systems.

If: If the state is classically correlated:

$$\rho_{\mathcal{S}} = \sum_{k,j} p_{k,j}|a_k, b_j\rangle\langle a_k, b_j|_{\mathcal{S}}, \tag{105}$$

the state after the interaction with the measurement apparatus represented by the unitary operation $U_{A:\mathcal{M}_A} \otimes U_{B:\mathcal{M}_B}$ will be:

$$\tilde{\rho}_{\mathcal{S}:\mathcal{M}} = \sum_{k,j} p_{k,j}|a_k, b_j\rangle\langle a_k, b_j|_{\mathcal{S}} \otimes |a_k, b_j\rangle\langle a_k, b_j|_{\mathcal{M}}, \tag{106}$$

which is clearly separable.

Only if: Given a general separable state between the system and the measurement apparatus:

$$\tilde{\rho}_{\mathcal{S}:\mathcal{M}} = \sum_{\alpha} p_\alpha|\phi_\alpha\rangle\langle\phi_\alpha|_{\mathcal{S}} \otimes |\psi_\alpha\rangle\langle\psi_\alpha|_{\mathcal{M}}, \tag{107}$$

and the fact that the interaction is unitary, there is a convex combination such that $\rho_{\mathcal{S}} = \sum_\alpha p_\alpha|\kappa_\alpha\rangle\langle\kappa_\alpha|$; therefore, the interaction must act in the following way:

$$U_{\mathcal{S}:\mathcal{M}}|\kappa_\alpha\rangle|0\rangle = |\phi_\alpha\rangle|\psi_\alpha\rangle. \tag{108}$$

On the other hand, as the state $\rho_{\mathcal{S}}$ is bipartite, the pure states $\{|\kappa_\alpha\rangle\}$ can be written in general as: $|\kappa_\alpha\rangle = \sum_{l,i} c_{l,i}^{\alpha} |a_l^{\alpha}\rangle |b_i^{\alpha}\rangle$, and after the interaction, the states will be:

$$U_{\mathcal{S}:\mathcal{M}} |\kappa_\alpha\rangle |0\rangle = \sum_{l,j} c_{l,j}^{\alpha} \left| a_l^{\alpha}, b_j^{\alpha} \right\rangle_{\mathcal{S}} \otimes \left| a_l^{\alpha}, b_j^{\alpha} \right\rangle_{\mathcal{M}}. \tag{109}$$

As the state in Eq. (109) must be separable, it implies that the coefficients must satisfy:

$$c_{i,j}^{\alpha} = c_{f(\alpha)} \delta_{i,j;f(\alpha)} \quad \text{and} \quad |c_{f(\alpha)}| = 1 \tag{110}$$

where $f(\alpha) \in \mathbb{N}^2$. As $f(\alpha)$ are orthogonal, it proves the theorem.

If the state of the system has quantum correlations, the local measurement process creates entanglement between the system and the measurement apparatus, for a every unitary interaction. Then, it is possible to fix the base of the ancilla and change the base of the system. Then, rewriting the evolution as $U_{\mathcal{S}:\mathcal{M}} = C_{\mathcal{S}:\mathcal{M}}(U_{\mathcal{S}} \otimes \mathbb{I}_{\mathcal{M}})$, where for bipartite systems $U_{\mathcal{M}} = U_A \otimes U_B$ is a local unitary operation and $C_{\mathcal{S}:\mathcal{M}} = C_{A:\mathcal{M}_A} \otimes C_{B:\mathcal{M}_B}$ is a Cnot gate acting on the system as the control, and the apparatus as the target. It is possible to quantify the amount of quantum correlation in a given system starting on the amount of entanglement created with the measurement apparatus.

Definition 34 ([21, 22]). *Each measure of entanglement used to quantify the entanglement between the system and the apparatus will result in a measure of quantumness of correlations.*

$$Q_E(\rho_{\mathcal{S}}) = \min_{U_{\mathcal{S}}} E_Q(\rho_{\mathcal{S}:\mathcal{M}}). \tag{111}$$

Different entanglement measures will lead, in principle, to different quantifiers for the quantumness of correlations. The only requirement is that the entanglement measure must be an entanglement monotone [21, 22, 66]. Some quantifiers of quantumness of correlations can be recovered with the activation protocol: the quantum discord [22], one-way work deficit [22], zero-way work deficit [21] and the geometrical measure of discord via trace norm [66], are some examples. Taking the distillable entanglement in Eq. (111) is quite simple to see that it results in zero-way work deficit. As shown in Eq. (106), the interaction with the measurement apparatus results in the state

$$\tilde{\rho}_{\mathcal{S}:\mathcal{M}} = \sum_{k,j} p_{k,j} |a_k, b_j\rangle\langle a_k, b_j|_{\mathcal{S}} \otimes |a_k, b_j\rangle\langle a_k, b_j|_{\mathcal{M}}. \tag{112}$$

That is named *maximally correlated state*, and as showed in Ref.[67], the distillable entanglement of this state attach the Hashing inequality [68]:

$$E_D(\tilde{\rho}_{\mathcal{S}:\mathcal{M}}) = -S(\mathcal{S}|\mathcal{M}), \tag{113}$$

where $S(\mathcal{S}|\mathcal{M}) = S(\tilde{\rho}_{\mathcal{S}}) - S(\tilde{\rho}_{\mathcal{S}:\mathcal{M}})$ is conditional entropy of $\tilde{\rho}_{\mathcal{S}:\mathcal{M}}$. On the other hand, the zero-way work deficit for $\rho_{\mathcal{S}}$ is:

$$\Delta^{\varnothing}(\rho_{\mathcal{S}}) = \min_{\Pi_{\mathcal{S}_A} \otimes \Pi_{\mathcal{S}_B} \in \mathcal{P}} \{S(\Pi_{\mathcal{S}_A} \otimes \Pi_{\mathcal{S}_B}[\rho_{\mathcal{S}}]) - S(\rho_{\mathcal{S}})\}, \tag{114}$$

where $\Pi_{\mathcal{S}_A} \otimes \Pi_{\mathcal{S}_B} \in \mathcal{P}(\mathbb{C}_{\mathcal{S}_A} \otimes \mathbb{C}_{\mathcal{S}_B})$ is a local dephasing on subsystem A and B. As $\tilde{\rho}_{\mathcal{S}}$ is the measured state of the system and $\tilde{\rho}_{\mathcal{S}:\mathcal{M}} = U_{\mathcal{S}:\mathcal{M}} \rho_{\mathcal{S}:\mathcal{M}} U^{\dagger}_{\mathcal{S}:\mathcal{M}}$, then:

$$S(\tilde{\rho}_{\mathcal{S}}) - S(\tilde{\rho}_{\mathcal{S}:\mathcal{M}}) = S(\Pi_{\mathcal{S}_A} \otimes \Pi_{\mathcal{S}_B}[\rho_{\mathcal{S}}]) - S(\rho_{\mathcal{S}}).$$

Therefore:

$$\Delta^{\varnothing}(\rho_{\mathcal{S}}) = \min_{U_{\mathcal{M}}} E_D(\tilde{\rho}_{\mathcal{S}:\mathcal{M}}). \tag{115}$$

This equation means that the activation protocol creates distillable entanglement between the system and the measurement apparatus during a local measurement. In other words, quantumness of correlations of the system can be converted resource for quantum information protocol, and this conversion is ruled by the activation protocol.

From Eq. (111), it is possible to show that quantum entanglement is a lower bound for quantumness of correlations.

Proposition 35 (Piani and Adesso [66]). *For* $\rho_{AB} \in \mathcal{D}(\mathbb{C}_A \otimes \mathbb{C}_B)$:

$$Q_E(\rho_{AB}) \geq E_Q(\rho_{AB}), \tag{116}$$

where Q_E *and* E_Q *are related by Eq.* (111).

To compare two measures of different quantities as quantumness of correlation and quantum entanglement, it is necessary a common rule. The activation protocol gives the rule to compare these two quantities and this rule says that the measures of quantumness of correlations and quantum entanglement must be related from Eq. (111). Entanglement is a lower bound for quantumness of correlations also in the geometrical approach [17, 56].

Activation protocol determines that a composed state is classically correlated if and only if it cannot create entanglement during the measurement process, for a given unitary interaction [21, 22, 66]. This result provides an important tool for characterization of quantum correlations in identical particle systems (bosons and fermions), once that system and apparatus are distinguishable partitions, even if the particles in the system are identical. This approach have been applied to identical particles systems to prove how are the classically correlated states of bosons and fermions [69]. The activation protocol device also allows to determine the class of classically correlated states of the modes of a fermionic system and its relation to the correlations of the fermions [70].

The entanglement generation by means of quantumness of correlations, as stated by the activation protocol, was experimentally evidenced using programmable quantum measurement [71]. In the experiment setup, the optimization on the unitary operations was performed by a set of programable quantum measurements in different local basis. As quantumness of correlation can be generated by local operations [10], activation protocol was explored experimentally in the generation of distillable entanglement via local operations on the measured partition of the system [72].

6. Conclusion

This chapter leads to the fundamental aspects of quantum correlations: entanglement and quantumness of correlations. The purpose of this chapter is to demonstrate that quantumness of correlations plays an important role in entanglement resource theory and by consequence in quantum information theory. It was presented that entanglement and quantumness of correlations connect each other in two different pictures. The relation derived by Koashi and Winter demonstrates the balance between quantumness of correlations and entanglement in the purification process. This balance leads to a formal proof for the irreversibility of the entanglement distillation protocol, in terms of quantumness of correlations. Indeed in this fashion quantumness of correlations revealed to play the main role in the state merging protocol, quantifying the amount of entanglement consumed during the protocol. In the named *activation protocol*, the quantumness of correlations of a given composed system can be converted into distillable entanglement with a measurement apparatus during the local measurement process. In resume, the entanglement created by the interaction between the system and the measurement apparatus is limited below by the amount of quantumness of correlations of the system.

Acknowledgements

This work is supported by INCT-Quantum Information.

Author details

Tiago Debarba

Address all correspondence to: debarba@utfpr.edu.br

Universidade Tecnológica Federal do Paraná (UTFPR), Campus Cornélio Procópio, Cornélio Procópio, Paraná, Brazil

References

[1] Nielsen M, Chuang I. Quantum Computation and Quantum Information. Cambridge UK: Cambridge University Press; 2000. DOI: 10.1017/CBO9780511976667.001

[2] Horodecki R, Horodecki P, Horodecki M, Horodecki K. Quantum entanglement. Reviews of Modern Physics. 2009;**81**:865. DOI: 10.1103/RevModPhys.81.865

[3] Devetak I, Winter A. Distillation of secret key and entanglement from quantum states. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science. 2005a;**461**:207. DOI: 10.1098/rspa.2004.1372

[4] Hayden PM, Horodecki M, Terhal BM. The asymptotic entanglement cost of preparing a quantum state. Journal of Physics A: Mathematical and General. 2001;**34**:6891. DOI: 10.1088/0305-4470/34/35/314

[5] Bennett CH, Brassard G, Popescu S, Schumacher B, Smolin JA, Wootters WK. Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels. Physical Review Letters. 1996a;**76**:722. DOI: 10.1103/PhysRevLett.76.722

[6] Bennett CH, Brassard G, Crépeau C, Jozsa R, Peres A, Wootters WK. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Physical Review Letters. 1993;**70**:1895. DOI: 10.1103/PhysRevLett.70.1895

[7] Bennett CH, DiVincenzo DP, Smolin JA, Wootters WK. Mixed-state entanglement and quantum error correction. Physical Review A. 1996b;**54**:3824. DOI: 10.1103/PhysRevA.54.3824

[8] Bennett CH, Brassard G. Theoretical Computer Science. 2014;**560**,Part 1:7. ISSN 0304-3975, theoretical Aspects of Quantum Cryptography – celebrating 30 years of {BB84}. DOI: 10.1016/j.tcs.2014.05.025

[9] Abeyesinghe A, Devetak I, Hayden P, Winter A. The mother of all protocols: restructuring quantum information's family tree. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science. 2009;**465**:2537. DOI: 10.1098/rspa.2009.0202

[10] Ollivier H, Zurek WH. Quantum Discord: A Measure of the Quantumness of Correlations. Physical Review Letters. 2001;**88**:017901. DOI: 10.1103/PhysRevLett.88.017901

[11] Henderson L, Vedral V. Classical, quantum and total correlations. Journal of Physics A: Mathematical and General. 2001;**34**:6899. DOI: 10.1088/0305-4470/34/35/315

[12] Oppenheim J, Horodecki M, Horodecki P, Horodecki R. A Thermodynamical Approach to Quantifying Quantum Correlations. Physical Review Letters. 2002;**89**:180402. DOI: 10.1103/PhysRevLett.89.180402

[13] Luo S. Using measurement-induced disturbance to characterize correlations as classical or quantum. Physical Review A. 2008;**77**:022301. DOI: 10.1103/PhysRevA.77.022301

[14] Nakano T, Piani M, Adesso G. Negativity of quantumness and its interpretations. Physical Review A. 2013;**88**:012117. DOI: 10.1103/PhysRevA.88.012117

[15] Luo S, Fu S. Geometric measure of quantum discord. Physical Review A. 2010;**82**:034302. DOI: 10.1103/PhysRevA.82.034302

[16] Modi K, Paterek T, Son W, Vedral V, Williamson M. Unified View of Quantum and Classical Correlations. Physical Review Letters. 2010;**104**:080501. DOI: 10.1103/PhysRevLett.104.08 0501

[17] Debarba T, Maciel TO, Vianna RO. Witnessed entanglement and the geometric measure of quantum discord. Physical Review A. 2012;**86**:024302. DOI: 10.1103/PhysRevA.86.024302

[18] Koashi M, Winter A. Monogamy of entanglement and other correlations. Physical Review A. 2004;**69**:022309. DOI:10.1103/PhysRevA.69.022309

[19] Fanchini FF, Cornelio MF, de Oliveira MC, Caldeira AO. Conservation law for distributed entanglement of formation and quantum discord. Physical Review A. 2011;**84**:012313. DOI: 10.1103/PhysRevA.84.012313

[20] Cornelio MF, de Oliveira MC, Fanchini FF. Entanglement Irreversibility from Quantum Discord and Quantum Deficit. Physical Review Letters. 2011;**107**:020502. DOI: 10.1103/PhysRevLett.107.020502

[21] Piani M, Gharibian S, Adesso G, Calsamiglia J, Horodecki P, Winter A. All Nonclassical Correlations Can Be Activated into Distillable Entanglement. Physical Review Letters. 2011;**106**:220403. DOI: 10.1103/PhysRevLett.106.220403

[22] Streltsov A, Kampermann H, Bruß D. Linking Quantum Discord to Entanglement in a Measurement. Physical Review Letters. 2011;**106**:160401. DOI: 10.1103/PhysRevLett.106.160401

[23] Bengtsson I, Zyczkowski K. Geometry of Quantum States. Cambridge University Press; 2006. DOI: 10.1017/CBO9780511535048

[24] Schumacher B. Quantum coding. Physical Review A. 1995;**51**:2738. DOI: 10.1103/PhysevA.51.2738

[25] Cavalcanti D, Aolita L, Boixo S, Modi K, Piani M, Winter A. Operational interpretations of quantum discord. Physical Review A. 2011;**83**:032324. DOI: 10.1103/PhysRevA.83.032324

[26] Madhok V, Datta A. Interpreting quantum discord through quantum state merging. Physical Review A. 2011;**83**:032323. DOI: 10.1103/PhysRevA.83.032323

[27] Horodecki M, Oppenheim J, Winter A. Partial quantum information. Nature. 2005;**436**:673. DOI: 10.1038/nature03909

[28] Devetak I. The private classical capacity and quantum capacity of a quantum channel. Information Theory, IEEE Transactions on. 2005;**51**:44. DOI: 10.1109/TIT.2004.839515

[29] Lloyd S. Capacity of the noisy quantum channel. Physical Review A. 1997;**55**:1613. DOI: 10.1103/PhysRevA.55.1613

[30] Shor PW. The quantum channel capacity and coherent information. lecture notes, MSRI Workshop on Quantum Computation, 2002. Avaliable at http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/

[31] Wilde MM. Quantum Information Theory. Cambridge University Press; 2013. ISBN: 9781107034259

[32] Popescu S. Bell's inequalities versus teleportation: What is nonlocality? Physical Review Letters. 1994;**72**:797. DOI: 10.1103/PhysRevLett.72.797

[33] Popescu S. Bell's inequalities and density matrices. Revealing hidden nonlocality. Physical Review Letters. 1995;**74**:2619. DOI: 10.1103/PhysRevLett.74.2619

[34] Życzkowski K, Horodecki P, Sanpera A, Lewenstein M. Volume of the set of separable states. Physical Review A. 1998;**58**:883. DOI: 10.1103/PhysRevA.58.883

[35] Werner RF. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. Physical Review A. 1989;**40**:4277. DOI: 10.1103/PhysRevA.40.4277

[36] Wootters WK. Entanglement of Formation of an Arbitrary State of Two Qubits. Physical Review Letters. 1998;**80**:2245. DOI: 10.1103/PhysRevLett.80.2245

[37] Majtey A, Lamberti P, Prato D. Jensen-Shannon divergence as a measure of distinguishability between mixed quantum states. Physical Review A. 2005;**72**:052310. DOI: 10.1103/PhysRevA.72.052310

[38] Lin J. Divergence measures based on the Shannon entropy. Information Theory, IEEE Transactions on. 1991;**37**:145. DOI: 10.1109/18.61115

[39] Lamberti P, Majtey A, Borras A, Casas M, Plastino A. On the metric character of the quantum Jensen-Shannon divergence. Physical Review A. 2008;**77**:052311. DOI: 10.1103/PhysRevA.77.052311

[40] Ferraro A, Aolita L, Cavalcanti D, Cucchietti FM, Acin A. Almost all quantum states have nonclassical correlations. Physical Review A. 2010;**81**:052318. DOI: 10.1103/PhysRevA.81.052318

[41] Fanchini FF, Castelano LK, Cornelio MF, de Oliveira MC. Locally inaccessible information as a fundamental ingredient to quantum information. New Journal of Physics. 2012;**14**:013027. DOI: 10.1088/1367-2630/14/1/013027

[42] Huang Y. Computing quantum discord is NP-complete. New Journal of Physics. 2014;**16**:033027. DOI: 10.1088/1367-2630/16/3/033027

[43] Ali M, Rau ARP, Alber G. Quantum discord for two-qubit X states. Physical Review A. 2010;**81**:042105. DOI: 10.1103/PhysRevA.81.042105

[44] Girolami D, Adesso G. Quantum discord for general two–qubit states: Analytical progress. Physical Review A. 2011;**83**:052108. DOI: 10.1103/PhysRevA.83.052108

[45] Lu X-M, Ma J, Xi Z, Wang X. Optimal measurements to access classical correlations of two-qubit states. Physical Review A. 2011;**83**:012327. DOI: 10.1103/PhysRevA.83.012327

[46] Piani M, Horodecki P, Horodecki R. No-Local-Broadcasting Theorem for Multipartite Quantum Correlations. Physical Review Letters. 2008;**100**:090502. DOI: 10.1103/PhysRevLett.100.090502

[47] Wu S, Poulsen UV, Mølmer K. Correlations in local measurements on a quantum state, and complementarity as an explanation of nonclassicality. Physical Review A. 2009;**80**: 032319. DOI: 10.1103/PhysRevA.80.032319

[48] Girolami D, Paternostro M, Adesso G. Faithful nonclassicality indicators and extremal quantum correlations in two-qubit states. Journal of Physics A: Mathematical and Theoretical. 2011;**44**:352002. DOI: 10.1088/1751-8113/44/35/352002

[49] Rulli C, Sarandy M. Global quantum discord in multipartite systems. Physical Review A. 2011;**84**:042109. DOI: 10.1103/PhysRevA.84.042109

[50] Horodecki M, Horodecki P, Horodecki R, Oppenheim J, De A, Sen U, Synak-Radtke B. Local versus non-local information in quantum information theory: formalism and phenomena. Physical Review A. 2005;**71**:062307. DOI: 10.1103/PhysRevA.71.062307

[51] Horodecki M, Horodecki K, Horodecki P, Horodecki R, Oppenheim J, Sen(De) A, Sen U. Local Information as a Resource in Distributed Quantum Systems. Physical Review Letters. 2003;**90**:100402. DOI: 10.1103/PhysRevLett.90.100402

[52] Devetak I. Distillation of local purity from quantum states. Physical Review A. 2005b;**71**:062303. DOI: 10.1103/PhysRevA.71.062303

[53] Horodecki M, Oppenheim J. (Quantumness in the context of) Resource Theories. International Journal of Modern Physics B. 2013;**27**:1345019. DOI: 10.1142/S0217979213450197

[54] Oppenheim J, Horodecki K, Horodecki M, Horodecki P, Horodecki R. A new type of complementarity between quantum and classical information. Physical Review A. 2003;**68**:022307. DOI: 10.1103/PhysRevA.68.022307

[55] Spehner D, Orszag M. Geometric quantum discord with Bures distance. New Journal of Physics. 2013;**15**:103001. DOI: 10.1088/1367-2630/15/10/103001

[56] Debarba T, Maciel TO, Vianna RO. Reply to "Comment on 'Witnessed entanglement and the geometric measure of quantum discord'" Physical Review A. 2013;**87**:046301. DOI: 10.1103/PhysRevA.87.046301

[57] Piani M. Problem with geometric discord. Physical Review A. 2012;**86**:034101. DOI: 10.1103/PhysRevA.86.034101

[58] Coffman V, Kundu J, Wootters WK. Distributed Entanglement. Physical Review A. 2000;**61**:052306. DOI: 10.1103/PhysRevA.61.052306

[59] Yu S, Zhang C, Chen Q, Oh C. Tight bounds for the quantum discord. arXiv:1102.1301v2. 2012;**85**:032109. URL: http://arxiv.org/abs/1102.1301v2

[60] Xi Z, Lu X-M, Wang X, Li Y. Necessary and sufficient condition for saturating the upper bound of quantum discord. Physical Review A. 2012;**85**:032109. DOI: 10.1103/PhysRevA.85.032109

[61] Xi Z, Lu X-M, Wang X, Li Y. The upper bound and continuity of quantum discord. Journal of Physics A: Mathematical and Theoretical. 2011;**44**:375301. DOI: 10.1088/1751-8113/44/37/375301

[62] Zhang C, Yu S, Chen Q, Oh CH. Observable estimation of entanglement of formation and quantum discord for bipartite mixed quantum states. Physical Review A. 2011;**84**:052112. DOI: 10.1103/PhysRevA.84.052112

[63] Chi DP, Lee S. Entanglement for a two-parameter class of states. Journal of Physics A: Mathematical and General. 2003;**36**:11503. DOI: 10.1088/0305-4470/36/45/010

[64] Cen LX, Li X-Q, Shao J, Yan Y. Quantifying quantum discord and entanglement of formation via unified purifications. Physical Review A. 2011;**83**:054101. DOI: 10.1103/PhysRevA.83.054101

[65] Fanchini FF, Karpat G, Akmak B, Castelano LK, Aguilar GH, Jimnez Faras O, Walborn SP, Souto Ribeiro PH, de Oliveira MC. Non-Markovianity through accessible information. Physical Review Letters. 2014;**112**:210402. DOI: 10.1103/PhysRevLett.112.210402

[66] Piani M, Adesso G. Quantumness of correlations revealed in local measurements exceeds entanglement. Physical Review A. 2012a;**85**:040301. DOI: 10.1103/PhysRevA.85.040301

[67] Hiroshima T, Hayashi M. Finding a maximally correlated state: Simultaneous Schmidt decomposition of bipartite pure states. Physical Review A. 2004;**70**:030302. DOI: 10.1103/PhysRevA.70.030302

[68] Devetak I, Winter A. Distillation of secret key and entanglement from quantum states. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science. 2005b;**461**:207. DOI: 10.1098/rspa.2004.1372

[69] Iemini F, Debarba T, Vianna RO. Quantumness of correlations in indistinguishable particles. Physical Review A. 2014;**89**:032324. DOI: 10.1103/PhysRevA.89.032324

[70] Debarba T, Vianna RO, Iemini F. Quantumness of correlations in fermionic systems. Physical Review A. 2017;**95**:022325. DOI: 10.1103/PhysRevA.95.022325

[71] Adesso G, D’Ambrosio V, Nagali E, Piani M, Sciarrino F. Experimental entanglement activation from discord in a programmable quantum measurement. Physical Review Letters. 2014;**112**:140501. DOI: 10.1103/PhysRevLett.112.140501

[72] Orieux A, Ciampini MA, Mataloni P, Bru D, Rossi M, Macchiavello C. Experimental Generation of Robust Entanglement from Classical Correlations via Local Dissipation. Physical Review Letters. 2015;**115**:160503. DOI: 10.1103/PhysRevLett.115.160503

Section 2

Quantum Channel Construction

Chapter 5

Information Loss in Quantum Dynamics

Er'el Granot

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.70395

Abstract

The way data is lost from the wavefunction in quantum dynamics is analyzed. The main results are (A) Quantum dynamics is a dispersive process in which any data initially encoded in the wavefunction is gradually lost. The ratio between the distortion's variance and the mean probability density increases in a simple form. (B) For any given amount of information encoded in the wavefunction, there is a time period, beyond which it is impossible to decode the data. (C) The temporal decline of the maximum information density in the wavefunction has an exact analytical expression. (D) For any given time period there is a specific detector resolution, with which the maximum information can be decoded. (E) For this optimal detector size the amount of information is inversely proportional to the square root of the time elapsed.

Keywords: quantum information, quantum encryption, uncertainty principle, quantum decoding

1. Introduction

The field of quantum information received a lot of attention recently due to major development in quantum computing [1–5], quantum cryptography, and quantum communications [6–8].

In most quantum computing, the wavefunction is a superposition of multiple binary states (qubits), which can be in spin states, polarization state, binary energy levels, etc. However, since the wavefucntion is a continuous function, it can carry, in principle, an infinite amount of information. Only the detector dimensions and noises limits the information capacity.

The quantum wavefunction, like any complex signal, carries a large amount of information, which can be decoded in the detection process. Its local amplitude can be detected by measuring the probability density in a direct measurement, while its phase can be retrieved in an interferometric detection, just as in optical coherent detection [9].

The amount of information depends on the detector's capabilities, i.e., it depends on the detector's spatial resolution and its inner noise level. Therefore, the maximum amount of information that can be decoded from the wavefunction is determined by the detector's characteristics. However, unlike the classical wave equation, the quantum Schrödinger dynamics is a dispersive process. During the quantum dynamics, the wavefunction experiences distortions. These distortions increase in time just like the dispersion effects on signals in optical communications [10, 11].

Nevertheless, unlike dispersion compensating modules in optical communications, there is no way to compensate or "undo" the dispersive process in quantum mechanics. Therefore, the amount of information that can be decoded decreases monotonically with time.

The object of this chapter is to investigate the way information is lost during the quantum dynamics.

2. Quantum dynamics of a random sequence

The general idea is to encode the data on the initial wavefunction. In accordance to signals in coherent optical communications, in every point in space the data can be encoded in both the real and imaginary parts of the wavefunction.

The amount of distortion determines the possibility to differentiate between similar values, and therefore, it determines the maximum amount of information that the wavefunction carries.

The detector width Δx determines the highest volume of data that can be stored in a given space, i.e., it determines the data density. All spatial frequencies beyond $1/\Delta x$ cannot be detected and cannot carry information. Moreover, due to this constrain, there is no point in encoding the data with spatial frequency higher than $1/\Delta x$.

A wavefunction, which consists of the infinite random complex sequence $\psi_n = \Re\psi_n + i\Im\psi_n$ for $n = -\infty, \dots -1, 0, 1, 2, \dots \infty$, which occupies the spatial spectral bandwidth $1/\Delta x$ (higher frequencies cannot be detected by the given detector) can be written initially as an infinite sequence of overlapping Nyquist-sinc functions [12, 13] (see **Figure 1**), i.e.,

$$\psi(x, t = 0) = \sum_{n=-\infty}^{\infty} \psi_n \mathrm{sinc}(x/\Delta x - n), \tag{1}$$

where $\mathrm{sinc}(\xi) \equiv \frac{\sin(\pi\xi)}{\pi\xi}$ is the well-known "sinc" function.

After a time period t, in which the wavefunctions obeys the free Schrödinger equation.

$$i\hbar \frac{\partial\psi(x,t)}{\partial t} = -\frac{\hbar^2}{2m}\frac{\partial^2\psi(x,t)}{\partial x^2}, \tag{2}$$

the wavefunction can be written as a convolution

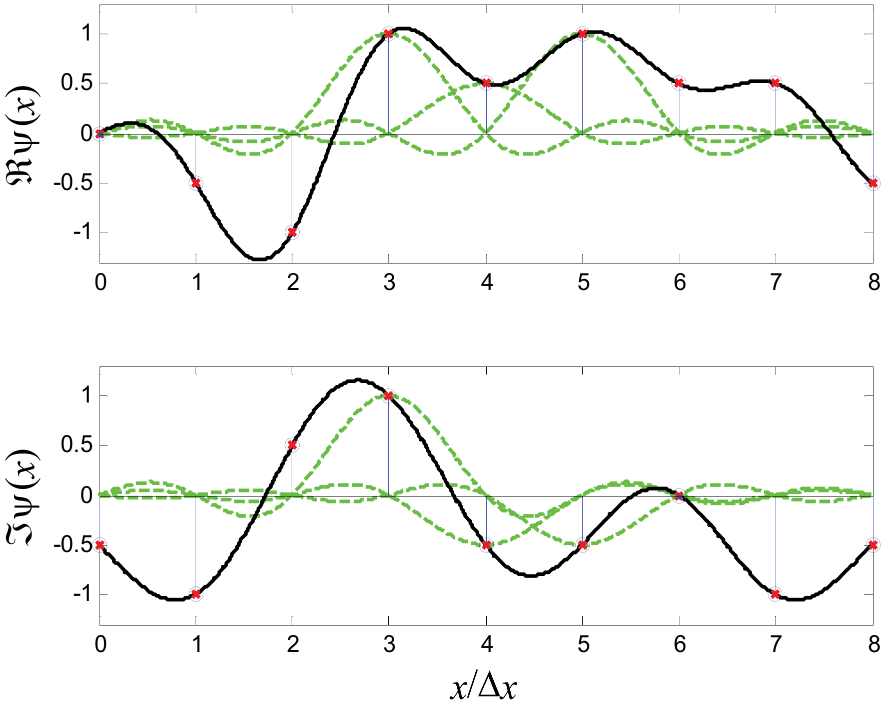


Figure 1. Illustration of the way the data is encoded in the wavefucntion. In every Δx, there is a single complex number $\psi_n = \Re\psi_n + i\Im\psi_n$ (the circles), while the continuous wavefunction is a superposition of these numbers multiplied by sinc's functions (three of which are presented by the dashed curves). The values in the y-axis should be multiplied by the normalization constant of the wavefucntion.

$$\psi(x,t) = \int_{-\infty}^{\infty} K(x-x',t)\psi(x',0)dx' \tag{3}$$

with the Schrödinger Kernel [14].

$$K(x-x',t) = \sqrt{\frac{m}{2\pi i\hbar t}}\,\exp\left[\frac{im}{2\hbar}\frac{(x-x')^2}{t}\right]. \tag{4}$$

Due to the linear nature of the problem, Eq. (3) can be solved directly

$$\psi(x,t>0) = \sum_{n=-\infty}^{\infty}\psi_n \mathrm{dsinc}\left(x/\Delta x - n, (\hbar/m)t/\Delta x^2\right) \tag{5}$$

where "dsinc" is the dynamic-sync function

$$\mathrm{dsinc}(\xi,\tau) \equiv \frac{1}{2}\sqrt{\frac{i}{2\pi\tau}}\exp\left(-i\frac{\xi^2}{2\tau}\right)\left[\mathrm{erf}\left(-\frac{\xi-\pi\tau}{\sqrt{i2\tau}}\right) - \mathrm{erf}\left(-\frac{\xi+\pi\tau}{\sqrt{i2\tau}}\right)\right]. \tag{6}$$

Equation (6) is the "sinc" equivalent of the "srect" function, that describes the dynamics of rectangular pulses (see Ref. [15]).

Note that $\lim_{\tau\to 0}\left[\mathrm{dsinc}(\xi,\tau)\right] = \mathrm{sinc}(\xi)$.

Some of the properties of the dsinc function are illustrated in **Figures 2** and **3**. As can be seen, the distortions form dsinc(n, 0) = $\delta(n)$ gradually increase with time.

Hereinafter, we adopt the dimensionless variables

$$\tau \equiv (\hbar/m)t/\Delta x^2 \text{and } \xi \equiv x/\Delta x. \tag{7}$$

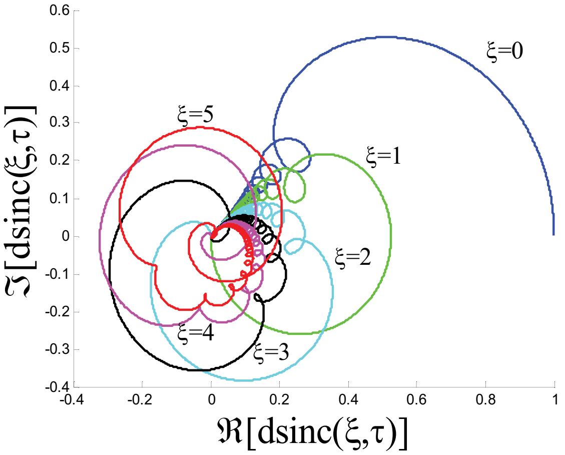


Figure 2. Several plots of the real and imaginary parts of the dsinc function for different discrete values of ξ = 0, 1, 2, … 5.

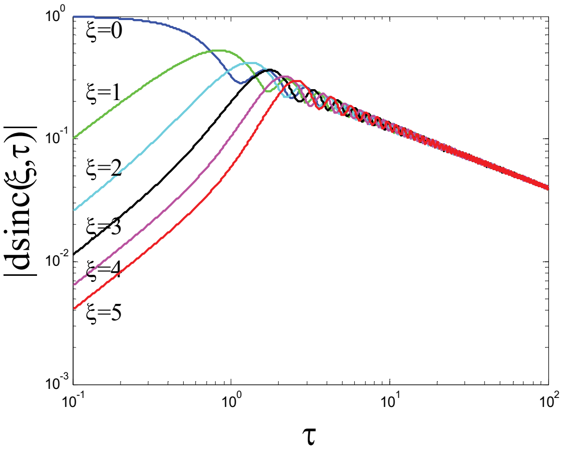


Figure 3. The dependence of the absolute value of the dsinc function on τ for different discrete values of ξ = 0, 1, 2, … 5.

Thus, Eq. (2) can be rewritten

$$i\frac{\partial\psi(\xi,\tau)}{\partial\tau} = -\frac{1}{2}\frac{\partial^2\psi(\xi,\tau)}{\partial\xi^2} \tag{8}$$

and Eq. (5) simply reads

$$\psi(\xi,\tau>0) = \sum_{n=-\infty}^{\infty}\psi_n \mathrm{dsinc}(\xi-n,\tau). \tag{9}$$

Therefore, the wavefunction at the detection point of the mth symbol (center of the symbol at $\xi = m$) is a simple convolution

$$\psi(m,\tau) = \sum_n \psi_n h(m-n) = \psi_m + \sum_n \psi_n \delta h(m-n) \tag{10}$$

where

$$h(n) \equiv \mathrm{dsinc}(n,\tau)\,\text{and}\ \delta h(n) \equiv \mathrm{dsinc}(n,\tau) - \delta(n). \tag{11}$$

Since

$$\left.\frac{\partial^2 \mathrm{sinc}(\xi)}{\partial\xi^2}\right|_{\tau=n\neq 0} = \frac{2}{n^2}(-1)^{n+1} \quad \text{and} \quad \left.\frac{\partial^2 \mathrm{sinc}(\xi)}{\partial\xi^2}\right|_{\tau=0} = -\frac{\pi^2}{3}, \tag{12}$$

then Eq. (9) can be written as a linear set of differential equations

$$\frac{d\psi(m,\tau)}{d\tau} = i\sum_n w(m-n)\psi(n,\tau) \equiv iw(m) * \psi(m,\tau) \tag{13}$$

with the dimensionless

$$w(m) \equiv \begin{bmatrix} \cdots & \frac{1}{3^2} & -\frac{1}{2^2} & 1 & -\frac{\pi^2}{6} & 1 & -\frac{1}{2^2} & \frac{1}{3^2} & \cdots \end{bmatrix} = \begin{cases} (-1)^{m+1}/m^2 & m \neq 0 \\ -\pi^2/6 & m = 0 \end{cases}. \tag{14}$$

It should be noted that the fact that Eq. (14) is a universal sequence, i.e. it is independent of time, is not a trivial one. It is a consequence of the properties of the sinc function. Unlike rectangular pulses, which due to their singularity has short time dynamics is mostly nonlocal (and therefore, time-dependent) [15, 16], sinc pulses are smooth and therefore, their dynamics is local and consequently $w(m)$ is time-independent.

3. Quantum distortion noise

After a short period of time, the error (distortion) in the wavefunction (i.e., the wavefunction deformation)

$$\Delta\psi(\xi,\tau) \equiv \psi(\xi,\tau) - \psi(\xi,0) \tag{15}$$

can be approximated by

$$\Delta\psi(\xi,\tau) \equiv \psi(\xi,\tau) - \psi(\xi,0) \cong \tau \left.\frac{\partial\psi(\xi,\tau)}{\partial\tau}\right|_{\tau=0}. \tag{16}$$

Then we can define the Quantum Noise as the variance of the error

$$N = \left\langle |\Delta\psi(\xi,\tau)|^2 \right\rangle \cong \tau^2 \left\langle \left| \left.\frac{\partial\psi(\xi,\tau)}{\partial\tau}\right|_{\tau=0} \right|^2 \right\rangle \tag{17}$$

where the triangular brackets stand for spatial averaging, i.e., $\langle f(x)\rangle \equiv \frac{1}{X}\int_{-X/2}^{X/2} f(x')dx'$.

Using the Schrödinger equation, Eq. (17) can be rewritten as follows:

$$N = \left\langle |\Delta\psi(\xi,\tau)|^2 \right\rangle \cong \frac{\tau^2}{4} \left\langle \left| \frac{\partial^2\psi(\xi,0)}{\partial^2\xi} \right|^2 \right\rangle. \tag{18}$$

Similarly, we can define the average density as

$$\rho = \left\langle |\psi(\xi,\tau)|^2 \right\rangle. \tag{19}$$

Now, from the Parseval theorem [12], the spatial integral (average) can be replaced by a spatial frequency integral over the Fourier transform, i.e.,

$$N = \frac{1}{2\pi} \left\langle |\Delta\psi(\kappa,\tau)|^2 \right\rangle \tag{20}$$

and

$$\rho = \frac{1}{2\pi} \left\langle |\psi(\kappa,\tau)|^2 \right\rangle \tag{21}$$

where

$$\psi(\kappa,\tau) \equiv (2\pi)^{-1} \int d\xi \exp(-i\kappa\xi)\psi(\xi,\tau) \text{ and } \Delta\psi(\kappa,\tau) \equiv (2\pi)^{-1} \int d\xi \exp(-i\kappa\xi)\Delta\psi(\xi,\tau). \tag{22}$$

Therefore, the ratio between the noise and the density (i.e., the reciprocal of the Signal-to-Noise Ratio, SNR) satisfies the surprisingly simple expression

$$\frac{N}{\rho} = \frac{\left\langle |\Delta\psi(\xi,\tau)|^2 \right\rangle}{\left\langle |\psi(\xi,0)|^2 \right\rangle} \cong \tau^2 \frac{\frac{1}{2\pi}\int d\kappa \frac{\kappa^4}{4} |\psi(\kappa,0)|^2}{\frac{1}{2\pi}\int d\kappa |\psi(\kappa,0)|^2} = \tau^2 \frac{\pi^4}{20} \tag{23}$$

and with physical dimensions

$$\frac{N}{\rho} = \frac{t^2}{\Delta x^4}\left(\frac{\hbar}{m}\right)^2 \frac{\pi^4}{20}. \tag{24}$$

We, therefore, find a universal relation: the relative noise (the ratio between the noise and the density) depends only on a single dimensionless parameter $\tau \equiv (\hbar/m)t/\Delta x^2$.

It should be stressed that this is a universal property, which emerges from the quantum dynamics. This relation is valid regardless of the specific data encoded in the wavefunction provided the data's spectral density is approximately homogenous in the spectral bandwidth $[-1/\Delta x, 1/\Delta x]$.

Clearly, since the noise increases gradually, it will becomes more difficult to decode the data from the wavefucntion. In fact, as is well known from Shannon celebrated equation [17], the amount of noise determines the data capacity that can be decoded. Therefore, the amount of information must decrease gradually.

4. The rate of information loss

We assume that at every Δx interval the wavefunction can have one of M different complex values. In this case, both the real and imaginary parts can have $\sqrt{M}$ different values (this form is equivalent to the Quadrature Amplitude Modulation, QAM, in electrical and optical modulation scheme [18]), i.e., any complex $\psi_n = \psi(n) = \Re\psi_n + i\Im\psi_n = \tilde{N}v_{p,q}$ can have one of the values

$$v_{p,q} = \frac{2p-\sqrt{M}-1}{\sqrt{M}-1} + i\frac{2q-\sqrt{M}-1}{\sqrt{M}-1} \text{ for } p,q = 1,2,\ldots\sqrt{M} \tag{25}$$

where $\tilde{N}$ is the normalization constant.

Since $b = \log_2 M$ is the number of bits encapsulated in each one of the complex symbol, then the difference between adjacent symbol

$$\Delta v = \Re v_{p,q} - \Re v_{p-1,q} = \Im v_{p,q} - \Im v_{p,q-1} \tag{26}$$

decreases exponentially with the number of bits, i.e.,.

$$\Delta v = \frac{2}{\sqrt{M}-1} = \frac{2}{2^{b/2}-1} \cong 2^{1-b/2} = 2\exp[-b(\ln 2/2)] \tag{27}$$

Therefore, as the number of bits per symbol increases, it becomes more difficult to distinguish between the symbols.

Clearly, maximum distortion occurs, when all the *other* symbols oscillates with maximum amplitude, i.e.,

$$\psi_n = \psi(n,0) = \begin{cases} \psi(m,0) & n = m \\ (-1)^{n-m} & n \neq m \end{cases}, \tag{28}$$

in which case the differential Eq. (13) can be written (for short periods)

$$\frac{d\psi_{\max/\min}(m,\tau)}{d\tau} = -iw(0)\psi_{\max/\min}(m,\tau) \mp i\sum_{n\neq 0} w(m-n)(-1)^n = i\frac{\pi^2}{6}\psi_{\max/\min}(m,\tau) \mp i\pi^2/3. \tag{29}$$

The solution of Eq. (29) is

$$\psi_{\max/\min}(m,\tau) = \psi(m,0)\exp\left(i\pi^2\tau/6\right) \pm 2\left(1 - \exp\left(i\pi^2\tau/6\right)\right). \tag{30}$$

Therefore, each cluster is bounded by a circle whose center is

$$\psi(m,0)\exp\left(i\pi^2\tau/6\right) \tag{31}$$

and its radius is

$$R = 2\left|1 - \exp\left(i\pi^2\tau/6\right)\right| = 4\left|\sin\left(\pi^2\tau/12\right)\right|. \tag{32}$$

Since this result applies only for short periods, then the entire cluster is bounded by the radius

$$R = \pi^2\tau/3, \tag{33}$$

which is clearly larger than the cluster's standard deviation $\sigma = \pi^2\tau/\sqrt{20} < R$.

A simulation based on Eq. (1) with $2^{11} - 1$ symbols, which were randomly selected from the pool (25) for $M = 16$ was taken. That is, the probability that ψ_n is equal to $v_{p,q}$ is $1/M$ for all ns, or mathematically

$$P\left(\psi_n = v_{p,q}\right) = 1/M, \text{ for } n = 1,2,3,\ldots,2^{11}-1, \text{ and } p,q = 1,2,\ldots\sqrt{M}. \tag{34}$$

The temporal dependence of the calculated SNR is presented in **Figure 4**. As can be seen, Eq. (23) is indeed an excellent approximation for short τ.

Since the symbols were selected randomly (with uniform distribution), then when all the symbols $\psi(n, 0) = \psi_n$ are plotted on the complex plain, an ideal constellation image is shown (see the upper left subfigure of **Figure 5**).

In **Figure 5**, a numerical simulation for a QAM 16 scenario is presented initially and after a time period, $\tau = 0.1$. Moreover, the dashed circles represents the standard deviation, i.e., the noise level (radius $\pi^2\tau/\sqrt{20}$), and the bounding circles (radius $R = \pi^2\tau/3 > \pi^2\tau/\sqrt{20}$).

Since the initial distance between centers of adjacent clusters is $\frac{2}{\sqrt{M-1}}$, then decoding is impossible for $\frac{1}{\sqrt{M-1}} = \frac{\pi^2\tau_{\max}}{3}$, i.e., we finally have an expression for the maximum time $\tau_{\max}$, beyond

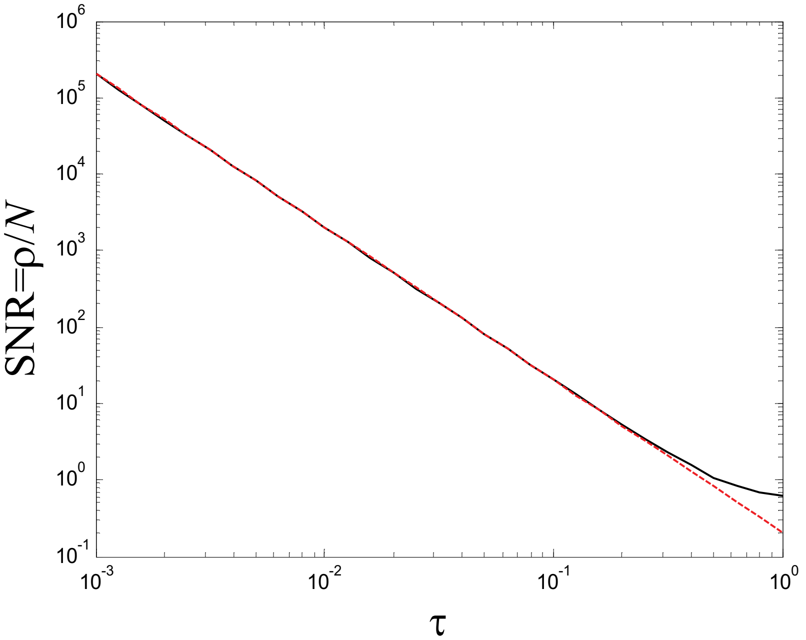


Figure 4. Plot of the SNR as a function of τ. The solid curve represents the simulation result, and the dashed line represents the approximation for short τ (the reciprocal of Eq. (23)).

which it is impossible to encode the data (i.e., to differentiate between symbols). This maximum time is

$$\tau_{\max} = \frac{3}{\left(\sqrt{M}-1\right)\pi^2} \tag{35}$$

It should be noted that this result coincides with the On-Off-Keying (OOK) dispersion limit, for which case $\sqrt{M} = 2$, and then $\tau_{\max} = 1/\pi \cong 3/\pi^2$ (see Ref. [19]).

Similarly, Eq. (35) can be rewritten to find the maximum M for a given distance, i.e.,

$$\sqrt{M_{\max}} = 1 + \frac{3}{\pi^2\tau}. \tag{36}$$

However, it is clear that this formulae for $\sqrt{M_{\max}}$ is meaningful only under the constraint that $\sqrt{M_{\max}}$ is an integer.

Since the number of bits per symbol is $\log_2 M$, then the maximum data density (bit/distance) is

$$S_{\max} = \frac{2}{\Delta x}\log_2\sqrt{M_{\max}} = \frac{2}{\Delta x}\log_2\left(1 + 3/\pi^2\tau\right). \tag{37}$$

Using $\Delta x = \sqrt{\frac{(\hbar/m)t}{\tau}}$, we finally have

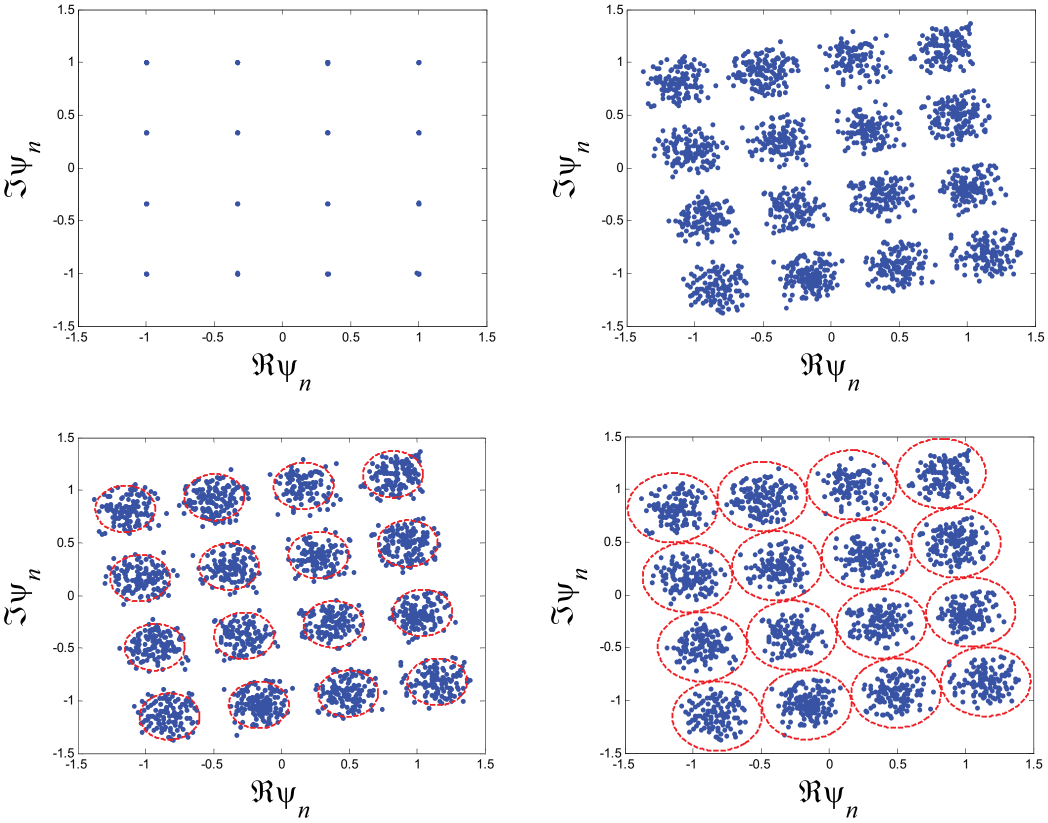


Figure 5. Upper left: the initial constellation of the data in the wavefunction. Upper right: the data constellation after τ = 0.1. Bottom left: the constellation with the circles that stands for the standard deviation $\sigma = \pi^2\tau/\sqrt{20}$. Bottom right: The constellation with the circles that represents the bounding circles $R = \pi^2\tau/3$.

$$S_{\max} = \frac{1}{\sqrt{(\hbar/m)t}} F(\tau) \tag{38}$$

where $F(\tau) \equiv 2\sqrt{\tau}\log_2\left(1 + 3/\pi^2\tau\right)$ is a universal dimensionless function, which is plotted in **Figure 6** and receives its maximum value $F(x_{\max}) \cong 1.28$ for $x_{\max} \cong 0.0775$. However, under the restriction that $\sqrt{M_{\max}}$ must be an integer, then as can be shown in **Figure 6**, the maximum bit-rate is reached for

$$M_{\max} = 25, \tag{39}$$

for which case

$$\tau_{\max} = \frac{3}{4\pi^2} \cong 0.076, \tag{40}$$

Which means that for a given time of measurement t, the largest amount of information would survive provided the detector size (i.e., the sampling interval) is equal to

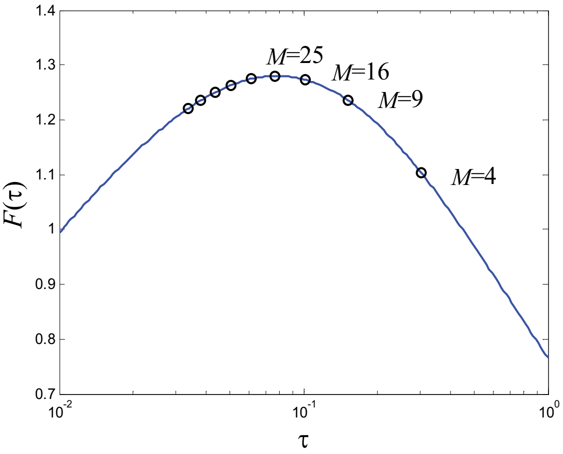


Figure 6. Plot of the function $F(x)\equiv 2\sqrt{x}\log_2\left(1+3/\pi^2 x\right)$. The circles stands for different values of integer $\sqrt{M}$ ($M = 2^2, 3^2, 4^2, \ldots 10^2$). The closest circle to the maximum point is $M = 5^2$.

$$\Delta x_{\max} = 2\pi\sqrt{\hbar t/3m}. \tag{41}$$

For this value $F(\tau_{\max}) = \frac{\sqrt{3}}{\pi}\log_2(5) \cong 1.28$, and therefore, the maximum information density that can last after a time period t is

$$S_{\max} = \sqrt{\frac{3}{(\hbar/m)t}}\frac{\log_2(5)}{\pi} \cong \frac{1.28}{\sqrt{(\hbar/m)t}}. \tag{42}$$

This equation reveals the loss of information from the wave function.

It should be stressed that this expression is universal and the only parameter, which it depends on, is the particle's mass. The higher the mass is, the longer is the distance the information can last.

5. Summary and conclusion

We investigate the decay of information from the wavefunction in the quantum dynamics.

The main conclusions are the following:

A. The signal-to-noise ratio, i.e., the ratio between the mean probability and the variance of the distortion, has a simple analytical expression for short times

$$SNR = \frac{\rho}{N} = \frac{20}{\tau^2\pi^4}$$

where $\tau \equiv (\hbar/m)t/\Delta x^2$ and Δx is the data resolution (the detector size).

B. When there are M possible symbols (as in QAM M), then the maximum time, beyond which the data cannot be decoded is $\tau_{\max} = \frac{3}{\left(\sqrt{M}-1\right)\pi^2}$

C. For a given symbol density (Δx) and a given measurement time, the maximum data density (bit/distance) is $S_{\max} = \frac{2}{\Delta x}\log_2\sqrt{M_{\max}} = \frac{2}{\Delta x}\log_2\left(1+3/\pi^2\tau\right)$.

D. For a given measurement time, the sampling interval with the highest amount of decoded information is $\Delta x_{\max} = 2\pi\sqrt{\hbar t/3m}$,

E. In which case the highest data density is $S_{\max} = \sqrt{\frac{3}{(\hbar/m)t}}\frac{\log_2(5)}{\pi}$

Author details

Er'el Granot

Address all correspondence to: erel@ariel.ac.il

Department of Electrical and Electronics Engineering, Ariel University, Ariel, Israel

References

[1] Nielsen MA, Chuang IL. Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge, UK: Cambridge University Press; 2011

[2] Rieffel EG, Polak WH. Quantum Computing: A Gentle Introduction (Scientific and Engineering Computation). Cambridge, MA: The MIT Press; 2014

[3] Yanofsky NS, Mannucci MA. Quantum Computing for Computer Scientists. 1st ed. Cambridge, UK: Cambridge University Press; 2008

[4] Kaye P, Laflamme R, Mosca M. Introduction to Quantum Computing. Oxford, UK: Oxford University Press; 2007

[5] Akama S. Elements of Quantum Computing: History, Theories and Engineering Applications. 1st ed. New York: Springer International Publishing; 2015

[6] Bendjaballah C, Hirota O, Reynaud S. Quantum Aspects of Optical Communications. 1st ed. New York: Springer; 1991

[7] Imre S, Gyongyosi L. Advanced Quantum Communications, An Engineering Approach. Hoboken, NJ: IEEE Press and WILEY & Sons, Inc. Publication; 2013

[8] Cariolaro G. Quantum Communications. New York: Springer; 2015

[9] Betti S, De Marchis G, Iannone E. Coherent Optical Communications Systems. Hoboken, NJ: J. Wiley & Sons, Inc.; 1995

[10] Agrawal GP. Fiber-Optic Communication Systems. New-York: J. Wiley& Sons; 2002

[11] Granot E, Luz E, Marchewka A. Generic pattern formation of sharp-boundaries pulses propagation in dispersive media. Journal of the Optical Society of America B. 2012;**29**:763

[12] Oppenheim AV, Schafer RW. Digital Signal Processing. 1st ed. London: Pearson; 1975

[13] Soto MA, Alem M, Shoaie MA, Vedadi A, Brès CS, Thévenaz L, Schneider T. Optical sinc-shaped Nyquist pulses of exceptional quality. Nature Communications. 2013;**4**:2898

[14] Feynman RP, Hibbs AR. Quantum Mechanics and Path Integrals. 1st ed. New-York: McGraw-Hill Companies; 1965

[15] Granot E, Luz E, Marchewka A. Generic pattern formation of sharp-boundaries pulses propagation in dispersive media. Journal of the Optical Society of America B. 2012;**29**: 763-768

[16] Granot E, Marchewka A. Generic short-time propagation of sharp-boundaries wave packets. Europhysics Letters. 2005;**72**:341-347

[17] Shannon CE . The Mathematical Theory of Communication. Urbana-Champaign, IL: University of Illinois Press; 1998 [originally 1949]

[18] Hanzo L, Ng SX, Keller T, Webb W. Quadrature Amplitude Modulation: From Basics to Adaptive Trellis-Coded, Turbo-Equalised and Space-Time Coded OFDM, CDMA and MC-CDMA Systems. 2nd ed. Hoboken, NJ: Wiley-IEEE Press; 2004

[19] Granot E. Fundamental dispersion limit for spectrally bounded On-Off-Keying communication channels and implications to Quantum Mechanics and the Paraxial Approximation. Europhysics Letters. 2012;**100**:44004

Chapter 6

Universal Microwave Photonics Approach to Frequency-Coded Quantum Key Distribution

Oleg G. Morozov, Airat J. Sakhabutdinov,
Gennady A. Morozov and Il'daris M. Gabdulkhakov

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.71974

Abstract

Design principles of universal microwave photonics system (MPS) for quantum key distribution (QKD) with frequency coding are concerned. Its main modulation concept lies in single photon generation on sidebands of optical carrier and determination of photons ground state through its registration and the amplitude value of its carrier frequency as reference channel. So, it is necessary to solve problems of signal-to-carrier ratio of single photon detector (SPD) and aspects of photon number splitting (PNS) attack, nonlinear phase modulation (NPM) between carrier and sidebands in fiber, and finally, spectral selection of carrier in receiver. The technologies, based on the modulation conversion of an optical carrier, are widely used in microwave photonics. Due to the natural symmetry of modulated signals and the highest achievable ratio of the modulation conversions, amplitude-phase modulation with complete or partial suppression of the optical carrier has found a particularly wide application in MPS. The characteristics of advanced MPS for QKD with frequency coding and carrier suppression based on tandem amplitude modulation and phase commutation are presented. New systems can have classical symmetric or non-classical asymmetric structure for QKD based only on spectral selection of carrier and subcarriers without re-modulation.

Keywords: quantum key distribution, frequency encoding and decoding, photon-modulated components, amplitude, phase and meshed amplitude/phase modulation, tandem amplitude modulation and phase modulation or commutation, re-modulation, passive spectral selection without re-modulation, microwave photonics decisions

1. Introduction

Quantum communication networks provide a unique opportunity of sharing a random sequence of bits between users with guaranteed security not achievable in classical open or special systems with cryptographic protection [1]. This is achieved by means of quantum key distribution (QKD) technology use.

Nowadays, there are at least four basic photonic QKD technologies: polarization [2], interferometric [3], differential phase shift [4] and frequency encoding [5]. The polarization technology is based on the features of four photons' fundamental states consideration and encoding, using one conjugate base of circular polarization and one of linear. The main disadvantage of this technology is the inability to maintain the polarization state of the photon along the entire length of fiber optic communication lines (FOCL). Interference technology relies on the use of optical delay lines and balanced interferometers in FOCL transmitter and receiver. The basic requirement for the implementation of this technology is to maintain the phase stroke difference of interferometers when exposed to temperature, vibration and other factors that are hard to realize. A phase technology is an approach based on the methods of differential phase shift, which allows implementing the QKD technology at FOCL lengths over 100 km, although with limited security [6].

The technology of frequency encoding allows determining the ground states of photons through the amplitude value of its carrier frequency, modulated in phase and/or amplitude by radiofrequency (RF) signal and the received high-order sidebands (subcarriers). This technology, based on the modulation conversion of multiphoton optical carrier, is widely used in microwave photonics, in its various classic applications [7–9].

Standard implementation of frequency encoding technology in quantum communication networks can be described as follows [10]. Alice (legal subscriber, transmitter) randomly changes the phase of the RF signal used to modulate the photons, among four discrete values $0;\pi,\ldots,\pi/2;3\pi/2$, which form a pair of conjugate bases, and sends it by FOCL quantum channel to Bob (legal subscriber, receiver). Bob modulates receiving photons again, using the same frequency RF signal as Alice, but with its own discrete phases, independent from Alice, from the same paired bases $0;\pi,\ldots,\pi/2;3\pi/2$. Along with this, the new order photon sidebands on the Bob's side will interfere with photons' sideband components received from the Alice's side. The interference result will determine the correctness of the adopted phase information and the encoded photon's state. For simplicity, quantum communication channel with sidebands only of first order is considered.

Over the last 20 years, this technology has been substantially modified and improved. Initially, it was used to implement the QKD in hardware, based on the modified cryptographic B92 protocol [11]. In this case, the level of constructive or destructive interference of the two lateral components, obtained by means of phase modulation (PM), was determined as a function of the cosine-squared type from the phase difference between the Alice and Bob signals. In more detailed characteristic consideration, the amplitude modulation (AM) application was used instead of phase technology to implement the QKD in hardware, based on the underlying cryptographic BB84 protocol [12], although the last one in theory was designed earlier than BB92 one. Thus, for the amplitude of the upper lateral components, the function of the sine square of the phases difference is characterized, and for the bottom—cosine-squared one. The optimal implementation of the QKD frequency encoding technology and the most clearly cryptography protocol BB84 can be obtained by using AM (Alice) and PM (Bob) (or PM-AM), which was shown in [13]. In the latter works, a broad understanding of frequency encoding principle is used, where to each state of the photons, instead of the phase of the modulating signal at a certain frequency, one or more lateral component frequencies either photon optical carrier [14] are put into line.

The symmetric pairs of the PM-PM, AM-AM and meshed AM-PM (PM-AM) are described by known electro-optical modulation and re-modulation schemes, where the first component determines the type of modulation and modulator on the side of Alice, and the other—on the side of Bob. The most important features of this type of QKD system are simplicity of schemes and phase shift matching decisions on both sides of quantum channel, efficient use of its bandwidth and capability to add quantity of subcarriers using one carrier source [15]. From another point of view [16], the smallest value of QBER is achieved in circuits with passive definition of photons states, without re-modulation and using only filter systems based on fiber Bragg gratings (FBG) or arrayed waveguide gratings (AWG) for subcarriers or carrier selection. Thus, we have to analyze as symmetrical systems with re-modulation, so and asymmetrical ones without re-modulation and only filter selection.

Disadvantages of above-described QKD systems are connected mainly with strong carrier and photon subcarrier levels' interaction along the optical fiber and its energy meshing. First, in [17], it was shown that effects of nonlinear phase modulation (NPM) are small on temporally separable sources utilizing symmetric group velocity matching but appreciably change the state of temporally entangled sources with the same group velocity-matching scheme. The largest changes to the state due to NPM occur in long FOCL with long pulse durations and low repetition rates (in limit, it is CW-technology of QKD with frequency coding). Second, in [18], it was shown that most quantum setups use simple attenuation of laser carrier as a source of quantum states. In such cases, average probability of single photon emission per time unit is equal to $\mu \approx 0.1$. The security condition in this case is no longer strict due to Poisson distribution of photons, so carrier or subcarriers may contain more than one photon. This fact can be easily used by Eve—illegal agent. She successfully can perform undetectable beam splitting or photon number splitting (PNS) attack without changing QBER and receive a part of the key, which can be significant at higher μ. Third, in [15], it was shown that quantum information transfer devices at subcarrier frequencies of modulated radiation required an exact separation of the quantum subcarrier signal and central wavelength. Inadequate extinction of the signal on the main frequency significantly reduces the signal-to-noise ratio of the system and leads to a significant increase in the number of errors in the quantum communication channel. Therefore, the QKD technology with frequency coding, based on the modulation conversion of an optical carrier with its complete or partial suppressing, is the actual problem to improve quantum channel characteristics.

Due to the natural symmetry of modulated signals and the highest achievable ratio of the modulation conversions, amplitude-phase modulation with complete or partial suppression of the optical carrier has found a particularly wide application in the systems of microwave photonics [19]. Let us apply microwave photonics principles to design of QKD systems with frequency encoding.

We present in this chapter the results of the universal QKD system design, based on a tandem electro-optic AMPM-PMAM scheme built on microwave photonics principles applied to photon carrier modulation. It allows us to implement all of the above-mentioned classical symmetrical schemes PM-PM, AM-AM and meshed AM-PM (PM-AM) and also to review the requirements for building a promising tandem AM and phase commutation (PC) scheme with the possibility of implementing a nonclassical asymmetric structure with passive filtering (FBG/AWG) on Bob's side and suppressed carrier.

The chapter in the main is based on the results of analytical review of [1–19], materials of Morozov et al. [20] and additional and new results of theoretical and experimental researches in QKD theme and miscellaneous applications. Next chapter sections are organized as follows. The second section shows the principles of design of QKD systems with frequency encoding based on the classical approaches; key nodes involved for the implementation of PM-PM, AM-AM and meshed AM-PM (PM-AM) schemes are described; the descriptions of protocol bases and some experimental results are given; the advantages and disadvantages of classical schemes are evaluated, and the ways of its development are discussed. The third section discusses the design of promising universal tandem AMPM-PMAM scheme and its microwave photonic (MWP) basis; version of QKD system with tandem amplitude modulation and phase commutation of photons is proposed; the capabilities of re-modulation and possibilities of re-commutation procedures, or their absent and using only passive filtering structure realizations. In conclusion, the received results are analyzed and the key development challenges for QKD systems with frequency encoding are highlighted.

2. Implementation of classical QKD schemes with frequency encoding

Let us consider implementation of various modulation schemes, relying on the chronology of QKD systems with frequency encoding. The protocols BB84 [12] and B92 [11] are two main protocols used for their construction. During the BB84 protocol realization, Alice prepares and sends to Bob a lot of random qubits, chosen from the four main states:

$$\begin{gathered} \begin{cases} |\psi_0\rangle = |0\rangle \\ |\psi_1\rangle = |1\rangle \end{cases} \\ \begin{cases} |\psi_+\rangle = \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]^{\cdot} \\ |\psi_-\rangle = \frac{1}{\sqrt{2}}[|0\rangle - |1\rangle] \end{cases} \end{gathered} \qquad (1)$$

The first two states in (1) form one basis of two-dimensional quantum system, and the other two form second basis.

It is necessary to fulfill the terms $\langle\psi_0|\psi_1\rangle = 0$ and $\langle\psi_+|\psi_-\rangle = 0$, corresponding to the scalar production of their components. At the same time, the mentioned states of different bases are not orthogonal and maximum overlap [12]. Therefore, there is no measurement procedure, at which Eve can determine the state prepared by Alice and sent to Bob at 100% probability [21].

B92 protocol [11] is the modernization of BB84 protocol and is used to encode one of the two presented in (1) bases.

2.1. PM-PM schemes

One of the first PM-PM scheme variants is based on the B92 protocol [22]. Its OptiSystem model is presented in **Figure 1**.

Alice modulates photon $|\omega_0\rangle$ in left PM by RF signal from sine generator with frequency Ω and phase $\Phi = \Phi_A$, getting:

$$|A\rangle \; = \; \sum_{n=-\infty}^{n=+\infty} J_n \, exp^{jn\Phi_A} | \, \omega_n \rangle, \tag{2}$$

where, for simplicity of display, the argument of the Bessel's function J_n is not specified. On the receiving end, Bob modulates the input radiation synchronized with Alice RF signal from its sine generator (right) phase $\Phi=\Phi_B$. At Bob's PM output, one will receive:

$$|B\rangle \; = \; \sum\nolimits_{n,k} J_n \, J_{k-n} \, exp^{jn\Phi_A} \, exp^{j(k-n)\Phi_B} | \, \omega_k \rangle \tag{3}$$

It should be noted that modulation effect is to transfer energy from carrier on the sidebands (subcarriers). Its effectiveness depends on modulation and corresponding phases Φ_A and Φ_B. Transfer efficiency $P(\omega_0 \rightarrow \omega_0 \pm \Omega)$ is proportional to the function $\cos^2(\Delta\Phi/2)$, where $\Delta\Phi = \Phi_B - \Phi_A$, and is at maximum when $\Delta\Phi = 0$, which indicates the same basis chosen by Alice and Bob (**Figure 2**).

Further exchange of information between Alice and Bob allows them to set a secure connection with the implementation of the B92 protocol. The definition of a key with probability equal to one for Eve is impossible.

Determination of phase's compliance level in the scheme is actually implemented by the amplitude of the subcarriers. That is also the evidence of these scheme drawbacks, taking into account the small power of optical subcarriers and the presence of noise in the communication channel and single photon detector (SPD).

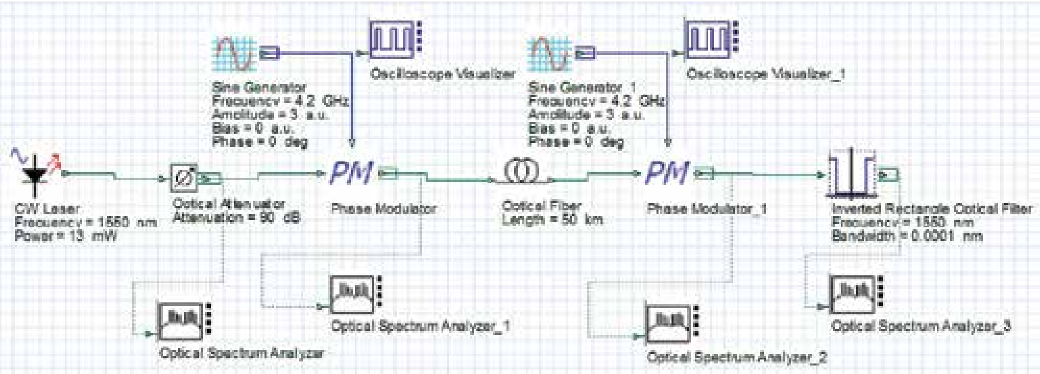


Figure 1. Modeling of PM-PM scheme for QKD system with frequency coding.

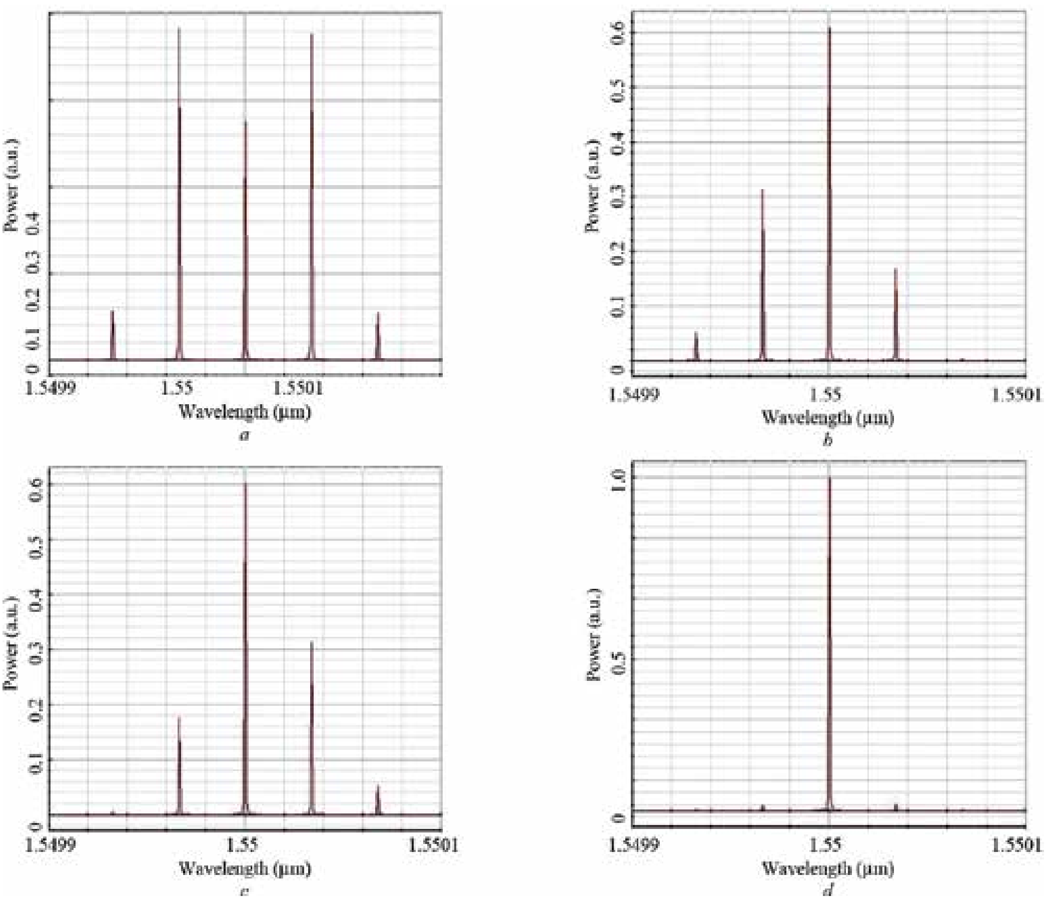


Figure 2. Constructive ΔΦ = 0 (a) and destructive ΔΦ = π/2 (b), ΔΦ = 3π/2 (c), ΔΦ = π (d) interferences on the output of Bob's PM, when Alice's $\Phi_A = 0$.

A second version of the PM-PM scheme [14] was proposed for elimination of given drawbacks. It is based on nonlinear interaction of the RF signal and the photon in the electro-optic modulator and implements a more advanced BB84 protocol. Notch filter on ω_0 frequency is set prior to sideband SPD, which reflects the carrier at the corresponding receiver, transmitting all the remaining subcarriers on $\omega_0 \pm \Omega$ and $\omega_0 \pm 2\,\Omega$ frequencies.

For BB84 protocol realization, two bases are set as following:

$$\begin{cases} |+;\ 1\rangle = \frac{1}{\sqrt{2}}\,|1\rangle_{\omega_0} + \frac{1}{2}\,|1\rangle_{\omega_0+\Omega} - \frac{1}{2}\,|1\rangle_{\omega_0-\Omega} \\ |-;\ 1\rangle = \frac{1}{\sqrt{2}}\,|1\rangle_{\omega_0} - \frac{1}{2}\,|1\rangle_{\omega_0+\Omega} + \frac{1}{2}\,|1\rangle_{\omega_0-\Omega} \end{cases} . \qquad \begin{cases} |+;\ 2\rangle = |1\rangle_{\omega_0} \\ |-;\ 2\rangle = \frac{1}{\sqrt{2}}\,|1\rangle_{\omega_0+\Omega} - \frac{1}{\sqrt{2}}\,|1\rangle_{\omega_0-\Omega} \end{cases} \tag{4}$$

The |±;2⟩ states are determined without applying the re-modulation, by the use of filter sets based on FBG or AWG and logic conditions. Scheme decision shows the lowest QBER value. Only sideband SPD also works during the transfer of |±;1⟩ states, because at specified conditions of modulation and re-modulation the component at frequency ω_0 is equal to 0. The error level in transmission |±;1⟩ states is 4.7%.

AM-AM schemes use for elimination of PM-PM ones shortcomings. One of them was implemented only on the acousto-optic modulators [16].

2.2. AM-AM schemes

The first AM-AM scheme is based on BB84 protocol [23]. Its OptiSystem model is presented in **Figure 3**, and constructive and destructive interferences are shown in **Figure 4**.

It should be noted that the modulator on the of Alice's side is modulated according to the law $\cos(\Omega t + \Phi_A)$, and on the Bob's side according to $\sin(\Omega t + \Phi_B)$. Transfer efficiency $P(\omega_0 \rightarrow \omega_0 \pm \Omega)$ in this case is proportional to function $\cos^2(\Delta\Phi/2)$ and $\sin^2(\Delta\Phi/2)$ for the upper and lower side bands, respectively, at $\Phi_A = \pi/2$ and $\Phi_B = 3\pi/2$. Determination of phase's compliance level in the scheme is also implemented by the amplitude of the lateral components.

2.3. Meshed AM-PM (PM-AM) schemes

AM-PM or PM-AM scheme implementation intuitively appears to be based on the principles set out, respectively, for AM-AM and PM-PM schemes. One of its OptiSystem model is presented in **Figure 5**.

Determination of phase's compliance level in the scheme is also implemented by the amplitude of the lateral components (**Figure 6**).

It should be noted that we have some conflicting information about the possibility [13] and impossibility [23] of meshed AM-PM (PM-AM) scheme realization as for protocol BB84, so

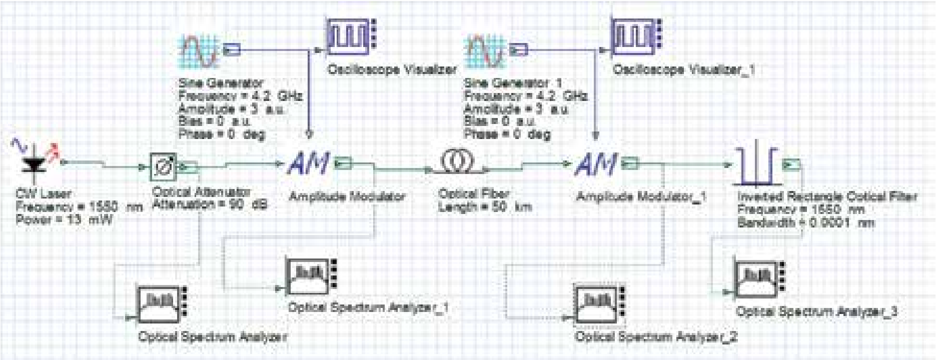


Figure 3. Modeling of AM-AM scheme for QKD system with frequency coding.

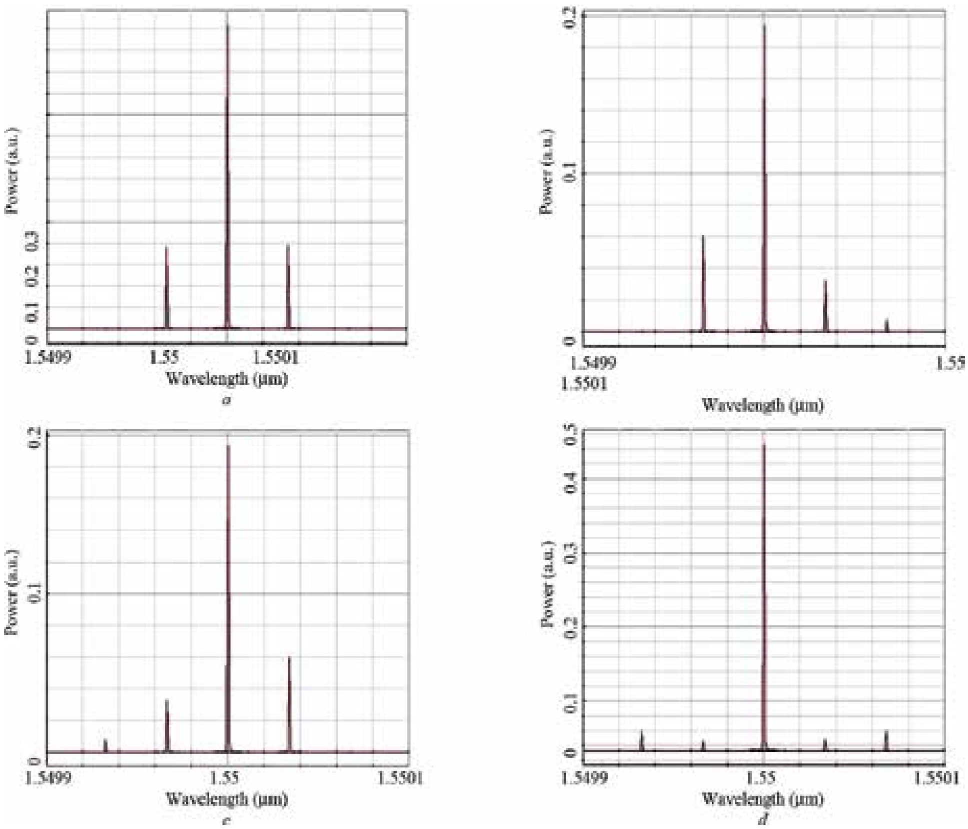
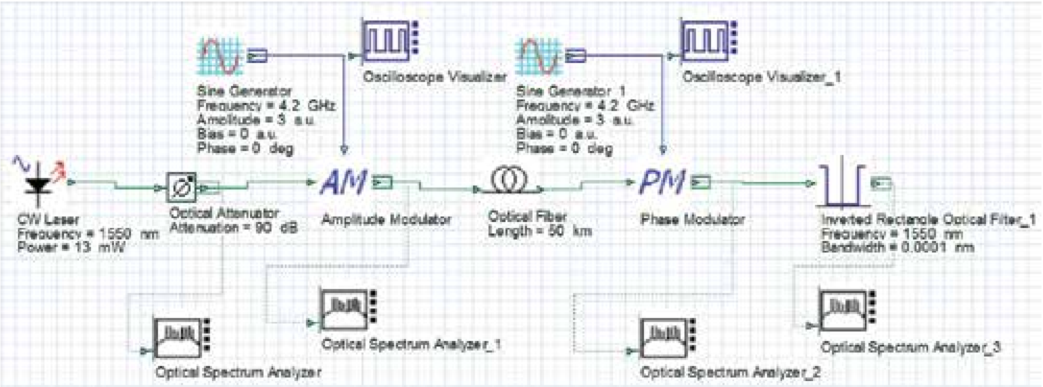


Figure 4. Constructive ΔΦ = π (a) and destructive ΔΦ = π/2 (b), ΔΦ = 3π/2 (c); ΔΦ = 0 (d) interferences on the output of Bob's PM, when Alice's $Φ_A$ = 3π/2.


Oscilloscope Visualizer
Oscilloscope Visualizer_1
AM
PM
Amplitude Modulator
Phase Modulator
Optical Spectrum Analyzer
Optical Spectrum Analyzer_1
Optical Spectrum Analyzer_2
Optical Spectrum Analyzer_3

Sine Generator
Frequency = 4.2 GHz
Amplitude = 3 a.u.
Bias = 0 a.u.
Phase = 0 deg

Sine Generator_1
Frequency = 4.2 GHz
Amplitude = 3 a.u.
Bias = 0 a.u.
Phase = 0 deg

CW Laser
Frequency = 1550 nm
Power = 13 mW

Optical Attenuator
Attenuation = 90 dB

Optical Fiber
Length = 50 km

Inverted Rectangle Optical Filter_1
Frequency = 1550 nm
Bandwidth = 0.0001 nm

Figure 5. Modeling of AM-PM scheme for QKD system with frequency coding.

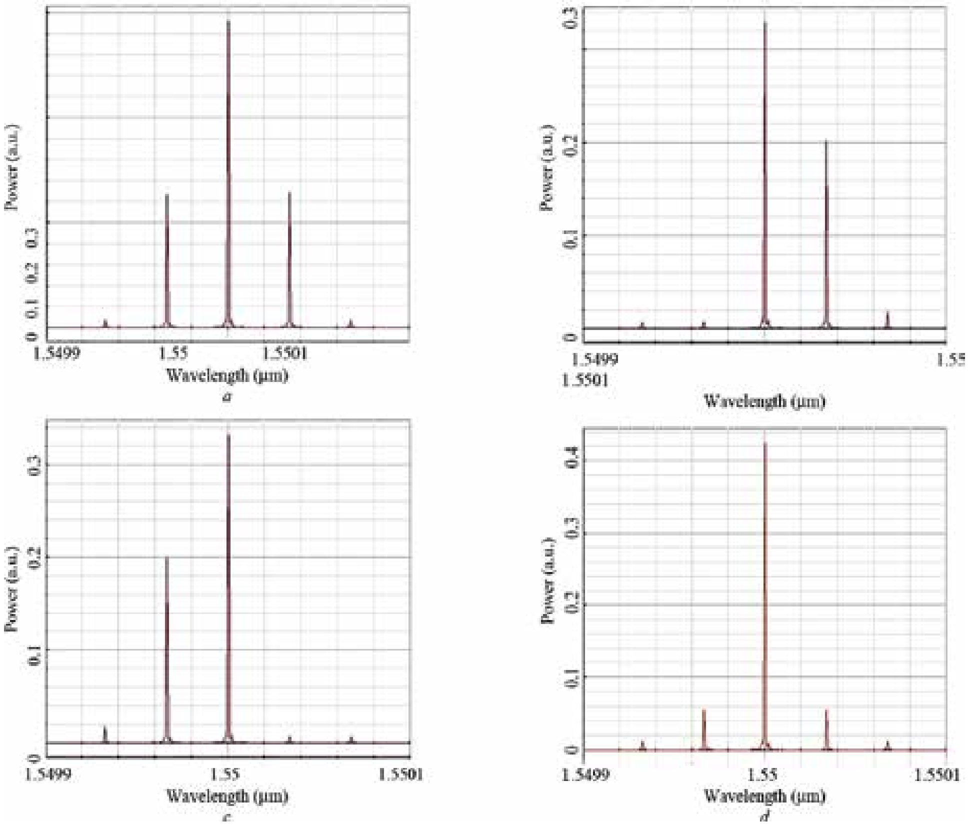


Figure 6. Constructive ΔΦ = 0 (a) and destructive ΔΦ = π/2 (b), ΔΦ = 3π/2 (c), ΔΦ = π (d) interferences on the output of Bob's PM, when phase of Alice's AM $\Phi_A = 0$.

and B92 one. Taking into account that the definition of truth in these statements is not the aim of our chapter, let us consider some results of practical experiments for AM-AM schemes based on acoustic-optical modulators [16], which show us second attempt to implement QKD system without re-modulation.

2.4. Acousto-optic modulation for AM-AM schemes

There is a nonelectro-optical solution of AM-AM scheme based on acousto-optic modulation on Alice's side as well as on Bob's side [16].

In the case of Bragg diffraction, all orders of diffracted radiation except the first become negligibly small, and the frequency offset depends from the direction of laser radiation and sound wave propagation.

For BB84 protocol, two bases are set:

$$\begin{cases} |+;\ 1\rangle = |1\rangle_{\omega_0+\Omega} \\ |-;\ 1\rangle = |1\rangle_{\omega_0-\Omega} \end{cases}$$
$$\begin{cases} |+;\ 2\rangle = \frac{1}{\sqrt{2}}|1\rangle_{\omega_0+\Omega} + \frac{1}{\sqrt{2}}|1\rangle_{\omega_0-\Omega} \\ |-;\ 2\rangle = \frac{1}{\sqrt{2}}|1\rangle_{\omega_0+\Omega} - \frac{1}{\sqrt{2}}|1\rangle_{\omega_0-\Omega} \end{cases}. \qquad (5)$$

The first pair of states $|+;1\rangle$ and $|-;1\rangle$ can be identified without re-modulation, using the filter block consisted from FBG or AWG, tuned on the frequencies $\omega_0 \pm \Omega$ or one of them, similar to the filtering implemented in the second variant of PM-PM scheme [14].

The second pair of states $|+;2\rangle$ and $|-;2\rangle$ is transmitted with the help of modulation on Alice's side. If we use filters without re-modulation on Bob's side, the error can occur, because both photosensors with $\omega_0 \pm \Omega$ filters will trigger. The given states are determined uniquely if re-modulation is used.

Replacing status $|+;1\rangle$ and $|+;2\rangle$ to '1' and $|+;1\rangle$ and $|-;1\rangle$ to '0', Alice and Bob will get an exact match of the sent qubits. This ensures an exact match of QKD protocol to BB84.

Certain difficulty, associated with spatial alignment of used devices as on Alice's so and Bob's sides, characterizes using of acousto-optic modulators in QKD system implementation with frequency encoding. Search for ways to implement bases, described in (5), with the help of electro-optic modulation, led us to use Il'in-Morozov's method [24, 25] for the photon carrier modulation transform.

Il'in-Morozov's method belongs to the methods with full or partial suppression of optical carrier. The theoretical justification for this application and synthesized conjugated bases is obtained by amplitude-phase modulation according to Il'in-Morozov's method we consider in the next section.

3. Tandem AMPM-PMAM structure of QKD system with frequency encoding

3.1. Serial and parallel microwave photonic AMPM one port units

The general model shown in **Figure 7** for a single-port parallel system, where either intensity or phase modulation (or both simultaneously in parallel) can be applied, can represent all the former examples from the point of view of traditional simple microwave photonic (MWP) links.

The impact of all intermediate optical components of quantum channel placed between the electro-optical (EO) and the optoelectronic (OE) conversion stages can be united into an optical transfer function H(ω) (in our case, its FBG as filter for carrier, fiber of channel with losses and so on). Authors of [26], in order to classify these systems, use the term 'filtered MWP links' (FMWPL).

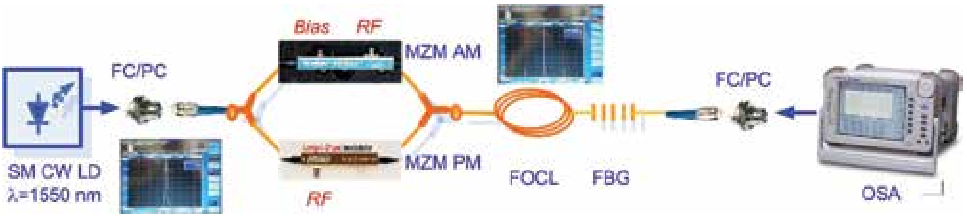


Figure 7. Schematic representation of a general parallel single-port filtered MWP link [25].

The features of FMWPL are evaluated in terms of figures of merit set: the radiofrequency link gain, the noise figure and the spurious free dynamic range [27]. These metrics have been computed for a wide variety of configurations in [26].

In principle, the interest was focused on intensity-modulated direct detection (IMDD) point-to-point links with direct or external modulation, and models were developed detailed description of the effects of the electronic biasing circuits and impedance matching networks [27]. Paper [28] reciprocally considers the inclusion of an arbitrary optical filter, acting as an FM discriminator, for the particular case of directly modulated FMDD links if synchronizing channel will change frequency.

For the AMPM feature analysis, classical generalized scheme of single-port FMWPL was converted from parallel to serial circuit type (**Figure 8**) in order to implement Il'in-Morozov's method.

On the basis of studies carried out in this section, the feasibility of AMPM scheme realized on the amplitude, and phase MZM was theoretically demonstrated. We carried out equations for the calculation of the AMPM scheme output spectrum [29]. The spectrum consists mainly from two components, if phase of PM triggered on π in the minimum of envelope of amplitude-modulated carrier. The difference frequency is equal to modulating one in synchronizing channel.

Figure 9 shows the spectrums of the original quasi-harmonic oscillations of the amplitude-modulated signals structure (**Figure 9a**) and the two frequency structure with partly suppressed carrier obtained by MZM AM in 'zero' point (**Figure 9b**) and fully suppressed carrier

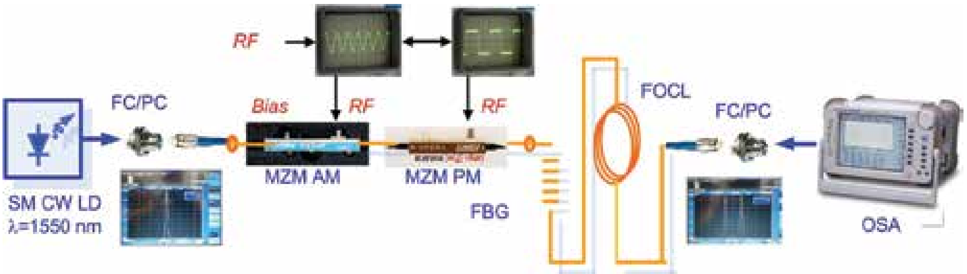


Figure 8. Schematic representation of a general serial single-port filtered MWP link [28].

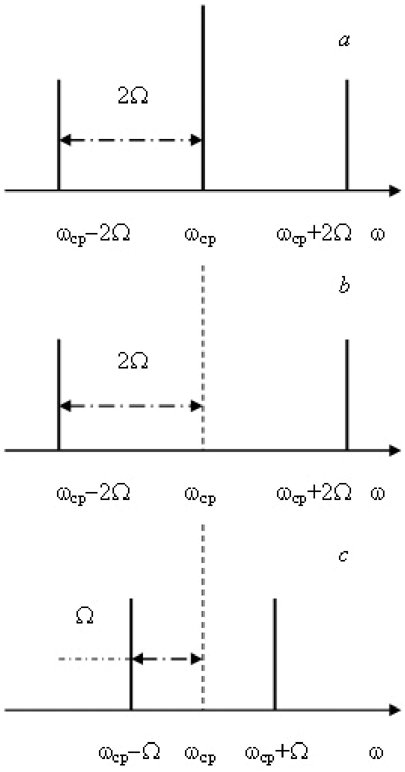


Figure 9. The spectrums of initial AM radiation (a) and output ones from amplitude MZM (b), operating in 'zero' point, and AMPM system based on tandem amplitude and phase MZM (c).

by AMPM method (**Figure 9c**). If these oscillations expose the amplitude detector, the frequency of their envelopes will be different in two times.

As seen from **Figure 9**, the difference frequency between two frequency components of radiation is equal to the frequency 2 Ω or modulating waveforms. Components of higher harmonics can be ignored because of the smallness of their amplitudes.

We obtained the doubled narrowing of the difference frequency if compared to classical schemes of modulation applicable in practice and using a single-amplitude MZM, operating in the 'zero' point of the modulation characteristics [29].

3.2. Tandem AMPM-PMAM scheme

Functional scheme of tandem AMPM-PMAM QKD system with frequency encoding is presented in **Figure 10**.

Alice's side—transmitter, based on a transmitting part of a single-port serial type FMWPL, consists of low-power single mode (frequency) continuous wave laser diode (SM CW LD)—simulator of single photons with carrier frequency ω, amplitude Mach-Zehnder modulator (MZM 1AM) and phase Mach-Zehnder modulator (MZM 1PM).

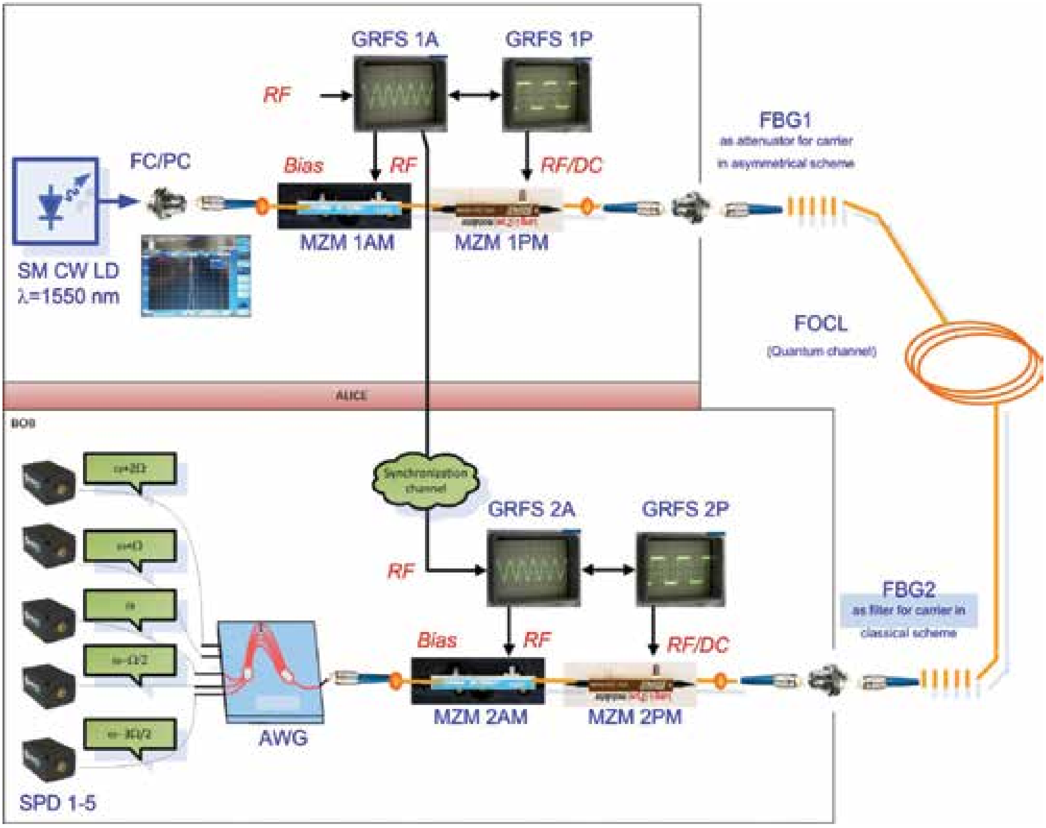


Figure 10. Functional scheme of AMPM-PMAM QKD system with frequency encoding.

Orthogonal polarization controllers, allowing carrier amplitude modulation and controlling the modulator transmission index, when no modulation is needed, can be installed at MZM 1AM input and output. Amplitude and phase modulation parameters are controlled by generator of radiofrequency signals GRFS 1 (A or P) with angular frequency Ω ≪ ω and selectable phase Φ of a pair of conjugate bases 0;π or π/2;3π/2. A source of DC bias serves to select the operating point of the MZM 1 AM modulation characteristics, providing amplitude modulation at zero, quarter-wave and half-wave operating points by submitting to its corresponding 0, Uπ/2 or Uπ input voltage, where Uπ—half-wave voltage of modulator. The modulation factors of MZM 1AM and MZM 1PM are selected to ensure their operation in the linear range. Thus, the radiation at the output port in classical schemes will be limited by components in the range from ω to ω ± 2 Ω, and the filter on FBG2 additionally selects ω [15]. The setting of FMWPL provides the opportunity to work with and without amplitude and phase modulation of photons. In latter, the DC voltage put in MZM 1PM for its opening.

Bob's side—receiver, based on receiving part of single-port serial FMWPL, consists of MZM 2PM, MZM 2AM, filter units (FBG1/AWG) and the block of SPD for emission registration at frequencies ω, ω ± Ω and ω ± 2 Ω (for classical schemes, half part of SPD is shown) and ω, ω ± Ω/2, and ω ± 3 Ω/2 (for advanced schemes, half part of SPD is shown). A more detailed filter pack description will be given below when discussing the variants of QKD scheme implementation.

Special synchronization channel from Alice to Bob [15] serves to transmit information about a modulating signal at frequency Ω, which allows to use on Bob's side radiofrequency modulating signal with the same frequency as Alice and control it with local GRFS 2 (A or P). MZM 2AM and MZM 2PM Bob's modulators are controlled analogously to Alice's ones.

3.3. AMPM-PMAM system implementation for classical QKD schemes

General view of the AMPM-PMAM experimental setup is presented in **Figure 11**.

For amplitude modulation, an amplitude modulator JDSU APE microwave analog is used with operating frequencies band over 4.2 GHz and a half-wave voltage of 3.3 V. The size of the modulator reaches a length of 120 mm and a width of 15 mm. Irregularity of frequency response in the range of 0.13–20 GHz is 7 dB. For the phase modulation, the phase modulator JDSU APE with the working frequency band above 10 GHz was used. The sizes of phase modulator are close to the dimensions of the intensity modulator. It does not require the input (bias) of the operating point.

The range of wavelengths includes an operating wavelength of 1550 nm. Losses of both types of modulators are about 3 dB. Maximum input power is up to 200 mW. As far as the small signal approaches, we are interested in the power of 1 mW, the use of which does not result in nonlinear effects in an optical fiber such as stimulated Mandelstam-Brillouin or Raman scattering [20].

Let us consider the modeling implementation of PM-PM scheme. Laser radiation from the Alice's side, as the source of which the laser optical spectrum analyzer was used, allowing realization of low-power laser analogue, arrived on the MZM 1AM in an open state and a phase modulator MZM 1PM. Further on across the bay of optical fiber SMF-28 of 2 km length, the radiation was received on the Bob's side, where it was re-modulated within the MZM 2PM (MZM 2AM was open) and recorded in the optical spectrum analyzer and photodetector

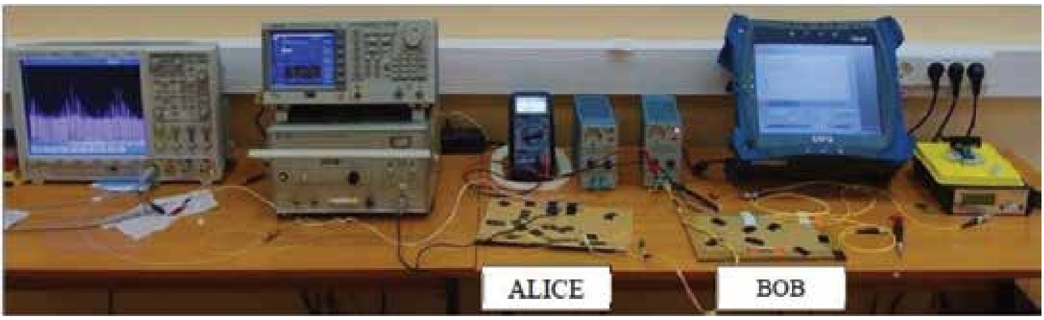


Figure 11. General view of the AMPM-PMAM experimental setup.

devices LSIPD-A75-FA, using filters based on FBG2. The modulation frequency was 4.2 GHz. **Figure 12** shows signal spectrograms in destructive and constructive interference on the lateral frequencies ω ± Ω.

Thus, it was shown that AMPM-PMAM system could be implemented, for example, as PM-PM QKD scheme with frequency encoding based on classical approaches. It should be highlighted that in classical approaches transfer efficiency $P(\omega \rightarrow \omega \pm \Omega)$ at low modulation coefficients does not reach high values. The main energy is concentrated at the carrier frequency, and the proportion of energy of the side components is very small. Then, in order to compensate NPM, we have to extract carrier, so the efficiency of photon registration on subcarriers is very small also.

This factor gave us additional arguments to implement modulation transformation of photon carrier based on Il'in-Morozov's method [24, 25]. The procedures are concluded in amplitude modulation and phase commutation (PC) of optical carrier with its suppression and full energy transfer in subcarriers.

Let us evaluate the possibility of perspective AMPC-PCAM system implementation in two variants. First is symmetrical structure with amplitude modulation and phase commutation at the Alice's side and amplitude re-modulation and phase re-commutation on the Bob's side. Second is variant, in which the asymmetric structure of the QKD with amplitude modulation and phase commutation on the Alice's side and only passive filtering based on the FBG1/AWG on the side of Bob are implemented.

3.4. Estimation of possibility AMPC-PCAM scheme implementation

The operation of AMPC-PCAM QKD system with frequency encoding is based on amplitude-phase modulation conversion of the photon carrier realized with the procedures described by Il'in-Morozov's method and its implementations on one or two modulators [29, 30]. Variants of constructive AM interference are shown in **Figure 13** in the case of constructive PC on Alice and Bob sides.

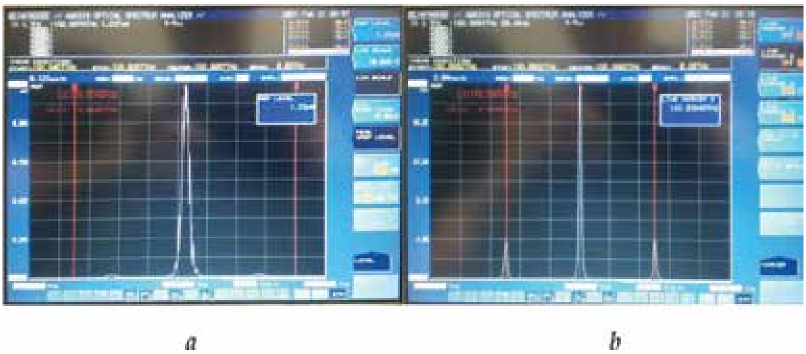


Figure 12. The spectrogram of the signal in destructive (a) and constructive (b) interference on the lateral frequencies ω ± Ω in PM-PM scheme implementation.

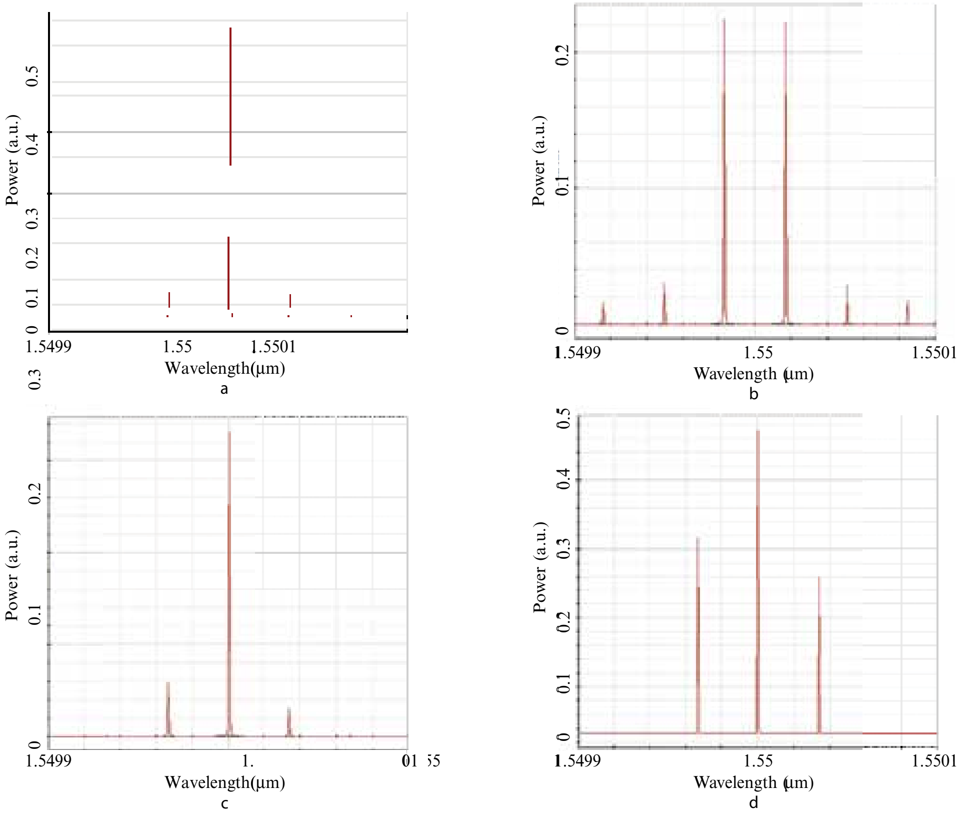


Figure 13. Variants of constructive interference with the coincidence of the parameters AM and PC on the side of Alice and Bob: the results of AM (a) and PC (b) at the output of modulators on the side of Alice; the results of PC (c) and AM (d) at the output of modulators on the side of Bob.

To simulate the scheme and carry out the project evaluations, the modeling principles of single-port modulation radio photon of serial link type proposed by us in [29, 31, 32] and photonic simulation of electro-optic modulators [33] were used.

The implementation of Il'in-Morozov's method for the modulation conversion P(ω → ω ± nΩ), where n is the number of subcarriers, will provide:

1. high-efficiency optical carrier transfer into subcarrier left and right components (up to 0.6–0.8 amplitude for each of them), high level of spectral purity under the optimal conversion parameters (only first or additionally third number subcarriers are existing);

2. NPM decreasing (carrier is absent), to exclude spectrum filter, which separates carrier and sidebands, to increase signal-to-noise ratio, because we can register photon by envelope amplitude on difference frequency Ω, which lies in SPD spectrum region with minimum level of noises;

3. synthesis of whole number subcarriers (n ≥ 1) and fractional ones (n/2, for n ≥ 1) that will improve the cryptographic protection level of the communication system, in case of Eve discoveries the frequency of synchronization channel;

4. implementation of an asymmetric system with a totally passive data filtering sent by Alice, on the of Bob's side without re-modulation or re-commutation.

Let us make the first three statements plain.

Figure 14 shows the output spectrum of AMPC procedure, which can be described as two-frequency symmetrical radiation with fully suppressed carrier and fractional harmonics nΩ/2 (here n = 1 for **Figure 14a** and n = 2 for **Figure 14b**).

In this case, we can decrease NPM (carrier is absent) in FOLC and increase signal-to-noise ratio, because we can register photon by envelope amplitude on difference frequency Ω, which lies in SPD spectrum region with minimum level of noises. The point about separation filter necessity is a question.

Thus, if we realize full re-modulation of Alice's phases in phases on Bob's side, we get spectrum, as shown in **Figure 12b**, after Bob's PM, and, as shown in **Figure 12a**, after Bob's AM. Therefore, the carrier is present, but only in receiver, not in quantum channel, and its influence on channel characteristics is minimized.

Let us clarify the last from above four statements.

Analysis shows that we can realize classical symmetrical QKD scheme with modulation and re-modulation. To do this, we are going to select the two bases for frequency-encoding the photon states in AMPC of asymmetrical type without re-modulation/re-commutation and explain the order they are received.

$$\begin{cases} |+;\ 1\rangle = |1\rangle_{\omega_0} \\ |-;\ 1\rangle = \frac{1}{\sqrt{2}}|1\rangle_{\omega_0+\Omega} - \frac{1}{\sqrt{2}}|1\rangle_{\omega_0-\Omega} \end{cases}$$
$$\begin{cases} |+;\ 2\rangle = \frac{1}{\sqrt{2}}|1\rangle_{\omega_0+\Omega/2} - \frac{1}{\sqrt{2}}|1\rangle_{\omega_0-\Omega/2} \\ |-;\ 2\rangle = \frac{1}{\sqrt{2}}|1\rangle_{\omega_0+3\Omega/2} - \frac{1}{\sqrt{2}}|1\rangle_{\omega_0-3\Omega/2} \end{cases} \tag{6}$$

The state $|+;1\rangle$ is the unmodulated photon transmitted from SM CW LD, through the open Alice's modulators. The state $|-;1\rangle$ is amplitude-modulated photon (frequency of modulation is Ω; 'zero' operating point of MZM 1 AM; absence of phase commutation). The state $|+;2\rangle$

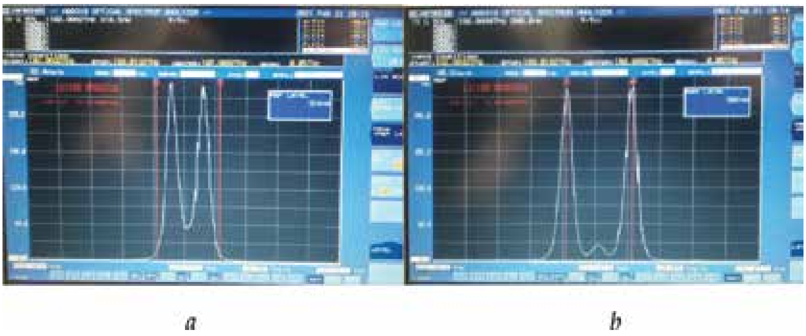


Figure 14. The output spectrum of AMPC procedure for propagation in FOLC: frequency encoding of second $|-;\ 1\rangle$ and third $|+;\ 2\rangle$ photon states is shown.

is full tandem amplitude-modulated and phase-commutated photon (quadrature operating point of MZM 1 AM; amplitude modulation coefficient m = 0.59; phase commutation 0/π with frequency Ω/2 in MZM 1 PM). The state $|-;2\rangle$ is described by lateral components obtained at the same parameters of amplitude modulation, but MZM 1 PM had phase commutation 0/π with frequency 3 Ω/2. The parameter control of the amplitude modulation and phase commutation is performed by GRFS 1A and 1P with a corresponding change in functions.

Frequency encoding of second $|-;\ 1\rangle$ and third $|+;\ 2\rangle$ photon states is presented in **Figure 14b** and **a**, respectively. As can be seen from last paragraph and in **Figure 14**, all four photons states can be passively allocated through a system of filters tuned respectively to frequencies $\omega_0 \rightarrow |+;1\rangle$, $\omega_0 \pm \Omega/2 \rightarrow |+;2\rangle$, $\omega_0 \pm \Omega \rightarrow |-;1\rangle$, $\omega_0 \pm 3\,\Omega/2 \rightarrow |-;2\rangle$. Thus, AMPC-FBG/AWG asymmetric system can be constructed as shown in **Figure 10**, but without modulators on Bob's side.

4. Conclusion

The implementation of tandem AMPM(C)-PM(C)AM schemes of symmetric and asymmetric types and analysis of their advantages and disadvantages will be considered in subsequent publications and are the goal of future work. In this chapter, we demonstrate only the opportunity of its creation, the theoretical justification of their bases and preliminary evaluation of its characteristics. We show that tandem AMPM(C)-PM(C)AM QKD system, based on microwave photonic principles transferred to photon level, can be used as universal frequency encoding system.

The application of such type QKD system will allow us to use multiple levels of cryptographic security, including modulation, commutation schemes and protocol choices, so and choice from re-modulation (re-commutation) and passive detection procedures. The two-time increase of electro-optic modulator number will undoubtedly increase the cost of the system. However, this increasing can be minimized by its universality, and therefore, the expanded functionality, in comparison with each of the known and described by us earlier systems with frequency encoding.

In addition, the high spectral purity and stability of photon tandem modulation based on Il'in-Morozov's method should be highlighted. Qualitatively, we presented the advantages of carrier excluding from quantum communication channel. First, it was shown that effects of nonlinear phase modulation are decreased. Second, in this case, the security condition is stricter to a level of single photon transmission. Third, the signal-to-noise ratio of the system is increased and leads to a significant decrease in the number of errors in the given channel.

For the first time, it was shown the possibility of constructing a nonclassic asymmetric structure using modulators only on the Alice's side and passive filters based on fiber Bragg or arrayed waveguide gratings on the Bob's side.

Therefore, the QKD technology with frequency coding, based on the modulation conversion of an optical carrier with its complete or partial suppressing in the case of tandem amplitude modulation and phase modulation/commutation, is the promising tool for designing perspective quantum communication channels.

Acknowledgements

Ministry of Education and Science of Russian Federation supported this work: state R&D task to Kazan National Research Technical University n.a. A.N. Tupolev—Kazan Aviation Institute ("Asymmetry", base task no. 8.6872.2017/8.9).

Author details

Oleg G. Morozov[1]*, Airat J. Sakhabutdinov[1], Gennady A. Morozov[1] and Il'daris M. Gabdulkhakov[2]

*Address all correspondence to: microoil@mail.ru

1 Kazan National Research Technical University n.a. A.N. Tupolev-KAI, Kazan, Republic of Tatarstan, Russia

2 PJSC «Tattelecom», Kazan, Russia

References

[1] Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Lütkenhaus N, Peev M. The security of practical quantum key distribution. Reviews of Modern Physics. 2009;**81**:1301-1310. DOI: 10.1103/RevModPhys.81.1301

[2] Muller A, Breguet J, Gisin N. Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km. Europhysics Letters. 1993;**23**:383-388. DOI: 10.1209/0295-5075/23/6/001

[3] Zbinden H, Gautier JD, Gisin N, Huttner B, Muller A, Tittel W. Interferometry with Faraday mirrors for quantum cryptography. Electronics Letters. 1997;**33**:586-588. DOI: 10.1049/el:19970427

[4] Inoue K, Waks E, Yamamoto Y. Differential phase shift quantum key distribution. Physical Review Letters. 2002;**89**:037902. DOI: 10.1103/PhysRevLett.89.037902

[5] Duraffourg L, Merolla J-M, Goedgebuer J-P, Mazurenko Y, Rhodes WT. Compact transmission system using single-sideband modulation of light for quantum cryptography. Optics Letters. 2001;**26**(18):1427-1429. DOI: 10.1364/OL.26.001427

[6] Dixon AR, Yuan ZL, Dynes JF, Sharpe AW, Shields AJ. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. Optics Express. 2008;**16**:18790-18799. DOI: 10.1364/OE.16.018790

[7] Sadeev TS, Morozov OG. Investigation and analysis of electro-optical devices in implementation of microwave photonic filters. Proceedings of SPIE. 2012;**8410**:841007. DOI: 10.1117/12.923121

[8] Mora J, Ruiz-Alba A, Amaya W, Garcia- Muñoz V, Martinez A, Capmany J. Microwave photonic filtering scheme for BB84 subcarrier multiplexed quantum key distribution. IEEE Topical Meeting on Microwave Photonics. 2010:286-289. DOI: 10.1109/MWP.2010.5664176

[9] Aybatov DL, Morozov OG, Sadeev TS. Dual port MZM based optical comb generator for all optical microwave photonic devices. Proceedings of. SPIE. 2011;**7992**:799202. DOI: 10.1117/12.887273

[10] Merolla J-M, Mazurenko Y, Goedgebuer J-P, Duraffourg L, Porte H, Rhodes WT. Quantum cryptographic device using single-photon phase modulation. Physical Review. 1999;**A60**(3):1899-1905. DOI: 10.1103/PhysRevA.60.1899

[11] Bennett CH. Quantum cryptography using any two nonorthogonal states. Physical Review Letters. 1992;**68**:3121-3124. DOI: 10.1103/PhysRevLett.68.3121

[12] Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. 1984. pp. 175-179. DOI:10.1016/j.tcs.2014.05.025

[13] Xavier GB, Weid JP. Modulation schemes for frequency coded quantum key distribution. Electronics Letters. 2005;**41**(10):607-608. DOI: 10.1049/el:20050466

[14] Bloch M, McLaughin SW, Merolla J-M, Patois F. Frequency-coded quantum key distribution. Optics Letters. 2007;**32**(3):301-303. DOI: 10.1364/OL.32.000301

[15] Gleim AV, Egorov VI, Nazarov YV, Smirnov SV, Chistyakov VV, Bannik OI, et al. Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference. Optics Express. 2016;**24**(3):2619-2633. DOI: 10.1364/OE.24.002619

[16] Zang T, Yin Z-Q, Han Z-F, Guo G-C. A frequency-coded quantum key distribution scheme. Optics Communications. 2008;**281**:4800-4802. DOI: 10.1016/j.optcom.2008.06.009

[17] Smith RA, Reddy DV, Vitullo DL, Raymer MG. Verification of a heralded, two-photon fock state with a gang of detectors. Frontiers in Optics. 2015;**FTu3G**:FTu3G.2. DOI: 10.1364/FIO.2015.FTu3G.2

[18] Gaidash AA, Egorov VI, Gleim AV. Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices. Journal of Physics: Conference Series. 2016;**735**:012072. DOI: 10.1088/1742-6596/735/1/012072

[19] Morozov OG, Il'in GI, Morozov GA, Nureev II, Misbakhov RS. External amplitude-phase modulation of laser radiation for generation of microwave frequency carriers and optical poly-harmonic signals: An overview. Proceedings of SPIE. 2015;**9807**:980711. DOI: 10.1117/12.2231948

[20] Morozov OG, Gabdulkhakov IM, Morozov GA, Zagrieva AR, Sarvarova LM. Frequency-coded quantum key distribution using amplitude-phase modulation. Proceedings of SPIE. 2015;**9807**:98071F. DOI: 10.1117/12.2230665

[21] Ruiz-Alba A, Calvo D, Garcia-Munoz V, Martinez A, Amaya W, Rozo JG, Mora J, Capmany J. Practical quantum key distribution based on BB84 protocol. Waves. 2011;**3**:4-14. URL: https://riunet.upv.es/handle/10251/53967

[22] Mérolla J-M, Mazurenko Y, Goedgebuer J-P, Porte H, Rhodes WT. Phase-modulation transmission system for quantum cryptography. Optics Letters. 1999;**24**:104-106. DOI: 10. 1364/OL.24.000104

[23] Kumar KP. Optical modulation schemes for frequency-coded quantum key distribution. IEEE National Conference on Communications; Chennai, India; 29-31 Jan. 2010; 2010. pp. 1-5. DOI: 10.1109/NCC.2010.5430155

[24] Morozov OG, Aybatov DL. Spectrum conversion investigation in lithium niobate Mach-Zehnder modulator. Proceedings of SPIE. 2010;**7523**:75230D. DOI: 10.1117/12.854957

[25] Morozov OG. RZ, CS-RZ and soliton generation for access networks applications: Problems and variants of decisions. Proceedings of SPIE. 2012;**8410**:84100P. DOI: 10.1117/12. 923115

[26] Gasulla I, Capmany J. Analytical model and figures of merit for filtered microwave photonic links. Optics Express. 2011;**19**(20):19758-19774. DOI: 10.1364/OE.19.019758

[27] Cox CH III. Analog Photonic Links: Theory and Practice. Cambridge: Cambridge University Press; 2004. 289 pp

[28] Wyrwas JM, Wu MC. Dynamic range of frequency modulated direct-detection analog fiber optic links. Journal of Lightwave Technology. 2009;**27**(24):5552-5562. DOI: 10.1109/ JLT.2009.2031986

[29] Il'In GI, Morozov OG, Il'In AG. Theory of symmetrical two-frequency signals and key aspects of its application. Proceedings of SPIE. 2014;**9156**:91560M. DOI: 10.1117/12.2054753

[30] Petoukhov VM, Akhtiamov RA, Morozov OG, Il'in GI, Pol'ski YE. Two-frequency IR CW LFM lidar for remote sensing of hydrocarbons and gas vapor. Proceedings of SPIE. 1997;**3122**:339-346. DOI: 10.1117/12.292705

[31] Morozov GA, Morozov GA, Il'in GI, Il'in AG. Instantaneous frequency measurements of microwave signal with serial amplitude-phase modulation conversion of optical carrier. Proceedings of SPIE. 2014;**9533**:95330Q. DOI: 10.1117/12.2181435

[32] Morozov OG, Talipov AA, Nurgazizov MR, Denisenko PE, Vasilets AA. Instantaneous frequency measurement of microwave signals in optical range using «frequency-amplitude» conversion in the π-phase shifted fibre Bragg grating. Proceedings of SPIE. 2014;**9136**:91361B. DOI: 10.1117/12.2051126

[33] Capmany J, Fernandez-Pousa CR. Quantum modelling of electro-optic modulators. Laser & Photonics Reviews. 2011;**5**(6):750-772. DOI: 10.1002/lpor.201000038

Chapter 7

Stochastic Quantum Potential Noise and Quantum Measurement

Wei Wen

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.74253

Abstract

Quantum measurement is the greatest problem in quantum theory. In fact, different views for the quantum measurement cause different schools of thought in quantum theory. The quandaries of quantum measurement are mainly concentrated in "stochastic measurement space", "instantaneous measurement process" and "basis-preferred measurement space." These quandaries are incompatible with classical physical laws and discussed many years but still unsolved. In this chapter, we introduce a new theory that provided a new scope to interpret the quantum measurement. This theory tells us the quandaries of quantum measurement are due to the nonlocal correlation and stochastic quantum potential noise. The quantum collapse had been completed by the noised world before we looked, and the moon is here independent of our observations.

Keywords: quantum measurement, quantum collapse, quantum potential noise, Feynman path integral

1. Introduction

Schrödinger cat was born from the thought experiment of Schrödinger in 1935. However, after more than 80 years, we still do not know whether it is dead or alive in its sealed box. According to the modern quantum mechanics, based on Copenhagen interpretation, the fate of this cat is entangled with the Geiger counter monitor in its box, and the cat is in a "mixed state"—both dead and alive—if we do not open the box to look at it. It is a miserable and mystical cat, which seems its fate depends on our look. Yes, it just seems, because we deeply doubt that the power of our glimpse can really make the cat alive or dead. This doubt is not the business about human self-confidence, but the fear of our fate determination. If the glimpse of us can determine the cat's fate, who determines our fate? Trouble never singly comes; many researches find that "the moon is not there" in experiments [1] responding to what Albert Einstein said, "I like to think that the moon is there even if I don't look at it." According to the physicist's research, Albert Einstein seems worried because the world is quantum world and all things obey quantum mechanics. This means all the definite statuses we have observed are due to "a glimpse" of us or the god. Really? Is really the moon not here if we do not look at it, does really the cat not exist if we do not look at it, and do we not exist if the god does not look at us?

It must be something to worry because the moon exists more than 4.5 billion years as the astronomer finding, which is much more than human history. We are not going to discuss the superpower of human and if the god exists or not in this book. We return to the fundamental of quantum mechanics and find that the hidden actor, quantum measurement, is the crime culprit that causes these puzzling questions.

There is a confliction in modern quantum physics after its birth. The confliction is concerning the full description between the superposition state for the behavior of matter on the microscopic level and the definite-status appearance as what we can observe on the macroscopic level in the real world. Schrödinger proposed Schrödinger cat in his essay to illustrate the "putative incompleteness" of quantum mechanics, but many researches show that quantum mechanics is still the best one of these "not satisfied theories." To alleviate the theory-to-world confliction, a new conception, quantum measurement, is brought out. It is the basic assumption in quantum mechanics, thought that the superposition state will be collapsed into one of the eigenstates with the square of amplification probability if we do a quantum measurement. Although the quantum measurement bridges the gap of the different behaviors of subatomic level and the macro-world, some problems still remain. For example, its physical mechanism is dim. We do not know what will lead to the quantum measurement and how the process that the quantum measurement undergoes. The words "stochastic", "instantaneous" and "irreversible" torment us more than 70 years, and we still have no way to integrate them into the "determinate", "time-costed" and "reversible" quantum evolution. In fact, the manual division for the world into two parts, quantum world and quantum measurement apparatus, is not satisfied, and we are finding a uniform description.

In this chapter, we will overview the mechanism of quantum measurement and the main kinds of interpretation of quantum measurement. Among these interpretations, a promised theory which can well interpret the quantum measurement quandaries—why the quantum state collapses into some eigenstates with "stochastic" and "instantaneity", and what causes the "basis-preferred"—is detailed. The advantage of this theory is it is just an extension of Feynman path integral (FPI) and is obviously compatible with the classical quantum theory. According the conclusions of this theory, we show that the "noise" world (or apparatus here when we do an experiment) causes the "random" and "nonlocal" mechanism of the quantum collapse. Actually, the world exists due to itself, and the god can go to have a rest.

2. What is the quantum measurement?

Quantum measurement is different from the classical measurement, in which the measurement accuracy is dependent on the measurement instruments. It means, we could infinitely approach the "absolute exact value" by upgrading instruments or improving methods in the classical measurement realm. However, the things change when we access to the quantum world. In quantum world, the "accuracy" does not exist. We cannot speak that the velocity of an electron is 1376.5 m/s or the distance of two electrons is 20 nm, etc., because these physical quantities exist in the form of quantum states in quantum world. Objects are always in the superposition states of these kinds of the basis state, such as momentum, position, energy, spin and so on. We can just get one of the basis states under every measurement, and the "absolute exact value" is never revealed under one measurement unless the state of the object is in the basis state.

In quantum mechanics, the projection operator is defined as $\widehat{P}_{\varphi_i} = |\varphi_i\rangle\langle\varphi_i|$, where $|\varphi_i\rangle$ is an element of the basis-state set $\{|\varphi_k\rangle\}$. The measurement output for a mechanical quantity operator $\widehat{Q}$ under one quantum measurement is $Q_i = \left\langle \varphi_i \middle| \widehat{Q} \middle| \varphi_i \right\rangle = Tr\left(\widehat{P}_{\varphi_i}\widehat{Q}\right)$, and the initial state will instantaneously collapse into the basis state $|\varphi_i\langle$ with the probability $p_i = Tr\left(\widehat{P}_{\varphi_i}\widehat{\rho}_I\right)$, where $\widehat{\rho}_I$ is the initial density matrix of an object, after the quantum measurement. For multi-measurements, the output we get is the average value $\tilde{Q} = \sum_i p_i Q_i = Tr\left(\widehat{Q}\,\widehat{\rho}_I\right)$, and the final state of the many object systems becomes $\rho_O = \sum_i p_i \widehat{P}_{\varphi_i}$, which is very different from the initial state ρ_I.

This kind of measurement, to be exact, is the projective measurement. A more general formulation of measurement is the positive-operator valued measure (POVM), which can be seemed as the partial measurement in the subsystem of a projective measurement system. No matter what kind of quantum measurements there is, it is the kind of destructive manipulations and irreversible. It destroys the old state and rebuilds a new mixed state. The definition of the quantum measurement is simple and definite, but the problem is that we do not know why the quantum measurement acts as these strange behaviors. The irreversibility and unpredictability are incompatible with the smooth Schrodinger differential equation and are hated by physicists. What kind of objects has priority to do the quantum measurement? Taking the experiment of two-slit interference of electrons, for example, the detector behind the slits usually is regarded as a measurement tool, but the detector itself, which may be a microcavity or atom ensemble, is also a physical system and obeys the quantum mechanism. Therefore, it seems that the process of a quantum measurement is the interaction between the detector and electrons and should be a "quantum evolution process". However, the quantum evolution process is non-destructive and reversible. In fact, in the real world, it is hard for us to distinguish strictly which is the quantum evolution operation and which is the quantum measurement.

The second problem is the space–time nonlocality in the quantum measurement process. This nonlocality exists not only in the correlation between particles but also in the wave function of single particle. We still take the experiment of two-slit interference of electrons, for example. If the detector behind the slits has detected the signal and we can distinguish which slit the electrons pass, then the interference phenomenon will disappear. In language of quantum mechanics, the diffused wave function $\psi(x,t)$ of the electron will collapse into $\delta(x_0,t)$ immediately after this measurement. This process is very fast and does not seem to need to cost time. How this process happens and whether this process violates the law of causation of relativity theory are still unclear for us.

The third problem is the basis-preferred problem. The basis-preferred problem refers to a quantum system that is measured which prefers to collapse to a set of eigenstates. For example, a spin system with an initial state $|\psi\rangle\rangle = a|\uparrow\rangle\rangle + b|\downarrow\rangle\rangle$ can collapse into the state of the set $\{|\uparrow\rangle\rangle, |\downarrow\rangle\rangle\}$, and it can also collapse into the state of the set $\left\{1/\sqrt{2}(|\uparrow\rangle\rangle + |\downarrow\rangle\rangle), 1/\sqrt{2}\,(|\uparrow\rangle\rangle - |\downarrow\rangle\rangle)\right\}$, but under a certain measurement, this state prefers one of these sets. Why the state prefers some basis set under quantum measurement? Does it have awareness?

Without any exaggeration, quantum measurement is one the most interesting and fascinating topics in quantum theory. There are too many unsolved mysteries in quantum measurement, and these spur us to further understand the quantum measurement and find the answers.

3. The main kinds of interpretation for quantum measurement

There are more than 10 kinds of interpretations for quantum measurement in quantum mechanics, such as Copenhagen interpretation, quantum logic, many worlds interpretation, stochastic interpretation, many-minds interpretation, etc. In this chapter, we just choose four of them to expound. According this section, we will know how difficult for physicists to solve these problems in one theory.

3.1. The Copenhagen interpretation

The Copenhagen interpretation was formed in 1925 to 1927 by Niels Bohr and Werner Heisenberg. In fact, it is still the most commonly taught interpretations of quantum mechanics today.

According to the Copenhagen interpretation, the physical law that microscopic objects obey are different from that the macroscopic objects obey. Microscopic objects can be in superposition states, but the macroscopic objects are forbidden. According to the Copenhagen interpretation, the statuses of macroscopic objects are definite. We can say a macroscopic object is in this status or not, but cannot say this macroscopic object is both in this status and not. Now that the laws in microscopic world and macroscopic world are different, then the Copenhagen interpretation assumes the existence of macroscopic measurement apparatuses that obey classical physics to make measurement for microscopic objects that obey quantum mechanics.

However, this assumption does not solve the problems of quantum measurement. It throws all the problems to the macroscopic apparatuses, but it even cannot answer how to distinguish the macroscopic object that obeys the classical laws and microscopic ensemble that obeys the quantum mechanics. Moreover it also cannot answer how the nonlocality produces in quantum measurement process because, there is no seed for nonlocality growing no matter in classical physics or quantum mechanics.

3.2. Many worlds interpretation

Many worlds interpretation was proposed by Hugh Everett in 1952. It supposes that there are a large, perhaps infinite, number of universes and every alternate state is in one of these universes [2, 3]. Many worlds interpretation denies the wave function collapse under quantum measurement. It asserts that the object that will be measured and the observer that will do the measurement are in a relative state. Each measurement will be a branch point and makes observer enter a universe. According to the thought of many worlds interpretation, the Schrödinger cat is alive in a universe and dead in the other universe. After the measurement, the observer will enter one of these two universes.

The advantage of this interpretation is that the discussion of collapse mechanism is avoided. However, the basis-preferred problem is still the big issue in many worlds interpretation although the quantum decoherence had been introduced into in the period of "post-Everett". Some researchers still think the many worlds interpretation of quantum theory exists only to the extent that the associated basis problem is solved [4–6]. Using the decoherence to define the Everett branches will lead to an approximate specification of a preferred basis and contradicts with the "exact" definition of the Everett branches.

3.3. Many-minds interpretation

Many-minds interpretation is the extension of many worlds interpretation. It was proposed by Heinz-Dieter Zeh in 1970 to solve the "branch determining problem" and the puzzling concept of observers being in a superposition with themselves in many worlds interpretation [7–9]. The thought of this interpretation is when an observer measures a quantum system, then a state that is consistent with minds which produced by the observer brain, called mental states, will entangle with this quantum system. The mental state of the brain corresponding with this system is involving, and ultimately, only one mind is experienced, leading the others to branch off and become inaccessible. In this way, every sentient being is attributed with an infinity of minds, whose prevalence corresponds to the amplitude of the wave function. As an observer checks a measurement, the probability of realizing a specific measurement directly correlates to the number of minds they have where they see that measurement.

However, like the many worlds interpretation, the many-minds interpretation is still a local theory. Although the correlations of individual minds and objects could be the violation of Bell's inequality, the interactions between them that only take place are local, and only the separated events that are space-like separated could influence the minds of observers. Additionally, it tosses the basis-preferred problem to the mentality of observer and makes this physical problem fall into an endless discussion of mental state of human.

3.4. Dynamical reduction models

The theory of dynamical reduction models is a nonlinear and stochastic modification of the Schrödinger equation. It is proposed by Bassia and Ghirardia [10]. They integrated the master equation and linear Schrödinger equation and proposed a new nonlinear differential equation. This theory successfully solves the problems of "stochastic output" and "preferred basis" in quantum measurement and deduced the Born probability rule basing on the white noise model. However, it is still a nonrelativistic theory and remains the nonlocality problem.

4. The extended Feynman path integral and quantum measurement

4.1. Why is it concerning with the Feynman path integral?

As we know, in the history of the quantum theory, there are three equivalent expressions, namely, the differential equation of Schrödinger, the matrix algebra of Heisenberg and the path integral formulation of Feynman. However, these three expressions have their own focuses. The Schrodinger and Heisenberg expressions focus on the evolution of states and operations, respectively, whereas the path integral formulation of Feynman on the "correlation" of point to point as states is evolving [11]. On the other hand, in quantum mechanics, when do a measurement on a wave function diffusing in all of space, such as the measurement of the position of an electron in the experiment of double-slit interference, we will find that the whole wave function will instantaneously collapse to this position measured with some probabilities. Obviously there may be some inner "correlation" in wave function transferring the action of the measurement from local part to whole. These two "correlations" have common characters and may be unified to be one.

Moreover, we notice that the action integral in Feynman path integral formulation is the classical form. The classical physics is born to be a local theory and of course cannot exhibit the character of nonlocality. However, the relativity theory is different. In relativity theory, the time and space are coupling. Beyond the light cones in Minkowski space, the space-time causality is broken, and this may cause the nonlocality. The superluminal velocities are forbidden in real world, but for a connection description of virtual paths in the path integral theory, it might be practicable. What will happen when we extend the classical action to relativistic action? Could the superluminal trajectories included in possible paths to calculate quantum amplitude in the Feynman theory cause the nonlocality? How is the relationship between "unitary evolution operation" and "quantum measurement"? These questions will be revealed when we extend the Feynman path integral.

4.2. How to extend the Feynman path integral?

The formulation for Feynman path integral can be written as

$$K(r, r_0; t, t_0) = C\sum\nolimits_{allpaths} \exp\left(iS/\hbar\right) \tag{1}$$

where the coefficient C is a constant independent of paths and S is the action with classical form

$$S(t_0, t_1) = \int_{t_0}^{t_1} L(\acute{r}(t), r(t))dt \tag{2}$$

$K(r, r_0; t, t_0)$ in Eq. (1) is the propagator and defined into

$$K(r, r_0; t, t_0) = \langle\left\langle r \middle| \widehat{U}(t, t_0) \middle| r_0\rangle\right\rangle \tag{3}$$

Eq. (1) reveals an important assumption in Feynman path integral: the weights of different paths for propagator are the same. This assumption makes Feynman path integral very successful in nonrelativistic quantum theory, but it is also the top offender that impedes the integration between Feynman path integral and relativity in non-field theory. Why should this be?

For the extension, it is necessary to break up this assumption, and Eq. (1) should be written into a more general formulation in the following:

$$F(r, r_0; t, t_0) = R\sum\nolimits_{allpaths} W(\wp)\exp\left(iS/\hbar\right) \tag{4}$$

where R is the parameter that is independent of paths and $W(\wp)$ is the weight function with paths [13]. Additionally, some rules should be set to limit the range of choices for R and $W(\wp)$:

a. The formulation should be simple and concise.

b. It should obey the combination rule because the propagator is linear.

c. It is consisted by the four-dimension scalars, vectors and tensors.

d. It should be transformed into Feynman path integral in low-energy and low-velocity condition.

Under these four limitations, the forms of R and $W(p)$ are very few. The final forms of R and $W(p)$ chosen in extended Feynman path integral are

$$R = \frac{1}{\sqrt{2i\pi\hbar c^2}}\frac{H'}{\sqrt{mc^2 + H'}}; W(\wp) = \frac{\mathbb{P}(\wp)}{\mathcal{P}(\wp)}(\varDelta\tau)^{-1/2} \tag{5}$$

The H' in Eq. (5) is the main Hamiltonian:

$$H' = \sqrt{m^2c^4 + (p - A_0)^2c^2} \tag{6}$$

and

$$\mathbb{P}(\wp) = \int_{t_0}^{t} |P| d\tau; \mathcal{P}(\wp) = \int_{t_0}^{t} \left|\sqrt{2mT}\right| d\tau \tag{7}$$

P, T and $\varDelta\tau$ are called the momentum, kinetic energy and proper time in terms of four-dimensional space–time, respectively:

$$|P| = \frac{mv}{\sqrt{1 - v^2/c^2}}, T = \frac{mc^2}{\sqrt{1 - v^2/c^2}} - mc^2, \varDelta\tau = \int_{t_0}^{t} \frac{1}{\sqrt{1 - v^2/c^2}} d\tau \tag{8}$$

The expressions of $W(\wp)$ and R are very interesting. As we can see, under the low-energy and low-velocity condition, $H' \ll mc^2$ and $v \ll c$, then $R = \frac{1}{\sqrt{2i\pi\hbar c^2}}$ and $W(\wp) = (t - t_0)^{1/2}$ because $|P| = \sqrt{2mT}$ in classical physical theory. This means Eq. (4) can be transformed into the Feynman path integral if we choose the formulations of $W(p)$ and R as shown in Eq. (5). What is concerning then for us is what we can get from Eq. (4) under very high energy and velocity.

4.3. The new differential equation and Klein-Gordon equation

It is hard to directly calculate the value of Eq. (4) because the path integral is not normal integral term and the normal integral method is invalid for Eq. (4). A way to get some results from Eq. (4) is to follow the method that Feynman used [11, 12]. We consider a minimal evolution time process, $t = t_0 + \varepsilon$, where $\varepsilon \to 0$. In this process:

$$\psi(r, t_0 + \varepsilon) = \int_{-\infty}^{\infty} \psi(r_0, t_0) F(r, r_0; t_0 + \varepsilon, t_0) dr_0 = R \int_{-\infty}^{\infty} \psi(r_0, t_0) W(\wp) dr_0 \tag{9}$$

When $\varepsilon \to 0$, the weight function $W(\wp)$ can be simply expressed the term of

$$W(\wp) = \frac{\left(1 + \sqrt{1 - v^2/c^2}\right)^{1/2}}{\varepsilon^{1/2}\sqrt{1 - v^2/c^2}} \tag{10}$$

where $v = (r - r_0)/\varepsilon$. This value can be greater than the superluminal velocity, and $F(r, r_0; t_0 + \varepsilon, t_0)$ therefore will become the complex function when $v > c$. The integral form should be departed into two parts: the part that contains the low-velocity paths and the part that contains superluminal-velocity paths:

$$I = \int_{-\infty}^{\infty} \psi(r_0, t_0) F(r, r_0; t_0 + \varepsilon, t_0) dr_0 = \int_{-ct}^{ct} \cdots dr_0 + \left(\int_{ct}^{\infty} \cdots dr_0 + \int_{-\infty}^{-ct} \cdots dr_0 \right) = I_0 + I_1 \tag{11}$$

This can be exactly calculated. The amazing thing is **the final result calculated for I that contains the term** $\sqrt{m^2c^4 + (-i\hbar\nabla + A_0)^2 c^2}$. In the following context, we will detail this calculation in 1D space for simplification. The methods of the calculation in 2D and 3D are the same. Before this calculation, we define two parameters as $\tau_0 = \hbar/\left(mc^2\right)$ and $\varepsilon_0 = \varepsilon/\tau_0$:

$$\begin{aligned}
I_0 &= \int_{-ct}^{ct} \cdots dr_0 = \varepsilon \int_{-ct}^{c} \cdots dv = 2R\tau_0^{1/2} \int_{-ct}^{ct} \frac{\left(1+\sqrt{1-v^2/c^2}\right)^{1/2}}{\varepsilon_0^{1/2}\sqrt{1-v^2/c^2}} \varepsilon_0 \exp\left(-i\sqrt{1-v^2/c^2}\varepsilon_0\right)\psi(r_0,t_0)dv \\
&= \int_{-\infty}^{\infty} \varphi_p dp \left(2R\tau_0^{1/2} \int_0^c \frac{\left(1+\sqrt{1-\frac{v^2}{c^2}}\right)^{1/2}}{\varepsilon_0^{1/2}\sqrt{1-\frac{v^2}{c^2}}} \varepsilon_0 \exp\left(-i\sqrt{1-\frac{v^2}{c^2}\varepsilon_0}\right) \exp\left(-ipv\varepsilon/\hbar\right)dv \right) \exp\left(ipx/\hbar\right) \\
&= \int_{-\infty}^{\infty} \varphi_p dp \left(2R\tau_0^{1/2} \int_0^1 (1-u)^{-1/2} \varepsilon_0^{1/2} \exp\left(-iu\varepsilon_0\right) \sum\nolimits_m \left(i\frac{p\varepsilon}{\hbar}\right)^{2m} \frac{\left(1-u^2\right)^m}{2m!} du \right) \exp\left(ipx\right) \\
&= \sum\nolimits_m 2R\left(i\frac{pc}{\hbar}\right)^{2m} \frac{c\varepsilon^{2m+1/2}}{2m!} \int_{-\infty}^{\infty} \varphi_p \exp\left(ipx\right)dp \left(\int_0^1 u^{\frac{-1}{2}} \left(1-(1-u)^2\right)^m \exp\left(iu\varepsilon_0 - i\varepsilon_0\right)du \right)
\end{aligned} \tag{12}$$

Similarly, we can also get the expression of I_0:

The contour integral is used in the last step as shown in **Figure 1**.

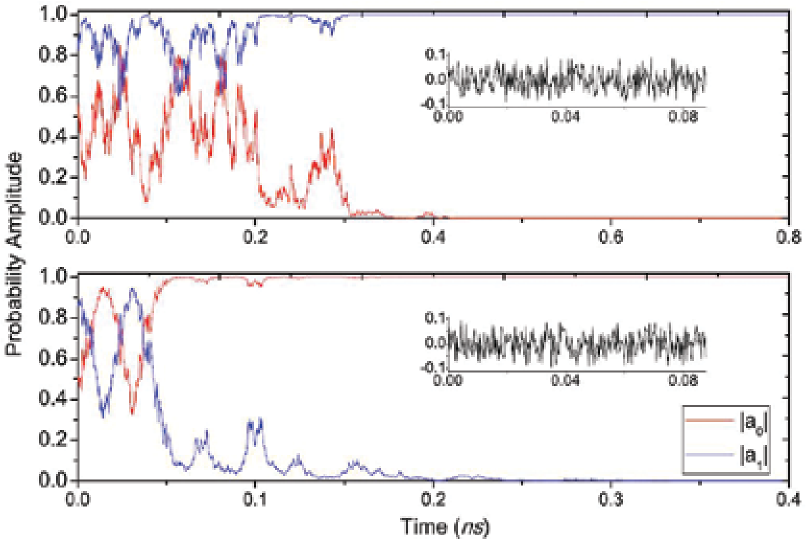


Figure 1. Contour integral. This figure shows the contour integral in a complex plane. The black line in figure denotes the integral $-\int_1^{1+i\infty} \cdots du - \int_0^1 \cdots du$; the blue line denotes $\int_0^\infty \cdots du$. The integral on the red line is always zero when $|z| \to \infty$. For this contour integral, there is no singular point, and of course the total integral value is zero. Therefore, $\int_1^{1+i\infty} \cdots du = \int_1^\infty \cdots du$:

$$\begin{aligned} I_0 &= \int_{ct}^{\infty}\cdots dr_0+\varepsilon\int_{-\infty}^{-ct}\cdots dr_0=2R\tau_0^{1/2}\int_{ct}^{\infty}\frac{\left(1+\sqrt{1-v^2/c^2}\right)^{1/2}}{\varepsilon_0^{1/2}\sqrt{1-v^2/c^2}}\varepsilon_0\exp\left(-i\sqrt{1-v^2/c^2}\varepsilon_0\right)\\ &\times(\psi(r_0,t_0)+\psi(-r_0,t_0))du=\sum\nolimits_m 2R\left(i\tfrac{pc}{\hbar}\right)^{2m}\frac{c\varepsilon^{2m+1/2}}{2m!}\int_{-\infty}^{\infty}\varphi_p\exp\left(ipx\right)\\ &\times dp\left(\int_1^{1+i\infty}u^{\frac{-1}{2}}\left(1-(1-u)^2\right)^m\exp\left(iu\varepsilon_0-i\varepsilon_0\right)du\right)\\ &=\sum\nolimits_m 2R\left(i\tfrac{pc}{\hbar}\right)^{2m}\frac{c\varepsilon^{2m+1/2}}{2m!}\int_{-\infty}^{\infty}\varphi_p\exp\left(ipx\right)dp\left(\int_1^{\infty}u^{\frac{-1}{2}}\left(1-(1-u)^2\right)^m\exp\left(iu\varepsilon_0-i\varepsilon_0\right)du\right) \end{aligned} \tag{13}$$

Integrating Eq. (12) and Eq. (13), we get the conclusion finally:

$$\begin{aligned} I &= \sum\nolimits_m 2R\left(i\tfrac{pc}{\hbar}\right)^{2m}\frac{c\varepsilon^{2m+1/2}}{2m!}\int_0^{\infty}\varphi_p\exp\left(ipx\right)dp\left(\int_0^{\infty}u^{\frac{-1}{2}}\left(1-(1-u)^2\right)^m\exp\left(iu\varepsilon_0-i\varepsilon_0\right)du\right)\\ &=\int_0^{\infty}\sum\nolimits_m 2R\left(i\tfrac{pc}{\hbar}\right)^{2m}\frac{c\varepsilon^{2m+\frac{1}{2}}}{2m!}\Gamma\left(2m+\frac{1}{2}\right)M\left(-m,\frac{1}{2}-2m,-2i\varepsilon_0\right)\varphi_p\exp\left(ipx\right)dp \end{aligned} \tag{14}$$

The function $M(a,b,z)$ is the Kummer's function (confluent hypergeometric function) and equals

$$M\left(-m,\frac{1}{2}-2m,-2i\varepsilon_0\right)=\sum\nolimits_n\frac{m!}{n!}\frac{(4m-1)!}{n!}(-i\varepsilon_0)^n \tag{15}$$

Summation in Eq. (14) is then

$$\sum\nolimits_m 2R\left(i\frac{pc}{\hbar}\right)^{2m}\frac{c\varepsilon^{2m+\frac{1}{2}}}{2m!}\Gamma\left(2m+\frac{1}{2}\right)M\left(-m,\frac{1}{2}-2m,-2i\varepsilon_0\right)=\exp\left(\frac{-i\sqrt{m^2c^4+p^2c^2}\varepsilon}{\hbar}\right) \tag{16}$$

And Eq. (14) can be further simplified:

$$\begin{gathered} I=\int_0^{\infty}\exp\left(\frac{-i\sqrt{m^2c^4+p^2c^2}\varepsilon}{\hbar}\right)\varphi_p\exp\left(ipx\right)dp\\ \exp\left(\frac{-i\sqrt{m^2c^4+(-ic\hbar\nabla_x)}\varepsilon}{\hbar}\right)\int_0^{\infty}\varphi_p\exp\left(ipx\right)dp=\exp\left(\frac{-i\sqrt{m^2c^4+(-ic\hbar\partial_x)}\varepsilon}{\hbar}\right)\psi(x,t_0) \end{gathered} \tag{17}$$

It is, namely:

$$\psi(x,t_0+\varepsilon)=\exp\left(\frac{-i\sqrt{m^2c^4+(-ic\hbar\partial_x)^2}\varepsilon}{\hbar}\right)\psi(x,t_0) \tag{18}$$

Hence, the new differential equation we get in this extended Feynman path integral is

$$i\hbar\frac{d}{dt}\psi(x,t) = \sqrt{m^2c^4 + (-ic\hbar\partial_x)^2}\psi(x,t) \tag{19}$$

The more general formulation in 3D is

$$i\hbar\frac{d}{dt}\psi(r,t) = \left(\sqrt{m^2c^4 + (-i\hbar\nabla - A_0)^2c^2} + V(r)\right)\psi(r,t) \tag{20}$$

It is more complicated to get Eq. (20), and we will not detail it in this chapter. The detailed deduction can be seen in supplementary online material of the reference [13].

It should be mentioned that Eq. (20) is not a covariant equation under the Lorentz transformation. To construct a Lorentz covariant, the antiparticle wave function should be introduced. The antiparticle wave function is denoted as ϕ_- to be distinguished from the particle wave function ϕ_+. ϕ_+ satisfied the relation that Eq. (20) has shown and ϕ_- is satisfied

$$\left(i\hbar\frac{d}{dt} - V(r)\right)\phi_- = -\sqrt{m^2c^4 + (-i\hbar\nabla - A_0)^2c^2}\phi_- \tag{21}$$

Combining Eqs. (20) and (21), we get these two equations:

$$\left(i\hbar\frac{d}{dt} - V(r)\right)\psi_+ = -\sqrt{m^2c^4 + (-i\hbar\nabla - A_0)^2c^2}\psi_+ \tag{22}$$

$$\left(i\hbar\frac{d}{dt} - V(r)\right)\psi_- = -\sqrt{m^2c^4 + (-i\hbar\nabla - A_0)^2c^2}\psi_- \tag{23}$$

where $\psi_+ = 1/\sqrt{2}(\phi_+ + \phi_-)$ and $\psi_- = 1/\sqrt{2}(\phi_+ - \phi_-)$. Eqs. (22) and (23) are the Klein-Gordon equation.

In 1926, Oskar Klein and Walter Gordon proposed this relativistic wave equation. However, it was found later that this equation is not suitable for one particle because the probability density is not a positive quantity, which means the particle can be created and annihilated arbitrarily in Klein-Gordon equation [14]. The extended Feynman path integral shows the explanation for this non-positive probability density here. The wave function that is determined by Klein-Gordon equation is the mixed state of the particle and its antiparticle. Because particles and antiparticles can be annihilated each other to a vacuum state, and the vacuum state can produce particles and antiparticles, so the mixed state with superposition state of a particle and an antiparticle is a matter of course of a non-positive quantity. This is the physical interpretation for Klein-Cordon equation by EFPI theory.

4.4. The extended Feynman path integral and density-flux equation

In quantum mechanics, the continuity equation describes the conservation of probability density in the transport process. It is a local form of conservation laws. It says the probability cannot be created or annihilated and, at the same time, also cannot be teleported from one place to another. However, in the extended Feynman path integral, the density-flux equation will be revised, and the local conservation is broken.

In extended Feynman path integral, the density-flux equation can be written as the following formula:

$$\frac{\partial \rho(r,t)}{\partial t} + \nabla \cdot j + \sum\nolimits_{n=2}^{\infty} B_n \nabla^n \cdot Q_n(r,t) = 0 \tag{24}$$

where $Q_n(r,t) = \psi^* \nabla^n \psi - \psi \nabla^n \psi^*$ and $B_n = -(-i\hbar)^{2n-1} c^2 n / \left(mc^2\right)^{2n-1}$. The last term in the right of Eq. (24) is caused by relativistic effect and breaks the local conservation.

4.5. The wave function collapse in extended Feynman path integral

From the theory of Neumann, the difficulties of understanding collapse are the probability, which seems incompatible with the deterministic time-evolution equation, and the instantaneity, which seems that it breaks the special relativity theory. In this section, we will show that these puzzling characters are due to the potential noise and nonlocal correlation (or relativistic effect).

Let us return to Eq. (9). The superluminal paths are included when we calculate the propagator. The superluminal paths will support complex phases in Eq. (9), and these phases cannot be canceled by each other like the real phases in Feynman path integral theory. These complex phases are the main culprits that cause the nonlocal correlation.

To describe this mechanism concisely, the nonlocal correlation produced in 1D space is just detailed here. Assume a system in the potential field with the scalar potential $U(x)$ and vector $A_0(x)$. A potential noise $A_I(t)$ is under this system and satisfies the white noise equations, namely:

$$\langle A_I(t_1) A_I(t_0) \rangle = \frac{2mk_b T}{\eta} \delta(t_1 - t_0); \langle A_I(t) \rangle = 0 \tag{25}$$

The Hamiltonian of this system is then

$$H = \sqrt{m^2 c^4 + \left(-i\hbar \partial_x - (A_0 + A_I)\right)^2 c^2} + V(x) \tag{26}$$

And we define a new Hamiltonian without potential noise as

$$H_0 = \sqrt{m^2 c^4 + \left(-i\hbar \partial_x - A_0\right)^2 c^2} + V(x) \tag{27}$$

We will see later that H_0 is very important in quantum measurement, because it determines the basis-state-space that the wave function collapses into. The basis-preferred problem puzzles us for many years; we do not know why the system measured prefers to collapse into some set of basis state. According to the extended Feynman path integral theory, the preferred basis is depended by the Hamiltonian H_0. This will be detailed in the following.

Considering a minimum time-evolution process, the propagator is

$$F(x_1, x_0; t_0+\varepsilon, t_0) = \hat{R}\sqrt{\frac{c}{i\eta}}\exp(-mc|\eta|\hbar^{-1} + i\hbar^{-1}\int_{x-\eta}^{x} A_0(x_0, t)dx_0) \tag{28}$$

Because the term $\int_{x-\eta}^{x} A_0(x_0, t)d_0$ exists in the integral formula of Eq. (28), then $\lim_{\varepsilon\to 0} F(x_1, x_0; t_0+\varepsilon, t_0) \neq \delta(x_1 - x_0)$. This is different from the normal propagator $K(x, x_0; t_0+\varepsilon, t_0)$ shown in Eq. (2), because $\lim_{\varepsilon\to 0} K(x, x_0; t_0+\varepsilon, t_0) = \delta(x - x_0)$. This difference, caused by relativistic effect of paths, is the root that produces the nonlocality in quantum measurement process.

In fact:

$$\int_{t_0}^{t_0+\varepsilon} -mc^2\sqrt{1 - v^2/c^2}\, dt = \int_{t_0}^{t_0+\varepsilon} -mc^2\sqrt{(dt)^2 - dx^2/c^2} = imc(\Delta x);$$

$$\int_{t_0}^{t_0+\varepsilon} (-U(x) + Av)dt = A\Delta x$$

Therefore

$$F(x_1, x_0; t_0+\varepsilon, t_0) = \frac{1}{\sqrt{2i\pi\hbar c^2}}\frac{H'}{\sqrt{mc^2+H'}}\sqrt{\frac{c}{i\eta}}\exp(-mc|\eta|\hbar^{-1} + i\hbar^{-1}\int_{x-\eta}^{x} A_0(x_0, t)dx_0) \tag{29}$$

$$\psi_- = 1/\sqrt{2}(\phi_+ - \phi_-)$$

$\lim_{\varepsilon\to 0} F(x_1, x_0; t_0+\varepsilon, t_0) \neq \delta(x_0 - x_0)$ means the change of arbitrary point should spend time to propagate the other point and exhibit stronge nonlocal space-time character. If the value of wave function at $x = x_0$ changes, the whole wave function will change for the nonlocal propagator. In the followings, we will detail this character.

We define $\widehat{R}_0 = \frac{1}{\sqrt{2i\pi\hbar c^2}}\frac{H_0}{\sqrt{mc^2+H_0}}$; then

$$\widehat{R} \approx \widehat{R}_0\left(1 - \frac{A_I c^2(\widehat{p} - A_0)}{H_0}\right) \tag{30}$$

After this definition, we will show how the measurement happens under the potential noise. Considering an initial state with the form $\psi(x, t_0) = \sum_m a_m \varphi_m(x)$, where φ_m is the eigenstate of H_0, if we put the potential noise in this system, the initial state will change. We denote the evolution state in arbitrary time t as $\psi(x, t)$. The $\psi(x, t)$ can be expanded with basis states φ_m *as* $\psi(x, t) = \sum_m a_m \varphi_m$. The task for us is to find out the varying value of a_m under each perturbational noise:

$$\begin{aligned} a_n(t+\delta) &= \int_{-\infty}^{\infty} \varphi_n(u,t) * \phi(u,t)du \\ &= \int_{-\infty}^{\infty} \varphi_n(u,t) * c^{\frac{1}{2}}\Re(u,t) * \int_{-\infty}^{\infty} (i\eta)^{-\frac{1}{2}} \exp\left(-\frac{mc|\eta|}{\hbar}\right) \exp(\xi_I)\phi(u-\eta,t)\,d\eta \\ &= \sum_m a_m(t)\,\lambda_{n,m}(t-\delta)\left(1+\frac{A_I c^2 p_n}{E_n}\delta_{n,m}\right) \end{aligned}$$

After rearranging the equation above, we get

$$a_n(t+\delta) = \sum\nolimits_m a_m(t)D_{m,n}(t-\delta) \tag{31}$$

where

$$D_{m,n}(t-\delta) = \lambda_{n,m}(t-\delta)\left(1+\frac{A_I c^2 p_n}{E_n}\delta_{n,m}\right)$$

$$\lambda_{n,m}(t-\delta) = \int_{-\infty}^{+\infty} \varphi_n(x)R(x,t-\delta)*\widehat{R}_0^{-1}\varphi_m(x)dx$$

$$R(x,t) = \frac{\psi(x,t)}{\widehat{R}_0^{-1}\psi(x,t)}$$

δ is the time interval of the neighbor potential noise pulses. In fact, to simulate the process of quantum measurement under potential noise, we let

$$A_I = \sum\nolimits_{n=0}^{\infty} \left(\frac{2mk_bT}{\eta\Delta}\right)^{1/2} Random(n)(\theta(t-n\delta)-\theta(t-(n-1)\delta)) \tag{32}$$

We simulate the collapse process of a wave function with the form $|\psi\rangle = 1/2|0\rangle + \sqrt{3}/2|1\rangle$, where $|0\rangle$ and $|1\rangle$ are the harmonic-oscillator basis. According the simulation, we show the $|\psi\rangle$ will randomly collapse into $|0\rangle$ or $|1\rangle$ quickly (**Figure 2**).

5. Conclusions

Measurement, in quantum theory, is not just a theory concerning the Schrödinger cat that is alive or dead, or the moon being here or not, but also the key and basis to the problem of the interpretation of quantum mechanics. In fact, the different views for the quantum measurement yield different interpretation for quantum mechanics, such as the Copenhagen interpretation, relative-state interpretation, Bohmian mechanics and so on. It has attracted many

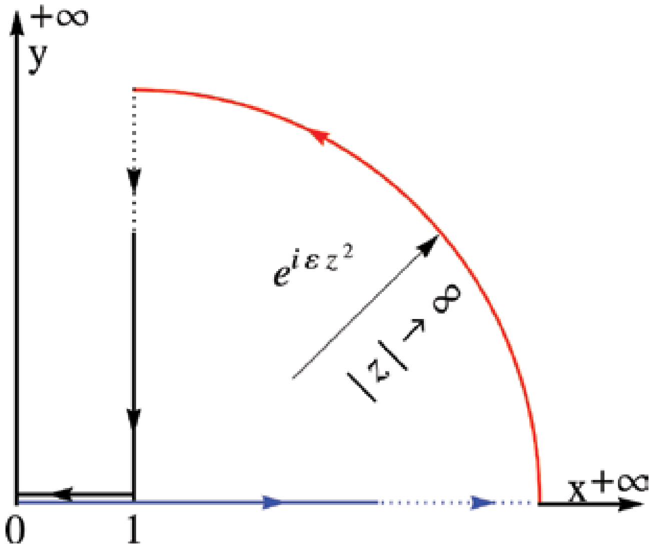


Figure 2. The process of collapse under a "potential noise". (a) The red line denotes the absolute value of probability amplitude $a_0(t)$ with the initial value 1/2, and the blue one denotes $a_1(t)$ with the initial value $\sqrt{3}/2$. The black oscillatory line is the function of potential. The different sets of noise cause the different collapse results. According the simulation, the process time of collapse is 0.3 ns in the top picture and 0.1 ns in the bottom picture. (b) The function of A_I shown in Eq. (32).

attentions of physicists since the beginning of the quantum theory establishment, but there is still no consensus. The measurement problem blocks up the way for us to understand the nonlocality and manipulate quantum state. Can the quantum measurement be controlled? Can we get the definite output we want under every measurement? If the quantum measurement can be controlled, the teleportation without classical communication channel can be realized, and the aim of superfast manipulation for quantum state will arrive. We can even transfer the energy thought nonlocality under controlled quantum measurement and make more novel encryption scheme for quantum communication. However, the key problem is "can we control the quantum measurement?" If yes, how? If no, why?

The extended Feynman path integral mechanism answered this question. According to this mechanism, the character, "stochastic output" and "instantaneous collapse process" of quantum measurement are rooted in the "random" potential noise and "nonlocal" wave function inner correlation. The "nonlocality" is caused by the "relativistic effect" of superluminal paths in path integral theory. The superluminal paths will support a complex action function S in Eq. (4) for the expression $\sqrt{1 - v^2/c^2}$ of S. This complex action that acted as a phase in integral theory cannot be canceled and makes $F(x_1, x_0; t_0, t_0) \neq \delta(x_1 - x_0)$. This relation reveals that the propagator is no longer a local correlation. All points in space are correlated simultaneously, and any local perturbation will simultaneously transfer into the whole space. The extended Feynman path integral gives a simulation for two-energy-level system and exhibits that the potential noise can indeed lead to the collapse state randomly and rapidly. Therefore, the key to control the quantum measurement is to control the potential noise exactly. "Potential noise" is caused by thermal fluctuation of potential filed or irregularity potential boundary. How to control this potential noise is still an unsolved topic.

The extended Feynman path integral mechanism also solves the "basis-preferred" problem in quantum measurement. It exhibits the reason that the state prefers to collapse some set of basis states, which is due to the main Hamiltonian H_0 defined in Eq. (27). H_0 is the Hamiltonian that contains no noise. The eigenstates are the basis state that wave function prefers to collapse into.

The extended Feynman path integral mechanism shows the relation between "quantum measurement" and "unitary evolution operation". They are one and the same thing but are departed by jumpy potential noise. In mathematics, the function of potential noise is nowhere differentiable functions, and therefore, the path integral shown in Eq. (4) is not the regular path integral function under a noised potential. This is the main difference between "quantum measurement" and "unitary evolution operation" in mathematics. In physics, each potential noise point can be quickly absorbed by wave function through the nonlocality correlation, and the amounts of noise points will quickly accumulate to be a big quantity to change the whole wave function $|\widehat{R}|$.

Additionally, besides the potential noise, the condition that the quantum measurement happens is that the interaction of system and environment should be big enough to distinguish the preferred basis state "$\{\varphi_n\}$". If the interaction is not big enough, $\left\langle \varphi_n|\widehat{R}|\varphi_n \right\rangle \approx \left\langle \varphi_m|\widehat{R}|\varphi_m \right\rangle$ and then $D_{mn} \rightarrow \delta_{m,n}$ in Eq. (31), then the collapse will not happen. In other words, the instrument that can realize the quantum measurement should be "macro" enough to produce enough noise and have big enough energy gaps of a system measured.

Author details

Wei Wen

Address all correspondence to: chuxiangzi@semi.ac.cn

Science of College, Hunan University of Technology, China

References

[1] Mooij JE. Quantum mechanics: No moon there. Nature Physics. 2010;**6**:401-402. DOI: 10.1038/nphys1698

[2] Everett H. "Relative state" formulation of quantum mechanics. Reviews of Modern Physics. 1957;**29**(3):454-462. DOI: 10.1103/RevModPhys.29.454

[3] Schlosshauer M. Decoherence, the measurement problem, and interpretations of quantum mechanics. Reviews of Modern Physics. 2005;**76**(4):1267-1305

[4] Stapp HP. The Basis Problem in many-worlds Theories. Springer; 2007. DOI: https://doi.org/10.1007/978-3-540-72414-8_11

[5] Żurek WH. Decoherence and the transition from quantum to classical. Physics Today. 1991;**44**(10):36-44

[6] Żurek WH. Decoherence, einselection, and the quantum origins of the classical. Reviews of Modern Physics. 2003;**75**:715-775

[7] Zeh HD. On the interpretation of measurement in quantum theory. Foundations of Physics. 1969;**1**(1):69-76

[8] Albert D, Loewer B. Interpreting the many-worlds interpretation. Synthese. 1988;**77**:195-213

[9] Zeh HD The problem of conscious observation in quantum mechanical description. Foundation of Physics Letters. 2000;**13**:221-233

[10] Bassia A, Ghirardia GC. Dynamical reduction models. Physics Report. 2003;**379**:257-456. DOI: 10.1016/S0370-1573(03)00103-0

[11] Feynman RP. Space-time approach to non-relativistic quantum mechanics. Reviews of Modern Physics. 1948;**20**:367. DOI: https://doi.org/10.1103/RevModPhys.20.367

[12] Claude Grrrod. Hamiltonian Path-Integral Methods. Reviews of Modern Physics. 1966; **38**(3):483

[13] Wen W, Bai Y. Quantum measurement and extended Feynman path integral. Communications in Theoretical Physics. 2012;**57**(6)

[14] Herman F, Felix V. Elementary relativistic wave mechanics of spin 0 and spin 1/2 particles. Reviews of Modern Physics. 1958;**30**(1):24. DOI: 10.1103/RevModPhys.30.24

The Concept of Mass Based on Accelerated Conservation of Energy within Asymmetric Space-Time Phases

Agaddin Khanlar Mamedov

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.75988

Abstract

This chapter presents a new look to the conservation laws and suggests a model for discrete non-uniform localization of energy portions (quanta's) within conjugated space and time phases. The model connects electromagnetism with the space-time and shows that electromagnetic energy is the Planck's scale product of the generation of asymmetric space and time phases. In the reverse order, at the Black Hole's scale with complete consumption of electromagnetic energy, decay of space-time frame takes place with accumulation of energy in virtual space phase, which translates energy to the background in the form of gravitation. Huge amounts of negative energy accumulated within background space leads to the generation of elementary space-time unit, which carries non-uniform energy conservation in the form of electromagnetic energy. Translation of background uniform energy, accumulated within minimum space, to the non-uniform energy conservation phase generates a non-baryonic heavy particle, which is the precursor of the ingredients of elementary space-time frame of matter. The background spontaneous symmetry break is a phenomenon, related to the discrete translation of uniform energy conservation phase to the phase of non-uniform conservation, carried by electromagnetic field within asymmetric space-time unit.

Keywords: generation of mass, conservation of energy, origin of space-time

1. Introduction

The topic related to the generation of mass by elementary particles is a very important area of particle physics. The recent discovery of Higgs boson is a big triumph for theoretical physics.

However, many questions related to Standard Model of particle physics are waiting for answers, such as locality of elementary particles in space-time frame and its connection with the principles of quantum mechanics.

In our previous papers [1–4], we showed that discrete performance of space-time frame is the necessary background for unification of quantum physics with the relativity theory. In the present paper, we will expand our analysis on non-uniform conservation of energy to show that the space-time phenomenon arises from the non-uniform conservation of energy to carry locality of photons within space and time frame. The non-uniform conservation of energy becomes the only reason for generation of mass and gravity within asymmetric boundaries of space-time frame to eliminate singularities from physical laws.

In this paper, we will describe that the elementary particles appear as an energy portions, distributed within conjugated asymmetric space-time fields, where energy contents of space and time phases generate different particles, such as bosons and leptons, emerging from the asymmetric background translation of space-time phases and energy content of the space-time frame. On this basis, we will discuss performance of space-time as an energy-mass carrying non-invariant field, generated from background coupling of space and time ingredients of light photons.

2. The concept of mass

Mechanism of symmetry breaking and generation of mass is the main problem of particle physics. Three independent groups, Higgs [5], Englert and Brout [6], and Guralnik et al. [7–10], published mechanisms on how particles get mass. All three, starting from very different viewpoints, proposed essentially the same mechanism based on spontaneous symmetry breaking. It postulates that matter obtains mass by interacting with a field, known as Higgs field.

In accordance with that mechanism, universe is filled with remarkable new Higgs field and Higgs boson of the field gives mass to gauge bosons and to all other particles. The mass of the Higgs particle itself is not explained in the theory, but appears as a free parameter [10]. Higgs mechanism does not describe how Higgs boson itself gets a mass and the origin of mass in all its forms is not clear [10, 11]. A standard model does not involve gravity therefore, the primary role of mass in this model is not known. The reason why spontaneous symmetry breaking causes and leads to generation of mass remains one of the questions of quantum physics [12–18].

It is necessary to note that the concept of mass needs understanding of the true nature of space-time. The space-time phenomenon was the hot subject of long debates between Newtonian and Leibniz physics [19, 20]. Later, Kant analyzed Newtonian and Leibniz space-time concepts within his metaphysical principles. Kant's metaphysical understanding of space-time was close to the Newtonian absolute space and time representation. In accordance with Kant's metaphysics, "space and time are substances in their own right (as Newtonian absolute space) and they exist independently of all objects and relations" [19].

Leibniz's view on space and time was different [20]. By Leibniz's opinion, the space-time is "inhere" in objects and relations [19], which is close to Einstein's representation of space-time [21, 22].

In accordance with Einstein's general relativity theory, space and time are relative and consist in the form of space-time unit. The gravitational force between masses leads to the warping of space-time. However, Einstein's space-time is geometric and does not give explanation as to where space-time comes from.

Zeeya, in his paper published in nature [23], very correctly concluded that, "many researchers believe that physics will not be complete until it can explain not just the behavior of space and time, but where these entities come from."

Raamsdonk [23] suggested, "In some sense, quantum entanglement and space-time are the same thing." By Maldacena's opinion "quantum is the most fundamental and space-time emerges from it [23]. However, Barbouir [24] believes that if time is removed from the foundation of physics, we shall not all suddenly feel that the flow of time has ceased".

Therefore, our present knowledge does not give any information about the origin of space-time and what we know is only our representation of space, produced from Euclidean geometry.

Description of locality of a matter and energy within space-time frame is the main problem for unification of physical laws. First, for description of mass it is necessary to understand the main principle of Newton's law: when a system having constant velocity tends to continue its constant velocity in a straight line. Where does a system get this behavior from and what are the energy resources that a system uses for motion in space with the non-vanishing constant velocity in straight line in infinite time? It is clear that conservation of energy at this particular condition of Newton's physics becomes a very abstract concept.

If a system tends to keep its constant velocity in straight line in infinite time during its motion in abstract space, as Newton's first law states, it has to consume constant amount of energy to carry a body within space in time independent infinite uniform motion otherwise it cannot keep constant velocity.

Newton's first law is valid only in inertial frame of reference, but the inertial frame itself needs condition to be in a state of uniform motion. We can expand the above-mentioned discussion on energy resources for uniform motion of time independent inertial frame as well, which also has to follow principles of energy conservation. Here appears one important question, which needs clarification. If different frames of reference have different uniform velocities, there should not be any preference in selection of the particular reference frame. In this case, translation from one reference frame with constant velocity to another one with the other constant velocity will change space-time coordinates and produce acceleration, which will vary with the variation of reference frames. The difference between inertial frames with different uniform velocities appears in the form of different space-time frame and generation of some identity, which we call mass.

From an energy point of view, when different inertial frames have the same velocity, they are not energetically different inertial frames. In accordance with the energy conservation principle, frame of references comprise the set of space-time coordinates and the difference between such a frame of reference has to be related to the energy, distributed in space-time structure of that reference frames. As we have shown [1–4], to be the same reference frame, these frames should have the same energy/momentum relation. It is clear that when energy applied to the systems is completely consumed, all reference frames moved from some state of constant velocity by application of energy, and have to "fall back" to the initial state for restoration of energy. In this case [1–4], there should be a uniform "gravitational free fall" for all of the reference frames to the initial state, which is the only reference frame, produced by the non-uniform conservation of energy. This statement is the modification of Newton's second law, where the uniform acceleration is explained through the cancelation of each other's ingredients in the formula of F/m.

In our earlier papers, we showed [1–4] that conservation of energy does not exist without localization in space-time frame and the localization has to be non-uniform. It is easy to show that the space and time are the resulting non-unitary portions of non-uniform distribution of energy, consumed in space phase (forming mass) and restored in time phase:

$$\frac{\frac{\Delta \mathbf{S}}{\mathbf{S_1}}}{\frac{\Delta \mathbf{t}}{\mathbf{t_1}}} = \frac{\mathbf{E_{ap}} - \mathbf{E_s}}{\mathbf{E_s}} \tag{1}$$

where $\mathbf{E_{ap}}$ is the applied energy, and $\mathbf{E_s}$ is the local energy of a body. When carrying of energy, the parameters $\Delta\mathbf{S}/\mathbf{S}_1$ and $\Delta\mathbf{t}/\mathbf{t_1}$ represent the changes of space and time variables in relation to their local values as spinning of the change around their local state, respectively. The detailed features of the model will be explained later. Model (1) can be written as follows:

$$\frac{\frac{\Delta \mathbf{S}}{\mathbf{S_1}}}{\frac{\Delta \mathbf{t}}{\mathbf{t_1}}} = \frac{\mathbf{E_{ap}}}{\mathbf{E_s}} - \mathbf{1} \tag{2}$$

$$\frac{\frac{\mathbf{S_1}}{\mathbf{t_1}} + \frac{\Delta \mathbf{S}}{\Delta \mathbf{t}}}{\frac{\mathbf{S_1}}{\mathbf{t_1}}} = \frac{\mathbf{E_{ap}}}{\mathbf{E_s}} \tag{3}$$

We will consider that due to the carrying of energy, the space and time phases are energetic fields, having all the behavior that is a characteristic for any energy field. The special feature of the model (3) is that acceleration as a phenomenon appears as the change of space-time in relation to the initial local space-time position. The special feature of this approach is that the effect of the action is determined as the result of exchange interaction (Eqs. (1) and (2)). When $\mathbf{E_{ap}}$-$\mathbf{E_s} \neq 0$, change of velocity is proportional to the applied energy ($\mathbf{E_{ap}}$) and while at $\mathbf{E_{ap}} = 0$, "inertial" and "local" energy contents of different masses cancel each other.

This concept is completely different from Newton's acceleration, which describes acceleration as the derivative of the velocity or second-order derivative of space-time in abstract space within universal time.

The left side of Eq. (3) shows addition of change of a position to the initial space-time frame in the form of acceleration. The right side of Eq. (3), in the form of non-unitary energy portion, is the relation of the energy of a force carrier field to the initial energy content of a body of the space-time frame.

Equation (3) at $\Delta S/\Delta t = 0$, could be considered as the symmetry of an energy carrier field with the energy of a particle or unification of energy-mass relation within space-time frame. In this case, use of equivalence between energy and mass of a particle in simple form is not an approximation. Later, we will show that during exchange interaction, $\mathbf{E_{ap}}$ and $\mathbf{E_s}$ may exchange their behavior, and $\mathbf{E_s}$ of Eq. (3) describes inertial energy of a particle, which at background state of space-time frame is equivalent to the mass. Using this principle in conversion of entities, we can get the equation of classic physics:

$$\mathbf{a} = \frac{\mathbf{F}}{\mathbf{m}} \tag{4}$$

In accordance with Eqs. ((1)–(3)), the portion of energy, consumed for locality of a zero mass virtual particle in space-time frame, can be described as "transformation of energy to mass," which presents the non-uniform conservation of energy within energy-mass relations. The non-consumed portion of energy determines the local strength of the "force carrier particle." This approach explains the nature of mass in more details than that of Newtonian inertia of a body. Here, mass appears as the response of an initial local energy state of a body to the change of its space-time frame, which appears as an exchange interaction with the applied energy. On this basis, mass in the dynamical model (3) changes with the content of the energy portion, which is consumed in the space-time frame of a particle.

Description of an event as a change of velocity in relation to the local initial space-time frame gives more information on the dynamics of an event and nature of mass than that of description of force as a change of the momentum or double change of space-time with the non-vanishing mass in the abstract space within change of universal time.

The effect of a force is the action and the local initial content of the energy of a body (Eq. (1)) describes conservation of action through the action-response exchange relation, while Newton's effect of force does not involve action-response exchange relation that is why Newtonian response appears in the form of independent uniform inertia. That is why action in Newton's formulation is not conserved. Model (1) describes the response of a system in exchange interaction $(\mathbf{E_{ap}} - \mathbf{E}_{\mathrm{s}})/\mathbf{E}_{\mathrm{s}}$ in the form of $\mathbf{E}_{\mathrm{s}}$, which appears as the carrier of dynamic inertia (or gravitational mass) of a body to the non-uniform flux of the available portion of energy to the space-time field.

It is necessary to note that presently there is no complete theory of dynamics, which may describe change phenomenon where action is conserved. The action is the integral of a Lagrangian over time between the initial and final time of the system. For the action integral to be well defined, the trajectory should have its boundary simultaneously in time and space. However, Lagrangian action principle does not cover these requirements, therefore is not a complete theory for analysis of the simultaneous change of variables and cannot be a proper law for conservation of energy. Feynman applied Lagrangian action to quantum mechanics.

However, Feynman's Lagrangian action is not conserved and even modified Lagrangian for strong interactions needs renormalization [25].

Another important feature of the model (3) is that from classic physics position it is possible to get limitation of velocity by the speed of light, which cannot follow from Newton's second law and does not need special relativity formulation. When energy of a body is equal to the light energy (**$E_{ap}/E_s = 1$**), **$\Delta S/\Delta t$** parameter in Eq. (3) became zero, and therefore there is no change of velocity in relation to the initial state (background state) and there is no acceleration. Besides that, with the expansion of space (1) and accumulation of energy in space in the form of mass, more energy is required to move a body with the same velocity therefore a body never can reach the speed of light.

It is the boundary of maximum velocity. Such an outcome from Eq. (3) on the limitation of maximum velocity to the speed of light is completely different from principles of special relativity. Model (3) describing the velocity in relation to the initial local space-time frame and the relation of the action energy to the initial energy content of a particle in the form of exchange interaction unifies **F/m** formulation of classic physics and **E/m** relation of special relativity. Model (3) shows that if a particle will have velocity equals to the speed of light, there will be no acceleration and universe will not undergo the change.

The above-mentioned analysis of model (1) reveals one very important question: a particle to feel the effect of force or effect of any type of field should have minimum non -zero mass, otherwise a particle will not have limited velocity.

It is necessary to explain one question, which has no explanation in the special relativity theory. The question is why there should be a maximum velocity, which is limited by the speed of light. In accordance with our concept, maximum velocity of light is necessary to hold conservation of energy, elimination of infinite energy and space-time singularity. In addition, the finite maximum velocity limit needed for translation of space-time variables to each other through **$\Delta S/\Delta t$**. Without boundary velocity, there cannot be finite space-time frame and no energy conservation. It is obvious that boundary of light velocity leads to the boundary of space-time frame, which correlates this boundary through translation of variables.

Based on model (1), we may analyze energy-mass equivalence and the concept why energy conversion to mass is needed. This question has a connection to the discussion given above. Our concept shows that there is no static Noether's conservation of energy [26], and only non-uniform conversion of energy from one form to another can hold conservation principle. The non-invariance of energy-mass relation is the only way for conservation of energy during its conversion from one form to another, which is carried within non-uniform space-time frame. This is an alternative approach on the existence of mass and energy-mass equivalence for limitation of velocity to the speed of light. This approach is different from the relativity concept of increase of relativistic mass with the increase of velocity.

3. Generation of classic space-time field model

The new concept, which we present, involves conjugation of the change of a function (**Δf**) with the local value which is the relative locality of a particle (**f_n**). In this formulation, the reciprocal discrete transform within change ($\mathbf{\Delta f}$) and function ($\mathbf{f_n}$) can be generalized within boundary of canonical variables. In this case, we have a purpose eliminating problem of classic physics and quantum mechanics, which describes an event as a change of state of something without relation to something itself. The formulation ($\mathbf{\Delta f}$)/$\mathbf{f_1}$ is useful while it allows description of an interaction of a body and force carrying field through exchange interaction.

The formulation ($\mathbf{\Delta f}$)/$\mathbf{f_1}$ has also "quantum mechanics behavior:" the new classic operator in the form of ($\mathbf{\Delta f}$)/$\mathbf{f_1}$ describes change (spinning or vibration) of the function around dynamical initial locality to repeat its origin. Similarly, the operator $\Delta\mathbf{S}/\mathbf{S}_1$ describes the fluctuation of space around its origin due to the applied force, while operator $\Delta\mathbf{t}/\mathbf{t}_1$ describes the fluctuation of time about instant of action. On this basis, space and time phases, which carry energy, get features of an energetic field.

In the conjugated space-time field, a position of a particle, located within space-time frame is not a point; it exists within very certain discrete non-virtual space-time manifold, commuting dynamic energy, and is distributed within space and time fields.

In accordance with the non-uniform energy conservation concept, the space-time is the resulting non-unitary inner product of energy distribution, which comprises portions of energy consumed in space phase (event mass) and restored in time phase.

$$\frac{\frac{\mathbf{\Delta S}}{\mathbf{S_1}}}{\frac{\mathbf{\Delta t}}{\mathbf{t_1}}} = \frac{\mathbf{E_{ap}} - \mathbf{E_s}}{\mathbf{E_s}} \tag{5}$$

$$\frac{\mathbf{\Delta S}}{\mathbf{\Delta t}} = \frac{\mathbf{S_1}}{\mathbf{t_1}}\left(\frac{\mathbf{E_{ap}}}{\mathbf{E_s}} - \mathbf{1}\right) \tag{6}$$

$$\boldsymbol{\lambda} = \frac{\mathbf{E_{ap}}}{\mathbf{E_s}} - \mathbf{1} \tag{7}$$

at $\lambda = 1$, $E_{ap} = 2E_s$.

where $\mathbf{S}_1$ and $\mathbf{t}_1$ are the space and time variables corresponding to the dynamic local boundary, $\mathbf{E_{ap}}$ and $\mathbf{E_s}$ are the energies of action and under action systems of interaction at conditions corresponding to the local boundaries of $\mathbf{S}_1$ and $\mathbf{t}_1$. In accordance with model (5), energy portion inserted to the space-time frame, travels through wave of exchange interaction, which determines the exact pathway of a particle. The right side of the model describes the frequency of energy consumption by the matter particles, while the left side shows the frequency of the change of space and time waves fields. The entities $\Delta\mathbf{t}$, $\mathbf{t}_1$ and $\Delta\mathbf{S}$, $\mathbf{S}_1$ perform as the same identities of energy carrier, existing differently in the opposite phases.

Model (5) treats the matter field through space phase, while antimatter field with the time phase which couples in space-time unit carries the non-uniform conservation of energy. Later, we will show in detail how the boundary mapped space-time frame, involving limitation of maximum velocity to the speed of light is the requirement for conservation of energy. Model (5) presents the boundary of space-time by the local position, dynamically growing in accordance with the available portion of energy. In a simple form, if there is a local position, there should be a boundary of the change of the energy that carries a space-time field.

The left side of model (5) involves the dynamic conservation of space-time frame as the non-unitary "grains," while the right side shows the non-uniform conservation of energy-mass exchange relation, carrying the dynamic flux of energy portion to the local $\mathbf{S_1/t_1}$ metric of space-time frame (6). The gradient of energy in relation to the initial state $\mathbf{(E_{ap} - E_s)/E_s}$ as an equivalent form of space-time "grains" becomes the non-unitary quanta, which describe change of local space-time frame as an exchange interaction of a particle with the applied force. The portion of energy, distributed in space and time phases, determines the strength of a force and repulsive reaction of a matter.

The model of non-uniform energy conservation (5) shows that space-time is the energetic field, which carries localization of energy conservation within dynamical space-time frame. The space-time, which has to carry conservation of energy, generates a non-virtual local frame, and moves it relative to the state of energy restoration.

The condition $\mathbf{E_{ap}} = 0$ of model (5) is the background state of discrete space-time field, where asymmetric space and time variables, for holding of conservation cycles, undergoes to the discrete translation as the portions of energy in the different fields. At this state, all types of the interactions discretely unified.

In accordance with model (5), energy appears as the non-uniform inner product of coupling of space and time fields (right-handed translation) and in reverse order, the origin of space-time variables is the decay of space-time into virtual space and time entities (left-handed translation), with the discrete restoration of energy at background state. This is the non-uniform non-static conversion of energy from one form to another. On this basis, time appears as the product and boundary of the discrete non-Noetherian dynamic conservation of energy, carrying energy within space-time frame.

Time takes its origin only from discrete energy conservation cycle and starts when energy, accumulated in time phase, translated to the formation and expansion of space-time frame with exchange interaction, controlling the boundary of space-time framework. Due to the relation of motion to the discrete local frame of space-time, description of time only by unitary intervals leads to the uncertainty.

Model (5) eliminates singularity in space-time frame and energy: the zero boundary of energy $\mathbf{E_{ap}} = 0$ and its product zero time instant ($\mathbf{t_1}$, frequency) cancel each other. The zero $\mathbf{E_s}$ and its product zero space ($\mathbf{S_1}$) similarly cancel each other, which generates singularity free dynamic model of an event.

4. Gravity

Model (5) shows that when the entire available energy portion is consumed for expansion of space ($\mathbf{E_{ap}} = 0$), space-time decays which has to radiate energy, accumulated in the space-time frame (negative $\boldsymbol{\lambda} = -\mathbf{1}$). In this case, the energy, consumed in space-time frame of any scale, has to move to the initial state through translation of asymmetric boundaries of space-time variables. While space and time are the phase fields of energy conservation, translation of variables presenting conversion of energy from one form to another became an obvious event. The space-time frame in this case decays to virtual space and time field particles moving to the background state, where generation of new space-time frame takes place.

In accordance with these principles, gravity is not a space-time geometric curvature itself, but a result of discrete non-uniform conservation of energy, localized within finite space-time field. The parameter ($\mathbf{E}_{\mathbf{ap}}/\mathbf{E}_{\mathrm{S}} - 1$) of Eq. (6), in the form of energy-mass exchange interaction, generates gravity for controlling of space-time and energy boundaries. Therefore, gravity is not a result of simple existence of energy itself in space-time, but it is the result of non-uniform conservation of energy through space-time field.

The right side of model (5) as the energy-momentum content of space-time frame leads to the "warping of space-time structure" as general relativity suggests.

The flux of energy to space-time frame expands Planck scale space in direction of localization of background energy in the expanded space-time frame. The non-uniform conservation of energy (5) involves two space-time structures: non-uniform conservation of energy in differential form within discrete, non-virtual space-time frame and in integral form when space-time decays to virtual space and time phases with restoration of energy at background state with the continuous spectrum ($\mathbf{E}_{\mathbf{ap}} = 0$) of uniform conservation. At this condition, there is no exchange interaction and the difference between inertial and gravitational masses disappears. Therefore, the key ingredient of the space-time is not the gravity itself, but non-uniform conservation of energy, which generates mechanism (gravity) restoring energy at its origin. On this basis, gravity appears as the gradient of the energy between background vacuum state and the condition where energy portion transformed to the local space-time phase with generation of space mass.

In the non-uniform energy conservation concept, energy and mass appear as two forms of the same unit, distributed differently within asymmetric coordinates of space-time field. This approach is different from special relativity concept, which connects energy-mass relation with the uniform speed of light. Without mass, there is no non-virtual space-time frame, which has to carry conservation energy. At the background state, emerged non-virtual space-time frame leads to the consumption of energy and growth of the non-virtual space-time frame of the matter.

The statement of general relativity (GR) that "space-time of GR is the gravitational field" [27] does not explain origin of space-time. GR does not explain why space-time has to involve gravity and curvature if its space-time has no boundary. These questions have direct connection with the classic physics concept of inertia, which does not explain why a body resists in its uniform motion to the applied force. In accordance with Eq. (5), the dynamics of a body is the result of the coupling of energy with the space-time frame: a body has a tendency to keep its local state, but it cannot hold this state uniformly because energy applied to a system is non-uniformly conserved. This leads to the growth of the internal force of inertia (called gravitation), which has a trend to return a system uniformly back to the energy restoration state.

At $\mathbf{E_{ap}} = 0$ of model (5), the space-time field undergoes to the decay which leads to the loss of the information, generated by the energy flux. Therefore, generation of a new cycle of space-time frame is the generation of new event and "an event when it travels backward does not meet with itself" because an event returns with the loss of space-time information. Without space-time frame, there is no ordinary matter to carry information.

It is necessary to note very important statement of special relativity (SR) that space and time do not exist separately, but form a four-dimensional space-time unit. In accordance with the principles of SR, conservation of energy has to be valid in "flat space-time." This statement of SR is based on Minkowsii concept [28] of a flat four-dimensional space-time frame. Special relativity describes energy-mass equivalence through uniform relation $\mathbf{E = mc^2}$ **(or** $\mathbf{E_o = mc^2}$**)**, but conservation of energy-mass relation within non-uniform space-time field eliminates invariant features of the conservation laws. The additional statements of SR such as "space contraction" and "time delay" do not explain mass-velocity relation, while these supplementary concepts follow from Lorentz's invariant translation principles.

In accordance with the non-uniform energy conservation model (5), "flat space-time" without mass does not comprise a frame of the non-virtual space-time and cannot carry any information on energy conservation. On this basis, model (5) treats mass as a discrete space-time field of energy-mass unit of non-uniform conservation of energy.

Different phases of energy conservation in space-time field appear as the virtual fields of different entities, such as particles and antiparticles, representing energy-mass relationship. Light energy exists through conservation between two fields, which appears in the form of particles with positive and antiparticles with negative energy states. However, positive and negative energy states do not follow invariant translations to each other. At $\mathbf{E}_{\mathrm{app}} = 0$, model (5) describes negative energy solution of antimatter, while $\mathbf{E}_{\mathrm{app}} - \mathbf{E}_{\mathrm{s}} > 0$ represents positive energy solution of matter being localized within space-time frame. The condition when energy content of local state ($\mathbf{E}_{\mathrm{app}} - \mathbf{E}_{\mathrm{s}}$) is equal to the energy content of background state $\mathbf{E}_{\mathrm{s}}$ ($\mathbf{E_{ap} = 2E_s}$) describes space-time symmetry or symmetry of matter-antimatter particles.

Our concept describes space-time in a new representation, responsible for symmetry breaking. The space-time is the product of energy distribution within two phases, which in reverse order is the carrier of energy conservation. The "warping of space-time with energy and matter in it," suggested by general relativity, is the requirement of cyclic performance of space-time for conservation of energy and matter.

At background Planck scale, the space-time appears within annihilation of space and time phases in the form of matter and antimatter annihilation. This transformation leads to the consumption of photons energy by generated space-time frame with formation of matter and expansion of it in space-time frame. In accordance with our concept, spontaneous symmetry breaking is the change of time phase to space-time frame with the generation of mass, carrying discrete conservation of energy.

As follows from model (7), one energy carrier particle is in symmetry with the two matter carrying particles which forms three particles tandem (three particles distribution of quarks in proton and neutron). This is the necessary condition for symmetrical existence of a matter.

The antimatter having no space-time frame is the "dark" ingredient of energy phase of Higgs field. Running Eq. (6) at $E_{ap} = 0$ to background Planck scale generates phase translation of "dark" ingredient of energy to the visible space-time matter. Dark energy does not carry space-time frame. It has only time phase in the form of condensate, which after interaction with the generated space-time frame forms vector bosons with integer spin. Photon energy is the reversed reflection from space-time frame. Photon transforms to electron/positron pairs, which absorbs photon to produce vector bosons as the precursors of quarks.

It is necessary to note that the non-invariant translation of variables of space-time gives alternative mechanism for generation of spin property of particles. In accordance with quantum mechanics, the spin number is the quantum state where fermions are half spin particles and have to follow Pauli Exclusion Principle. This means that one fermionic particle can occupy only one quantum energy state. Quantum theory suggests that spin appears as the momentum of a particle around its own axis.

Model (5) suggests that the spin is the space-time phenomenon, which appears in the form of energy-mass and action-response relation $(\mathbf{E_{ap}} - E_s)/\mathbf{E}_s$. Conservation of energy takes place through its distribution within space-time phases, which generates energy-mass exchange relation. Consumption of energy in right-handed space expansion is carried by electromagnetic energy, while accumulation of energy in space-time frame is in the form of mass that moves the space-time in the left-handed direction. The opposite forces of exchange interaction curves space-time and produce angular momentum, rotating particles of space-time frame around local position.

The spin as the identity is the "face" of a particle: every particle with its energy content can have only one local space-time structure. Fermion has "face" as a particle of baryonic structure that exists within non-virtual space-time frame in discrete symmetry at $\mathbf{E_s} = \mathbf{1/2E_{ap}}$ (7) of nuclear. This structure generates half spin number for fermionic particles. Model (7) shows that half spin behavior of fermions $\mathbf{E_s} = \mathbf{1/2E_{ap}}$ and spin one performance of bosons is generated from exchange interactions to carry discrete symmetry through translation of energy to space-time field. The full recovery of discrete symmetry of a fermionic particle involves two pieces of full cycle between discrete exchanges of quarks within **n-p** frame.

In the absence of $\mathbf{E_{ap}}$, $(\mathbf{E_s} = \mathbf{0})$ all the particles lose space-time frame and spin: helicity becomes the dynamical behavior for conservation of energy at the origin. Later, we will show that without helicity of neutrinos space-time cannot restore energy conservation at background state.

Based on model (5), we can explain the quantum level particle-antiparticle interactions in deterministic way. At $\mathbf{E_{ap}} = \mathbf{0}$, particle radiates energy and loses its space-time field (virtual for non-baryonic particles, non-virtual for baryonic particles), where two states of energy merge together forming neutral particle. This is the phenomenon which divides fermionic particles "face" between two states.

From non-uniform conservation of energy follows, that gravitation together with the electroweak force holds nuclear stability in discrete mode. On this basis, all the forces unified within three families: decomposition of strong force generates week and gravitation forces and coupling of these forces in reverse order in cyclic mode re-generates strong force. Later, we will describe these forces in detail.

5. Unification of quantum mechanics and relativity

It is easy to show that the non-uniform conservation of energy has to be the ground concept for unification of relativity and quantum physics. Starting from the basic statement of general physics that energy conserved through its conversion from one form to another, we will arrive to the concept that a dynamical event of energy conversion has to have locality within finite space and time coordinates. In principle, the features of energy conservation during its conversion from one form to another are clear from Planck's black body radiation, which changes the frequency of energy with radiation. Change of frequency of radiation is the result of non-uniform locality of energy within space-time field.

The non-uniform conservation of energy leads to the collapse of the concepts on uniformly moving different reference frames in relation of which all physical laws are valid. It is clear that even light cannot be the reference frame, while light energy is non-uniformly conserved.

In this case, the question "in relation to what background state all physical laws are the same" appears to be a big problem for physics. General relativity, describing space-time "as a geometrical structure, curved by existence in it energy and matter," does not produce a reference frame and mechanism of space-time behavior, while mathematical formulation of GR has no background state. The theory of special relativity, describing constant speed of light in vacuum, does not help much; while within non-uniform conservation of energy in space-time, light is not a space-time independent uniformly moving reference frame.

Within principles of non-uniform conservation of energy, the concept of uniform reference frames without uniform energy resources has no meaning at all. The main problem of quantum mechanics and relativity is the reference frame: we cannot determine the position and momentum at the same time because when we determine momentum, position also will change and its change will be uncertain.

Therefore, the problem described by quantum mechanics appears due to the absence of local position and deterministic formulation of local position by dynamical laws of classic physics. The general relativity has the same problem. The importance of local position arises from the non-uniform conservation of energy, localized in space-time field through change of space and time coordinates of a local position.

Here, it is necessary to give analysis of uncertainty principles in more detail, where changes in position and momentum shown as a change of simple gradients. Description of space-time frame and dynamical events only through gradients of energy and space-time variables or tensors leads to the problems, associated with the loss of local positions (boundary) of space-time field, carrying distribution of energy. The boundary or local position is the energy density of the phase field. The same question related to the change of momentum, which also needs description in the form of exchange interaction relative to the local momentum of a particle. It is clear that in case of mathematical formulation of dynamical events, involving a local position of a particle in space-time field and its local energy content, the prediction of quantum mechanics could be completely different.

In accordance with the non-uniform energy conservation principle, coupling of local space-time field and local energy state of a particle is the necessary approach for elimination of singularity and for removal of renormalization from particle physics theories. Without involvement of local position and exchange interaction, it is impossible to get mathematic formulation of conservation laws.

It is necessary to note that Dirac's relativistic quantum theory [29] on existence of an antiparticle appeared due to the uncertainty in position. Dirac suggested that uncertainty in position can be solved if there will be another particle (antiparticle) with the different position to maintain the balance for conservation of quantum number. However, conservation of energy, involving coupling of local position with the energy flux to the space-time frame leads naturally to the existence of oppositely charged particles.

The concept of non-uniform conservation of energy explains why charges are needed. Coupling of space and time variables within elementary space-time frame of baryonic particle and distribution of energy in extended space-time structure takes place through involvement of charged particles. However, restoration of energy at origin takes place through decay of space-time field and translation of energy in the form of neutral current to the initial background state. The energy is restored at the origin ($E_{ap} = 0$) when phase difference, leading to the generation of charges, disappears (5). Conservation of energy through phase difference is the origin of generation of discrete performance of physical laws.

In accordance with model (5), relation of an event to local position of space-time is not separable from the energy flux to space-time frame because local position, which undergoes to the growth, is the product of energy distribution in space-time frame. In reverse order, change in relation to the energy flux also is not separable from the local position, while the outcome of energy flux determined by the consumption of energy in dynamical local position.

Therefore, change of velocity is the product of conjugation of local space-time position of a particle with the exchange interactions, generated from the energy flux to space-time field. This is the deterministic physical law of nature. Without conjugation of local position and energy resources through exchange interactions within space-time field of a particle there is no conservation of energy and there is no correct concept of mass. The position and momentum conjugate of uncertainty principle does not involve resources of action that is why its outcome is uncertain.

In accordance with the quantum field theory, during short time intervals violation of energy conservation is restored. The common view on this statement is that conservation of energy can be temporarily violated and energy can be borrowed from the universe as long as it is returned within a short duration of time. However, Griffits [30] showed that "this principle is based on the false axiom that the energy of the universe is an exactly known parameter at all times."

The general view of quantum mechanics on conservation of energy is that the energy-time uncertainty has a meaning that a state of a body that exists only for a short time cannot have a definite energy because to have a definite energy, the frequency of a state must be accurately defined. It is easy to show that model (5), which conjugates energy flux of exchange interactions and local position of a state, covers the above-mentioned requirements.

In accordance with the non-uniform conservation of energy, the deterministic state of a body requires description of an event in the form of exchange interaction, comprising action-response conservation. The parameter $(\mathbf{E_{ap}} - \mathbf{E}_s)/\mathbf{E}_s$ of model (5) describes exchange interaction that conjugates with the local space-time frame for generation of deterministic path of a particle. In quantum field theory, the space-time metric does not vary with the flux of energy. However, our concept presents dynamical space-time metric, which is the dynamical local space-time field.

It is clear that an event can have its own reference frame if its energy-mass conservation is described by the true mathematical space-time formulation. Model (5) involves interaction of an event space-time field with its own reference frame. The condition $\mathbf{E_s \neq 0}$ describes an acceleration of event dynamics in relation to the initial condition, while the condition $E_{ap} = 0$ is the uniform translation of an event to the initial state. In this case, the laws of classic and relativistic classic physics unified with the quantum mechanics within singularity free deterministic physical frame of non-uniform conservation of energy. In the absence of the energy flux "moving in space became equivalent to the moving relative to the space," which restores the classic physics concept of relation of a motion to the space "ether."

Thus, the non-uniform conservation of energy comprises the acceleration of space expansion in forward direction and uniform backward process of energy restoration at the initial state.

6. Unification of space-time frame with the electromagnetism

While energy is non-uniformly conserved within space-time frame with asymmetric boundaries, unification of electromagnetism with the space-time frame becomes an obvious concept. The multiple $\mathbf{S}_1/t_1$ $(\mathbf{E_{ap}/E_s} - \mathbf{1})$ of model (6) is the combination of electromagnetic field $(\mathbf{E_{ap}/E_s} - \mathbf{1})$, which describes flux of the energy to the space-time frame and local position in space-time, where $\mathbf{S}_1/t_1$ metric is not fixed and changes with the change of the energy flux field. The energy flux $(\mathbf{E_{ap}/E_s} - \mathbf{1})$ is not uniform and presents local energy portion, remained from the exchange interactions with the particle. That is why electromagnetism is not Galilean invariant. Due to the coupling of the local energy portion with the local space-time position the multiple $\mathbf{S}_1/t_1$ $(\mathbf{E_{ap}/E_s} - \mathbf{1})$, as a deterministic function, describes trajectory of a particle. In the multiple $\mathbf{S}_1/t_1$ $(\mathbf{E_{ap}/E_s} - \mathbf{1})$, the space-time and energy-mass relation have reciprocal relations: the non-uniformity of energy-mass relation generates asymmetry of space-time variables and in reverse order, asymmetric space-time leads to the non-uniformity of energy-mass relation.

The asymmetric boundaries of space-time variables allow only global conservation laws. On this basis, during discrete non-uniform conservation of energy in space-time frame the change of energy is non- invariant translation, therefore cannot give local symmetry of general relativity or even any type of invariant translations. In dynamical events, comprising non-uniform conservation of energy within space-time frame cannot be any static state of rest or uniform motion, accepted as a reference frame. The static energy conservation law does not fit with the conservation of finite amount of energy. Without coupling of local energy state and local space-time frame, energy conservation in GR is approximate and leads to the singularity.

With the increase of energy of a body $\mathbf{E_s}$ (classic inertial energy/mass content of a body), the space-time unit requires more energy flux to keep the initial action of exchange interactions. This principle appears as a trapping of more energy by the space phase leading to the "acceleration of space expansion;" but in reality, it is the acceleration of energy conservation. Consumption of energy and expansion of space leads to the condition, where any amount of energy trapped in space-time "black hole" structure. When all available portion of energy is consumed, ($\mathbf{E_{act} = 0}$), the energy trapped in the space-time frame, has to be radiated back to the initial state through translation of asymmetric energy conservation phases. The frame called "black hole" is the boundary of space-time frame, where the entire portion of energy is going to be consumed. At $\mathbf{E_{ap}} = 0$, the local discreteness of electromagnetism is invariant with the global discreteness of gravity which is the integral equivalent of Maxwell's differential invariance $\mathbf{dF} = 0$.

Model (5) shows that for inversion of space-time from one local frame to its previous state more energy portion than locally available is necessary to apply, therefore the temporal Galilean transformation is non-invariant. This prediction of model (6) is the alternative to the statement of special relativity that with the increase of mass of a particle, more energy is necessary to apply to get constant velocity. This effect is the internal "gravitational property" of energy conversion from one form to another within space-time frame, which can be called "acceleration of non-uniform conservation of energy."

Acceleration of non-uniform conservation of energy arises from exchange interaction and conservation itself produces the exchange interaction. With the growth of space-time frame and consumption of energy, more flux of energy required to keep the local state. In reverse order, when space-time collapses, more energy portion than locally available is necessary to apply to stop decay of space-time of matter, moving to the background to start a new cycle of discrete conservation of energy.

In relativity theory, the concept of mass is the part of energy-momentum tensor; but in model (5), mass is the part of energy-momentum exchange interactions ($\mathbf{E_{ap}/E_s - 1}$), coupled with the local position of space-time. The positive value of exchange interaction plays a role of right-handed Lagrangian.

In accordance with the non-uniform conservation of energy, the main problem of conservation laws is the description of energy conservation in Lagrangian or Hamiltonian in the form of sum of energies. Energy exists and conserved as a waves, passing through space and time fields with formation of different energy density within these phases. That is the reason why model (5) describes an event dynamics through exchange interaction of the energy portions, distributed in space and time waves. $\mathbf{E_{ap}} - \mathbf{E_s}$ describes the available portion of energy in time phase, while E_s presents the portion of energy consumed in space phase. The condition $(\mathbf{E_{ap}} - \mathbf{E}_s)/\mathbf{E}_s \geq 1$ comprises positive electromagnetic energy, while $\mathbf{E_{ap}} = 0$ leads to the negative energy solution.

The rate of acceleration of energy conservation has a trend to approach the background speed of light. That is why any event has a trend to move to the maximum velocity through minimum space and maximum available portion of energy.

The origin of matter in GR has no connection with the space-time frame and GR's space-time cannot remove matter from its structure and return to the background space-time state, while GR has no background state. However, the non-uniform energy conservation concept shows that any space-time frame, which does not involve mass, is not able to be the energy carrier.

The non-uniform conservation of energy in space-time frame gives very specific concept of mass: the mass is the energy density in space field. As follows from model (5), discrete non-uniform energy conservation may generate only non-invariant dynamical mass in the form of location of energy in the certain space-time frame. The energy flux $(\mathbf{E_{ap}}/\mathbf{E_s} - \mathbf{1})$ determines the density of energy in space phase, therefore mass changes with the change of frequency of the energy conservation. Thus, space is the materialization phase of energy, while time phase destroys everything material and returns the space matter discretely to the initial state, carrying the phenomenon, called "Poincare paradox" [31].

The discrete, non-uniform conservation of energy, leading to the non-invariance of action-response parity of energy-mass relation within space-time field and asymmetry of their boundaries is the missing quantity in the equation of general relativity.

Due to the discrete non-uniform conservation, energy as the resulting quantity of exchange interactions, distributed within dynamic space-time phases, has no meaning as the static quantity. This is the "quantization" of discrete non-uniform energy conservation, which makes all of the interactions as the "classic resulting quantity," having the same meaning of quanta.

The forces of virtual space-time frame at $\boldsymbol{\lambda} = -\mathbf{1}$ annihilates each other as the electromagnetism and gravity, but in the non-virtual space-time frame they get a new feature—action-response parity of exchange interactions: electromagnetic force at long distance generates gravity, but at short range with the weak force leads to the generation of strong nuclear force. Transformation of energy from space phase to time phase generates gravitational force, while transformation of energy from time phase to space phase generates electromagnetic interaction.

Later, we will describe the weak force in detail, which is needed for generation of discrete symmetry at minimum atomic space scale to make performance of atomic scale space-time grain stable.

7. Transformation of variables and conservation of energy

Here it is necessary to give Sean Carrol analysis of energy conservation who gave excellent comments on the conservation of energy in general relativity. By his opinion [32], "if energy and momentum evolve in response to the behavior of space-time around it, as GR suggests, when space-time is not constant, energy will change in a completely unambiguous way. Therefore, you cannot find the energy or curvature of space-time at every point in space. Photons loss energy as space expands, so total energy decreases. It leads to the violation of energy conservation. Energy is not conserved because space-time changes."

We will show that the problems of conservation of energy within energy-momentum and space-time framework, described by Carrol [32], cannot be solved without dynamical model, involving local asymmetric space-time position.

The non-uniform conservation of energy, which holds due to discrete space-time frame (5), is valid only through transformation of asymmetric space and time variables. Consumption of energy during non-uniform conservation in space phase (change of space in relation to the local position—$\Delta\mathbf{S}/\mathbf{S}_1$) generates its conjugate variable—gradient of time in the form of time arrow in relation to the local origin—$\boldsymbol{\Delta t/t_1}$. Generation of non-virtual space-time frame through coupling of its variables and translation of time phase energy to space-time frame leads to the non-uniform consumption of energy. Consumption of energy in space-time frame and decrease of frequency of photons energy leads to the decrease of frequency of change of local (instant) time.

If to apply Noether's theorem to quantum physics, time translational antimatter-matter symmetry should be associated with the conservation of energy. However, quantum physics time independent antimatter-matter annihilation or classic space-time translations need application of continuous unlimited resources of energy to hold the continuous symmetry.

In accordance with model (6), conversion of energy from one phase to another is possible only if conversion takes place within asymmetric space-time translations. If there is no uniform energy resources, space-time translation in any local position will end in space phase. On this basis, matter-antimatter annihilation ends at the matter formation phase. The amount of energy repulsed after matter generation phase is less than initial amount of applied energy. That is why the repulsive energy in the form of electromagnetic force is not translational invariant.

Model (6) shows that at $\mathbf{E_{ap}} = 0$, decay of space-time and contraction of space back to Planck's scale generates negative energy of antimatter (called gravitational energy) which approaches to its maximum value (vacuum value) where takes place change of sign to positive energy, distributed in space- time frame with space expansion. The state of zero space has no sense while it leads to the runaway of energy to infinity. The state of minimum, non-zero space is needed for change of sign of negative energy of antimatter to positive energy of space-time frame of matter.

The condition when portion of energy, conserved in space phase is equal to the portion of energy of time phase (8), we can call this condition as uniform conservation of energy at background state of "super-symmetry." At this condition, unlimited fluctuation should lead to the generation of unlimited amount of energy. On this basis, there cannot be a continuous uniform state of super-symmetry or even usual symmetry, which can exist on permanent basis. Therefore, the non-uniform conservation of energy does not allow existence of continuous symmetry.

Super-symmetry is a theory of particle physics that connects boson with integer spin and fermions with half integer spin. In accordance with this theory, "each particle from one group is associated with a particle from the other group known as super partner."

The non-uniform energy conservation concept, as we described above, gives different requirement for symmetry: the symmetry is the condition where total spin numbers of particles, forming this symmetry is equal. It follows from the condition when energy portions, distributed within space and time phases are equal (8), which corresponds to the condition $\mathbf{E_{act} = 2E_s}$. This state corresponds to the discrete symmetric performance of space-time grain containing three family quarks. The total spin numbers of bosons and fermions and triplet performance of quarks family arise from the discrete symmetry of space-time variables of baryonic frame at $\mathbf{E_s = 1/2E_{ap}}$.

Equation (5) at $\mathbf{(E_{ap}/E_s - 1) \neq 1}$ describes electromagnetic force, while condition $\mathbf{E_s = 1/2\ E_{ap}}$ represents the strong force. Model (5) describes the identity of particles as bosons and fermions through exchange interactions. The energy flux makes position and momentum as separable variables; but at $\mathbf{E_{ap} = 0}$, these variables merge together to form non-separable boson compensates of indistinguishable particles, occupying the same state.

The non-uniform conservation of energy requires existence of "three particles tandem" only in discrete mode. The Exclusion Principle on existence of a particle in a certain energy state does not consider energy conservation principle and does not involve time ingredient of the conserved energy to keep a particle at this energy state.

Therefore, photons, holding Bose-Einstein statistics, exist in discrete mode within three family particles frame, which appears in the form of three-color frame. Similar to the existence of binuclear structure of matter, the antimatter structure of photons exists within discrete flavor of three colors ($\mathbf{E_{ap} = 2E_s}$), changing between two frames. Light photons travel through waves of space-time color flavors, alternating within two frames of three-color flavors. Therefore, change of photons' frequency is not possible without the three family color flavors.

The space-time frame of non-uniform energy conservation explains classic physics clarification of light photons. The condition $\mathbf{E_{ap} = 2E_s}$, produced from energy-mass exchange interaction shows that coupling of two identical half integer particles produces a particle with the integer spin, called boson. This prediction of model (5) corresponds to the quantum physics statement that the wave function of the identical half-integer spin particles changes sign when two particles swapped.

By quantum mechanics, two fermion particles cannot occupy the same quantum energy state. However, in accordance with the non-uniform energy conservation principles, two particles cannot exist unlimited time at the same position of these particles. The particle having certain space-time position may temporarily move and occupy the state of another particle through absorption or radiation of energy.

Here we may show that the non-uniform conservation of energy leads to the understanding of electron self-interaction problem as well. By literature information [33, 34], the electron mass and spin can be identified with the energy and angular momentum of the electromagnetic self-interaction.

However, as we showed earlier, the spin and mass, as the non-separable entities, arrive from the non-uniform conservation of energy in space-time field. The electron mass is not due to the electromagnetic self-interaction and its energy is not due to the potential self-energy; its energy, mass, and spin are results of the energy-mass exchange interaction that carried within space-tine field.

Hestenes [34] showed that spin may arise from helical world line of space-time, but classical arguments do not produce the properties of spin. It is necessary to note that the above-mentioned approach describes quantum level interactions without space-time frame. For example, Dirac equation describes energy-momentum relation, spin, and position for a point particle.

The energy-momentum exchange interaction, coupled with the dynamical local space-time frame, eliminates point particle problem. Model (5), which describes conservation of energy in space-time field, is the wave function of energy distribution involving asymmetric space and time variables.

Formation and expansion of space-time takes place by the non-uniform electromagnetic force with the participation of charged particles, while decay of space-time field and delivery of the energy to the background takes place by neutral current of weak force. The weak force makes a distinction between left and right due to the non-uniformity in energy-mass exchange interaction during conversion of energy from one form to another. Conversion of energy from one form to another does not involve invariant translation.

The non-uniform conservation of energy requires two opposite motions: electromagnetic acceleration of energy consumption with the expansion of space-time frame, and decay of space-time frame with the uniform restoration of energy at background state by neutral current. In accordance with model (5), coupling of space-time variables generates separate charges and electromagnetic energy, while coupling of charges generates separate space-time variables moving uniformly to the background state.

The static continuous energy conservation described by Noether's theorem does not involve locality of an event and does not limit the boundary of the conserved quantity, therefore leads to the singularity in the dynamical laws of classic physics.

The traditional concept of continuous energy conservation, described by Noether's time independent frame "energy can be neither created and not be destroyed, but it transforms from one form to another" is not a complete theory, while it describes conservation of energy in the form of time independent symmetry in abstract space, similar to Newton's abstract space. It does not involve driving force of conservation and transformation of energy from one form to another in space-time frame that is why continuous conservation of energy within unlimited time is not a valid concept to use in dynamical laws.

Model (5) has a feature of quantum physics, while energy and the produced space-time entity within non-uniform energy distribution have discrete performance and are the non-continuum "quantum portions." Model (1) at $\mathbf{E_{ap} = 0}$ describes restoration of energy and virtual asymmetric space and time products at background state. It is similar to the asymmetric wave equation of quantum mechanics:

at $\mathbf{E_{ap} = 0}$,

$$\frac{\Delta \mathbf{S}}{\mathbf{S_1}} + \frac{\Delta \mathbf{t}}{\mathbf{t_1}} = \mathbf{0} \tag{8}$$

In accordance with Eq. (8), the energy consumed in space phase is equal to the energy restored in time phase. The total energy in opposite phases is conserved **E = 0**.

When energy is inserted to space-time frame for space expansion, one of time variables (instant of time) gets performance of space coordinate for expansion of space with the decrease of frequency of energy: **(2;2)** → **(3;1)**. Generation of an event starts with the translation one of time variables to space variable. The arrow of time, which is due to the consumption of energy in space phase (appears as an energy $\mathbf{E_{ap}} - \mathbf{E_s}$ gradient), generates thermodynamic arrow of heat loss. Decrease of energy frequency $\mathbf{E_{ap}} - \mathrm{E_s}$ leads to the increase of time arrow $\Delta \mathbf{t}$, which is the move from the past to the future, carrying energetic information of the past.

This is the mechanism of generation arrow of time. Therefore, the phenomenon called entropy is due to the translation of time phase energy to the space-time frame with the loss of frequency of energy. Due to the maximum frequency of time phase energy in the past and consumption of energy in space phase, the parameter called "entropy" has its minimum value in the past.

The condition $\mathbf{(E_{ap} - E_s)/E_s = 1}$ of model (1) describes the minimum space-time frame, where the condition $\mathbf{E_{ap} = 2E_s}$ is in hold. This condition corresponds to the state where space-time frame exist as Planck's scale unit, carrying energy portion in discrete symmetry. In this case, there is no difference in performance of time and space variables. However, this condition takes place only in discrete mode.

The background state $\mathbf{E_{ap} = 0}$ of model (8) is the vacuum state of particle physics and classic field, where all the components of stress-energy tensor is zero. At $\mathbf{E_{ap} = 0}$, the space-time frame is broken to the separate space and time fields and there is no arrow of time. At $\mathbf{E_{ap}} = 0$, the gravitational energy appears as the separate force through inversion of variables. In this case, the entire energy portion, distributed in space phase (with negative sign) absorbed by the initial background state. On this basis, gravitation appears as energy-mass relation of asymmetric space-time variables rather than mass-mass relation of Newton's physics.

8. Generation of mass

One of the main problems related to the generation of mass by spontaneous breakdown of continuous symmetry, given by Higgs mechanism, is that this mechanism does not connect generation of mass with the space-time locality of a particle, which gets mass and does not explain why background continuous symmetry has to be broken by un-natural way. The mechanism of mass generation also has to explain why collision experiments produce more matter particles than antimatter particles.

In this chapter, we will discuss how the non-uniform energy conservation concept is to be the alternative mechanism of mass generation. The non-uniform distribution of energy portions within asymmetric space and time phases requires generation of the fields with the different energetic properties (frequency and amplitude), which is the only way for carrying conservation of energy through these fields. Coupling of two fields with the different energetic properties as an energy consuming and energy restoration phases generates the non-virtual space-time frame, which appears to be the non-uniform conservation of energy through energy-mass exchange transformations ($\mathbf{E_{ap}/E_s - 1}$).

The background state of space-time frame is the relation of virtual asymmetric space and time phases, which proceeds conversion of energy from one form to another (8), through translation of asymmetric entities, such as $\Delta\mathbf{S/S_1}$, $\Delta\mathbf{t/t_1}$, carrying energy portions as a virtual matter and antimatter particles.

We can describe the non-uniform background energy-mass translation by conversion of light photons to electron/positron pairs, which is well-known quantum mechanics translation event. Quantum mechanics states that during this translation, energy conservation is hold by fluctuations, such as particles borrow energy and after very short time return the borrowed energy back:

$$\gamma/\gamma = \mathbf{e}^+/\mathbf{e}^- \tag{9}$$

The energy-matter translation given by relation (9) does not count time phase of energy conservation and locality of the produced particles, while photons-leptons translation takes place in the abstract space. Equation (9) could be the discrete translation of energy in the form of infinite fluctuations of the background quantum state. It is clear that in this case there is no natural way for breaking of the continuous symmetry of discrete fluctuations, forming time independent infinite symmetry of matter-antimatter relations. Equation (9) does not reflect the borrowed time in the change of energy.

Conservation of energy requires a certain finite frame for locality that is why space and time cannot exist as separate variables. Formation of a particle within any time scale without locality in space phase leads to the missing of energy conservation. By Landau's opinion [35], infinite fluctuations of virtual matter-antimatter pairs should lead to the "Ultraviolet Catastrophe due to the accumulation of infinite amount of energy of collisions and it is impossible to prove the mathematical basis of elimination of "Ultraviolet Catastrophe."

On this basis, we replaced Eq. (9) with the relation:

$$\gamma/\gamma = -(\mathbf{e}^+/\mathbf{e}^- + \mathbf{\nu_e}/\mathbf{\nu_e}^-) \tag{10}$$

The right side of Eq. (10) involves additional identity in the form of neutrinos to cover missing part of energy conservation in time dependent frame. Equation (10) represents mechanism of energy conservation, which involves decay of energy into asymmetric space and time fields particles having different energy density. Conversion of light photons from one form to another for conservation needs generation of phase difference, which appears with the formation of $\mathbf{e^+/e^- + \nu_e/\nu_e^-}$ pairs.

The space field particles, comprising $\mathbf{e}^-/\mathbf{e}^+$ pairs have more energy density, while time phase particles, comprising ν_e/ν_e^- pairs, have energy portions of high frequency. That is why the mass for neutrinos is significantly less than that of an electron's mass. The right-handed antineutrino and left-handed neutrino pair together with the electron/positron pair represent distribution of energy within virtual space and time phases. Due to the locality within space, close to Planck's size, performance of virtual matter particles became time dependent and it get velocity less than speed of light photons that is why parity translation (10) became non-invariant.

Generation of $\mathbf{e}^-/\mathbf{e}^+ + \nu_e/\nu_e^-$ particles (10) is the translation of photons energy to virtual space and time phase particles which could be specified as an "empty space" particles. The "empty space" is the medium where $\mathbf{e}^-/\mathbf{e}^+ + \nu_e/\nu_e^-$ particles form fluid with continuum spectrum. In the absence of energy flux, $\mathbf{E}_{\mathbf{ap}} = \mathbf{0}$ (5), takes place loss of the virtual space frame (10) and translation of virtual particles backward to photons. However, particles before giving the "borrowed' energy back should loss localization in space phase and loss some portion of energy which has to go in parallel with the absorption of photons by $\mathbf{e}^-/\mathbf{e}^+$ pairs. This phenomenon is the main feature of energy non-conservation during return of "borrowed" energy of quantum fluctuations. Generation of space phase and distribution of energy in space field leads to the non-uniform conservation of energy in space by absorption of photons by $\mathbf{e}^-/\mathbf{e}^+$ pairs with formation of pairs of heavy bosons:

1. Generation of mass for bosons: passing of photons through $\mathbf{e}^+/\mathbf{e}^- + \nu_e/\nu_e^-$ field

$$\mathbf{m}\gamma\gamma + (\mathbf{e}^+/\mathbf{e}^- + \nu_e/\nu_e^-) = \mathbf{n}\gamma\gamma + \mathbf{e}^+/\nu_e(\mathbf{W}^+) + \mathbf{e}^-/\nu_e^-(\mathbf{W}^-) \tag{11}$$

2. Generation of mass for leptons

$$\mathbf{n}\gamma\gamma + \mathbf{e}^+/\nu_e(\mathbf{W}^+) + \mathbf{e}^-/\nu_e^-(\mathbf{W}^-) = (\mathbf{udd}\ldots\mathbf{Gluons}\ldots\mathbf{ddu}) \tag{12}$$

In accordance with condition (10), the pair of leptons $\mathbf{e}^-/\mathbf{e}^+ + \nu_e/\nu_e^-$ has a performance of virtual bosons (similar to the Nambu Goldstone bosons) and in the form of four leptons describes the "fermionic quanta" or virtual particles of space phase. From model (5) and Eqs. (10) and (11), it is followed that photons energy may be conserved only through exchange interaction with the non-zero mass particles.

The two pair of particles $\mathbf{e}^-/\mathbf{e}^+ + \nu_e/\nu_e^-$ in the form of virtual neutral boson field is the alternative to the Higgs field which absorbing photons generates heavy W bosons.

Exchange interaction of **yy** photons with the $\mathbf{e}^-/\mathbf{e}^+ + \nu_e/\nu_e^-$ particles lead to the observance of light which became a composite particle. When $\mathbf{E}_{\mathbf{ap}} = \mathbf{0}$, the leptons in the form of pair of particles $\mathbf{e}^-/\mathbf{e}^+ + \nu_e/\nu_e$ do not form space-time frame and do not obey Pauli exclusive principle and perform as bosons condensate with the integer spin number. Composite fermions with bosonic "face" due to the absence of exchange interactions, has a performance similar to Bose-Einstein bosons condensate, which in the form of superconductive neutral fluid carry energy to the background state. The left side of Eq. (10) describes bosons superconductive fluid, while the right side presents superconductive fermionic medium.

At $E_{ap} = 0$, decay of the ordinary matter particles $\mathbf{e^{+}/\nu_{e} + e^{-}/\nu_{e}^{-}}$ takes place with the generation of gravitational force. The energy, released from the continuous decay of space-time frame, through longitudinal wave of neutral current $e^{+}/\mathbf{e^{-}} + \nu_{e}/\nu_{e}^{-}$ of complex bosons condensate moves to the background state. The absence of exchange interaction generates longitude wave.

In the absence of energy flux, decay of space-time frame leads pairing of electron/positron and neutrino/antineutrino pairs to composite bosons with continuous spectrum. The composite bosons do not obey Pauli Exclusion Principle and can occupy the same ground to form fluid, which gets peculiar properties of superconductivity.

The empty space is the medium where particles form fluid with continuous spectrum. They become as massless particles moving with superconductivity to the initial state. The uniform fluid motion of complex boson to the background state appears as the uniform gravitational field.

Addition of neutrinos to Eq. (9) replaces the concept of electron self-interaction. The condition of space expansion describes positive energy solution while consuming all the energy in space-time ($\mathbf{E_{ap}} = 0$) represents negative energy solution.

Separation of $\mathbf{e^{-}/e^{+} + \nu_{e}/\nu_{e}^{-}}$ pairs and transformation to the frame of quarks $\mathbf{e^{+}/\nu_{e} + e^{-}/\nu_{e}^{-}}$ consumes huge amount of energy which makes produced $\mathbf{W^{+}}$, $\mathbf{W^{-}}$ bosons very heavy. However, heavy bosons are not a fermions because they do not have own non-virtual space-time frame. As in the case of Eq. (10), when there is no energy flux (absence of force carrier scalar bosons) to hold the condition of Eq. (11), due to the absence of non-virtual space-time frame, $\mathbf{W^{+}}$, $\mathbf{W^{-}}$ vector bosons have a trend to decay back to γ/γ photons in the form of beta decay. The $\mathbf{W^{+}}$, $\mathbf{W^{-}}$ bosons have a performance as left- and right-handed particles, which is why they are vector bosons. Generation of mass and its stable existence is possible if $\mathbf{W^{+}}$, $\mathbf{W^{-}}$ bosons could form a non-virtual space-time frame. On this basis, non-uniform conservation of energy requires translation of background asymmetric time phase energy to space-time frame, which leads to the generation of baryonic space-time structure. Here, it is necessary to give specifications: baryonic particles are the particles, which have space-time frame, and leptons are the particles, which in individual form have no space-time frame.

Energy of **YY** photons converted to energy of massive $\mathbf{W^{-}}$ and $\mathbf{W^{+}}$ vector bosons for generation of virtual space-time frame. In the second step, flux of the energy for generation of non-virtual space-time frame of quarks takes place within **n-p** structure. The energy of exchange interactions composes energy of gluons to hold discrete locality of quarks in the non-virtual space-time frame. The difference of the energy of **W** bosons and quarks in relation to quarks mass (at discrete symmetry energy-mass equivalence is in hold) becomes the energy flux for discrete exchange interactions. That is why quarks mass is less than that of **W** bosons. Due to the three body interactions ($\mathbf{E_{act} = 2E_{s}}$) which keeps discrete symmetry of **n-p** transformations (8), gluons participate in exchange interactions also in the form of non-zero mass particles in three family frame comprising of three-color structure.

Due to the existence of quarks family in proton-neutron frame in discrete mode, energy portion consumed from force carrier scalar in exchange interactions $\mathbf{(E_{act} - E_{s})/E_{s}}$ generates the symmetric three particles frame of quarks. In the process of cyclic **n-p** transformations, the total energy conserved.

Generation of space-time frame of quarks through alignment of "empty space field" particles $\mathbf{e^+/e^- + \nu_e/\nu_e^-}$ to "Dirac particles" $\mathbf{e^+/\nu_e + e^-/\nu_e^-}$ requires huge amount of energy flux from force carrier scalar bosons. The decay of mass and translation of space-time energy back takes place at $\mathbf{E_{act} = 0}$, $\mathbf{(\lambda = -1)}$ with transformation of $\mathbf{e^+/\nu_e + e^-/\nu_e^-}$ ingredients (Dirac particles) to the longitudinal wave of neutral current correlating the helicity of neutrinos with the negative Eigen value:

$$\mathbf{e^+/\nu_e(W^+) + e^-/\nu_e^-(W^-) \rightarrow (e^+/e^- + \nu_e/\nu_e^-) + YY} \tag{13}$$

The transformations, described by Eqs. (10)–(13), are symmetrical only in discrete mode within closed loop. The absence of invariant translations between ingredients of Eqs. (10)–(13) is due to the non-uniform conservation of energy. In accordance with model (6), in the presence of energy for reverse translation, matter particle in exchange interaction $\mathbf{(E_{act} - E_s)/E_s}$ should have more energy than that of force carrier scalar (gluons). Due to the same reason, it is impossible to separate quarks-antiquarks pairs. Separation of individual quarks is possible only at $\mathbf{E_{act}} = 0$, when three family space-time frame of proton collapses. This behavior of quarks describes color confinement phenomenon.

Model (5) explains the phenomenon called "nonlocality" or entanglement paradox of quantum mechanics. The function $\mathbf{E_{ap} - E_s/E_s}$ of model (5), which describes action-response parity, is the origin of local action. At $\mathbf{E_{ap} = 0}$, particle has no space-time frame and has no certain locality. When particle has no space-time $\mathbf{(E_{ap} = 0)}$, all particles are the non-distinguishable ingredients of antimatter "condensate."

At $\mathbf{E_{ap} - E_s > 0}$, particle has its own space-time frame and therefore independent locality. The condition $\mathbf{E_{ap} = 0}$, eliminates action-response behavior of a particle which losing spin response moves to the background state with the velocity not less than speed of light.

You cannot isolate virtual space phase from virtual time phase that is why it is impossible to separate the quark-antiquark frame. Meson alone has no space-time frame that is why it is not observable as a separate particle, but it is a piece of non-virtual space-time frame of **p-n** frame, having a motion in baryon structure.

The exchange interaction of model (5) $\mathbf{(E_{ap} - E_s)/E_s}$ explains why the weak interaction acts only on left-handed particles and right-handed antiparticles. The right-handed particles in exchange interactions lead to the expansion of space matter, while left-handed matter particles generate gravitational force to hold the boundary of the conserved energy. The non-invariant translation of a body to the initial state takes place with the decay of space-time frame and realignment of the neutrinos helicity with formation of neutral current. Composite bosons with the continuum spectrum comprise the phenomenon called gravitation.

The first step described by Eqs. (10) and (11) is the generation of non-zero mass virtual particles having virtual space-time frame, while the step (12) involves transformation of a lepton particles from virtual space-time manifold to the minimum grain of non-virtual space-time frame. That is why mechanism of generation of mass for space-time frame particles (quarks) and bosons is different.

From model (1), it follows that at zero value of $\mathbf{E_s}$, the space-time frame moves to the singularity. Therefore, the inertial energy of a particle in cyclic mode can never have zero value and when more energy portion applied to the space-time frame, the gravitational mass added. The gravitational mass appears as the energy portion distributed in space-time frame to control conservation of energy within certain boundary of this frame. $\mathbf{E_{ap}}$ in energy flux $(\mathbf{E_{ap}} - \mathbf{E_s})/\mathbf{E_s}$ is the bosonic part of the frame, while **Es** is the fermionic ingredient of exchange interactions. The energy flux $(\mathbf{E_{ap}} - \mathbf{E_s})/\mathbf{E_s}$ through coupling with the local position of space-time $\mathbf{S_1/t_1}$ describes interaction of bosonic and fermionic particles through exchange of energy. In case when interaction takes place between two fermions, the ingredients of the energy flux $(\mathbf{E_{ap}} - \mathbf{E_s})/\mathbf{E_s}$ describes interaction of energy or mass content of these fermions. Therefore, model (5) connects all the interactions of particles physics.

Generation of mass is the combination of electromagnetic and weak forces. The electromagnetic force needed for generation of non-virtual space-time frame, while weak force is necessary to keep the existence of space-time frame of a matter "grain" through discrete symmetry, which requires violation of local CPT symmetry. Weak interactions are the result of non-uniform discrete conservation of energy, which takes place with translation of asymmetric boundaries of space-time phases, carrying non-uniform conservation of energy.

Now appears a question, why electromagnetic force is carried by charged particles, while neutral particles are responsible for gravitation. Charged bosons are needed for generation of non-zero mass quarks of space-time frame to carry conservation of energy in expansion phase of space, while neutral bosons are needed for translation of space-time energy back to the background state. At $\mathbf{E_{ap} = 0}$, decay of space-time frame releases graviton in the form of neutral current back to the initial state.

Within non-uniform conservation of energy in space-time frame we may explain how space-time, carrying energy distribution may lead to the generation of chargers. The space-time to carry non-uniform conservation of energy leads to the formation of phase difference between space and time coordinates which appears in the form of charges.

In non-uniform conservation of energy, boundary of space and time variables is asymmetrically different, and background coupling of asymmetric space-time variables does not produce symmetrical particles-antiparticles pairs. At Planck scale, when space boundary is small, the left side of Eq. (8) has a huge trend to change and the duration of change at this scale is very small. Therefore, space and time variables, carrying the same portions of energy, have very asymmetric boundaries, which is the driving force for selection of the direction in non-uniform distribution of energy.

Due to this reason, the symmetry of strong force and permanent performance of the proton-neutron pairs is possible only through discrete uniform translation of scalar energy to the "three particles tandem of" space-time-energy frame (5).

Due to the requirement of discrete symmetry $\mathbf{E_{ap} = 2E_s}$, neutrinos also exists in three family mode; Two types of neutrinos couple and produce third type neutrino; asymmetric decay of the third neutrino leads back to the realization of discrete symmetry of neutrino's existence. At $\mathbf{E_{ap} = 0}$, neutrinos do not participate in electromagnetic force but at $\mathbf{E_{ap} \neq 0}$, neutrino, being part of quark structure, participates in the discrete symmetry of baryon frame. The neutrino's mass is small for realization of neutron-proton discrete symmetry with high frequency.

The weak force is needed to hold permanent performance of the "space-time frame of elementary grain" of the matter in discrete mode within minimum space frame. The conservation of matter "grain" in the form of proton cannot hold continuous symmetry, while in this case there cannot be conservation of energy.

The discrete performance of three particles frame $\mathbf{E_{ap} = 2E_s}$ explains why there are three families of quarks. For generation of discrete stable performance of an **n-p** pair the energy flux to space-time frame of baryon quarks needs to meet the condition $\mathbf{E_{ap} = 2E_s}$. The baryon alone is not stable therefore cannot be the fundamental matter: the two nucleons are coupled with the meson field **TB** (top-antibottom) to form three flavor structure of space-time frame $\mathbf{E_{ap} = 2E_s}$. In this case, the **n-p** frame holds discrete symmetry with high frequency and **n-p** transformation event which "after the change looks the same" (8).

The non-uniform conservation concept explains "mass gap problem" of Yang-Mills theory [36], which states "quantum particles have positive mass with regard to the vacuum state." The positive Eigen value of $(\mathbf{E_{ap}} - \mathrm{E_S})/\mathbf{E}_\mathrm{S}$ exchange interactions shows that "quantum" particle has a positive mass in relation to the vacuum while translation of time phase vacuum energy to the space-time frame generates positive Eigen value $(\mathbf{E_{ap}} - \mathrm{E_S})/\mathbf{E}_\mathrm{S}$ and positive mass. Conversion of mass to energy produces energy with negative sign and this process does not response to the change of time.

Description of the energy flux of model (6) in the form Eigen value $(\mathbf{E_{ap}/E}_\mathrm{S} - \mathbf{E}_\mathrm{S}/\mathbf{E}_\mathrm{S})$ involves two terms: the term $\mathbf{E_{ap}/E}_\mathrm{S}$ describes performance of charged particles through electromagnetic flux of energy, while $\mathbf{E}_\mathrm{S}/\mathbf{E}_\mathrm{S}$ involves neutral particles—neutrinos which have self-coupling performance and do not experience effect of forces.

Recently, due to the dark energy phenomenon of Universe, the subject of energy conservation got more attention. For example, Ref. [37] suggest that without dark energy and dark matter, Einstein's gravitational field equations should not hold conservation of energy-momentum relation.

In accordance with the non-uniform energy conservation concept, we may give specification of ordinary and dark energy. The dark energy generated due to the non-invariant translation of ordinary energy to the virtual space-time frame. Ordinary matter exists when there is space-time frame; but when space-time frame decays, it disappears with the decay of space-time frame of ordinary matter. Dark matter is not a baryonic matter and has no non-virtual space-time frame. Matter may have observance when it has non-virtual space-time frame.

The non-uniform phenomenon of energy conservation and non-invariant weak interaction are the necessary laws of nature to give different shapes to the different events: without non-uniform conservation of energy and non-invariant exchange interaction, the events would form a non-separable dark matter without any shape and structure.

In accordance with model (5), both energy and matter to be observable should have space-time frame. In the background, energy and space-time are not observable. On this basis, the non-observable time phase energy has features of dark energy.

Thus, the space and time are the products of non-uniform energy conservation and in reverse order, energy and mass identities are the inner products of space-time discrete dynamics. This concept completely changes our views on the fundamental interactions and symmetrical laws of nature. Therefore, nature requires description only within very precise energy conservation principles.

9. Conclusion

We replaced two pieces of conservation laws, comprising conservation of energy as uniformity in time and conservation of momentum as uniformity in space by the new conservation concept suggesting non-uniform conservation of energy within discrete space-time frame. We replaced particles concept of classic physics and wave equation of quantum physics by the boundary mapped discrete space-time frame, which carries the non-uniform conservation of energy. Uniform manifestation of energy in time and uniform manifestation of momentum in space is not possible within space-time frame, which carries energy conservation within the non-uniform framework.

Therefore, the energy-mass equivalence, limitation of velocity with the speed of light, breaking of background symmetry all originate from the non-uniform conservation of energy. The background state of discrete space-time frame describes quantum level interactions through discrete transformation of space-time variables to each other with generation of discrete virtual particle-antiparticle pairs. Consumption of energy from the background field leads to the formation of the "grain" of the non-virtual space-time frame with generation of mass, energy-momentum relation of general relativity and classic physics.

With the increase of energy portion consumed in space phase, it consumes more energy to continue its velocity that is why expansion of space is "accelerated," which is the result of non-uniform conservation of energy. Conservation of energy is accelerated which appears in the form of non-uniform distribution of energy within asymmetric space and time boundaries.

Our concept suggests that the laws of nature comprise simple deterministic formulation of space-time, which holds conservation of energy in a unique way through non-spontaneous background translations of space-time phases. The consumption of energy photons by the space-time matter with the expansion of space generates backup reaction, which becomes the origin of gravity.

Finally, discrete, non-invariant translation of asymmetric boundaries of space and time variables to each other for carrying energy portions is the deterministic mathematical beauty of energy conservation and discrete existence of nature.

Author details

Agaddin Khanlar Mamedov

Address all correspondence to: aghaddinm@gmail.com

Petrochemical Company, Technology Center, Sugar Land, Texas, USA

References

[1] Mamedov AK. Unification of quantum mechanics and general relativity based on non-continuous space/time framework. European Journal of Scientific Research. 2009;**36**:570-584

[2] Mamedov AK. Unification of dynamical laws through frequency based discrete space-time and symmetry principle. European Journal of Scientific Research. 2010;**42**:359-384

[3] Mamedov AK. Unification of quantum mechanics and relativity based on discrete energy conservation law 4. The new classic physics formulation of interactions versus standard model. European Journal of Scientific Research. 2011;**57**(2):314-365

[4] Mamedov AK. Unification of quantum mechanics and relativity based on discrete conservation of energy. In: The Selected Topics of Quantum Mechanics. Rijeka, Croatia: InTech; 2014

[5] Higgs PW. Broken symmetries and the masses of gauge bosons. Physical Review Letters. 1964;**13**:508-509

[6] Englert F, Brout R. Broken symmetry and the mass of gauge vector bosons. Physical Review Letters. 1964;**13**:321-323

[7] Guralnik GS. Photon as a symmetry-breaking solution to field theory. I. Physics Review. 1964;**136**:B1404-B1416

[8] Guralnik GS. Photon as a symmetry-breaking solution to field theory. II. Physics Review. 1964;**136**:B1417-B1422

[9] Kibble TWB. Symmetry breaking in non-Abelian gauge theories. Physics Review. 1967; **155**:1554-1561

[10] Wilczek F. Quantum field theory. Reviews of Modern Physics. 1999;**71**:S85

[11] Wilczek F. Quantum mechanics of fractional spin particles. Physical Review Letters. 1982; **49**(14):957

[12] Wilczek F. Origins of Mass. arXiv: 1206.7114v2 [hep-ph]. August 22, 2012

[13] Glashow SL. Partial symmetries of weak interactions. Nuclear Physics. 1961;**22**:579-588

[14] Salam A, Ward C. Electromagnetic and weak interactions. Physics Letters. 1964:**13**(2):168-171

[15] Goldstone J, Salam A, Weinberg S. Broken symmetries. Physics Review. 1962;**127**:965-970

[16] Salam A. In: Proceedings of the 8th Nobel Symposium on Elementary particle theory, relativistic groups and analyticity; Lerum, Stockholm, Sweden; 19–25 May 1968; pp. 367-377

[17] Elitzur S. Impossibility of spontaneously breaking local symmetries. Physics Review. 1975;**12**:3978-3982

[18] Van der Bij JJ. Cosmotopological relation for a unified field theory. Physical Review. 2007; **12**(D76):121702

[19] Janiak A. Kant's views of space and time. In: Stanford Encyclopedia of Philosophy. 4th ed. Stanford, USA: Stanford University; 2009

[20] Kant I. Critique of Pure Reason. Cambridge University Press. Translated by Guyer P, Wood A. Cambridge, UK: Cambridge University Press. Press Syndicate of the University of Cambridge; 1998

[21] Overduin IJ. Gravity probe B. In: Testing Einstein's Universe. Stanford, USA: Stanford University; 2007

[22] Ferraro R. Einstein's Space-Time: An Introduction to Special and General Relativity. 2007th ed. Buenos Aires: Springer Sciences <Business Media, LLC

[23] Merali Z. Theoretical physics: The origins of space and time. Nature. 2013;**500**:516-519

[24] Barbour J. The End of Time: The Next Revolution in Physics. Oxford: Oxford University Press; 1999

[25] Feynman RP. The development of the space-time view of quantum electrodynamics. Nobel Lecture. December 11, 1965

[26] Hanca J, Tuljab S, Hancova M. Symmetries and conservation laws: Consequences of Noether's theorem. American Journal of Physics. 2004;**72**(4):428-435

[27] Van der Bijj JJ. Gravitational anomaly and fundamental forces. 2011;**43**(9):2499

[28] Naber G.L. The Geometry of Minkowski Spacetime, 2012

[29] Relativistic OT. Quantum Physics: From Advanced Quantum Mechanics to Introductory Quantum Field Theory. Cambridge University Press; 2011. p. 86

[30] Griffits DJ. An Introduction to Quantum Mechanics. Pearson Prentice Hall; 2005

[31] Haddad WM, Chellboina V, Nersesov SG. Thermodynamics. A dynamical Systems Approach. Princeton University Press; 1961

[32] Carroll SM. Energy is not conserved. Posted on February 22, 2010

[33] Feynman RP. Electrons and their interactions. In: QED: The Strange Theory of Light and Matter. Vol. 1985. Princeton, New Jersey: Princeton University Press; 1985. p. 115

[34] Hestenes D. Quantum mechanics from self-interaction. Foundations of Physics. 1983; **15**(1):63

[35] Wilczek F. Nobel lecture. Asymptotic freedom: From Paradox to Paradigm. December 8, 2004

[36] Chaves M. An Introduction to Generalized Yang Mills Therores. arXiv: [hep -th], 0102055v2. January 2003

[37] The Daily Galaxy. New Dark Matter and Energy Alters Einstein's view of Space-time. Available from: http://www.DailyGalaxy.com [Accessed: September 6, 2012]

Chapter 9

Quantum Calculus with the Notion $\delta_\pm$-Periodicity and Its Applications

Neslihan Nesliye Pelen, Ayşe Feza Güvenilir and
Billur Kaymakçalan

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.74952

Abstract

The relation between the time scale calculus and quantum calculus and the $\delta_\pm$-periodicity in quantum calculus with the notion is considered. As an application, in two-dimensional predator–prey system with Beddington-DeAngelis-type functional response on periodic time scales in shifts is used.

Keywords: predator prey dynamic systems, Beddington-DeAngelis-type functional response, $\delta_\pm$-periodic solutions on quantum calculus, periodic time scales in shifts

1. Introduction

The traditional infinitesimal calculus without the limit notion is called calculus without limits or quantum calculus. After the developments in quantum mechanics, q-calculus and h-calculus are defined. In these calculi, h is Planck's constant and q stands for the quantum. These two parameters q and h are related with each other as $q = e^{ih} = e^{2\pi i\tilde{h}}$. This equation $\tilde{h} = \frac{h}{2\pi}$ is the reduced Planck's constant. h-calculus can also be seen as the calculus of the differential equations, and this was first studied by George Boole. Many other scientists also made some studies on h-calculus, and it was shown that it is useful in a number of fields, among them, combinatorics and fluid mechanics. The q-calculus is more useful in quantum mechanics, and it has an intimate connection with commutative relations [1]. In the following, the main notions and its relation to the time scale calculus will be discussed.

In [2], in classical calculus when the equation

$$\frac{f(x) - f(x_0)}{x - x_0}$$

is considered and as x tends to $x_0,$ the differentiation notion is obtained. When the differential equations are considered, the difference of a function is defined as $f(x + 1) - f(x)$. In quantum calculus, the q-differential of a function is equal to the following:

$$d_q(f(x)) = f(qx) - f(x)$$

and

$$d_q(x) = qx - x = (q - 1)x.$$

Then the q-derivative is defined as follows:

$$\frac{d_q(f(x))}{d_q(x)} = \frac{f(qx) - f(x)}{(q - 1)x}.$$

The differentiation in time scale calculus is given in Theorem 1, and if the differentiation notion in this theorem is applied when $\mathbb{T} = q^{\mathbb{N}},$ one can easily see that the same q-derivative is obtained.

As an inverse of q-derivative, one can get q-integral that is also very significant for the structure of this calculus. A function $F(x)$ is a q-antiderivative of $f(x)$ if $D_qF(x) = f(x)$ is satisfied where

$$F(x) = \int f(x)d_qx = (1 - q)\sum_{0}^{\infty} xq^jf\left(xq^j\right).$$

This is also called the Jackson integral [3]. When the definition of the antiderivative of a function in time scale calculus is considered, it can be easily seen that when $\mathbb{T} = q^{\mathbb{N}_0},$ these two definitions become equivalent. Therefore, to understand the quantum calculus, it is very important to understand the time scale calculus. In addition to these, the $\delta_{\pm}$-periodicity notion in time scale calculus is defined in Definition 1 in [4] for the application. In this study, by using time scale calculus, the application of $\delta_{\pm}$-periodicity notion of $q^{\mathbb{N}},$ which overlaps with the q-calculus, to a predator–prey system with Beddington-DeAngelis-type functional response is studied.

To understand this application in a much better sense, the following information about the predator–prey dynamic systems is given. Predator–prey equations are also known as the Lotka-Volterra equations. This model was initially proposed by Alfred J. Lotka in the theory of autocatalytic chemical reactions in 1910 [5, 6] which was effectively the logistic Equation [7] and originally derived by Pierre Françis Verhulst [8]. In 1920, Lotka extended this model to "organic systems" by using a plant species and a herbivorous animal species. The findings of this study were published in [9]. In 1925, he obtained the equations to analyze predator–prey interactions in his book on biomathematics [10] arriving at the equations that we know today.

After the development of the equations for predator–prey systems, it becomes important to obtain the type of functional response. The first functional response was proposed by C. S. Holling in [11, 12]. Both the Lotka-Volterra model and Holling's extensions have been used to model the moose and wolf populations in Isle Royale National Park [13]. In addition to these, there are many studies that use the predator–prey dynamic systems with Holling-type functional responses. These studies especially analyze the permanence, stability, periodicity, and such different aspects of these systems. The papers [14], [15, 16] can be some of its examples.

Arditi and Ginzburg made some changes and extension on the functional response of Holling, and this new functional response is known as the ratio-dependent functional response. Also, from this functional response, the semiratio-dependent functional responses are also derived. Again, there are many studies that are about the several structures of the predator–prey dynamic systems such as [14, 17–19], [20, 21].

2. Preliminaries about time scale calculus

The main tool we have used, in this study, is time scale calculus, which was first appeared in 1990 in the thesis of Stephen Hilger [22]. By a time scale, denoted by $\mathbb{T}$, we mean a non-empty closed subset of $\mathbb{R}$. The theory of time scale calculus gives a way to unify continuous and discrete analysis.

The following informations are taken from [14, 23]. The set $\mathbb{T}^{\kappa}$ is defined by $\mathbb{T}^{\kappa} = \mathbb{T}/\left(\rho\left(\sup\mathbb{T}\right), \sup\mathbb{T}\right]$, and the set $\mathbb{T}_{\kappa}$ is defined by $\mathbb{T}_{\kappa} = \mathbb{T}/[\inf\mathbb{T}, \sigma(\inf\mathbb{T}))$. The forward jump operator $\sigma : \mathbb{T} \to \mathbb{T}$ is defined by $\sigma(t){:=}in\,(t, \infty)_{\mathbb{T}}, for \;\; t \in \mathbb{T}$. The backward jump operator $\rho : \mathbb{T} \to \mathbb{T}$ is defined by $\rho(t){:=}\sup(-\infty, t)_{\mathbb{T}}, for \;\; t \in \mathbb{T}$. The forward graininess function $\mu : \mathbb{T} \to \mathbb{R}_0^+$ is defined by $\mu(t){:=}\sigma(t) - t, for \;\; t \in \mathbb{T}$. The backward graininess function $\nu : \mathbb{T} \to \mathbb{R}_0^+$ is defined by $\nu(t){:=}t - \rho(t), for \;\; t \in \mathbb{T}$. Here, it is assumed that $\inf 0/ = \sup\mathbb{T}$ and $\sup 0/ = \inf\mathbb{T}$.

For a function $f : \mathbb{T} \to \mathbb{T}$, we define the Δ-derivative of f at $t \in \mathbb{T}^{\kappa}$, denoted by $f^{\Delta}(t)$ for all $\epsilon > 0$. There exists a neighborhood $U \subset \mathbb{T}$ of $t \in \mathbb{T}^{\kappa}$ such that

$$|f(\sigma(t)) - f(s) - f^{\Delta}(t)(\sigma(t) - s)| \leq \epsilon |\sigma(t) - s|$$

for all $s \in U$.

For the same function, the ∇-derivative of f at $t \in \mathbb{T}_{\kappa}$, denoted by $f^{\nabla}(t)$, for all $\epsilon > 0.$, is defined. There exists a neighborhood $V \subset \mathbb{T}$ of $t \in \mathbb{T}_{\kappa}$ such that

$$|f(s) - f(\rho(t)) - f^{\nabla}(t)(s - \rho(t))| \leq \epsilon |s - \rho(t)|$$

for all $s \in V$.

A function $f : \mathbb{T} \to \mathbb{R}$ is rd-continuous if it is continuous at right-dense points in $\mathbb{T}$ and its left-sided limits exist at left-dense points in $\mathbb{T}$. The class of real rd-continuous functions defined on a time scale $\mathbb{T}$ is denoted by $C_{rd}(\mathbb{T}, \mathbb{R})$. If $f \in C_{rd}(\mathbb{T}, \mathbb{R}),$ then there exists a function $F(t)$ such that $F^{\Delta}(t) = f(t)$. The delta integral is defined by $\int_a^b f(x)\Delta x = F(b) - F(a)$.

Theorem 1. [23] *Suppose that $f : \mathbb{T} \to \mathbb{R}$ is a function and $t \in \mathbb{T}^{\kappa}$. Then, we have the following*:

1. *If f is delta differentiable at $t,$ then f is continuous at t.*
2. *If f is continuous at a right scattered t, then f is delta differentiable at t with*

$$f^{\Delta}(t) = \frac{f(\sigma(t)) - f(t)}{\mu(t)}.$$

3. *If t is right dense, then f is delta differentiable at t if and only if the limit*

$$\lim_{s \to t} \frac{f(t) - f(s)}{t - s}$$

exists as a finite number. In this case,

$$f^{\Delta}(t) = \lim_{s \to t} \frac{f(t) - f(s)}{t - s}.$$

4. *If f is delta differentiable at $t,$ then*

$$f^{\sigma}(t) = f(t) + \mu(t) f^{\Delta}(t).$$

Theorem 2. [23] *If $a, \ b, \ c, \ d \in \mathbb{T}, \ \alpha \in \mathbb{R}$, and $f, g : \mathbb{T} \to \mathbb{R}$ are rd-continuous, then*

- $\int_a^b [f(t) + g(t)]\Delta t = \int_a^b f(t)\Delta(t) + \int_a^b g(t)\Delta t;$
- $\int_a^b \alpha f(t)\Delta t = \alpha \int_a^b f(t)\Delta t;$
- $\int_a^b f(t)\Delta t = -\int_b^a f(t)\Delta t;$
- $\int_a^b f(t)\Delta t = \int_a^c f(t)\Delta t + \int_c^b f(t)\Delta t;$
- $\int_a^a f(t)\Delta(t) = 0;$
- $\int_a^b f(t) g^{\Delta}(t)\Delta t = fg(b) - fg(a) - \int_a^b f^{\Delta}(t) g(\sigma(t))\Delta t;$
- $\int_a^b f(\sigma(t)) g^{\Delta}(t)\Delta t = fg(b) - fg(a) - \int_a^b f^{\Delta}(t) g(t)\Delta t.$

Theorem 3. [23] *If $a, b \in \mathbb{T}, \ \alpha \in \mathbb{R}$, and $f : \mathbb{T} \to \mathbb{R}$ are rd-continuous, then*

- If $\mathbb{T} = \mathbb{R}$, then

$$\int_a^b f(t)\Delta t = \int_a^b f(t)dt,$$

where the integral on the right is the Riemann integral from calculus.

- *If $\mathbb{T}$ consists of only isolated points and $a < b$, then*

$$\sum_{t \in [a,b)} f(t)\mu(t).$$

Theorem 4. [14] *(Continuation Theorem). Let L be a Fredholm mapping of index zero and C be L-compact on Ω. Assume*

a. *For each $\lambda \in (0,1)$, any y satisfying $Ly = \lambda Cy$ is not on $\delta\Omega$, i.e., $y \notin \delta\Omega$*

b. *For each $y \in \delta\Omega \cap KerL$, $VCy \neq 0$ and the Brouwer degree $\deg\{JVC, \delta\Omega \cap KerL, 0\} \neq 0$. Then, $Ly = Cy$ has at least one solution lying in $DomL \cap \delta\Omega$.*

We will also give the following lemma, which is essential for this chapter.

Definition 1. [4] *Let the time scale $\mathbb{T}$ including a fixed number $t_0 \in \mathbb{T}^*$ where $\mathbb{T}^*$ be a non-empty subset of $\mathbb{T}$, such that there exist operators $\delta\pm : [t_0;\infty)_{\mathbb{T}} \times \mathbb{T}^* \to \mathbb{T}^*$ which satisfy the following properties:*

P.1 With respect to their second arguments, the functions $\delta\pm$ are strictly increasing, i.e., if

$$(S_0, v), (S_0, s) \in D_{\pm} := \{(u, v) \in [t_0, \infty)_{\mathbb{T}} \times \mathbb{T}^* : \delta \pm (u, v) \in \mathbb{T}^*\},$$

then

$S_0 \leq v < s$ implies $\delta \pm (S_0, v) < \delta \pm (S_0, s)$,

P.2 If (S_1, s), $(S_2, s) \in D_-$ with $S_1 < S_2$, then $\delta_-(S_1, s) > \delta_-(S_2, s)$,, and if $(S_1, s), (S_2, s) \in D_+$ with $S1 < S2$, then $\delta_+(S_1, s) < \delta_+(S_2, s)$,

P.3 If $v \in [t_0;\infty)_{\mathbb{T}}$, then $(v, t_0) \in D_+$ and $\delta_+(v, t_0) = s$. Moreover, if $v \in \mathbb{T}^*$, then $(t_0, v) \in D_+$ and $\delta_+(t_0, v) = v$ holds

P.4 If $(u, v) \in D_{\pm}$, then $(u, \delta_{\pm}(u, v)) \in D_{\pm}$ and $\delta_{\mp}(u; \delta_{\pm}(u, v)) = v$, respectively.

P.5 If $(u, v) \in D_{\pm}$ and $(s, \delta_{\pm}(u, v)) \in D_{\pm}$, then $(u, \delta_{\mp}(s, v)) \in D_{\pm}$ and

$$\delta_{\mp}(s, \delta_{\pm}(u, v)) = \delta_{\pm}(u, \delta_{\mp}(s, v)), \textit{respectively}$$

Then the backward operator is δ_-, and the forward operator is δ_+ which are associated with $t_0 \in \mathbb{T}^*$ (called the initial point). Shift size is the variable $u \in [t_0; \infty)_{\mathbb{T}}$ in $\delta_{\pm}(u, v)$. The values $\delta_+(u, v)$ and $\delta_+(u, v)$ in $\mathbb{T}^*$ indicate u unit translation of the term $v \in \mathbb{T}^*$ to the right and left, respectively. The sets $D_{\pm}$ are the domains of the shift operators $\delta_{\pm}$, respectively.

Definition 2. [4] *Let $\mathbb{T}$ be a time scale with the shift operators $\delta\pm$ associated with the initial point $t_0 \in \mathbb{T}^*$. The time scale $\mathbb{T}$ is said to be periodic in shifts $\delta\pm$ if there exists a $q \in (t_0, \infty)_{\mathbb{T}^*}$ such that $(q, t) \in D_{\pm}$ for all $t \in \mathbb{T}^*$. Furthermore, if*

$$Q{:=}\inf\left\{q \in (t_0, \infty)_{\mathbb{T}^*} : (q, t) \in D_{\pm} \ \ for \ \ all \ \ t \in \mathbb{T}^*\right\} \neq t_0$$

then P is called the period of the time scale $\mathbb{T}$.

Definition 3. [4] *(Periodic function in shifts δ_+ and δ_-). Let $\mathbb{T}$ be a time scale that is periodic in shifts δ_+ and δ_- with the period Q. We say that a real valued function g defined on $\mathbb{T}^*$ is periodic in shifts if there exists a $\tilde{T} \in [Q, \infty)_{\mathbb{T}^*}$ such that*

$$g\left(\delta_{\pm}\left(\tilde{T}, t\right)\right) = g(t).$$

The smallest number $\tilde{T} \in [Q, \infty)_{\mathbb{T}^*}$ such that is called the period of f.

Definition 1, Definition 2, and Definition 3 are from [4].

[24]

Notation 1 $\delta_+^2(T, \kappa) = \delta_+(T, \delta_+(T, \kappa))$,

$$\delta_+^3(T, \kappa) = \delta_+(T, \delta_+(T, \delta_+(T, \kappa))), \ldots$$

$$\delta_+^n(T, \kappa) = \delta_+(, \delta_+(T, \delta_+(T, \delta_+(\ldots.)))).$$

Lemma 1. [24] *Let our time scale $\mathbb{T}$ be periodic in shifts, and for each $t \in \mathbb{T}^*$, $\left(\delta_+^n(T, t)\right)^{\Delta}$ is constant. Then, $\frac{\int_{\kappa}^{\delta_+(T,\kappa)} u(t)\Delta t}{mes(\delta_+(T,\kappa))}$ is also constant $\forall \kappa \in \mathbb{T}$,*

where $\kappa = \delta_{\pm}^m(T, t_0)$ for $m \in \mathbb{N}$ and $mes(\delta_+(T, \kappa))$ = $\int_{\kappa}^{\delta_+(T,\kappa)} 1\Delta t$. Here, $u(t)$ is a periodic function in shifts.

Proof. We get the desired result, if we can be able to show that for any $\kappa_1 \neq \kappa_2$ ($\kappa_1, \kappa_2 \in \mathbb{T}$).

$$\frac{\int_{\kappa_1}^{\delta_+(T,\kappa_1)} u(t)\Delta t}{mes(\delta_+(T,\kappa_1))} = \frac{\int_{\kappa_2}^{\delta_+(T,\kappa_2)} u(t)\Delta t}{mes(\delta_+(T,\kappa_2))}.$$

Since $\mathbb{T}$ is a periodic time scale in shifts (WLOG $\kappa_2 > \kappa_1$), there exits $n \in \mathbb{N}$ such that $\kappa_2 = \delta_+^n(T,\kappa_1)$. Hence, it is also enough to show that

$$\frac{\int_{\kappa_1}^{\delta_+(T,\kappa_1)} u(t)\Delta t}{mes(\delta_+(T,\kappa_1))} = \frac{\int_{\delta_+^n(T,\kappa_1)}^{\delta_+\left(T,\delta_+^n(T,\kappa_1)\right)} u(t)\Delta t}{mes(\delta_+(T,\delta_+^n(T,\kappa_1)))}.$$

Because of the definition of the time scale and u, $u(\kappa_1) = u\big(\delta_+^n(T,\kappa_1)\big)$, $u(\delta_+(T,\kappa_1)) = u\big(\delta_+^{n+1}(T,\kappa_1)\big)$, and for each $t \in [\kappa_1, \delta_+(T,\kappa_1)]$, $u(t) = u\big(\delta_+^n(T,t)\big)$. By using change of variables, we get the result. If $s = \delta_+^n(T,t)$, then by the assumption of the lemma $\Delta s = \tilde{c}\Delta t$. When $s = \delta_+^n(T,\kappa_1)$, then $t = \delta_-^n(T,s) = \kappa_1$, and when $s = \delta_+^{n+1}(T,\kappa_1)$, then $t = \delta_-^n(T,s) = \delta_+(T,\kappa_1)$.

$$\int_{\delta_+^n(T,\kappa_1)}^{\delta_+^{n+1}(T,\kappa_1)} u(s)\Delta s = \tilde{c}\int_{\kappa_1}^{\delta_+(T,\kappa_1)} u(t)\Delta t,$$
$$\int_{\delta_+^n(T,\kappa_1)}^{\delta_+^{n+1}(T,\kappa_1)} 1\Delta t = \tilde{c}\int_{\kappa_1}^{\delta_+(T,\kappa_1)} 1\Delta t,$$

and

$$\frac{\int_{\kappa_1}^{\delta_+(T,\kappa_1)} u(t)\Delta t}{mes(\delta_+(T,\kappa_1))} = \frac{\tilde{c}\int_{\kappa_1}^{\delta_+(T,\kappa_1)} u(t)\Delta t}{\tilde{c}\ \ mes(\delta_+(T,\kappa_1)).}$$

Hence, proof follows. □

Remark 1. [24] *It is obvious that if* $\mathbb{T} = \{0\}\cup q^{\mathbb{Z}}$, *then* $mes(\delta_+(T,t))$ *is equal for each* t *in* $\{0\}\cup q^{\mathbb{Z}}$.

The equation that we investigate is

$$\begin{aligned} x^{\Delta}(t) &= a(t) - b(t)\,exp\,(x(t)) - \frac{c(t)\,exp\,(y(t))}{\alpha(t)+\beta(t)\,exp\,(x(t)) + m(t)\,exp\,(y(t))}, \\ y^{\Delta}(t) &= -d(t) + \frac{f(t)\,exp\,(x(t))}{\alpha(t)+\beta(t)\,exp\,(x(t)) + m(t)\,exp\,(y(t))}, \end{aligned} \tag{2.1}$$

In Eq. (2.1), let $a(t) = a(\delta_\pm(T,t))$, $b(\delta_\pm(T,t)) = b(t)$, $c(\delta_\pm(T,t)) = c(t)$, $d(\delta_\pm(T,t)) = d(t)$, $f(\delta_\pm(T,t)) = f(t)$, $\alpha(\delta_\pm(T,t)) = \alpha(t)$, $\beta(\delta_\pm(T,t)) = \beta(t)$, and $m(\delta_\pm(T,t)) = m(t)$, and $\int_\kappa^{\delta_+(T,\kappa)} a(t)\Delta t$, $\int_\kappa^{\delta_+(T,\kappa)} b(t)\Delta t$, $\int_\kappa^{\delta_+(T,\kappa)} d(t)\Delta t > 0$. $\beta^l = \min_{t\in[\kappa,\delta_+(T,\kappa)]}\beta(t)$, $m^l = \min_{t\in[\kappa,\delta_+(T,\kappa)]}$

$m(t)$, $\beta^u = \max_{t\in[\kappa,\delta_+(T,\kappa)]}\beta(t)$, and $m^u = \max_{t\in[\kappa,\delta_+(T,\kappa)]}m(t)$, such that $\kappa = \delta_\pm^m(T, t_0)$ for $m\in\mathbb{N}$. $m(t) > 0$ and $c(t), f(t), b(t) > 0$ $\alpha(t)\geq 0$, $\beta(t) > 0$. Each function is from $C_{rd}(\mathbb{T}, \mathbb{R})$.

Lemma 2. [24] *Let* $t_1, t_2\in[\kappa, \delta_+(T,\kappa)]$ *and* $t\in\{0\}\cup q^{\mathbb{Z}}$. κ *is defined as in Lemma 1. If* $g : \{0\}\cup q^{\mathbb{Z}} \to R$ *is periodic function in shifts, then*

$$g(t)\leq g(t_1) + \int_\kappa^{\delta_+(T,\kappa)} |g^\Delta(s)|\Delta s \qquad \text{and} \qquad g(t)\geq g(t_2) - \int_\kappa^{\delta_+(T,\kappa)} |g^\Delta(s)|\Delta s.$$

Proof. We only show the first inequality as the proof of the second inequality is similar to the proof of the other one. Since g is a periodic function in shifts, without loss of generality, it suffices to show that the inequality is valid for $t\in[\kappa, \delta_+(T,\kappa)]$. If $t = t_1$ then the first inequality is obviously true. If $t > t_1$

$$g(t) - g(t_1)\leq |g(t) - g(t_1)| = \left|\int_{t_1}^t g^\Delta(s)\Delta s\right| \leq \int_{t_1}^t g^\Delta(s)|\Delta s\leq \int_\kappa^{\delta_+(T,\kappa)} |g^\Delta(s)|\Delta s.$$

Therefore,

$$g(t)\leq g(t_1) + \int_\kappa^{\delta_+(T,\kappa)} |g^\Delta(s)|\Delta s.$$

If

$$t < t_1$$

$$g(t_1) - g(t)\geq - |g(t_1) - g(t)| = -\left|\int_t^{t_1} g^\Delta(s)\Delta s\right| \geq - \int_t^{t_1} |g^\Delta(s)|\Delta s\leq - \int_\kappa^{\delta_+(T,\kappa)} |g^\Delta(s)|\Delta s,$$

that gives $g(t)\leq g(t_1) + \int_\kappa^{\delta_+(T,\kappa)} |g^\Delta(s)|\Delta s$.

The proof is complete. □

Remark 2. [14] *Consider the following equation:*

$$\begin{aligned} \tilde{x}'(t) &= a(t)\tilde{x}(t) - b(t)\tilde{x}^2(t) - \frac{c(t)\tilde{y}(t)\tilde{x}(t)}{\alpha(t) + \beta(t)\tilde{x}(t) + m(t)\tilde{y}(t)}, \\ \tilde{y}'(t) &= -d(t)\tilde{y}(t) + \frac{f(t)\tilde{x}(t)\tilde{y}(t)}{\alpha(t) + \beta(t)\tilde{x}(t) + m(t)\tilde{y}(t)}. \end{aligned} \tag{2.2}$$

This is the predator–prey dynamic system that is obtained from ordinary differential equations. Let $\mathbb{T} = \mathbb{R}$. *In* (2.1), *by taking* $exp\,(x(t)) = \tilde{x}(t)$ *and* $exp\,(y(t)) = \tilde{y}(t)$, *we obtain the equality* (2.2), *which is the standard predator–prey system with Beddington-DeAngelis functional response.*

Let $\mathbb{T} = \mathbb{Z}$. *By using equality* (2.1), *we obtain*

$$x(t+1)-x(t)=a(t)-b(t)\exp(x(t))-\frac{c(t)\exp(y(t))}{\alpha(t)+\beta(t)\exp(x(t))+m(t)\exp(y(t))},$$
$$y(t+1)-y(t)=-d(t)+\frac{f(t)\exp(x(t))}{\alpha(t)+\beta(t)\exp(x(t))+m(t)\exp(y(t))}$$

Here, again by taking $\exp(x(t))=\tilde{x}(t)$ *and* $\exp(y(t))=\tilde{y}(t)$, *we obtain*

$$\begin{aligned}\tilde{x}(t+1)&=\tilde{x}(t)\exp\left[a(t)-b(t)\tilde{x}(t)-\frac{c(t)\tilde{y}(t)}{\alpha(t)+\beta(t)\tilde{x}(t)+m(t)\tilde{y}(t)}\right],\\ \tilde{y}(t+1)&=\tilde{y}(t)\exp\left[-d(t)+\frac{f(t)\tilde{x}(t)}{\alpha(t)+\beta(t)\tilde{x}(t)+m(t)\tilde{y}(t)}\right],\end{aligned} \tag{2.3}$$

which is the discrete time predator–prey system with Beddington-DeAngelis-type functional response and also the discrete analogue of Eq. (2.2). *This system was studied in* [25, 26]. *Since Eq.* (2.1) *incorporates Eqs.* (2.2) and (2.3) *as special cases, we call Eq.* (2.1) *the predator–prey dynamic system with Beddington-DeAngelis functional response on time scales.*

For Eq. (2.1), $\exp(x(t))$ *and* $\exp(y(t))$ *denote the density of prey and the predator. Therefore,* $x(t)$ *and* $y(t)$ *could be negative. By taking the exponential of* $x(t)$ *and* $y(t)$, *we obtain the number of preys and predators that are living per unit of an area. In other words, for the general time scale case, our equation is based on the natural logarithm of the density of the predator and prey. Hence,* $x(t)$ *and* $y(t)$ *could be negative.*

For Eqs. (2.2) and (2.3), *since exp*$(x(t))=\tilde{x}(t)$ *and exp*$(y(t))=\tilde{y}(t)$, *the given dynamic systems directly depend on the density of the prey and predator.*

3. Application of $\delta_{\pm}$-periodicity of Q-calculus

The following theorem is the modified version of Theorem 8 from [24].

Theorem 5. *Assume that for the given time scale* $\mathbb{T}=\{0\}\cup q^{\mathbb{Z}}$, *while* $T\in q^{\mathbb{Z}}$, *mes*$(\delta_+(T,t))$ *is equal for each* $t\in\mathbb{T}$. *In addition to conditions on coefficient functions and*

Lemma 1 if $\int_{\kappa}^{\delta_+(T,\kappa)}a(t)\Delta t-\int_{\kappa}^{\delta_+(T,\kappa)}\frac{c(t)}{m(t)}\Delta t>0$ *and*

$$\left(\frac{\int_{\kappa}^{\delta_+(T,\kappa)}a(t)\Delta t-\int_{\kappa}^{\delta_+(T,\kappa)}\dfrac{c(t)}{m(t)}\Delta t}{\int_{\kappa}^{\delta_+(T,\kappa)}b(t)\Delta t}\right)exp\left[-\left(\int_{\kappa}^{\delta_+(T,\kappa)}|a(t)|\Delta t+\int_{\kappa}^{\delta_+(T,\kappa)}a(t)\Delta t\right)\right]$$
$$\cdot\int_{\kappa}^{\delta_+(T,\kappa)}f(t)\Delta t-\beta^u\left(\int_{\kappa}^{\delta_+(T,\kappa)}d(t)\Delta t\right)-\alpha^u\left(\int_{\kappa}^{\delta_+(T,\kappa)}d(t)\right)\Delta t>0$$

are satisfied, then there exist at least one $\delta_{\pm}$-periodic solution.

Proof. $X{:=}\left\{\begin{bmatrix} u \\ v \end{bmatrix} \in C_{rd}\left(\{0\}\cup q^{\mathbb{Z}}, \mathbb{R}^2\right) : u(\delta_{\pm}(T,t)) = u(t), v(\delta_{\pm}(T,t)) = v(t)\right\}$ with the norm:

$$\left\| \begin{bmatrix} u \\ v \end{bmatrix} \right\| = \max_{t\in[t_0,\delta_+(T,t_0)]_{\mathbb{T}}}(|u(t)|, |v(t)|)$$

$Y{:=}\left\{\begin{bmatrix} u \\ v \end{bmatrix} \in C_{rd}\left(\{0\}\cup q^{\mathbb{Z}}, \mathbb{R}^2\right) : u(\delta_{\pm}(T,t)) = u(t), v(\delta_{\pm}(T,t)) = v(t)\right\}$ with the norm:

$$\left\| \begin{bmatrix} u \\ v \end{bmatrix} \right\| = \max_{t\in[t_0,\delta_+(T,t_0)]_{\mathbb{T}}}(|u(t)|, |v(t)|)$$

Let us define the mappings L and C by $L : DomL \subset X \to Y$ such that

$$L\left(\begin{bmatrix} u \\ v \end{bmatrix}\right) = \begin{bmatrix} u^{\Delta} \\ v^{\Delta} \end{bmatrix}$$

and $C : X \to Y$ such that

$$C\left(\begin{bmatrix} u \\ v \end{bmatrix}\right) = \begin{bmatrix} a(t) - b(t)\,exp\,(u(t)) - \dfrac{c(t)\,exp\,(v(t))}{\alpha(t) + \beta(t)\,exp\,(u(t)) + m(t)\,exp\,(v(t))} \\ -d(t) + \dfrac{f(t)\,exp\,(u(t))}{\alpha(t) + \beta(t)\,exp\,(u(t)) + m(t)\,exp\,(v(t))} \end{bmatrix}$$

Then, $KerL = \left\{\begin{bmatrix} u \\ v \end{bmatrix} : \begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}\right\}$, c_1 and c_2 are constants.

$$ImL = \left\{\begin{bmatrix} u \\ v \end{bmatrix} : \begin{bmatrix} \int_{\kappa}^{\delta_+(T,\kappa)} u(t)\Delta t \\ \int_{\kappa}^{\delta_+(T,\kappa)} v(t)\Delta t \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}\right\}.$$

ImL is closed in Y. Its obvious that $dimKerL = 2$. To show $dimKerL = codimImL = 2$, we have to prove that $KerL \oplus ImL = Y$. It is obvious that when we take an element from Ker L, an element from Im L, we find an element of Y by summing these two elements. If we take an element $\begin{bmatrix} u \\ v \end{bmatrix} \in Y,$ and WLOG taking $u(t)$, we have $\int_{\kappa}^{\delta_+(T,\kappa)} u(t)\Delta t = I$ where I is a constant. Let us define a new function $g = u - \frac{I}{mes(\delta_+(T,\kappa))}$. Since $\frac{I}{mes(\delta_+(T,\kappa))}$ is constant by Lemma 1, if we take the integral of g from κ to $\delta_+(T,\kappa),$ we get

$$\int_{\kappa}^{\delta_+(T,\kappa)} g(t)\Delta t = \int_{\kappa}^{\delta_+(T,\kappa)} u(t)\Delta t - I = 0.$$

Similar steps are used for v. $\begin{bmatrix} u \\ v \end{bmatrix} \in Y$ can be written as the summation of an element from Im L and an element from Ker L. Also, it is easy to show that any element in Y is uniquely expressed as the summation of an element Ker L and an element from Im L. So, *codimImL* is also 2, we get the desired result. Hence, L is a Fredholm mapping of index zero. There exist continuous projectors $U : X \to X$ and $V : Y \to Y$ such that

$$U\left(\begin{bmatrix} u \\ v \end{bmatrix}\right) = \frac{1}{mes(\delta_+(T,\kappa))}\begin{bmatrix} \int_{\kappa}^{\delta_+(T,\kappa)} u(t)\Delta t \\ \int_{\kappa}^{\delta_+(T,\kappa)} v(t)\Delta t \end{bmatrix}$$

and

$$V\left(\begin{bmatrix} u \\ v \end{bmatrix}\right) = \frac{1}{mes(\delta_+(T,\kappa))}\left(\begin{bmatrix} \int_{\kappa}^{\delta_+(T,\kappa)} u(t)\Delta t \\ \int_{\kappa}^{\delta_+(T,\kappa)} v(t)\Delta t \end{bmatrix}\right).$$

The generalized inverse $K_U = ImL \to DomL \cap KerU$ is given:

$$K_U\left(\begin{bmatrix} u \\ v \end{bmatrix}\right) = \begin{bmatrix} \int_{\kappa}^{t} u(s)\Delta s - \frac{1}{mes(\delta_+(T,\kappa))}\int_{\kappa}^{\delta_+(T,\kappa)}\int_{\kappa}^{t} u(s)\Delta s \\ \int_{\kappa}^{t} v(s)\Delta s - \frac{1}{mes(\delta_+(T,\kappa))}\int_{\kappa}^{\delta_+(T,\kappa)}\int_{\kappa}^{t} v(s)\Delta s \end{bmatrix}.$$

$$VC\left(\begin{bmatrix} u \\ v \end{bmatrix}\right) =$$

$$\frac{1}{mes(\delta_+(T,\kappa))}\left(\begin{bmatrix} \int_{\kappa}^{\delta_+(T,\kappa)} a(s) - b(s)\,exp\,(u(s)) - \frac{c(s)\,exp\,(v(s))}{\alpha(s) + \beta(s)\,exp\,(u(s)) + m(s)\,exp\,(v(s))}\Delta s \\ \int_{\kappa}^{\delta_+(T,\kappa)} -d(s) + \frac{f(s)\,exp\,(u(s))}{\alpha(s) + \beta(s)\,exp\,(u(s)) + m(s)\,exp\,(v(s))}\Delta s \end{bmatrix}\right)$$

Let

$$a(t) - b(t)\,exp\,(u(t)) - \frac{c(t)\,exp\,(v(t))}{\alpha(t) + \beta(t)\,exp\,(u(t)) + m(t)\,exp\,(v(t))} = C_1$$

$$-d(t) + \frac{f(t)\,exp\,(u(t))}{\alpha(t) + \beta(t)\,exp\,(u(t)) + m(t)\,exp\,(v(t))} = C_2$$

$$\frac{1}{mes(\delta_+(T,\kappa))}\int_{\kappa}^{\delta_+(T,\kappa)} a(s) - b(s)\,exp\,(u(s)) - \frac{c(s)\,exp\,(v(s))}{\alpha(s) + \beta(s)\,exp\,(u(s)) + m(s)\,exp\,(v(s))}\Delta s = \overline{C}_1$$

and

$$\frac{1}{mes(\delta_+(T,\kappa))}\int_\kappa^{\delta_+(T,\kappa)} -d(s)+\frac{f(s)\,exp\,(u(s))}{\alpha(s)+\beta(s)\,exp\,(u(s))+m(s)\,exp\,(v(s))}\Delta s=\overline{C}_2$$

$$K_U(I-V)C\left(\begin{bmatrix} u \\ v \end{bmatrix}\right)=K_U\left(\begin{bmatrix} C_1-\overline{C}_1 \\ C_2-\overline{C}_2 \end{bmatrix}\right)$$
$$=\begin{bmatrix} \int_\kappa^t C_1(s)-\overline{C}_1(s)\Delta s-\dfrac{1}{mes(\delta_+(T,\kappa))}\displaystyle\int_\kappa^{\delta_+(T,\kappa)}\int_\kappa^t C_1(s)-\overline{C}_1(s)\Delta s \\ \int_\kappa^t C_2(s)-\overline{C}_2(s)\Delta s-\dfrac{1}{mes(\delta_+(T,\kappa))}\displaystyle\int_\kappa^{\delta_+(T,\kappa)}\int_\kappa^t C_2(s)-\overline{C}_2(s)\Delta s \end{bmatrix}.$$

Clearly, VC and $K_U(I-V)C$ are continuous. Here, X and Y are Banach spaces. Since for the given time scale $\mathbb{T}$ while T is constant, $mes(\delta_+(T,t))$ is equal for each $t\in\mathbb{T}$; then, we can apply Arzela-Ascoli theorem, and by using Arzela-Ascoli theorem, we can find that $\overline{K_U(I-V)C(\overline{\Omega})}$ is compact for any open bounded set $\Omega\subset X$. Additionally, $VC(\overline{\Omega})$ is bounded. Thus, C is L-compact on $\overline{\Omega}$ with any open bounded set $\Omega\subset X$.

To apply the continuation theorem, we investigate the below operator equation:

$$\begin{aligned} x^\Delta(t)&=\lambda\left[a(t)-b(t)\,exp\,(x(t))-\frac{c(t)\,exp\,(y(t))}{\alpha(t)+\beta(t)\,exp\,(x(t))+m(t)\,exp\,(y(t))}\right] \\ y^\Delta(t)&=\lambda\left[-d(t)+\frac{f(t)\,exp\,(x(t))}{\alpha(t)+\beta(t)\,exp\,(x(t))+m(t)\,exp\,(y(t))}\right] \end{aligned}\tag{3.1}$$

Let $\begin{bmatrix} x \\ y \end{bmatrix}\in X$ be any solution of system (3.1). Integrating both sides of system (3.1) over the interval $[0,w]$, we obtain

$$\begin{cases} \int_\kappa^{\delta_+(T,\kappa)} a(t)\Delta t=\int_\kappa^{\delta_+(T,\kappa)} b(t)\,exp\,(x(t))+\dfrac{c(t)\,exp\,(y(t))}{\alpha(t)+\beta(t)\,exp\,(x(t))+m(t)\,exp\,(y(t))}\Delta t & , \\ \int_\kappa^{\delta_+(T,\kappa)} d(t)\Delta t=\int_\kappa^{\delta_+(T,\kappa)} \dfrac{f(t)\,exp\,(x(t))}{\alpha(t)+\beta(t)\,exp\,(x(t))+m(t)\,exp\,(y(t))}\Delta t & , \end{cases}\tag{3.2}$$

From (3.1) and (3.2), we get

$$\begin{aligned} \int_\kappa^{\delta_+(T,\kappa)} |x^\Delta(t)|\Delta t &\leq \lambda\left[\int_\kappa^{\delta_+(T,\kappa)} |a(t)|\Delta t+\int_\kappa^{\delta_+(T,\kappa)} b(t)\,exp\,(x(t))+\frac{c(t)\,exp\,(y(t))}{\alpha(t)+\beta(t)\,exp\,(x(t))+m(t)\,exp\,(y(t))}\Delta t\right], \\ &\leq \lambda\left[\int_\kappa^{\delta_+(T,\kappa)} |a(t)|\Delta t+\int_\kappa^{\delta_+(T,\kappa)} a(t)\Delta t\right] \\ &\leq \int_\kappa^{\delta_+(T,\kappa)} |a(t)|\Delta t+\int_\kappa^{\delta_+(T,\kappa)} a(t)\Delta t:=M_1 \end{aligned}\tag{3.3}$$

$$\begin{aligned} \int_\kappa^{\delta_+(T,\kappa)} |y^\Delta(t)|\Delta t &\leq \lambda\left[\int_\kappa^{\delta_+(T,\kappa)} |d(t)|\Delta t+\int_\kappa^{\delta_+(T,\kappa)} \frac{f(t)\,exp\,(x(t))}{\alpha(t)+\beta(t)\,exp\,(x(t))+m(t)\,exp\,(y(t))}\Delta t\right] \\ &\leq \lambda\left[\int_\kappa^{\delta_+(T,\kappa)} |d(t)|\Delta t+\int_\kappa^{\delta_+(T,\kappa)} d(t)\Delta t\right] \\ &\leq \int_\kappa^{\delta_+(T,\kappa)} |d(t)|\Delta t+\int_\kappa^{\delta_+(T,\kappa)} d(t)\Delta t:=M_2 \end{aligned}\tag{3.4}$$

Since $\begin{bmatrix} x \\ y \end{bmatrix} \in X$, then there exist η_i, ξ_i and $i = 1, 2$ such that

$$\begin{aligned} &x(\xi_1) = \min_{t\in t\in[\kappa,\delta_+(T,\kappa)]} x(t), x(\eta_1) = \max_{t\in t\in[\kappa,\delta_+(T,\kappa)]} x(t), \\ &y(\xi_2) = \min_{t\in t\in[\kappa,\delta_+(T,\kappa)]} y(t), y(\eta_2) = \max_{t\in t\in[\kappa,\delta_+(T,\kappa)]} y(t) \end{aligned} \tag{3.5}$$

If ξ_1 is the minimum point of $x(t)$ on the interval $[\kappa, \delta_+(T,\kappa)]$ because $x(t)$ is a function that is periodic in shifts for any $n\in\mathbb{N}$ on the interval $\left[\delta_+^n(T,\kappa_1), \delta_+^{n+1}(T,\kappa_1)\right]$, the minimum point of $x(t)$ is $\delta_+^n(T,\xi_1)$ and $x(\xi_1) = x\left(\delta_+^n(T,\xi_1)\right)$. We have similar results for the other points for ξ_2, η_1, and η_2.

By the first equation of systems (3.2) and (3.5)

$$\begin{aligned} \int_\kappa^{\delta_+(T,\kappa)} a(t)\Delta t &\le \int_\kappa^{\delta_+(T,\kappa)} \left[b(t)\, exp\left(x(\eta_1)\right) + \frac{c(t)}{m(t)}\Delta t\right] \\ &= exp\left(x(\eta_1)\right) \int_\kappa^{\delta_+(T,\kappa)} b(t)\Delta t + \int_\kappa^{\delta_+(T,\kappa)} \frac{c(t)}{m(t)}\Delta t. \end{aligned}$$

Since $\int_\kappa^{\delta_+(T,\kappa)} b(t)\Delta t > 0$, so we get

$$x(\eta_1) \ge \ln\left(\frac{\int_\kappa^{\delta_+(T,\kappa)} a(t)\Delta t - \int_\kappa^{\delta_+(T,\kappa)} \frac{c(t)}{m(t)}\Delta t}{\int_\kappa^{\delta_+(T,\kappa)} b(t)\Delta t}\right) := l_1$$

Using the second inequality in Lemma 2, we have

$$\begin{aligned} x(t) &\ge x(\eta_1) - \int_\kappa^{\delta_+(T,\kappa)} |x^\Delta(t)|\Delta t \\ &\ge x(\eta_1) - \left(\int_\kappa^{\delta_+(T,\kappa)} |a(t)|\Delta t + \int_\kappa^{\delta_+(T,\kappa)} a(t)\Delta t\right) \\ &= l_1 - M_1 := H_1 \end{aligned} \tag{3.6}$$

By the first equation of systems (3.2) and (3.5)

$$\begin{aligned} \int_\kappa^{\delta_+(T,\kappa)} a(t)\Delta t &\ge \int_\kappa^{\delta_+(T,\kappa)} b(t)\, exp\left(x(\xi_1)\right)\Delta t \\ &= exp\left(x(\xi_1)\right) \int_\kappa^{\delta_+(T,\kappa)} b(t)\Delta t. \end{aligned}$$

Then, we get

$$x(\xi_1) \le \ln\left(\frac{\int_\kappa^{\delta_+(T,\kappa)} a(t)\Delta t}{\int_\kappa^{\delta_+(T,\kappa)} b(t)\Delta t}\right) := l_2$$

Using the first inequality in Lemma 2, we have

$$\begin{aligned} x(t) &\leq x(\xi_1) + \int_{\kappa}^{\delta_+(T,\kappa)} |x^{\Delta}(t)|\Delta t \\ &\leq x(\xi_1) + \left(\int_{\kappa}^{\delta_+(T,\kappa)} |a(t)|\Delta t + \int_{\kappa}^{\delta_+(T,\kappa)} a(t)\Delta t\right) \\ &= l_2 + M_1 := H_2 \end{aligned} \tag{3.7}$$

By Eq. (3.6) and (3.7), $\max_{t\in[\kappa,\delta_+(T,\kappa)]}|x(t)| \leq \max\{|H_1|, |H_2|\} := B_1$. From the second equation of system (3.2) and the second equation of system (3.6), we can derive that

$$\begin{aligned} \int_{\kappa}^{\delta_+(T,\kappa)} d(t)\Delta t &\leq \int_{\kappa}^{\delta_+(T,\kappa)} \frac{f(t)\, exp\,(x(t))}{\beta^l\, exp\,(x(t)) + m^l\, exp\,(y(t))}\Delta t \\ &\leq \int_{\kappa}^{\delta_+(T,\kappa)} \frac{f(t)e^{H_2}}{\beta^l e^{H_2} + m^l\, exp\,(y(\xi_2))}\Delta t \\ &= \frac{e^{H_2}}{\beta^l e^{H_2} + m^l\, exp\,(y(\xi_2))}\int_{\kappa}^{\delta_+(T,\kappa)} f(t)\Delta t. \end{aligned}$$

Therefore,

$$exp\,(y(\xi_2)) \leq \frac{1}{m^l}\left(\frac{e^{H_2}\int_{\kappa}^{\delta_+(T,\kappa)} f(t)\Delta t}{\int_{\kappa}^{\delta_+(T,\kappa)} d(t)\Delta t} - \beta^l e^{H_2}\right)$$

By the assumption of the Theorem 5, we get,

$$\int_{\kappa}^{\delta_+(T,\kappa)} f(t)\Delta t - \beta^l\left(\int_{\kappa}^{\delta_+(T,\kappa)} d(t)\right)\Delta t > 0 \text{ and}$$

$$y(\xi_2) \leq \ln\left(\frac{1}{m^l}\left(\frac{e^{H_2}\int_{\kappa}^{\delta_+(T,\kappa)} f(t)\Delta t}{\int_{\kappa}^{\delta_+(T,\kappa)} d(t)\Delta t} - \beta^l e^{H_2}\right)\right) := L_1$$

Hence, by using the first inequality in Lemma 2 and the second equation of system (3.2)

$$\begin{aligned} y(t) &\leq y(\xi_2) + \int_{\kappa}^{\delta_+(T,\kappa)} |y^{\Delta}(t)|\Delta t \\ &\leq y(\xi_2) + \left(\int_{\kappa}^{\delta_+(T,\kappa)} |d(t)|\Delta t + \int_{\kappa}^{\delta_+(T,\kappa)} d(t)\Delta t\right) \\ &\leq L_1 + M_2 := H_3. \end{aligned} \tag{3.8}$$

Again, using the second equation of system (3.2), we obtain

$$\begin{aligned} \int_{\kappa}^{\delta_+(T,\kappa)} d(t)\Delta t &\geq \int_{\kappa}^{\delta_+(T,\kappa)} \frac{f(t)\, exp\,(x(t))}{\alpha^u + \beta^u\, exp\,(x(t)) + m^u\, exp\,(y(t))}\Delta t \\ &\geq \int_{\kappa}^{\delta_+(T,\kappa)} \frac{f(t)e^{H_1}}{\alpha^u + \beta^u e^{H_1} + m^u\, exp\,(y(\eta_2))}\Delta t \\ &= \frac{e^{H_1}}{\alpha^u + \beta^u e^{H_1} + m^u\, exp\,(y(\eta_2))}\int_{\kappa}^{\delta_+(T,\kappa)} f(t)\Delta t, \end{aligned}$$

$$exp\left(y(\eta_2)\right) \geq \frac{1}{m^u}\left(\frac{e^{H_1}\int_{\kappa}^{\delta_+(T,\kappa)} f(t)\Delta t}{\int_{\kappa}^{\delta_+(T,\kappa)} d(t)\Delta t} - \beta^u e^{H_1} - \alpha^u\right).$$

Using the assumption of the Theorem 5, we obtain

$$e^{H_1}\left(\int_{\kappa}^{\delta_+(T,\kappa)} f(t)\Delta t - \beta^u\left(\int_{\kappa}^{\delta_+(T,\kappa)} d(t)\Delta t\right)\right) - \alpha^u\left(\int_{\kappa}^{\delta_+(T,\kappa)} d(t)\Delta t\right) > 0$$

and

$$y(\eta_2) \geq \ln\left(\frac{1}{m^u}\left(\frac{e^{H_1}\int_{\kappa}^{\delta_+(T,\kappa)} f(t)\Delta t}{\int_{\kappa}^{\delta_+(T,\kappa)} d(t)\Delta t} - \beta^u e^{H_1} - \alpha^u\right)\right) := L_2.$$

By using the second inequality in Lemma 2

$$\begin{aligned} y(t) &\geq y(\eta_2) - \int_{\kappa}^{\delta_+(T,\kappa)} |y^{\Delta}(t)|\Delta t \\ &\geq y(\eta_2) - \left(\int_{\kappa}^{\delta_+(T,\kappa)} |d(t)|\Delta t + \int_{\kappa}^{\delta_+(T,\kappa)} d(t)\Delta t\right) \\ &= L_2 - M_2 := H_4. \end{aligned} \tag{3.9}$$

By Eq. (3.8) and (3.9), we have $\max_{t\in[t_0,\delta_+(T,t_0)]}|y(t)| \leq \max\{|H_3|, |H_4|\} := B_2$. Obviously, B_1 and B_2 are both independent of λ. Let $M = B_1 + B_2 + 1$. Then, $\max_{t\in[t_0,\delta_+(T,t_0)]}\left\|\begin{bmatrix} x \\ y \end{bmatrix}\right\| < M$. Let $\Omega = \left\{\left\|\begin{bmatrix} x \\ y \end{bmatrix}\right\| \in X : \left\|\begin{bmatrix} x \\ y \end{bmatrix}\right\| < M\right\}$; then, Ω verifies the requirement (a) in Theorem 4. When $\begin{bmatrix} x \\ y \end{bmatrix} \in KerL \cap \partial\Omega$, $\begin{bmatrix} x \\ y \end{bmatrix}$ is a constant with $\left\|\begin{bmatrix} x \\ y \end{bmatrix}\right\| = M,$; then,

$$\begin{aligned} VC\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) &= \left(\begin{bmatrix} \int_{\kappa}^{\delta_+(T,\kappa)} a(s) - b(s)\,exp\,(x) - \dfrac{c(s)\,exp\,(y)}{\alpha(s) + \beta(s)\,exp\,(x) + m(s)\,exp\,(y)}\Delta t \\ \int_{\kappa}^{\delta_+(T,\kappa)} -d(s) + \dfrac{f(s)\,exp\,(x)}{\alpha(s) + \beta(s)\,exp\,(x) + m(s)\,exp\,(y)}\Delta t \end{bmatrix}\right) \\ &\neq \begin{bmatrix} 0 \\ 0 \end{bmatrix} \end{aligned}$$

$$JVC\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = VC\left(\begin{bmatrix} x \\ y \end{bmatrix}\right)$$

where $J : ImV \to KerL$ is the identity operator.

Let us define the homotopy such that $H_\nu = \nu(JVC) + (1-\nu)G$ where

$$G\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} \int_\kappa^{\delta_+(T,\kappa)} a(s) - b(s)\, exp\,(x)\Delta t \\ \int_\kappa^{\delta_+(T,\kappa)} d(s) - \dfrac{f(s)\, exp\,(x)}{\alpha(s) + \beta(s)\, exp\,(x) + m(s)\, exp\,(y)}\Delta t \end{bmatrix}$$

Take DJ_G as the determinant of the Jacobian of G. Since $\begin{bmatrix} x \\ y \end{bmatrix} \in KerL$, then Jacobian of G is

$$\begin{bmatrix} -e^x \int_\kappa^{\delta_+(T,\kappa)} b(s)\Delta t & 0 \\ \int_\kappa^{\delta_+(T,\kappa)} \dfrac{-e^x f(s)}{\alpha(s) + \beta(s)e^x + m(s)e^y}\Delta t + \displaystyle\int_\kappa^{\delta_+(T,\kappa)} \dfrac{(e^x)^2 f(s)\beta(s)}{\left(\alpha(s) + \beta(s)e^x + m(s)e^y\right)^2}\Delta t & -\int_\kappa^{\delta_+(T,\kappa)} \dfrac{e^x e^y f(s) m(s)}{\left(\alpha(s) + \beta(s)e^x + m(s)e^y\right)^2}\Delta t \end{bmatrix}$$

All the functions in Jacobian of G is positive; then, $signDJ_G$ is always positive. Hence,

$$\deg(JVC, \Omega \cap KerL, 0) = \deg(G, \Omega \cap KerL, 0) = \sum_{\begin{bmatrix} x \\ y \end{bmatrix} \in G^{-1}\left(\begin{bmatrix} 0 \\ 0 \end{bmatrix}\right)} signDJ_G\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) \neq 0.$$

Thus, all the conditions of Theorem 4 are satisfied. Therefore, system (2.1) has at least a positive $\delta\pm$-periodic solution. □

Example 1 *Let $\mathbb{T} = \{0\} \cup q^{\mathbb{Z}}$. $\delta_\pm(q, t)$ is the shift operator and $t_0 = 1$.*

$$\begin{aligned} x^\Delta(t) &= \left((-1)^{\frac{\ln|t|}{\ln(q)}} + 4\right) - \left((-1)^{\frac{\ln|t|}{\ln(q)}} + 0.5\right) exp\,(x(t)) - \frac{exp\,(y(t))}{exp\,(x(t)) + 2\,exp\,(y(t))}, \\ y^\Delta(t) &= -0.3 + \frac{\left((-1)^{\frac{\ln|t|}{\ln(q)}} + 7\right)\ exp\,(x(t))}{exp\,(x(t)) + 2\,exp\,(y(t))}, \end{aligned} \tag{3.10}$$

Each function in system (12) is $\delta_\pm\left(q^2, t\right)$ periodic and satisfies Theorem 1; then, the system has at least one $\delta_\pm\left(q^2, t\right)$ periodic solution. Here, $mes\left(\delta_+\left(q^2, t\right)\right) = 2$.

4. Conclusion

The important results of this study are:

1. The definition of $\delta_\pm$-periodicity notion is adapted to the quantum calculus.
2. The importance of time scale calculus is pointed out for the analysis of quantum calculus.
3. As an application, the $\delta_\pm$-periodicity notion for quantum calculus is used for the predator–prey dynamic system whose coefficient functions are $\delta_\pm$ periodic.

As a result, it is seen that one can define a periodicity notion that is applicable to the structure of the quantum calculus. Additionally, it is shown that this notion is useful for different applications. One of its applications is analyzed in this study with an example.

5. Discussion

There are many studies about the predator–prey dynamic systems on time scale calculus such as [14, 19, 27, 28]. All of these cited studies are about the periodic solutions of the considered system on a periodic time scale. However, in the world, there are many different species. While investigating the periodicity notion of the different life cycle of the species, the w-periodic time scales could be a little bit restricted. Therefore, if the life cycle of this kind of species is appropriate to the Beddington-DeAngelis functional response, then the results that we have found in that study are becoming more useful and important.

In addition to these, the $\delta_{\pm}$-periodic solutions for predator–prey dynamic systems with Holling-type functional response, semiratio-dependent functional response, and monotype functional response can be also taken into account for future studies. In that dynamic systems, delay conditions and impulsive conditions can also be added for the new investigations.

This is a joint work with Ayse Feza Guvenilir and Billur Kaymakcalan.

Acknowledgements

A major portion of the chapter is borrowed from the publication "Behavior of the solutions for predator-prey dynamic systems with Beddington-DeAngelis-type functional response on periodic time scales in shifts" [24].

Author details

Neslihan Nesliye Pelen*, Ayşe Feza Güvenilir and Billur Kaymakçalan

*Address all correspondence to: nesliyeaykir@gmail.com

Faculty of Science, Department of Mathematics, Ondokuz Mayis University, Samsun, Turkey

References

[1] Exton H. q-Hypergeometric Functions and Applications. New York: Halstead Press, Chichester: Ellis Horwood, 1983, ISBN0853124914, ISBN0470274530, ISBN9780470274538

[2] Kac V, Cheung P. Quantum Calculus. Springer Science and Business Media; 2001

[3] Jackson FH. On q-functions and a certain difference operator. Transactions of the Royal Society of Edinburgh. 1908;**46**:253-281

[4] Advar M. New periodicity concept for time scales. Mathematica Slovaca. 2013;**63**(4):817-828

[5] Lotka AJ. Contribution to the theory of periodic reaction. The Journal of Physical Chemistry. 1910;**14**(3):271274

[6] Goel NS et al. On the Volterra and Other Non-Linear Models of Interacting Populations. Academic Press Inc.; 1971

[7] Berryman AA. the origins and evolution of predator-prey theory. Ecology. 1992;**73**(5): 15301535

[8] Verhulst PH. Notice sur la loi que la population poursuit dans son accroissement. Correspondance mathématique et physique. 1838;**10**:113121

[9] Lotka AJ. Analytical note on certain rhythmic relations in organic systems. Proceedings of the National Academy of Sciences of the United States of America. 1920;**6**:410415

[10] Lotka AJ. Elements of Physical Biology. Williams and Wilkins; 1925

[11] Holling CS. The components of predation as revealed by a study of small mammal predation of the European Pine Sawfly. The Canadian Entomologist. 1959a;**91**:293320

[12] Holling CS. Some characteristics of simple types of predation and parasitism. The Canadian Entomologist. 1959b;**91**:385398

[13] Jost C, Devulder G, Vucetich JA, Peterson R, Arditi R. The wolves of Isle Royale display scale-invariant satiation and density dependent predation on moose. The Journal of Animal Ecology. 2005;**74**(5):809816

[14] Bohner M, Fan M, Zhang J. Existence of periodic solutions in predatorprey and competition dynamic systems. Nonlinear Analysis: RealWorld Applications. 2006;**7**:1193-1204

[15] Wang W, Shen J, Nieto J. Permanence and periodic solution of predator-prey system with holling type functional response and impulses. Discrete Dynamics in Nature and Society. 2007;**2007** Article ID 81756, 15 pages

[16] Xu R, Chaplain MAJ, Davidson FA. Periodic solutions for a predatorprey model with Holling-type functional response and time delays. Applied Mathematics and Computation. 2005;**161**(2):637654

[17] Fan M, Agarwal S. Periodic solutions for a class of discrete time competition systems. Nonlinear Studies. 2002;**9**(3):249261

[18] Fan M, Wang K. Periodicity in a delayed ratio-dependent predatorprey system. Journal of Mathematical Analysis and Applications. 2001;**262**(1):179190

[19] Fan M, Wang Q. Periodic solutions of a class of nonautonomous discrete time semi-ratio-dependent predatorprey systems. Discrete and Continuous Dynamical Systems. Series B. 2004;**4**(3):563574

[20] Huo HF. Periodic solutions for a semi-ratio-dependent predatorprey system with functional responses. Applied Mathematics Letters. 2005;**18**:313320

[21] Wang Q, Fan M, Wang K. Dynamics of a class of nonautonomous semi-ratio-dependent predatorprey systems with functional responses. Journal of Mathematical Analysis and Applications. 2003;**278**(2):443471

[22] Hilger S. Analysis on measure chains–A unified approach to continuous and discrete calculus. Results in Mathematics. 1990;**18**:1856

[23] Bohner M, Peterson A. Advances in Dynamic Equations on Time Scales. Boston, MA: Birkhäuser Boston; 2003

[24] Pelen NN, Güvenilir AF, Kaymakalan B. Behavior of the Solutions for Predator-prey Dynamic Systems with Beddington-DeAngelis Type Functional Response on Periodic Time Scales in Shifts. Abstract and Applied Analysis (Vol. 2016). Hindawi Publishing Corporation

[25] Xu C, Liao M. Existence of periodic solutions in a discrete predator-prey system with Beddington-DeAngelis functional responses. International Journal of Mathematics and Mathematical Sciences. 2011, Article ID 970763:18 pages

[26] Zhang J, Wang J. Periodic solutions for discrete predator-prey systems with the Beddington-DeAngelis functional response. Applied Mathematics Letters. 2006;**19**:13611366

[27] Güvenilir AF, Kaymakçalan B, Pelen NN. Impulsive predator-prey dynamic systems with Beddington-DeAngelis type functional response on the unification of discrete and continuous systems. Applied Mathematics. 2015;**6**(09):1649

[28] Liu X, Liu X. Necessary and sufficient conditions for the existence of periodic solutions in a predator-prey model on time scales, Electronic Journal of Differential Equations. 2012; **2012**(199):113. ISSN: 1072-6691

Edited by Sergiy Gnatyuk

This book explores both the state of the art and the latest developments in QKD. It describes the fundamental concepts and practical aspects of QKD from a viewpoint of information security and quantum channel efficiency improvement. The purpose of this book is to extend and update the knowledge of the readers in the dynamically changing field of QKD. The authors attempt to present in detail their results of scientific research, which is divided into two sections—Modern QKD Technologies and Quantum Channel Construction. It will be useful for researchers, engineers, graduates, and doctoral students working in quantum cryptography and information security–related areas.

Published in London, UK

IntechOpen

ISBN 978-1-83881-243-0

9 781838 812430