

ctive . modifier\_ob  
fier\_ob))

\$.new("w) 00" e(r, 1", x)st 00

**IntechOpen**

# Cryptography

## Recent Advances and Future Developments

*Edited by Riccardo Bernardini*





---

# Cryptography - Recent Advances and Future Developments

*Edited by Riccardo Bernardini*

Published in London, United Kingdom

---



## IntechOpen





*Supporting open minds since 2005*



Cryptography - Recent Advances and Future Developments

<http://dx.doi.org/10.5772/intechopen.87684>

Edited by Riccardo Bernardini

#### Contributors

Smitha Sasi, Bharadwaja V. Srividya, Adarsh Kumar, Deepak Kumar Sharma, Ferucio Laurentiu Tiplea, Cristian Andriesei, Cristian Hristea, Menachem Domb, Ahmed Drissi, Orhun Kara, Amal Hafsa, Mohamed Gafsi, Jihene Malek, Mohsen Machhout

© The Editor(s) and the Author(s) 2021

The rights of the editor(s) and the author(s) have been asserted in accordance with the Copyright, Designs and Patents Act 1988. All rights to the book as a whole are reserved by INTECHOPEN LIMITED. The book as a whole (compilation) cannot be reproduced, distributed or used for commercial or non-commercial purposes without INTECHOPEN LIMITED's written permission. Enquiries concerning the use of the book should be directed to INTECHOPEN LIMITED rights and permissions department ([permissions@intechopen.com](mailto:permissions@intechopen.com)).

Violations are liable to prosecution under the governing Copyright Law.



Individual chapters of this publication are distributed under the terms of the Creative Commons Attribution 3.0 Unported License which permits commercial use, distribution and reproduction of the individual chapters, provided the original author(s) and source publication are appropriately acknowledged. If so indicated, certain images may not be included under the Creative Commons license. In such cases users will need to obtain permission from the license holder to reproduce the material. More details and guidelines concerning content reuse and adaptation can be found at <http://www.intechopen.com/copyright-policy.html>.

#### 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, 2021 by IntechOpen

IntechOpen is the global imprint of INTECHOPEN LIMITED, registered in England and Wales, registration number: 11086078, 5 Princes Gate Court, London, SW7 2QJ, 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](mailto:orders@intechopen.com)

Cryptography - Recent Advances and Future Developments

Edited by Riccardo Bernardini

p. cm.

Print ISBN 978-1-83962-565-7

Online ISBN 978-1-83962-566-4

eBook (PDF) ISBN 978-1-83962-588-6

# We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

5,400+

Open access books available

132,000+

International authors and editors

160M+

Downloads

156

Countries delivered to

Our authors are among the  
Top 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index  
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?  
Contact [book.department@intechopen.com](mailto:book.department@intechopen.com)

Numbers displayed above are based on latest data collected.  
For more information visit [www.intechopen.com](http://www.intechopen.com)







# Meet the editor



Riccardo Bernardini graduated in Electrical Engineering from the University of Padova, Italy, in 1990. He spent the last year of his Ph.D. at the former AT&T Bell Labs (Murray Hill). After a postdoc period at the Ecole Polytechnique Federale de Lausanne (EPFL), he joined the University of Udine, Italy, as a professor. His research interests are diverse and include multidimensional signal processing, wavelets, filter banks, multimedia coding, robust transmission, bio-engineering, chaotic systems, P2P streaming, and some security-related areas such as random number generation, physical unclonable functions, and embedding random permutations on chips. He has been involved in many projects (both regional and national), sometimes as a partner and sometimes as principal investigator/coordinator.



# Contents

<b>Preface</b>	<b>XIII</b>
<b>Section 1</b> New Techniques	<b>1</b>
<b>Chapter 1</b> Hybrid Encryption Model Based on Advanced Encryption Standard and Elliptic Curve Pseudo Random <i>by Amal Hafsa, Mohamed Gafsi, Jihene Malek and Mohsen Machhout</i>	<b>3</b>
<b>Chapter 2</b> An Emphasis on Quantum Cryptography and Quantum Key Distribution <i>by Bharadwaja V. Srividya and Smitha Sasi</i>	<b>23</b>
<b>Chapter 3</b> Advancements in Optical Data Transmission and Security Systems <i>by Menachem Domb</i>	<b>41</b>
<b>Section 2</b> Security Analysis	<b>59</b>
<b>Chapter 4</b> Survey and Analysis of Lightweight Authentication Mechanisms <i>by Adarsh Kumar and Deepak Kumar Sharma</i>	<b>61</b>
<b>Chapter 5</b> Security and Privacy of PUF-Based RFID Systems <i>by Ferucio Laurențiu Țiplea, Cristian Andriesei and Cristian Hristea</i>	<b>85</b>
<b>Chapter 6</b> The Security of Cryptosystems Based on Error-Correcting Codes <i>by Ahmed Drissi</i>	<b>109</b>
<b>Chapter 7</b> Tradeoff Attacks on Symmetric Ciphers <i>by Orhun Kara</i>	<b>127</b>



# Preface

Cryptography is an ancient science. According to Svetonio, more than 2000 years ago Julius Caesar encrypted his messages by shifting the alphabet by three positions, using what is today known as the *Caesar cipher* (Mary Stuart also used it). After 2000 years, we know much more about cryptography and cryptanalysis, and no one would use the Caesar cipher anymore (although it experienced a rebirth with the ROT13 masking procedure in the Usenet newsgroup); much more secure and diverse algorithms have been designed. The cryptography toolbox nowadays includes not only encryption algorithms but also hash functions, signature protocols, zero-knowledge proofs, homomorphic encryption procedures, poker-by-phone protocols, and more.

Nevertheless, despite 2000 years of history, cryptography research is still very active, pursuing solutions to several interesting (and difficult) problems such as identity-based cryptography, fully (and practical) homomorphic encryption, physically unclonable functions (for hardware authentication), cryptography based on quantum mechanics (e.g., key distribution via entanglement), and cryptography robust against quantum computers.

Research in cryptography is expected to maintain its momentum in the future too, fueled by the still-increasing computational power and new needs like privacy and the Internet of Things (IoT).

This book is a snapshot of some recent results in this active field of research. It discusses quantum cryptography and quantum key distribution; lightweight protocols suited, for example, for the IoT; physical unclonable functions in the specific application of RFID systems; and security protocols based on optical approach.

Cryptography does not only study how to hide information but it also studies how to recover encrypted information. This is cryptanalysis, the other side of cryptography, which is as important as cryptography itself. This book gives space to cryptanalysis as well, analyzing the security of cryptosystems based on error correction codes, discussing tradeoff attacks for symmetric ciphers, and analyzing hybrid encryption models.

This book is not meant to be the final word on cryptography and cryptanalysis. It is designed to provide readers with useful tools and spark new research ideas

**Riccardo Bernardini**  
University of Udine – DPIA,  
Udine, Italy



---

Section 1

# New Techniques

---





# Hybrid Encryption Model Based on Advanced Encryption Standard and Elliptic Curve Pseudo Random

*Amal Hafsa, Mohamed Gafsi, Jihene Malek  
and Mohsen Machhout*

## Abstract

Securing multimedia applications becomes a major challenge with the violation of the information increasing currently. In this paper, a novel method for color image encryption is proposed. The procedure of encryption is performed using cooperation between Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES) with CTR (Counter) mode. In the cryptographic system, we have proposed to take advantage of the Elliptic Curve Random Generator to generate a sequence of arbitrary numbers based on the curve. The random generation step is founded on the public key sharing and a changing point  $G$ . Then, the AES-CTR is performed to these sequences using arbitrary keys for image encryption. The use of the AES alongside greatly distributed random results an interesting encryption method. Security analysis is successfully performed and our experiments prove that the suggested technique provides the basis of cryptography with more simplicity and correctness.

**Keywords:** hybrid scheme, AES, CTR ECC, random generator, image encryption

## 1. Introduction

Cryptography plays an important role to attain the privacy of images. There exist two main families of cryptographic algorithms. The asymmetric algorithm is inherently slow because of its associated hard calculations, while the symmetric algorithm shines with its rapidity. However, the latter suffers from a serious gap, the keys must be transmitted safely. To overcome these issues, we suggest an efficient version of AES-ECC hybrid encryption scheme which combines the benefits of the symmetric Advanced Encryption Standard (AES) and the asymmetric Elliptic Curve Cryptography (ECC). In [1], C. Junli et al propose an image encryption method using the AES-ECC hybrid cryptographic system. In that paper, the authors focus on the key sharing way. In fact, the AES key encryption is performed using ECC and the securing key is done by the digital signature of the ECC. Then, the AES is utilized for data encryption. An ameliorated version of this way is suggested in [2], an AES-ECC hybrid encryption system is developed for wireless sensor network. In this way, the AES Key is generated and encrypted by the ECC algorithm. After transmission, another pair of the ECC key (Key 2) is generated and ciphered using the symmetric algorithm. This token is transferred to the other part

and the encryption of the data input is performed using the Key 2. Therefore, the cipher ECC is achieved. Finally, the encryption of the cipher-ECC is performed using AES, and ciphertext output is obtained to be transferred via the network. The principle inconvenience of this paper is that the employ of the ECC asymmetric algorithm to encrypt all original text is highly time-consuming. Thus, the system is not efficacious in terms of using energy, particularly for weak sensors. Hajajneh et al. proposed in [3] a cryptographic system that secures multimedia application in FPGA. The goal of this work is to perform authentication and encryption using a Cipher Block Chaining Message Authentication code protocol (CCMP) and a counter (CTR) protocol. Though the results indicate an amelioration on the speed, the overall system risked to be attacked [3, 4] and these techniques do not furnish possibilities of enhancement. Attaya et al. [5] proposed the employ of a hybrid system that combines both chaos and AES algorithms. In the AES, both substitution box and Add-Round key are replaced by a chaos generator which leads to an increase in both diffusion and confusion and decreases the run time when compared with the standard. Yet encryption can outcome a feeble code when compared with the traditional AES since there is only one step that performs the entropy comparing with the different steps in the AES. Although the authors declare that the decryption process is impossible without the key [5]. In [6], K. Shankar et al. propose to encrypt images using an asymmetric encryption key. They utilized the genetic algorithm to get the ideal key. In this way, the ECC is utilized to encrypt all pixels one by one. Although, the employ of an asymmetric algorithm for every pixel and researching for the ideal keys are costly operations. In [7], A.A.A. El. Latif suggested an amalgamation between Elliptic Curve Cryptography (ECC) and a chaotic system. In that paper, authors utilized cyclic elliptic curves with LFSR (Linear Feedback Shift Register) and a chaos system for the keystream sequences generation. Then, image encryption is performed using the key streams. In [8], H. Liu et al. demonstrated that the previous model proposed in [7], is vulnerable to the chosen Plain text attacks. In order to dissolve this issue, they overcast the errors by using the Chirikov standard map [9] for the diffusion and the confusion of the image. Similarly, they employed a preceding stream of the encrypted images to encrypt the next stream. Although, some problems can be produced with the generated logic map because there exists a correlation between  $X_n$  values of the chaotic system.

The main contribution of our paper is to propound a way which is secure while addressing the issues of preceding works. In particular, a novel method for image encryption was suggested. The procedure of encryption is performed tacking benefits of Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES). The suggested technique utilizes the ECC as a random generator, where a sequence of random numbers is generated founded on Elliptic Curve parameters. Randoms are then employed to be as inputs for the key of the AES which generates the keystream for pixels encryption. The process of random number generation is founded on the NIST (National Institute of Sciences and Technology). Though the NIST way is employed extensively, it has some limitations. In this paper, the suggested random number generation addresses the limitation of this way employing a unique method of generating randoms by X and Y coordinates. Yet, using the Y coordinate, the entropy value of generated random numbers is improved. As known, no preceding works have used both coordinates (X and Y) for random number generation. In the following, proposed cryptographic algorithms are clearly explicated in Section 2. Section 3 details the suggested hybrid method for image encryption. Section 4 furnishes the experimental results followed by complete analysis over the propound technique. Finally, the last section concludes and recommends for future works.

## 2. Proposed cryptographic algorithms

A cryptographic function is founded on mathematical rulers. As well, a strong cryptographic algorithm requires an effective key that is large enough for the key space. The efficient key generation needs the right mathematical foundation. In this paper, the proposed technique utilized for the key generation is clearly explicated.

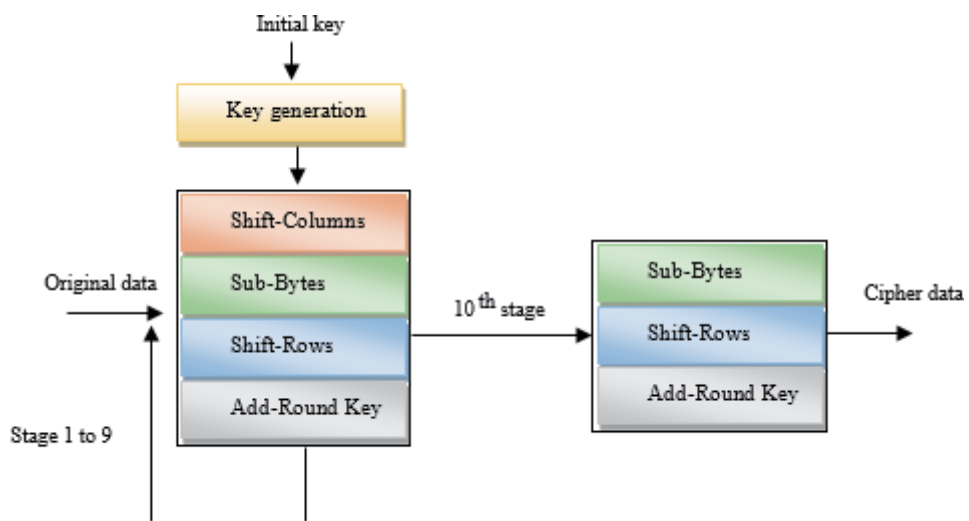
Nowadays, two fundamentals cryptographic systems are efficient and secure enough for image encryption:

- Advanced Encryption Standard (AES): It is characterized by its speed and its simplicity in implementation.
- Elliptic Curve Cryptography (ECC): Is characterized by its high security and its small key size to be employed in every system.

In this paper, by considering the advantages of both cryptosystems, a novel cooperative framework is proposed.

### 2.1 Advanced encryption standard (AES)

The Advanced Encryption Standard (AES) was firstly proposed in 2001. No successful attacks have been signaled on the AES. This latter involves key sizes and block sizes. The size of the information block is 128 bits, and the length of the key can be 128, 192, or 256 bits. In this work, the reduced processing time is needed. Then, a 128 bits key size is sufficient. For the encryption operation, round transformation is performed as a set of iterations, which includes the Sub-Bytes, Shift-Rows, Mix-Columns, and Add-Round key operations. For the Sub-Bytes operations, a Table S-box is utilized to substitute every block byte with a novel bloc. For the Shift-Rows, every row of the matrix is performed by a cyclic shift to the right according to its position. The mix-columns transformation consists of binary



**Figure 1.**  
*Flow design of AES algorithm.*

multiplying every element of the matrix state with polynomials from an auxiliary matrix. Finally, an exclusive OR between the round key and the matrix state is performed to obtain an intermediate matrix [10] (**Figure 1**).

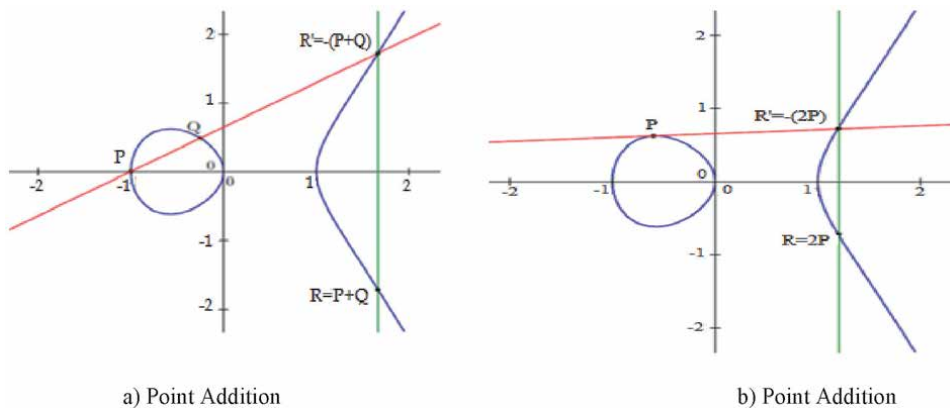
## 2.2 Elliptic curve cryptography (ECC)

In this section, an overview of the Elliptic Curve Cryptography (ECC) is given. Then the Montgomery scalar multiplication is used due to its resistance to side-channel attack.

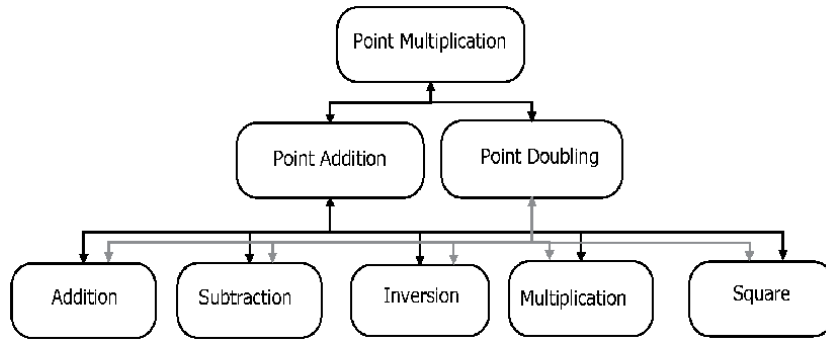
### 2.2.1 Overview

Cryptography based on elliptical curves (ECC) has enjoyed great interest since its introduction by Miller and Koblitz in 1987 [11, 12].

Cryptographic systems based on elliptical curves make it possible to gain efficiency in key management because of the small sizes of the keys used. In addition, the calculation algorithms linked to elliptical curves are faster, and therefore have a much higher key generation and exchange rate. Cryptographic systems based on elliptical curves are increasingly used in protocols using public key cryptography. Elliptic curves are used for encryption (ElGamal ECC), digital signatures (ECDSA), pseudo-random generators and other tasks. The Elliptic curve equation is of the form  $y^2 = x^3 + ax + b$ , the value of  $a$  and  $b$  is fixed and  $x, y$  belongs to finite field (prime or binary field). Encryption and decryption algorithms are based on point multiplications (usually referred to with  $kP$ , where  $k$  is the scalar). The base point  $P$  on which the point multiplication (a.k.a. scalar multiplication) is done is also fixed. All operations of ECC are done in the finite field (prime or binary field). Two basic operations over the curve are defined: The Point Addition and the Point Doubling. Point addition computes a third point on the curve taking two different input points, while Point Doubling computes a third point on the curve when the two inputs are the same Point as depicted in **Figure 2**. Both Point Addition and Point Doubling operations are built using modular arithmetic, where operations like addition, subtraction, multiplication, etc. are required. In **Figure 3**, the hierarchy of scalar multiplication is presented.



**Figure 2.**  
Point addition and point doubling operations.



**Figure 3.**  
 Hierarchy of scalar multiplication.

### 2.2.2 ECC montgomery scalar multiplication

Point Multiplication is the base of the ECC. It exists different algorithms to compute it. The Montgomery scalar multiplication, presented in Listing 1, is the most popular algorithm which is resistant against SCA (Side Channel Attacks) [13].

---

**Listing 1:** Montgomery Point multiplication

---

**Input:**  $k = (k_{n-1}, k_{n-2}, \dots, k_1, k_0)^2$  with  $k_{n-1}=1$ ,  $P(x, y) \in E(F_2^m)$   
**Output:**  $Q = k \cdot P$

- 1:  $R_0 \leftarrow 0$  and  $R_1 \leftarrow P$
- 2: For  $i=n$  down to 0 do
- 3: If  $k_i = 1$  then
- 4:  $R_1 \leftarrow R_1 + R_0$  Addition step
- 5:  $R_0 \leftarrow 2R_0$  Doubling step
- 6: Else
- 7:  $R_0 \leftarrow R_0 + R_1$  Addition step
- 8:  $R_1 \leftarrow 2R_1$  Doubling step
- 9: End if
- 10: End for
- 11: Return  $Q=R$

---

### 2.2.3 López-Dahab's montgomery scalar multiplication

Using López-Dahab's Montgomery point multiplication, inversion, which consumes a lot of resources in terms of memory as well as execution cycles, and power consumption, is avoided and the number of multiplication operations is optimized. Algorithm 5 gives the Montgomery point multiplication. We can see that, whatever the value of  $k_i$ , point addition (Madd) and point doubling (Mdouble) are computed simultaneously [14, 15].

---

**Listing 2.** López-Dahab's Montgomery scalar multiplication [15]

---

**Input:**  $k = (k_{n-1}, k_{n-2}, \dots, k_1, k_0)_2$  with  $k_{n-1}=1$   
**Output:**  $Q = k P(x, y) \in E(F_2^m)$   
 Set  $X_1 = x$ ;  $Z_1 = 1$ ;  $X_2 = x^4 + b$ ;  $Z_2 = x^2$   
**For**  $i$  from  $N-2$  down to 0 do  
   **If**  $k_i = 1$  then  
     Madd ( $X_1$ ;  $Z_1$ ;  $X_2$ ;  $Z_2$ );

```

Mdouble (X2; Z2); else
Madd (X2; Z2; X1; Z1);
Mdouble (X1; Z1);
End if
End for
x3=X1/Z1
y3=(x+X1/Z1).[(X1+xZ1)(X2+xZ2)+(x2+y)(Z1.Z1)].(xZ1Z1)-1
Return (x3, y3)

```

---

The point addition Madd (X<sub>1</sub>; Z<sub>1</sub>; X<sub>2</sub>; Z<sub>2</sub>) is computed as follow:

$$X_1 = x (X_1 Z_2 + X_2 Z_1)^2 + X_1 Z_1 X_2 Z_2; Z_1 = (X_1 Z_2 + X_2 Z_1)^2$$

The point doubling Mdouble (X<sub>2</sub>; Z<sub>2</sub>) is computed as follow:

$$X_2 = X_2^4 + b Z_2^4; Z_2 = X_2^2 Z_2^2$$

#### 2.2.4 Side channel attacks (SCA)

In computer security, a side-channel attack is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs). Timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited. Some side-channel attacks require technical knowledge of the internal operation of the system, although others such as differential power analysis are effective as black-box attacks. The rise of Web 2.0 applications and software-as-a-service has also significantly raised the possibility of side-channel attacks on the web, even when transmissions between a web browser and server are encrypted (e.g. through HTTPS or WiFi encryption), according to researchers from Microsoft Research and Indiana University [16] Many powerful side-channel attacks are based on statistical methods pioneered by Paul Kocher [17] Attempts to break a cryptosystem by deceiving or coercing people with legitimate access are not typically considered side-channel attacks: see social engineering and rubber-hose cryptanalysis.

General classes of side channel attack include:

**Cache attack:** attacks based on attacker's ability to monitor cache accesses made by the victim in a shared physical system as in virtualized environment or a type of cloud service.

**Timing attack:** attacks based on measuring how much time various computations (such as, say, comparing an attacker's given password with the victim's unknown one) take to perform.

**Power-monitoring attack:** attacks that make use of varying power consumption by the hardware during computation.

**Electromagnetic attack:** attacks based on leaked electromagnetic radiation, which can directly provide plaintexts and other information. Such measurements can be used to infer cryptographic keys using techniques equivalent to those in power analysis or can be used in non-cryptographic attacks, e.g. TEMPEST (aka van Eck phreaking or radiation monitoring) attacks.

**Acoustic cryptanalysis:** attacks that exploit sound produced during a computation (rather like power analysis).

**Differential fault analysis:** in which secrets are discovered by introducing faults in a computation.

**Data remanence:** in which sensitive data are read after supposedly having been deleted. (i.e. Cold boot attack).

**Software-initiated fault attacks:** Currently a rare class of side-channels, Row hammer is an example in which off-limits memory can be changed by accessing adjacent memory too often (causing state retention loss).

**Optical:** in which secrets and sensitive data can be read by visual recording using a high-resolution camera, or other devices that have such capabilities (see examples below).

One significant advantage of the ECC is that this method can be utilized for random number generation. Dual-EC-DRBG is recommended by the NIST as a random generator standard [18]. But it has a back door in random bit generator algorithm [19].

### 3. Proposed hybrid method

An image encryption method should be simple to implement, safe, and rapid enough to be used in real applications. In the suggested technique, the image is divided into its original color scheme. This scheme has three color channels having red, green, and blue. Every channel presents a matrix having  $M \times N$  size which is the input data for the cryptosystem. The mask of the color matrices is performed by the maskers where there are generated utilizing the primary key with the intervention of the ECC and AES algorithms. After the encryption step, channels are combined in order to produce a novel cipher image. The suggested model is effectuated in two steps which are: The key generation and the image encryption.

#### 3.1 Key generation step

In the first, the two parts compromise on the ECC curve. In the second, the shared key is performed utilizing the help of Diffie-Hellman. Because of this latter, is vulnerable to attack, the two parts share values of Diffie-Hellman with its own digital signature to avert the attack. The primary key is utilized as an initial input to generate random numbers. This latter is the primary step to gaining the key.

##### 3.1.1 Random number generation

Random Number Generator utilizes the benefits of Discrete Logarithm Problem (DLP) to generate sequence of number. The DLP in the elliptic curve cryptography permits to obtain irreversible numbers in order of  $P$  (a point on the curve) which is hard in the calculation. Ce cryptographic algorithm takes the strengths of the ECC principle operations, addition, and multiplication. Because it is unattainable to obtain the shared primary key; it's a DLP, sharing of point  $A$  and point  $G$  which are two points bellowing to the curve where  $A = [JK]$ .  $G$ , will not impact the security of the suggested way. The algorithm uses mainly point addition in the place of multiplication because this latter is very costly. In the final, because whole operations in the ECC are safe, the multiplication of  $X$  coordinates of points  $A$ ,  $B$ , and  $C$  are employed to produce the matrix  $D$ . The value of  $JK$  is updated utilizing the  $Y$  coordinate of points to furnish randomness of the suggested algorithm that covering the back-door issue. The propound method utilized for the random generation is detailed in Listing 3.

**Listing 3.** The Algorithmic of Random Number Generation Step

---

1. **Procedure:** RNG (Y, G, k, Primary Key)
2.  $J K_1 \leftarrow$  Primary Key
3. **for**  $i \leftarrow 1, i \leq k$  **do**
4.  $A(x, y) \leftarrow J K_i * G(x, y)$ , where  $*$  indicates the point multiplication in ECC
5.  $B(x, y) \leftarrow A(x, y) \otimes Y(x, y)$ , where  $\otimes$  indicates the point addition in ECC
6.  $C(x, y) \leftarrow B(x, y) \otimes G(x, y)$
7.  $D_i \leftarrow |x_A \times x_B \times x_C|$ , where  $x_A$  is the coordinate of point A,  $x_B$  is the coordinate of the point B,  $x_C$  is the coordinate of the point C
8.  $J K_{i+1} \leftarrow y_A + y_B + y_C$ , where  $y_A$  is the coordinate of point A,  $y_B$  is the coordinate of the point B,  $y_C$  is the coordinate of the point C
9. **end for**
10. **return** D
11. **End procedure**

---

When analyzing the proposed algorithmic, we note that the Primary Key consists of shared primary key betwixt parts. Both G and Y bellow on the curve having big orders. The  $k$  parameter presents the number of randoms needed for the generation where its value dependant on the execution system specifications. It can be defined based on the size of the image. it is preferable to set  $k$  value founded on the size of image for small images and to fix this value for large images.  $J K_1$  takes the value of the primary key. After that, the point  $A(x, y)$ , where  $x$  and  $y$  are the coordinates of the point on the elliptic curve, is performed using the point multiplication between  $J K_i$  and the point  $G(x, y)$ . Then, the point  $B(x, y)$  is acquired using the point addition of  $A(x, y)$  and  $Y(x, y)$ . To obtain  $C(x, y)$ , a point addition of  $B(x, y)$  and  $G(x, y)$  is performed. In the end,  $D_i$  is acquired using multiplication of  $|xA \times xB \times xC|$  and the  $J K_i$  value is updated by the simple addition of  $yA + yB + yC$ . D is the result of the algorithmic that contains generated numbers needed for the encryption. The D matrix presents the base for maskers' generation and initial ciphers.

### 3.1.2 Maskers generation step

After the generation, random numbers are utilized to produce maskers' matrices for the encryption process. Every masker is specific for its corresponding channel where it is ciphered using the AES. Maskers present the keyspace for cipher image and their entropy value tests the randomness in order to prove the effectiveness. The D array is utilized to create maskers for image encryption where the elements of Z are ciphered using AES with the primary key. In algorithmic 3, the RMR presents the masker result utilized to encrypt the red channel of the original image. After that, the RMR is employed as input for AES to obtain the green channel masker result (RMG). In the end, by applying the AES on the RMG, the blue channel masker RMB is obtained. An IV parameter is acquired using both Primary Key and  $\beta$  value where:

$$IV = (PrimaryKey) \bmod(K)$$

By utilizing this parameter,  $3 * 128$  bits initial cipher (IC) for every channel and a 128-bit IC\_Key are created where:

$$IC_{Key} = D(IV)$$



$$IC_{Key} = RMR(IV)$$

$$IC_{Key} = RMG(IV)$$

$$IC_{Key} = RMB(IV)$$

These values are removed from maskers. The Listing 4 presents the technique maskers and ICs gained.

---

**Listing 4.** The Algorithmic of Masker Generation Step

---

1. **Procedure:** masker (Array D, Primary Key, k)
  2. for  $i \leftarrow 1, i \leq k$  do
  3.  $RM_R \leftarrow \text{AES}(D, \text{Key})$
  4.  $RM_G \leftarrow \text{AES}(RM_R, \text{Key})$
  5.  $RMB \leftarrow \text{AES}(RM_G, \text{Key})$
  6.  $IV = (\text{Primary Key}) \bmod(k)$
  7.  $IC_{red} \leftarrow RM_R(IV)$
  8.  $IC_{green} \leftarrow RM_G(IV)$
  9.  $IC_{blue} \leftarrow RMB(IV)$
  10. **end for**
  11. **Return** (RM, IC)
  12. **End procedure**
- 

### 3.2 Image encryption step

The suggested image encryption procedure is founded on the stream cipher. Firstly, the permutation of the image is performed utilizing a random generator. Then, the image is split into red, green, and blue matrices. Every matrix is converted to 128 bits. After that, an XOR operation is performed between every bit of color matrix and every bit of ICs and maskers. Every information stream is masked utilizing the correspondent key channel matrices created in the proceeding part containing RMR, RMG, RMB, ICred, ICgreen, ICblue and IC\_Key. The suggested technique is presented in Listing 5. Here, the matrix of every color channel over keys utilized to cipher every channel is considered as input to the proposed algorithm. After that, every color matrix is split into 128 bits data path. Everyone has 16 pixels of individual color in its data. Then everyone is XORed with its initial cipher (IC) and its masker. When every data on the masker are employed, IC is updated utilizing the AES and XOR operation. At the end, when the encryption procedure is performed, the whole channels are combined to produce 24 bits of color pixels considered as a result of performing every channel side by side to obtain a novel cipher image. The decryption procedure is analogous to the encryption phase. But we must insert encrypted image input.

---

**Listing 5:** Algorithmic of Cipher Image Phase

---

1. **Procedure:** Image encryption (Mat<sub>red</sub>, Mat<sub>blue</sub>, Mat<sub>green</sub>, RM<sub>R</sub>, RM<sub>G</sub>, RM<sub>B</sub>, IC<sub>red</sub>, IC<sub>green</sub>, IC<sub>blue</sub>, IC<sub>Key</sub>)
2. **for**  $i \leftarrow 1, i, \text{ImageSize}/16$  **do**
3.      $Enc_{red,i} \leftarrow \text{Stream}_{red}(i) \oplus IC_{red} \oplus RM_R$
4.      $Enc_{green,i} \leftarrow \text{Stream}_{green}(i) \oplus IC_{green} \oplus RM_G$
5.      $Enc_{blue,i} \leftarrow \text{Stream}_{blue}(i) \oplus IC_{blue} \oplus RM_B$
6.     **if**  $i \bmod n(RM_R) = 0$  where (" $n(RM_R)$ " means the length of the RM<sub>R</sub>) **then**

7.  $IC_{red} = AES(IC_{key}, IC_{blue})$
  8.  $IC_{green} = IC_{green} \oplus IC_{red}$
  9.  $IC_{blue} = IC_{blue} \oplus IC_{green}$
  10. **end if**
  11.  $i \leftarrow i + 1$
  12. **end for**
  13. Encrypt\_Image = Combine Channels (S\_tream<sub>red</sub> , S\_tream<sub>green</sub>, S\_tream<sub>blue</sub>)
  14. **return** Encrypt\_Image
  15. **end procedure**
- 

## 4. Security analysis

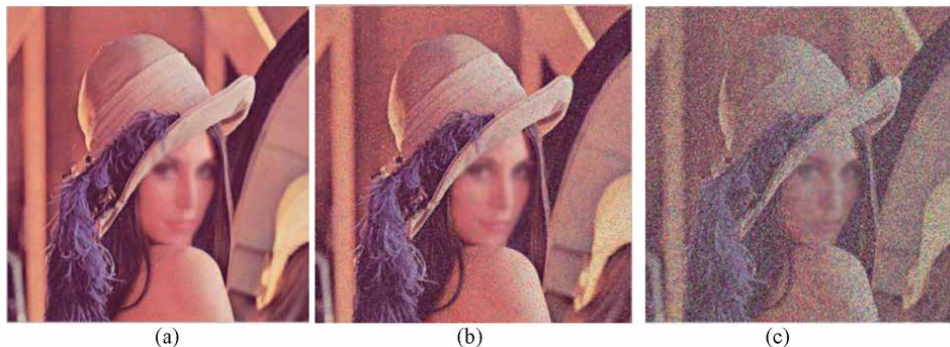
Images encryption security is a major challenge. Hence the exigency to an enhanced security approach to resist against various attacks. Experimental results are realized in this paper with various different color images. Many standard tests and evaluations are considered in this paper to access and analyze the security of image encryption containing the noise attack, known plain text and chosen plain text attack, the UACI (Unified Average Changing Intensity), NPCR (Number of Pixels Change Rate), correlation of adjacent pixels, histograms, entropy, and the key space. The primary key used for the key generation is 89762710306127702866241727433142015 and the  $k = 128$ .

### 4.1 Robustness against noise attack

During the image transmission via a network, the ciphered image can lose information or can be influenced by noise. Various cryptographic systems are sensitive to noise where a small change to the ciphered image can produce a strong distortion into the deciphered picture. **Figure 4** shows that the deciphered pictures keep the global clear image information for the man eye when the ciphered picture is affected by Salt & Pepper noise with various percentages. Therefore, the suggested method is robust and resist versus noise attack.

### 4.2 Differential attack analysis

Both NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) are utilized for the verification of the performance versus



**Figure 4.** Decrypted Lena of size  $512 \times 512 \times 3$  with salt & pepper noise: (a)  $d = 0.01$ , (b)  $d = 0.1$  and (c)  $d = 0.5$ .

differential attacks. Only one-bit modification over the clear image can result a considerable modification in the encrypted picture. NPCR and UACI parameters are presented in Eqs. (1) and (2). The desired average values for UACI is 33.46% and for NPCR is 99.56%.

$$NPCR : N(C1, C2) = \sum_{i,j} \frac{D(i,j)}{W * H} * 100\% \quad (1)$$

$$UACI = U(C1, C2) = \frac{1}{W * H} \sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{225} * 100\% \quad (2)$$

Where:

C1, C2 are the Ciphared pictures.

M is the size of pictures.

D: Bipolar matrix determined from C1 and C2.

The NPCR measures the pixels number that modifies value in differential attack. The elevated value is considered better. The UACI computes the average variance betwixt two paired encrypted pictures where a minimal value is the best. **Table 1** compares both NPCR and UACI results performed on Lena  $512 \times 512 \times 3$  using the suggested algorithm with some existing works. Results prove that the propound cryptographic technique has meet desired objective for resisting versus differential attacks.

### 4.3 Statistical Attack Analysis

Histogram of encrypted picture analysis and correlation of adjacent pixels are two fundamental parameters required to prove that the proposed cryptographic model is resistant versus statistical attacks.

#### 4.3.1 Histogram analysis

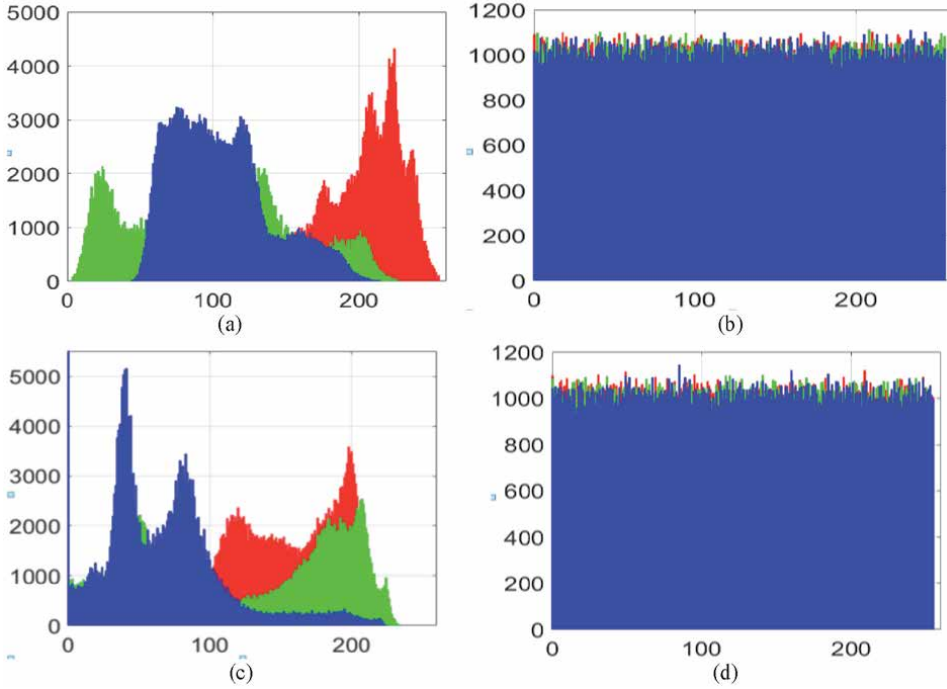
The histogram of the picture shows the frequency of every pixel. An improved cryptographic system must produce a uniform color distributed histogram. **Figure 5** shows the histogram of original and ciphared images. As you can see, histograms of ciphared images are uniform. The large dissimilarity between the two histograms from original and ciphared images denotes that images are greatly uncorrelated and no information can be detected from the cipher pictures which proves that the suggested cryptographic model is resistant versus statistical attacks.

#### 4.3.2 Correlation coefficient analysis

The correlation is a performance that evaluates the grade of similitude between two objects. If the original and the encrypted are different, therefore, the correlation factor is well low or highly close to zero. The reduced values prove that the encryption proceedings are capable to cover all characteristics of the transmitted

Algorithm	Proposed Model	[20]	[21]	[22]
NPCR	99.6215	99.6162	99.50	99.61
UACI	33.4631	33.3979	33.30	33.48

**Table 1.**  
 Comparison of the NPCR and UACI results with existing methods.



**Figure 5.** Histogram of original and cipher images: (a): Histogram of original Lena image, (b): Histogram of Lena cipher image, (c): Histogram of original pepper image, (d): Histogram of pepper cipher image.

image. **Figure 6** shows the distributions of 2000 pairs randomly selected adjacent pixels of the original and encrypted Lena  $512 \times 512 \times 3$  image, respectively in the horizontal, vertical, and diagonal direction.

The following equations are utilized for the study of the correlation between two adjacent pixels in the horizontal, vertical, and diagonal orientations for both clear and ciphered images.

$$E(x) = \frac{1}{N} \sum_{i=1}^N xi \quad (3)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (xi - E(x))^2 \quad (4)$$

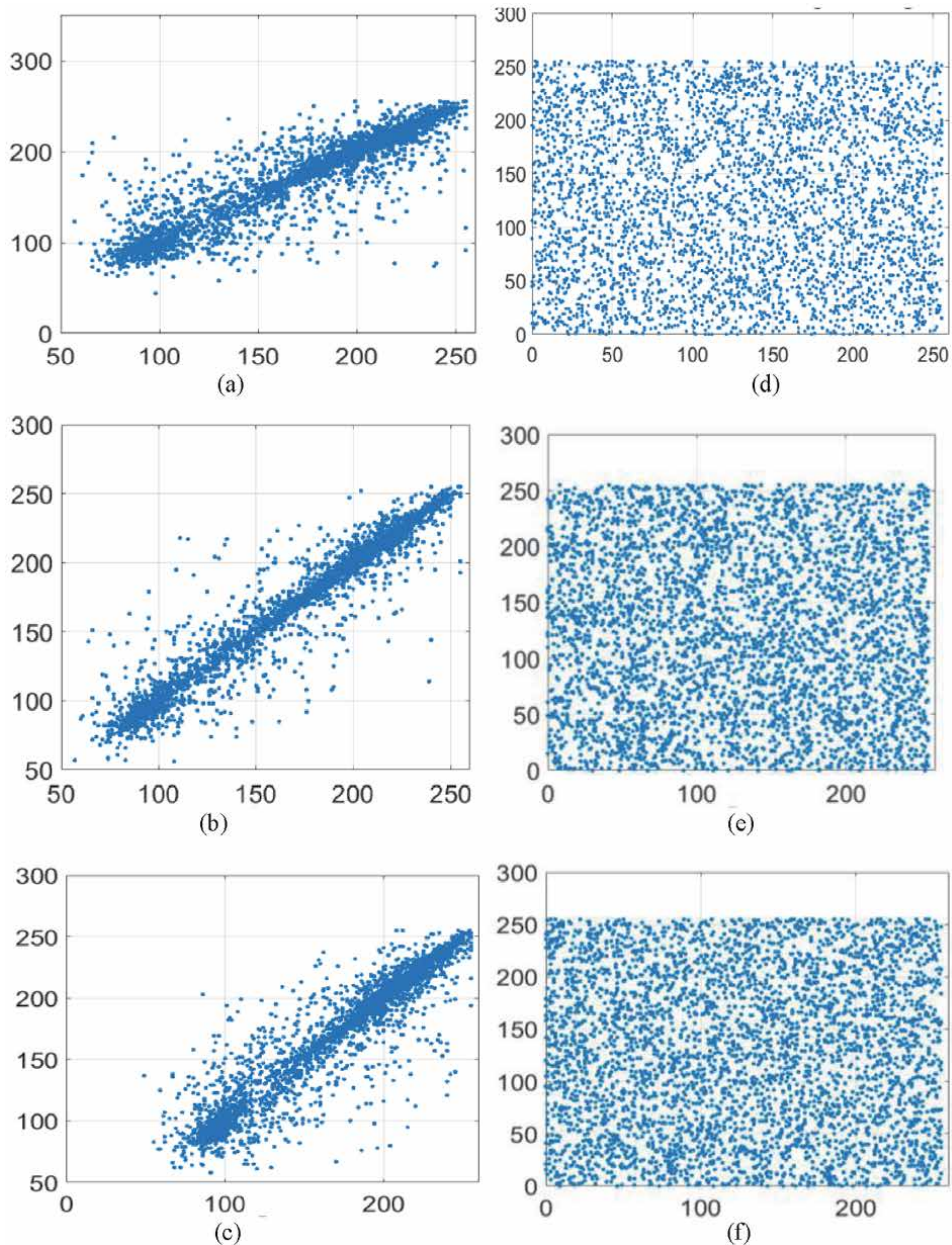
$$cov(x, y) = \frac{1}{N} \sum_{i=1}^N (xi - E(x))(yi - E(y)) \quad (5)$$

$$rx, y = \frac{cov(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \quad (6)$$

Where  $x, y$  are the intensity values of the two adjacent pixels in one image.  $N$  is the number of adjacent pixels chosen to compute the correlation.

We measured the correlation factor between the clear and ciphered images in each direction and findings are exposed in **Table 2**.

Findings show that coefficients are very reduced in the ciphered images in all directions and near to zero. On the other hand, the proposed cryptographic method is compared with other methods existing in the literature and results prove that the propound cryptosystem has a better correlation with the smallest coefficients in all



**Figure 6.** Correlation distribution of original and cipher Lena  $512 \times 512 \times 3$  color image in horizontal, vertical and diagonal directions: (a)-(c): Correlation distribution of original images; (d)-(f): Correlation distribution of cipher images.

directions which prove the effectuality of the algorithm and its capability for resisting statistical attack.

#### 4.4 Information entropy analysis

The entropy parameter is considered as the standard to test randomness. Entropy coefficient is utilized to obtain the incertitude performed in the ciphered image. If the entropy is elevated, the confidentiality is higher. Note that the utmost

Algorithm	Correlation coefficient		
	Horizontal	Vertical	Diagonal
Proposed Method (Lena)	-0.00871	-0.00141	-0.02039
Proposed Method (Baboon)	-0.00796	-0.01509	0.00196
Proposed Method (Peppers)	-0.03619	0.00295	0.013008
Ref. [20]	0.004639	0.006763	0.010818
Ref. [21]	0.00100	0.0017	0.01250
Ref. [22]	0.000101	0.00000958	0.000131

**Table 2.**  
The correlation coefficient comparison with different encryption methods.

Algorithm	Cipher image
Proposed Method (Lena 512*512*3)	7.99951
Ref. [20]	7.9989
Ref. [21]	7.9973
Ref. [22]	7.9994

**Table 3.**  
The entropy value comparison with different encryption methods.

entropy value for a gray scale image is 8 bits/pixel. The average value for  $H(m)$  for numerous preceding works was between 7.90 and 7.99. This value is depending on the image, the size of the key and the cryptographic model. Entropy is computed as:

$$H(m) = \sum_i^{2N-1} P(m||i) \log_2 \left( \frac{1}{P(mi)} \right) \quad (7)$$

Where:

$H(m)$ : Entropy image.

$P(mi)$ : Probability mass function.

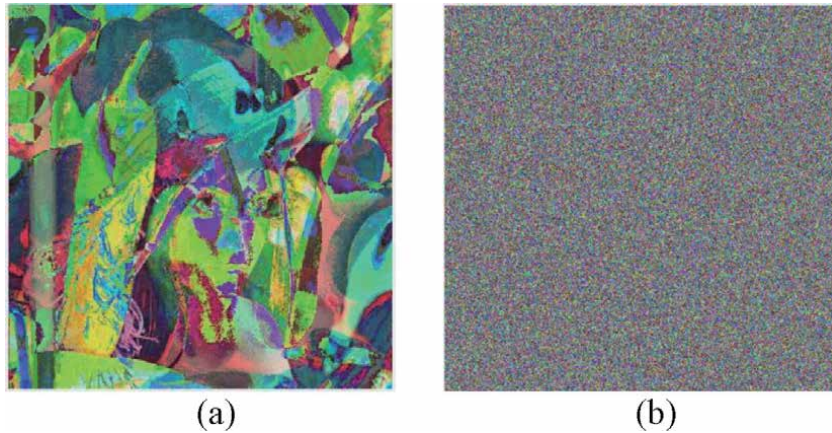
$2N - 1$ : number of gray levels.

**Table 3** compares the entropy value gained by the proposed model with other cryptographic methods. Results denote that the entropy value of the suggested cryptographic system is much closer the ideal case which prove the randomness of the system.

#### 4.5 Know plain text and chosen plain text attack

In the proposed algorithm, the diffusion process is performed by the XOR operation of the AES. Thus, it is very essential to evaluate its robustness against the chosen plain text attack. This type of attack uses the encrypted image with arbitrary plaintext data to crack the cryptosystem algorithm. According to reference [23], if the Eq. (8) is determined, the algorithm will be vulnerable to chosen plain text attacks. Otherwise, the algorithm resists chosen plain text attacks.

$$C_1(x, y) \oplus C_2(x, y) = P_1(x, y) \oplus P_2(x, y) \quad (8)$$



**Figure 7.**  
*Plain text analysis: (a) is the P1Xor P2, (b) is the C1 Xor C2.*

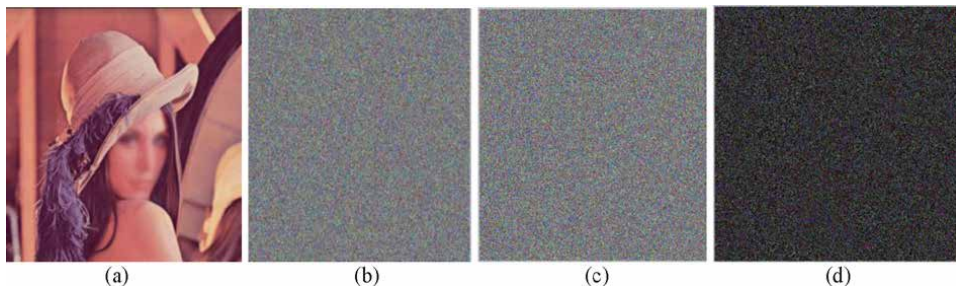
P1 and P2 are the plain Lena and Pepper images, while, C1 and C2 are their corresponding encrypted images, respectively. **Figure 7** shows that the XOR of encrypted image and clear image are not equal, i.e., the proposed cryptosystem algorithm resists chosen plain text attack.

#### 4.6 Security key analysis

An improved cryptographic model must have a large key size space. Because the suggested model employs a stream cipher encryption technique, the random generation period should be long. In order to guarantee the safety of the propound model, 128-bit AES is utilized that results in a large enough key space versus the brute force attack (requires  $2^{128}$  states to crack the key). The random generator employed in the suggested model is acquired from the elliptic Curve cryptosystem ECC, where its randomness is justified by the NIST. In the encryption step, the value of  $G(x, y)$  is modified at the debut of the encryption because the curve is changed. This result a dramatic modification in the created randoms and IV.

#### 4.7 Key sensitivity analysis

An enhanced encryption model should be greatly sensitive to key changes. Similarly, the suggested model must be resistant to the Brute-force attack obtained by large key space. For the Elliptic Curve Cryptosystem, we have employed a 256 key size and for the AES, we have selected the use of 128 bits key size which are big



**Figure 8.**  
*Test of the key encryption sensitivity: (a) plain image Lena  $512 \times 512$  (b) cipher image by the main key (c) cipher image by the modified key (d) encryption with the key difference between the two keys.*

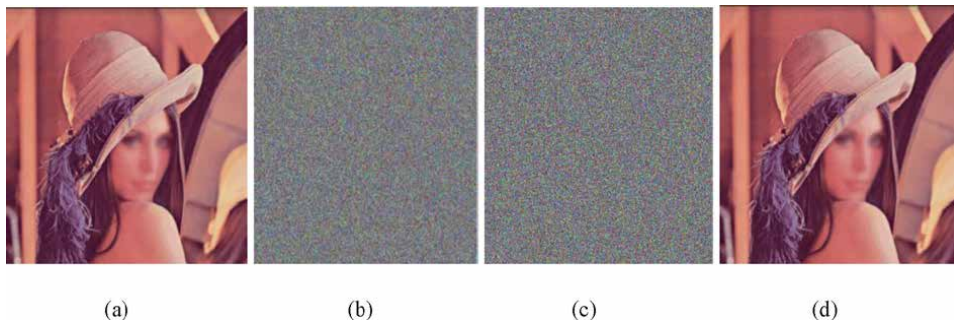
enough to resist versus attacks. To check the encryption process, the plain image is encrypted by three various keys: the first is the main key, the second is the same key with a small change in one bit and the last is a variance between the two keys. The finding of three different ciphered images are presented in **Figure 8**. Similarly, the ciphered image is decrypted by two keys: one is the original key and the other is the modified key. The changed key does not allow retrieval of the clear image as seen in **Figure 9**. As result, the suggested model is greatly sensitive to the key changes.

#### 4.8 Time complexity

In real-time image processing, the execution time is a major constraint. In a software implementation, the speed of execution mainly depends on CPU performance. The proposed algorithm is implemented using the Matlab R2017a software running on a personal computer with CPU Intel Core-i7-3770 3.4 GHz frequency. The time consumption is evaluated where  $\alpha$  was dynamic initiated based on image size. **Table 4** gives findings obtained by our hybrid model compared to original AES and ECC.

#### 4.9 Discussion

Through security analysis, it is shown that the histogram of the ciphered picture has uniform distribution and the correlation between pixels is decreased. The entropy value of Lena's standard image is 7.99951 (close to the ideal value). The suggested cryptographic model has an efficient encryption effect and a big secret keyspace. Further, findings prove that the proposed model can resist versus noise with various intensity and differential attacks. The execution time of the proposed scheme is executed with some images with different sizes. We note that our algorithm requires much less calculation time than the standard AES and ECC algorithms.



**Figure 9.** Test of the key decryption sensitivity: (a) original image Lena  $512 \times 512 \times 3$  (b) cipher image by the right key (c) decryption by 1-bit key change (d) decryption with the right key.

Encryption Model (s)	128×128	256×256	215×215	1024×1024
AES	0.64	1.320	2.987	5.315
ECC	22.215	40.320	87.120	-
Proposed Model	0.32	0.615	1.197	2.157

**Table 4.** Running time of proposed model for different image sizes.



## 5. Conclusion and future work

A novel technique for image encryption was suggested in this paper. The procedure of encryption is performed using cooperation between Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES). In this hybrid scheme, we have proposed to take the benefits of the Elliptic Curve Random Generator to generate a sequence of arbitrary numbers based on the curve. Then, the AES is performed to these sequences using arbitrary keys for image encryption. Security analysis over this model proved that it is resistant to known attacks. The histogram, correlation of adjacent pixels, and entropy of the encrypted image were computed and findings were hopeful. The optimal key space that can be used for encryption is 256-bit ECC and 128-bit AES key. As continuity to this work, we propose cooperation between Elliptic Curve Digital Signature (ECDSA) and AES cryptosystem. This prototype will be applied in large images and video signals.

### Author details

Amal Hafsa<sup>1\*</sup>, Mohamed Gafsi<sup>1</sup>, Jihene Malek<sup>1,2</sup> and Mohsen Machhout<sup>1</sup>

<sup>1</sup> Electronics and Micro-Electronics Laboratory, University of Monastir, Monastir, Tunisia

<sup>2</sup> Department of Electronics, Sousse University, Higher Institute of Applied Sciences and Technology, Sousse, Tunisia

\*Address all correspondence to: [hafsaamal12@gmail.com](mailto:hafsaamal12@gmail.com)

### IntechOpen

© 2020 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

## References

- [1] C. JunLi, Q. Dinghu, Y. Haifeng, Z. Hao, M. Nie, Email encryption system based on hybrid AES and ECC, in: *Wireless Mobile and Computing (CCWMC 2011)*, IET International Communication Conference on, IET, 2011, pp. 347–350.
- [2] A. R. Ganesh, P. N. Manikandan, S. P. Sethu, R. Sundararajan, K. Pargunarajan, An improved AES-ECC hybrid encryption scheme for secure communication in cooperative diversity based wireless sensor networks, in: *Recent Trends in Information Technology (ICRTIT)*, 2011 International Conference on, IEEE, 2011, pp. 1209–1214
- [3] H.T, Mohd BJ, A. Itradat, AN. Quttoum, Performance and information security evaluation with firewalls. *Int J Secur Appl* 7(6):355–372. <https://doi.org/10.14257/ijasia.2013.7.6.36>.
- [4] H. T, S. Ullah, B.J. Mohd, KS. Balagani, An enhanced WLAN security system with FPGA. *IEEE Syst J* 11(4): 2536–2545. <https://doi.org/10.1109/JSYST.2015.2424702.2017>.
- [5] A.M. Atteya, AH. Madian, A hybrid Chaos-AES encryption algorithm and its implementation based on FPGA, 2014, *New Circ Syst IEEE* 217–220. <https://doi.org/10.1109/NEWCAS.2014.6934022>.
- [6] K. Shankar, P. Eswaran, An efficient image encryption technique based on optimized key generation in ecc using genetic algorithm, in: *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, Springer, 2016, pp. 705–714.
- [7] A. A. A. El-Latif, X. Niu, A hybrid chaotic system and cyclic elliptic curve for image encryption, *AEU-International Journal of Electronics and Communications* 67 (2) (2013) 136–143.
- [8] H. Liu, Y. Liu, Cryptanalyzing an image encryption scheme based on hybrid chaotic system and cyclic elliptic curve, *Optics & Laser Technology* 56 (2014) 15–19.
- [9] F. Rannou, Numerical study of discrete plane area-preserving mappings, *Astronomy and Astrophysics* 31 (1974) 289.
- [10] Fips, N (2009). Announcing the advanced encryption standard, AES. *Technol. Lab. Natl.2001, Inst. Stand. Vol.*, pp. 8–12.
- [11] V. Miller, “Use of Elliptic Curves in Cryptography,” *Advances in Cryptology – CRYPTO’85*, vol. LNCS 218, pp. 417–426, 1986.
- [12] N. Koblitz, “Elliptic curve cryptosystems,” *Mathematics of Computation*, vol. 48, no. 177, pp. 203–203, Jan. 1987.
- [13] Montgomery, P. (2010) ‘Speeding the Pollard and elliptic curve methods of factorization’, *Mathematics of Computation*, Vol. 48, 243–264.
- [14] A.Hafsa; A. Sghaier; M. Zeghid; J. Malek; M. Machhout, (2020), An improved co-designed AES-ECC cryptosystem for secure data transmission, *International Journal of Information and Computer Security*, Vol.13 No.1, pp.118–140.
- [15] Tanja Lange, A note on López-Dahab coordinates. Source DBLP, January 2004.
- [16] Shuo Chen; Rui Wang; XiaoFeng Wang & Kehuan Zhang (May 2010). "Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow" (PDF). Microsoft Research. *IEEE Symposium on Security & Privacy* 2010.

[17] Kocher, Paul (1996). "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems". *Advances in Cryptology — CRYPTO '96. Advances in Cryptology—CRYPTO'96. Lecture Notes in Computer Science*. 1109. pp. 104–113. doi:10.1007/3-540-68697-5\_9. ISBN 978-3-540-61512-5. Retrieved 14 April 2014.

[18] Recommendation for random number generation using deterministic random bit generators, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf>.

[19] D. J. Bernstein, T. Lange, R. Niederhagen, Dual ec: A standardized back door, in: *The New Codebreakers*, Springer, 2016, pp. 256–281.

[20] Z. Lin, J. Liu, J. Lian, Y. Ma, X. Zhang (2019), A novel fast image encryption algorithm for embedded systems, *Multimedia Tools and Applications* 78:20511–20531 <https://doi.org/10.1007/s11042-018-6824-5>.

[21] A. A. A. El-Latif, X. Niu, (2013), A hybrid chaotic system and cyclic elliptic curve for image encryption, *AEU-International Journal of Electronics and Communications* 67 (2) 136–143.

[22] Y. Bentoutou, EL.H.Bensikadour, N. Taleb, N. Bounoua, (2019), An Improved Image Encryption Algorithm for Satellite Application, *Advances in Space Research*, Elsevier, Doi:<https://doi.org/10.1016/j.asr.2019.09.027>.

[23] Sundararaman Rajagopalan, Sivaraman Rethinam, Sridevi Arumugham, Har Narayan Upadhyay, John Bosco Balaguru Rayappan Rengarajan Amirtharajan, "Networked hardware assisted key image and chaotic attractors for secure RGB image communication», *Multimedia Tools Appl* (2018) 77:23449–23482 <https://doi.org/10.1007/s11042-017-5566-0>.



# An Emphasis on Quantum Cryptography and Quantum Key Distribution

*Bharadwaja V. Srividya and Smitha Sasi*

## Abstract

The application of internet has spiked up in the present-day scenario, as the exchange of information made between two parties happens in public environment. Hence privacy of information plays an important role in our day to day life. There have been incredible developments made in the field of cryptography resulting in modern cryptography at its zenith. Quantum computers are one among them creating fear into security agencies across the world. Solving the complex mathematical calculations is uncomplicated using quantum computers which results in breaking the keys of modern cryptography, which cannot be broken using classical computers. The concept of quantum physics, into the cryptographic world has resulted in the advancement of quantum cryptography. This technique utilizes the idea of key generation by photons, and communicates between peer entities by secured channel. Quantum cryptography adapts quantum mechanical principles like Heisenberg Uncertainty principle and photon polarization principle to provide secure communication between two parties. This article focuses on generation of a secret shared key, later converted into Quantum bits (Qbits) and transmitted to the receiver securely.

**Keywords:** quantum cryptography, Q bits, dirac vector notation, key distribution, secure transmission

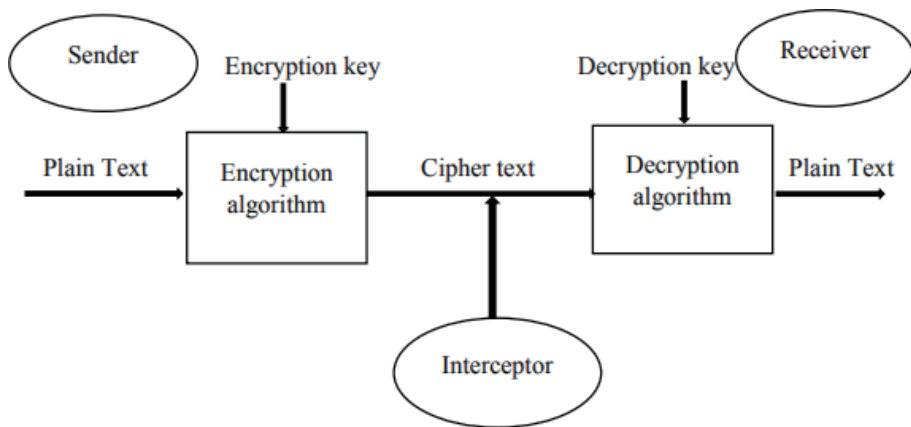
## 1. Introduction

Cryptography is dexterity of solving and writing codes. Cryptography is used in secured communication between peer parties. A cryptosystem is a network security model, which consists of design and implementation of cryptographic algorithms and associated frame work to contribute towards providing security for information. Basic Model of cryptosystem shown in **Figure 1** [1].

Network Security elements:

The important elements of cryptosystem are described –

- **Plain text:** This is the original data that needs to be secured over the unreliable channel.
- **Encryption Algorithm:** It is a mathematical model, which converts original plain text to cipher text, by using encryption key.



**Figure 1.**  
*Basic model of the cryptosystem.*

- **Cipher text:** The output generated by the mathematically oriented encryption algorithm is commonly referred to as cipher text. The cipher text is communicated to the peer over an unreliable channel.
- **Decryption Algorithm:** It is a inverse mathematically oriented algorithm which converts the cipher text to plaintext by using the appropriate decryption key.
- **Encryption Key:** It is an arbitrary value generated by the transmitter. This value helps in converting the original data to the scrambled version of the plain text by using an encryption algorithm.
- **Decryption Key.** It is a value shared to the receiver in case of shared key cryptosystem or mathematically generated by receiver in case of public key cryptosystem. This decryption key helps to convert the scrambled version of the plaintext to the original data.
- **Key Space:** This is a sample space consisting of all possible types of keys.
- An **interceptor** (an attacker) is an illegitimate peer who endeavors to detect the original data. This unauthorized peer may be aware of the decryption algorithm. But without the knowledge about the appropriate key, the decryption fails.

### **Types of Cryptosystems**

Cryptosystems are undoubtedly classified as two types namely: Symmetric Key Encryption and Asymmetric Key Encryption.

#### **Symmetric Key Encryption**

The process of enciphering and deciphering, utilizes the same shared key for in this cryptosystem. It is also known as secret key cryptosystem. The popular cryptosystem methods are:

- Digital Encryption Standard (DES),
- Triple-DES (3DES),
- Advanced Encryption Standard (AES)

- IDEA
- BLOWFISH.

### **Asymmetric Key Encryption**

The process of enciphering and deciphering utilizes different, but mathematically related pair of keys, in this cryptosystem. The popular algorithms are:

- Elliptic Curve Cryptography (ECC)
- RSA

However, as the data and innovation is expanding, traditional cryptographic methods are inadequate in giving the protection. Later quantum computation and quantum cryptography with quantum mechanics can be utilized to do the appropriation such that security cannot be traded off among clients. The methodology is known as quantum cryptography or quantum key distribution [2].

## **2. Recent trends in cryptography**

### **2.1 Dirac vector notation**

Dirac vector notation or Bra-ket notation is a standard way of representing classical bits as a vector [3, 4]. A Cbit (Special case of Qbit vectors) with a value 0 can also be written as  $|0\rangle$  or  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ .

A Cbit with a value 1 can also be written as,  $|1\rangle$  or  $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ .

Tensor product of vectors is given as,

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \otimes \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} = \begin{pmatrix} x_0 & \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \\ x_1 & \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} x_0y_0 \\ x_0y_1 \\ x_1y_0 \\ x_1y_1 \end{pmatrix} \text{ and } \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \otimes \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \otimes \begin{pmatrix} z_0 \\ z_1 \end{pmatrix} \\ = \begin{pmatrix} x_0y_0z_0 \\ x_0y_0z_1 \\ x_0y_1z_0 \\ x_0y_1z_1 \\ x_1y_0z_0 \\ x_1y_0z_1 \\ x_1y_1z_0 \\ x_1y_1z_1 \end{pmatrix}$$

## 2.2 Qbits

The Cbit vectors shown above are special cases of Qbit vectors. A Qbit comprises of 0 or 1. This is called superposition. In simpler words superposition means the Qbit is both 0 and 1 at the same time. A Qbit is represented by  $\begin{pmatrix} a \\ b \end{pmatrix}$  where a and b are complex numbers and,  $\|a\|^2 + \|b\|^2 = 1$ .

Examples of some Qbits are [5, 6],

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix} \begin{pmatrix} -1 \\ 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

During the measurement of the Qbit, it yields the actual value 0 or 1. This result is generally obtained at the termination of the Quantum computation. As mentioned a Qbit has a value  $\begin{pmatrix} a \\ b \end{pmatrix}$  which then encodes to 0 with a probability  $\|a\|^2$  and 1 with a probability  $\|b\|^2$ . The Qbit  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$  has a 100% chance of collapsing to 0 and Qbit  $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$  has a 100% chance of collapsing to 1 [5].

### 2.2.1 Operations on Qbits

To measure and operate on Qbits different gates are used in the form of matrices. These Matrix operators are used to design device, and manipulates Qbit spin/polarization without measuring and collapsing it. There are numerous popular matrix operators that can be used in Quantum computation. Quantum computing use only reversible operations [7]. Reversible means given the operation and output value, you can find the input value, For  $Ax = b$ , given b and A, you can find x [2].

#### 2.2.1.1 Hadamard (H) gate

Hadamard gate works on a single Qbit. It helps in creating superposition; where during measurement the probability of getting 0 or 1 is equal. The Hadamard gate takes a 1 or a 0 bit and disseminate it into exactly equal superposition. It comprises of two rotations  $\pi$  about the z-axis and  $\frac{\pi}{2}$  about the y- axis. The H gate shown in **Figure 2** [2]. Hadamard matrix is given by

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$



**Figure 2.**  
H-gate.



### 2.2.1.2 Controlled not-gate

Controlled “Not-gate” operates on bit-pairs, commonly referred to as “Control bit” and “Target bit”. The condition over bit-pairs are:

- Control-bit = 0; Then Target bit is “unchanged”
- Control-bit = 1: Then the Target bit is “Flipped”

In the binary pair shown, the most significant bit is referred to as control bit and the least significant bit as the target bit. The CNOT gate shown in **Figure 3** [2].

00 → 00  
 01 → 01  
 10 → 11  
 11 → 10.

It is represented by the matrix,

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

## 2.3 Quantum entanglement

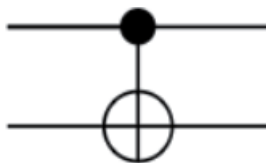
Quantum Key Distribution is also based on Quantum Entanglement principle according to which two particles can be entangled such that when of property is measured, on either of the particle the opposite state will be obtained on the entangled particle. This is totally independent of distance between particles, also the key feature of this is that, it is impossible to measure the state prior until it is discussed over classical channel [8].

## 2.4 Bloch sphere

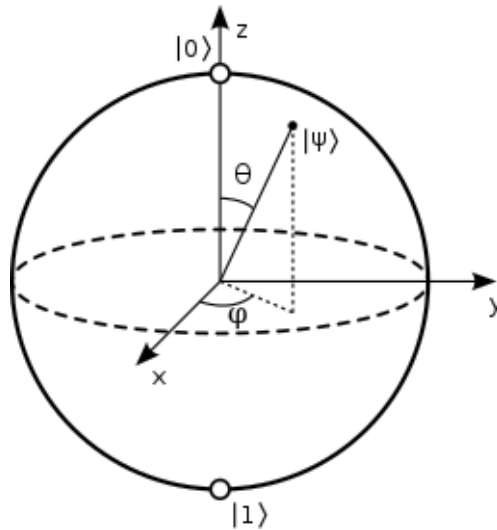
It is used to represent states of qbit on a unit sphere. The operations performed on qbit during qbit information processing is described in block sphere. The Bloch Sphere Representation is shown in **Figure 4** [1].

Representation of single qbit state is given by:

$$|\varphi\rangle = e^{i\gamma} \left( \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle \right)$$



**Figure 3.**  
 CNOT-gate.



**Figure 4.**  
*Bloch sphere representation.*

Where  $\gamma, \theta, \varphi$  are real numbers.

Bloch sphere is general representation of complex number  $z$  where  $|z|^2 = 1$  as point on circle in complex plane.

General Qbit:  $|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle$ .

## 2.5 BB84 protocol

BB84 was invented by Charles Bennet and Gills Brassard in 1984. This is first security protocol that was designed to implement QKD which uses idea of photon polarization. The key is transmitted as number of binary bits which are encoded on a random polarization basis [9].

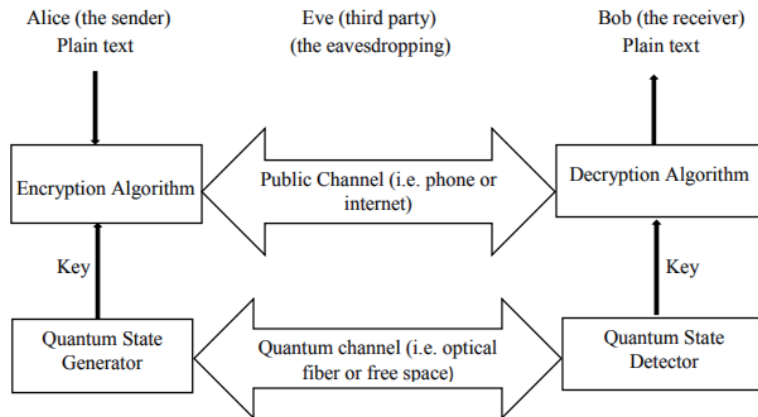
In this protocol there are two channels used mainly for transmission.

1. Quantum Channel
2. Classical Channel

Quantum channel is the one that is used to transmit secure information by converting into bits and transform information photons which is quantum information. This channel can be used to transmit classical information as well. Classical channel is the one that is used to transmit classical information. Examples include e-mail, message, phone lines etc. This protocol is mainly based on Heisenberg uncertainty principle that states measuring quantum state without disturbing is impossible. Hence introducing anomaly by intruder can be noticed by the user [2]. The quantum Key distribution is as shown in **Figure 5**.

### 2.5.1 Working

The **Figure 5** illustrates that Quantum Key Distribution system has two channels i.e. quantum channel and public channel. Quantum Channel is used to transmit and share the information of.



**Figure 5.**  
 Quantum key distribution.

Secret key in the form of polarized photon, called as quantum bit (qbit). In the meantime the open channel is utilized to examine the procedure of qbits transmission and make an arrangement about the mutual mystery key. For the most part, there are two medium kinds of quantum channel which is executed on QKD framework for example optical fiber and free space [10].

There are some famous character terms that is utilized in QKD framework to be specific Alice as the sender, Bob as recipient, and Eve as meddler. Quantum condition of photon is utilized to recognize nearness of outsider. The message is transmitted by means of polarization photon meant by zero or one that has one piece quantum data called as qbit. The sender transmits energized photon through quantum channel utilizing channel on arbitrary premise. Likewise beneficiary uses irregular channels to get the information and after that check for change in got bits.

There are two steps involved in key distribution

#### 1. One-way Communication (Via quantum Channel)

Step 1: user A (Alice) randomly chosen polarized photon and send it to user B (Bob) over Quantum channel.

Step 2: In this, user B receives photons using random basis either rectangular or diagonal.

#### 2. Two-way Communication (Via Public channel)

Step 1: User A will use public channel to inform user B about the polarization she chose for every bit sent to user B without disclosing the bit value.

Step 2: Now user B will compare the polarization sequence he received from user A with the sequence he generated.

Step 3: Bits of same orientation of those two sequences can be used as secret key.

#### 2.5.1.1 Post reception

##### a. Error Estimation:

Both sender and receiver discusses the basis used through a classical channel which is either through a e-mail, telephone. Then discards the bits which basis are not matched.

Whenever there is an intrusion, error is introduced and keys with users does not match. Hence errors are to be considered, if it exceeds QBER Threshold then key is discarded and recent.

b. Error correction:

This is performed by considering bits at both sender and the receiver by removing errors in key using certain protocols namely cascade, winnow. QKD is a technique that creates symmetric key by using quantum properties of light to communicate between users.

### *2.5.2 Eaves dropping*

If attacker (eve) tries hacking the bits secretly that is if he/she tries to tap channel then that is observed at the receiver end. According to No Cloning theorem, an unknown quantum state cannot be cloned therefore eve cannot have same information as Bob Probability of Eavesdropping [11]:

$$\text{For } N \text{ bits} = (3/4)^N$$

When N increases, detecting eavesdropping is also easier.

**Advantages:**

Detection of Eavesdropping

**Disadvantages:**

Loss of photon in transmission.

### *2.5.3 Photons*

The basic unit of the electromagnetic radiation is the photons. The classical computer uses bits to transfer the data, while quantum computing is based on quantum mechanics which make use of photons for communication. Qbits can be combination of both 0 s and 1 s having more than one state, such that retrieving the information about one qbit will give the result of other states too, unlike the classical computing where 0's and 1's are used [12].

### *2.5.4 Essentials of QKD*

The fundamental principles of Quantum Key Distribution protocol is based on the two Quantum mechanics laws.

According to Heisenberg Uncertainty without operating the system, it is not possible to carry out any sort of measurement on the system. For example, consider the two conjugate variables having momentum p and position x, both parameters cannot be measured concurrently [12].

Zurek and Wootters presented the first polarization principle on photons in the year 1972. According to this principle and also no-cloning theorem, any eaves dropper will not be able to duplicate the random qbits. This principle elaborates about polarization of light photons and its orientation in a specific direction. Photon destruction can result due to the utilization of erroneous photon filters. In cloning theorem, if the state of photon orientation are distorted, then passive attack of the system may occur. Therefore Quantum Mechanics key distribution recommends security.

### 2.5.5 Heisenberg uncertainty principle

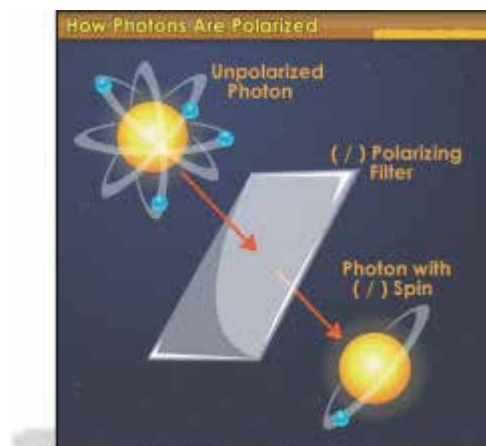
The impact of Heisenberg Uncertainty Principle is huge just for movement of infinitesimal articles and is insignificant for that of plainly visible items. The Heisenberg Uncertainty Principle expresses that it is difficult to know at the same time the precise position and force of a particle. That is, the more precisely the position is resolved, the less known the force, and the other way around. This standard is not an announcement about the points of confinement of innovation, yet a crucial farthest point on what can be thought about a particle at some random minute. This vulnerability emerges in light of the fact that the demonstration of estimating influences the item being estimated. The best way to gauge the situation of something is utilizing light, at the same time, on the sub-nuclear scale, the collaboration of the light with the article unavoidably changes the item's position and its course of movement [13].

Under the laws of quantum physics, a moving photon has one of four introductions; vertical, horizontal, or diagonal in opposing directions as shown in **Figure 6**. Quantum cryptographic gadgets transmit photons each one in turn, and every photon has a specific introduction. Photon sniffers can record the introduction of every photon, except in certain situations. Because as per Heisenberg's uncertainty guidelines, doing so will change the introduction of a portion of the particles which will caution both the sender and the receiver that their channel is being examined. Heisenberg's vulnerability rule is of gigantic advantage to information security that, if quantum cryptography is utilized to send keys by means of photons at that point consummate encryption is guaranteed.

### 2.5.6 Photon polarization

Basically polarization of light wave is restricting plane of vibration of electric field in a definite plane. There are 3 types of light polarization:

1. Plane polarized light
2. Circularly polarized light
3. Elliptical polarized light



**Figure 6.**  
*Polarization of photons.*

A device called a Polarizer allows us to place a photon in a particular polarization. A Pockels Cell can be used too. The polarization basis is mapping we decide to use for a particular state.

There are two types of Basis/Polarizer through which polarization can happen (Table 1),

1. Rectilinear Basis

2. Diagonal Basis

Spin of Rectilinear Basis,

If  $\theta = 0^\circ \rightarrow \text{State}|0\rangle$

$\theta' = 90^\circ \rightarrow \text{State}|1\rangle$

Spin of Diagonal Basis,

If  $\theta = 45^\circ \rightarrow \text{State}|0\rangle$

$\theta' = 135^\circ \rightarrow \text{State}|1\rangle$

		0	1
Rectilinear Basis			
Diagonal Basis			

**Table 1.**  
Polarization using basis.

Photon polarization principle explains how photons can be oriented in different directions. Polarized photons can be detected only with photon filter of correct polarization otherwise photon will be destroyed. Plane polarization of light can be done by ways like reflection, refraction, selective absorption, scattering, double reflection. In circularly and elliptically polarized light, electric field of light is confined in one direction but direction rotates as light propagates.

2.5.7 No cloning theorem

The eminent feature distinguishing between classical and quantum theory is No cloning theorem which restricts copying of quantum state.

Cloning in physics means much perfect copy where the reality of positions and momenta and energy levels of every particle and interaction are exactly the same in the copy as the original.

No cloning preliminaries:

Quantum properties that needs to be known:

1. Super positions

Particles can be in several states at once, in quantum mechanics the whole is the sum that is the superposition of its different possible parts

$$|A\rangle = |A\rangle + |A\rangle$$

## 2. Composite systems

The superposition of the product of component.

$$|AB\rangle = |A\rangle + |B\rangle$$

## 3. Transformations distribute

Any change to a particle that in superposition of a state affects all of the states independently.

$$T(|A1\rangle + |A2\rangle) = T(|A\rangle) + T(|A\rangle)$$

No cloning theorem states that “an identical copy of unknown quantum state cannot be created”.

### 2.5.8 Quantum channels

The communication for quantum network over optical networks and photon based qubits for wide range distances are used. Optical networks support the wide range of bandwidth. The Quantum bits can be transmitted reliably and at high velocity over an optical fiber channel.

### 2.5.9 Fiber optic networks

To design and implement Optical networks the contemporary Telecommunication equipment's can be utilized. At the transmitter, a unique photon source can be produced by densely attenuating a standard telecommunication laser such that the average number of photons per pulse is below 1. The receiver can have an avalanche photo detector. For the phase and polarization control, beam splitters and interferometers are used. Entangled photons are generated through continuous parametric down conversion of entanglement based protocols.

### 2.5.10 Free space networks

Fiber optic networks works based on free space quantum networks, but rely online of sight between the communicating parties. Free space networks provides higher bandwidth and better data rate than fiber optic networks and this does not have polarization scrambling like optical fiber.

### 2.5.11 Cavity-QED networks

Quantum key distribution based on Telecommunication lasers and parametric down converters is combined with photo detectors. To amalgamate and retransmit the quantum data, without disturbing the current states, is important in distributed quantum entangled system. Cavity quantum electrodynamics (Cavity QED) helps to generate such quantum entangled system. In this method, the quantum states can be transmitted to and from one atomic quantum states which is located in single atom and consists of optical cavities. This process supports transmission of quantum states between atoms over optical fiber for the creation of remote entanglement distributed systems [14].

### **3. Pros and cons of QKD**

Quantum key distribution is one of the techniques used for exchanging keys between two users. The main advantage of quantum communication is its security. Since any change made to a particle of an entangled pair is reciprocated by the other, quantum information secured through quantum cryptography cannot be tapped. This is also because of the no cloning and no destroying theorem. So the information can neither be duplicated nor be destroyed. Discrete variable QKD is limited to around 200 km until a quantum repeater is created and can be efficiently implemented. This currently requires a quantum memory. Continuous variable QKD is also limited to similar distances and cannot pass an Optic amplifier in a standard communication network yet also has no known repeater architecture. This will have to be overcome for global QKD to be taken up. There is a trade-off in speed over distance. The longer the distance, the slower the quantum communication. Therefore classical communication is currently faster and can propagate over global distances. It is possible satellite based QKD will allow longer distance quantum communication but this has not been performed to date. When sending quantum information one must also have some classical communication to ensure security, which means that both a classical and quantum network must exist side-by-side.

Despite these advantages, the technology needed to build a quantum computer is currently beyond our reach. This is due to the fact that the coherent state, fundamental to a quantum computer's operation, is destroyed as soon as it is measurably affected by its environment. Attempts at combating this problem have had little success, but the hunt for a practical solution continues.

QKD is advantageous when compared with conventional cryptographic techniques in certain aspects which are as follows:

1. Any attempts of eavesdropping can be identified with the help of two principles of quantum mechanics.
2. Quantum key distribution protocol can detect eavesdropping because the error level is more during this case.
3. The errors caused during communication between users can be detected.
4. Video can be transferred between the nodes with the rate of 128–1024 kbps without the consideration of any overhead data.
5. QKD generates new private key randomly and continuously so it is next to impossible to steal any key distributed by quantum cryptography.
6. Data security is increased with QKD protocol.
7. The actual information can never be revealed to any third party.
8. Security of QKD is based on the laws of quantum physics which can be proven.

QKD sounds too good when concerned with security but when it comes to practical considerations it takes back seat. There are certain technical weaknesses related to implementation.

1. High set up and installation cost for commercial use.



2. Long distance transmission is not feasible, range of QKD is restricted to few hundred kilometers and quantum repeaters do not have any practical application.
3. Equipment set up has to be done precisely.
4. Key distribution rate of QKD is 1000 to 10000 times slower than the conventional optical communication.
5. While transmitting video there is problem of delay.
6. These systems are sensitive to noise.
7. These devices are not independent [15].

## 4. Results and discussions

### 4.1 Generation of keys

The sender decides large sequence of binary bits, which are polarized on a random choice of rectilinear (0, 90 degree) and diagonal basis (45, 135 degree). Binary bits are encoded according to the table shown (**Table 2**).

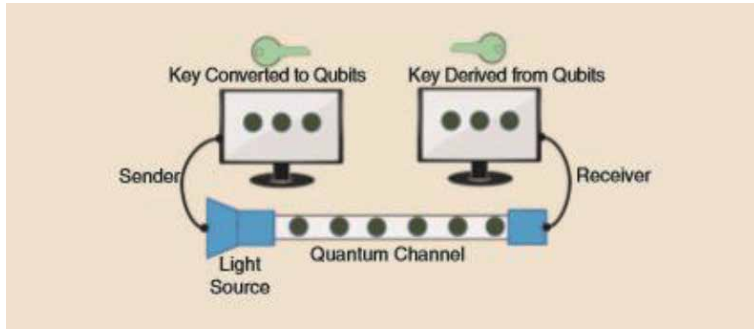
Bit	0	0	1	1
Base	+	X	+	X
Orientation	—	\		/

**Table 2.**  
Representation of binary bits.

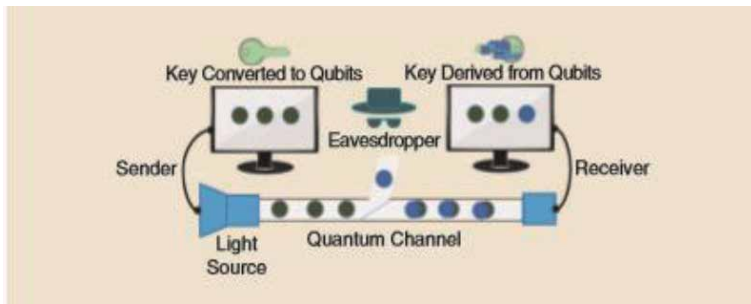
Encoded keys are transmitted as polarized photons through a quantum channel. Similarly receiver has to measure these polarized photons since the receiver does not have idea about the basis used by sender, receiver randomly chooses between diagonal and rectilinear basis. There are chances of receiver choosing wrong basis which results in misinterpreting the bit received. Once all the bits are received to clarify the bits used sender and receiver communicates over classical channel, and discusses the basis used to polarize each bit. Finally once sender and receiver reveals basis used for polarizing each bit they ignore all the photons for which receiver uses wrong base and consider only those bits that were decrypted using the same base as used by sender. In short, sender and receiver on a common basis generate key of shorter sequence of bits (**Table 3**).

Sender's bit	0	1	0	1
Base	+	+	X	X
Orientation	—		\	/
Receiver base	+	X	X	X
Received bit	0	0	0	1

**Table 3.**  
Comparison measurements.



**Figure 7.**  
*Illustration of QKD.*



**Figure 8.**  
*Impact of eaves dropping on QKD.*

The bits for which receiver uses wrong basis are discarded and the remaining bits are considered as key. QBER (Quantum Bit Error Rate) is measured for the chosen key and if its less than threshold value, in that case key is used for message encryption, else key is discarded and is expected for another key transmission (Figures 7 and 8).

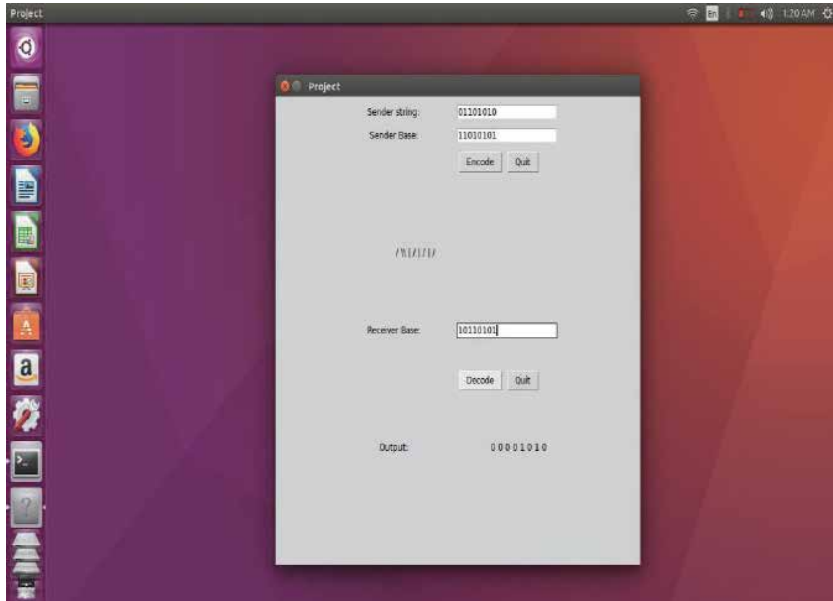
Quantum key distribution is not a replacement for the present day cryptography, but a more secured way of transmitting keys which are required for a encoding and decoding of the messages. The maximum speed and the amount of information that can be sent using quantum key distribution is not very large. But it is very secure [16, 17].

Sending:

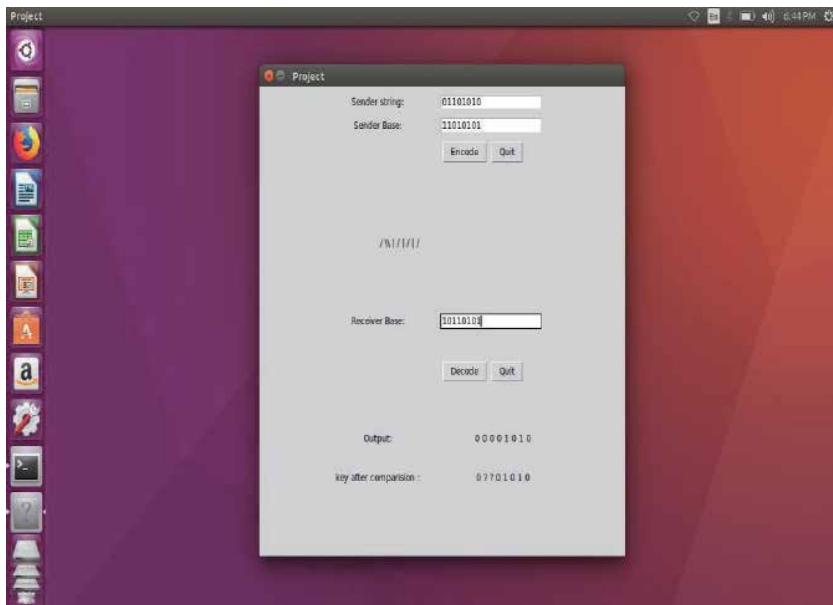
1. After deciding number of bits to exchange, Alice decides the stream of basis (rectilinear or diagonal) for each pulse of photons she is going to send. A lot of this bits are discarded later due to mismatch of basis, so the Main aim is not to transfer a specific key, but to agree on a common key.
2. Desired polarized Photons are generated using A light-emitting diode (LED) Or from a laser. Each pulse consists of a single Photon. In real-time it has to be a beam of light whose intensity is has to be maintained with care. Because if the intensity is too low, the receiver might not be able to detect the pulse of photon. Also, if the intensity is too high, then the eaves dropper can measure the beam of light with respect to both the basis without letting his presence known to the user as there will be no major change made to the spin. So, there as to be a threshold to be set for beam of light.

Receiving and converting.

3. Bob, who is the exclusive receiver of the information, chooses stream of basis (rectilinear or diagonal) to measure the spin of each photon.
4. Number of basis used in receiver end is also predetermined and equal to number of bits that was decided to be exchanged (**Figures 9 and 10**).



**Figure 9.**  
*Receiver entering the basis and decodes key.*



**Figure 10.**  
*Results key after discarding mismatched bits.*

5. Now, Bob will announce the basis that he used to receive each photon on a public channel without giving much attention if other people are hearing it.
6. Now, Alice publically announces the basis which has matched.
7. All the unnecessary bits whose basis was not matched are discarded.
8. Bits received through the correctly-chosen basis are now converted on to binary code.
9. Using the bits that have matched as keys, the actual plain text is encoded and sent over a public Channel without worrying about eavesdropping.

## 5. Applications

1. **Ultra-Secure Voting:** To detect and control voter fraudulent during elections, a more secured system is desired. By using Quantum cryptography the voting results are kept secured. Especially the important vulnerable part of the data transaction is uninterrupted. This technology is expected to escalate worldwide, as fraudulent elections may be faced by many countries.
2. **Secure Communications with Space:** Secure space communications with satellites and astronauts is of major concern. NASA is working on a project, with Quintessence Labs to guarantee the security of communication.
3. **Smarter Power Grid:** Normally power grids are at more risk, due to cyber-attacks. Smart grids are required for stabilizing the supply and demand. With adequate precautions, they are more efficient than the traditional grids. With Quantum cryptosystems, it is be possible to preserve the safety of the framework against any attacks.
4. **Quantum Internet:** Internet needs to be relatively fast and secured. By using Quantum cryptosystem, the speed of the internet greatly slows down. If the switching between the q-bits can be done at a significantly faster rate, then the sensitive data over the internet can be more secured and can be retrieved quickly.

## 6. Conclusion

In this article, the key distribution algorithm using quantum mechanics and concepts of physics is elaborated. Using famous BB84 algorithm and python programming, the system can successfully transfer the secret key from sender to receiver. Along with automatic generation and transmission of Qbits, a GUI can be designed for a user to send bits of their choice. Also the photon orientations/spin can be depicted in the transmission from sender end to receiver end. Quantum Cryptography is mainly designed to be future ready Quantum computer to face threats. It performs exceptionally well without any rigorous and complex mathematical calculations. At the receiver end the photons are received in an expected manner and provide accurate data to the user. The main advantage being 0% exposure of information to intruders and Quantum computers are efficient in transferring keys. The physical implementation which is still a challenge needs lot of

meticulous work to setup the system. Long distance transmission is limited as the photons might lose its energy. As the whole system is performing accurately up to this mark, error bit calculation and notifying the exclusive users about the presence of Eavesdropper is proposed as a future work. Any attempts to attack the communication will be notified to the user through error rate being higher than threshold.

## **Acknowledgements**

We would like to take this opportunity to thank all those who were kind enough to provide assistance when needed, which helped us in completing this article. We are grateful to the management of Dayananda Sagar College of Engineering, for their kind co-operation. We would like to express our heartfelt thanks to our beloved head of the department, Dr. A R Aswatha, for his constant encouragement and timely suggestions during the course of preparation of the article. We are very grateful to Dr. Nagamani A N, post-doctoral from IISc, Bangalore, Karnataka, India for her constant supervision, motivation and support provided during the completion of the article. We would like to thank Almighty, our parents for their support and encouragement throughout the work.

## **Author details**

Bharadwaja V. Srividya and Smitha Sasi\*  
Dayananda Sagar College of Engineering, Bangalore, Karnataka, India

\*Address all correspondence to: [smitha.sasi24@gmail.com](mailto:smitha.sasi24@gmail.com)

## **IntechOpen**

---

© 2021 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

## References

- [1] William Stallings, “Cryptography and Network Security”, Edition 4, Pearson Publishers
- [2] Logan O. Mailloux, Charlton D. Lewis II, Casey Riggs, and Michael R. Grimaila, “PostQuantum Cryptography What Advancements in Quantum Computing Mean for IT Professionals”, IEEE 2016
- [3] Harshad R. Pawar, Dr. Dinesh G. Harkut, “Classical and Quantum Cryptography for Image Encryption & Decryption”, IEEE 2018
- [4] C. G. Almudever; L. Lao; X. Fu; N. Khammassi; I. Ashraf; D. Iorga; S. Varsa mopoulos; C. Eichler; A. Wallraff; L. Geck “The engineering challenges in quantum computing”, Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017
- [5] Ashish Nanda, Deepak Puthal, Saraju P. Mohanty, and Uma Choppali, “A Computing Perspective on Quantum Cryptography”, IEEE Consumer Electronics Magazine 2018
- [6] Xiongfeng Ma, Hongyi Zhou, Kefan Lv, “Security level and information flow in a quantum key distribution network”, IEEE 2018
- [7] Songsheng Tang, Fuqiang Liu, “A one-time pad encryption algorithm based on one-way hash and conventional block cipher”, IEEE 2012
- [8] Farzan Jazaeri; Arnout Beckers; Armin Tajalli; Jean-Michel Sallese, “A Review on Quantum Computing: From Qubits to Front-end Electronics and Cryogenic MOSFET Physics”, 2019 MIXDES - 26th International Conference “Mixed Design of Integrated Circuits and Systems”
- [9] Huber Nieto-Chaupis, “Encrypted Communications through Quantum Key Distribution Algorithms and Bessel Functions”, IEEE 2018
- [10] P. Siva Lakshmi, G. Murali, “Comparison of Classical and Quantum Cryptography using QKD Simulator”, IEEE 2017
- [11] Ankur Raina and Shayan Garani Srinivasa, “Eavesdropping on a quantum channel with a unitarily interacting probe”, IEEE 2015
- [12] D N Kartheek, G Amarnath, P Venkateswarlu Reddy, “Security in Quantum computing using quantum key distribution protocols”, IEEE 2013
- [13] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”, *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484-1509, Oct. 1997, [online] Available: <http://dx.doi.org/10.1137/S0097539795293172>.
- [14] Ali Ibnun Nurhadi, Nana Rachmana Syambas, “Quantum Key Distribution (QKD) Protocols: A Survey”, IEEE 2018
- [15] Soumy jain” Quantum computer architectures: A survey”, IEEE 2nd International Conference on Computing for Sustainable Global Development (INDIACom) 2015
- [16] Masahide Sasaki, “Quantum Key Distribution and Its Applications”, IEEE 2018
- [17] J. Aditya, P. Shankar Rao “Quantum Cryptography”, [https://cs.stanford.edu/people/adityaj/Quantum Cryptography.pdf](https://cs.stanford.edu/people/adityaj/Quantum%20Cryptography.pdf)

# Advancements in Optical Data Transmission and Security Systems

*Menachem Domb*

## Abstract

Optical Communication (OC) for data transmission was introduced more than 30 years ago. It employs two main technologies, fiber optics using a physical wire and Free Space Optical (FSO) wireless transmission. Fiber optics has been well developed over the years in terms of distance, bandwidth, speed, reliability, and other enhancements that contribute to its use. Recent developments in FSO transmission has made it the mainstream and a better alternative compared to RF wireless transmission, concerning all parameters. In this chapter, we focus on advancements in OC that represent innovative ideas of how to enable new methods of secured optical data transmission in different ways and not simply as an extension to current methods and technologies.

**Keywords:** optical communication, free space optical (FSO), security, multiplexing, network coding (NC), optical wireless communication (OWC), orbital angular momentum (OAM), quantum key-distribution (QDK)

## 1. Introduction

The use of wireline and wireless communications is very common in a wide range of devices. The increased complexity of the core transmission systems is reflected in a set of advancements in data communications and specifically in Optical Communication [1]. The elastic Optical Network (EON) concept is an optical network architecture able to support the increased need for elasticity in allocating optical network resources. Flexible bandwidth allocation is performed to adapt to different transmission techniques, such as Orthogonal Frequency Division Multiplexing (OFDM), Nyquist WDM (NWDM), transponder types (BVT1, S-BVT), modulation formats (QPSK, QAM), and coding rates. This flexibility makes resource allocation much more challenging. Dynamic control, enables on-demand reconfiguration, virtualization, and reconfiguring the optical setup poses challenges in terms of network re-optimization, spectrum fragmentation, amplifier power settings, which requires strict integration between the control elements (controllers and orchestrators) and optical monitors working at the hardware level. EON is just an example of the recent expansion of the optical communication area. Hence, more information is presented in the rest of this chapter.

The chapter is organized as follows: Section 2 provides an overview of recent OC advancements in terms of capacity, speed, and error handling. Section 3 provides a brief overview of the security issues and corresponding solutions in the physical

layer of OC. In Section 4 we describe new concepts and technologies in implementing advanced OC capabilities. Section 5 presents two examples of constraint situations where OC provides the best solution in terms of capacity, throughput, and security strength. In Section 6 we describe the use of OC for ultra-distance and ultra-secure free-space key exchange mechanisms and in Section 7 we describe in detail a unique use of OC for secured key exchange. Section 8 provides the summary and conclusions of this chapter.

## **2. OC super-channel with high speed and high capacity**

In this section, we outline recent advancements in optical communications concerning capacity, speed, and security. Recent demands for high-speed optical transmission technology triggered the development of advanced modulation formats, such as dual polarization-1024-level-quadrature amplitude modulation, ultra-fast digital-to-analog converters at the transmitter terminal, and nonlinearity intolerance. A new technology called super-channel [2], provides a feasible solution that offers very high-speed, long-distance, spectral-efficient, and large data capacity links with reliable performance. It involves the use of multiple sub-carriers for data transmission over a single-channel using dual polarization-quadrature phase shift keying (DP-QPSK). These unique modulation formats have a capacity of more than 100 Gbps over a single channel. However, they suffer from multipath fading, nonlinearity loss, and phase distortion loss, and limitation of maximum supported links. These limitations are mitigated using coherent detection and digital signal processing (DSP) at the receiver terminal for enhanced performance. In Nyquist-WDM super-channel transmission, the spectral-efficiency of the link is improved by transmitting independent wavelength channels using lower-order advanced modulation formats with channel spacing equal to the baud rate of the system. Experiments demonstrated the transmission of 1 Tbps data over a 7200 km transoceanic link with 2.86 bits/s/Hz spectral efficiency using a digital Nyquist-WDM super-channel.

The transmission of 1.232 Tbps using DP-QPSK signals with a noise-suppressed Nyquist-WDM super-channel transmission over 2100 km single-mode fiber link with DSP at the receiver terminal for enhanced performance. The performance of dual polarized-binary phase shift keying, DP-QPSK, dual polarized-8-level-quadrature amplitude modulation, and DP-16-QAM based Nyquist-WDM super-channel transmission over pure silica-core fiber with Raman amplification. In high-speed optical fiber links, the main causes of signal deterioration are Kerr nonlinearities, polarization mode dispersion, chromatic dispersion, and optical fiber cable attenuation which limit the maximum link capacity. In contrast, in FSO links, signal attenuation offered by the external environmental condition is the main factor that determines the link performance.

Optical communication is sensitive to various environmental interference and noise, leading to transmission errors [3]. The main reasons are wind misalignment, beam divergence due to propagation, weather tempering losses due to fog, smoke, and snow, atmospheric turbulence, and background noise due to artificial lights, and in FSO the optical beam position may be missed due to misalignment between the transmitter and receiver structures.

To mitigate these effects new modulation schemes have developed such as on-off keying (OOK), forward error correction (FEC), pulse width modulation (PWM), pulse position modulation (PPM), multiple PPM, digital pulse interval modulation (DPIM), binary phase-shift keying (BPSK), concatenated RS codes, short hops systems leading to performance improvements, turbo codes, low-density parity-check codes, and spatial diversity.



Practical testing and simulations [4] of PPM show that the probability of error is minimum for the maximum likelihood estimate of the stationary beam position, and for the dynamically varying beam position, a filter with a large number of particles provides a close-to-optimal probability of error performance.

### 3. OC security threats and solutions

The continuous evolution of optical networks in terms of heterogeneity, flexibility, applications, data flow volume, bandwidth, and reliable performance, raises security issues which are unique to OC. Optical networks are vulnerable to several types of security breaches aiming to disrupt the service or gain unauthorized access to the system. The evolution of programmable and flexible node architecture software has resulted in new security vulnerabilities that need to be considered during network design and operation. This section provides an overview of potential security issues in current and future optical networks and identifies possible attacks that utilize the associated vulnerabilities. It includes privacy, authentication, integrity, denial of service, and confidentiality. An attacker can snoop by tapping into the optical fiber or by interference radiated from an adjacent spectrum of confidential signals and go undetected for quite some time. An overview of common security issues and attack methods targeting optical networks is presented below.

- **Eavesdropping** is a major security attack in optical networks. Eavesdropping entails breaching the encryption key by removing the fiber coating and bending the fiber to cause the signal to leak out of the core into a photodetector that captures the information. To detect such intrusions, the network uses an intrusion detection alarm, triggered by insertion loss changes in fiber connections. Such detections require an active monitoring system that runs across the network.
- **Monitoring ports** allow access to the channel, which is available in different network components, such as amplifiers, wavelength selective switches (WSSs), or multiplexers. The optical signal is mirrored by an optical splitter to allow the connection of monitoring devices without traffic interruption. By obtaining onsite access, an attacker can use these ports to capture the carried traffic. To protect the carried data from eavesdropping, encryption is implemented in the optical transponders. Encryption keys transferred over the network are isolated from the data load.
- **Insertion of harmful signals:** service denial and quality degradation occur when harmful signals are inserted into the network, such as excessive power optical signals that exceed the signal level used in the network.
- **Jamming signals:** Networks comprising Optical Add-Drop Multiplexers (OADMs) with variable optical silencers, high-power signals can damage the co-propagating user signals inside its optical fibers, amplifiers, and switches. Jamming signals can also affect normal signals by increasing the in-band crosstalk. Signals traversing common physical links with the jamming signal can suffer from out-of-band effects. Lead to out-of-band crosstalk by leaking to adjacent channels and increasing non-linear effects and gain competition, and instead of legitimate signals the stronger jamming signals are amplified, making the situation much worse.

- **Alien wavelength attacks:** Alien wavelength [5] refers to the ability to share the same fiber-optic-line by multiple telecom-service-providers. It is possible by “dividing” the communication line into separated “colors” or wavelengths such that each “color” is considered as a separate communication channel. Each provider uses one “color” and can transmit its data concurrently with others using the same physical fiber line. This technology expands the utilization of the fiber line. The possibility of Alien Wave insertion without any impact to existing services has a big advantage to the telecom industry. Alien wavelengths are implemented in the network to allow network upgrades and efficient transmission of high-capacity connections over the existing infrastructure. When there is no alien wavelength support, each connection is terminated and regenerated by a node at the edge of the domain, while alien wavelengths can pass through multiple domains without optical conversions, which create vulnerability in network security, especially due to the lack of control on the performance of the alien channels. In such systems, alien wavelengths can be subjugated to jamming risking the network. To overcome this security hazard, a control system is required to block any unauthorized messaging.
- **Mixed line rate (MLR)** networks enable the coexistence of different modulation formats in the same infrastructure. A severe security vulnerability of MLR networks stems from nonlinear effects between high-speed and low-speed signals of adjacent channels. Amplitude-modulated on-off-keyed (OOK) 10G channels deteriorate the quality of the higher bitrate, due to cross-phase modulation (XPM). This entails an extra penalty for the higher speed channels, depending on the modulation format and channel launch power. A service degradation attack in MLR networks is caused by inserting an OOK channel nearby a high-speed channel, without allowing sufficient guard band. Thus, the attacking signal could significantly deteriorate the legitimate signals.
- **Software-defined networking (SDN)** manages the interface between the hardware and the SDN applications, including traffic engineering and data collection applications. Malicious attackers who can gain access to the data potentially may hijack the network.
- **Architecture on Demand (AoD)** uses an optical backplane to support inter-connections among optical modules enabling the use of these modules, which are required for switching and processing. New modules are added to a node by plugging them into the optical backplane. This modularity exposes the network to security vulnerabilities.

Network Coding (NC) proposed to cope with physical OC security issues:

Network Coding (NC) is used in optical networks for protection against link failures, to improve spectral efficiency in multicasting, and protect confidential connections against eavesdropping attacks. The confidential signals are XOR-ed with other signals transmitted via different nodes in their path through the network. The signals are combined either at the source node or at intermediate nodes. To implement NC for confidential connections, a set of constraints for the NC and RSA are incorporated in the corresponding algorithms. The combination of signals through NC increases the security of confidential connections since an eavesdropper will receive a combination of signals from different connections, complicating the decryption of the confidential signal. Experiments show that NC provides comprehensive security envelop for confidential connections with minimum spectrum usage.

Using NC, connection data is merged with other connection data, generating a network-code that changes based on the connection's transmitted data. Encrypted Transmission (ET) relates to all links of the selected path transmitting an encrypted version of their data with at least one XOR operation with other established connections. To satisfy the ET constraint, an established connection has at least two common nodes with a confidential connection. The Frequency Slot Matching (FSM), which is a subset of the frequency slots utilized by the confidential connection, must have the same id and frequency as the slots of the rest of the established connections used in the XOR operations. It is assumed that the signals used for the XOR operation are on the same frequency. Thus, an established connection with at least two common nodes with the confidential connection can either provide security for the entire path of the confidential demand (source and destination as common nodes), or it can provide security for part of the connection (source/intermediate node to intermediate/destination node). For a confidential connection to be considered secure, the selected established connections must collectively secure all links of that connection. The confidential connection is considered as secure even if only part of the signal is XOR-ed since the eavesdropper would still have to access all connections used in the encryption process to decrypt the transmitted data.

#### **4. Selected technologies in implementing OC capabilities**

The demand for very large capacity and high-speed channels for heavy data transmission is growing increasing the demand for quick solutions. As a result, we are witness to a wide variety of proposed solutions using optical fiber and free-space wireless channels. Several solutions that have successfully coped with the transmission demand and the security challenges are presented below.

##### **4.1 OAM multiplexing for high capacity secured optical communications**

In this section, we outline recent advances in the use of Orbital Angular Momentum (OAM) to increase transmission capacity and speed [6]. It employs the orthogonality among OAM beams to enable efficient demultiplexing. Free-space communication links are widely used for data transfer applications, using optical communication or radiofrequency (RF) waves. The capacity of a communication system is increased by multiplexing and simultaneously transmitting multiple independent data streams. This is done by using the properties of the electromagnetic (EM) wave, such as time, wavelength, and polarization. Multiple data streams can be efficiently multiplexed and demultiplexed. To cope with the increasing demand for very high bandwidth, new forms of data channel multiplexing are used. One approach utilizes orthogonal spatially overlapping and copropagating spatial modes, where multiple channels, each identified by a different spatial mode, are multiplexed at the transmitter and separated at the receiver. The transmission capacity and spectral efficiency are increased by a factor equal to the number of transmitted spatial modes. Each data symbol is sequentially transmitted by a different OAM beam, within each time slot. A group of orthogonal OAM beams is used to spatially multiplex multiple data streams. Combining OAM multiplexing with polarization we can get very high xTpbs speed communications such as four OAM beams on each of the two orthogonal polarizations are combined resulting in multiplexed eight OAM modes. The received OAM beams are then de-multiplexed at the receiver and sequentially detected to recover the data streams. All eight OAM data channels are located on the same wavelength, providing spectral benefits. Then the experiment was expanded by adding the wavelength dimension, simultaneously

using OAM, polarization, and wavelength for multiplexing. A total of 1008 data channels were carried by 12 OAM values, two polarizations, and 42 wavelengths. Each channel was encoded with 50GBd quadrature phase-shift keying, providing an aggregate capacity of 100.8 Tbps. An additional experiment described the multiplexing process where multiple independent data channels, each on a different OAM beam, are spatially combined, and the resulting multiplexed OAM beams are then transmitted via a single aperture towards the receiver. After coaxially propagating through the same free-space channel, the arriving beams are collected at the receiver by another slot, and subsequently demultiplexed and detected for data recovery.

## **4.2 Chaos-based high-speed and high bandwidth secure OC**

Chaotic systems provide physical layer security in secure OC [7]. This began with a data rate of 2.4 Gbps for a distance of 120 km, and later was improved to 10-Gbps for a 100-km optical fiber link and even further to 30-Gbps secure transmission over 100 km using a chaotic carrier with a bandwidth of 10 GHz. The transmission capacity of chaos-based secure communication is limited by the bandwidth of the chaotic carrier. The wider the bandwidth of the chaotic carrier the higher the transmission rate it supports. To enhance the bandwidth of chaos, several methods have been proposed such as optical injection, mutual injection, fiber propagation, feedback with parallel-coupling ring resonators, heterodyning couplings, and self-phase-modulated feedback with microsphere resonator.

Following is a description of an enhanced wideband chaos generation scheme. To increase bandwidth, it is using an external-cavity semiconductor laser (ECSL) subject to optical-electronic hybrid feedback. The output is used to modulate the output of a continuous-wave laser by an electro-optical phase modulator. The constant-amplitude self-phase-modulated light is then inserted back into the ECSL. Experiments indicate that the effective bandwidth of the generated chaos is increased to over 20 GHz, and the spectrum flatness and the complexity of the generated chaos. The experiments demonstrated that high-quality synchronization between two wideband chaos signals with an effective bandwidth greater than 20 GHz is achieved, showing the valuable potential in chaos-based secure communication, such as enhancing the transmission capacity and improving the security. The experiments prove that the significant bandwidth and the complexity enhancement of chaos are achieved in the proposed chaos generation scheme. Results indicate that the proposed scheme can easily obtain a wideband chaotic signal with an effective bandwidth larger than 20 GHz.

## **4.3 Intensity modulation signals for physical layer security of optical communications**

The huge volume of data transmitted over optical networks requires the integration of a data protection mechanism adapted to the specific attributes of optical fiber communications. Y-00 [8] quantum-noise randomized stream cipher is built to prevent attackers from capturing the transmitted encrypted text. It merges the mathematical encryption of multi-level signaling and the physical randomness, thereby providing high performance and robust security. It uses extremely high-order modulation together with quantum and additive noises. The achieved secrecy level is high as the probability of the attackers guessing the encrypted data is very low. Experiments show that the Y-00 cipher transceiver on a 1000-km transmission range, with a data rate of 1.5-Gbps and using analytical high secrecy, performed successfully.

Y-00 cipher is a symmetric key encryption method combined with multi-level signaling of physical randomness to hide the transmitted ciphertext. A receiver recovers the original signal of plaintext from the cipher signal masked with noise using a shared key and mathematical signal processing. The light from a laser diode enables the cipher signal transmission to the receiver. The Quantum/ASE randomized noise cipher is dominant when the Y-00 cipher communication system is used in a long-haul link using optical amplifiers. Hence, masking the signal with an additive quantum noise is more robust against attackers and is a practical advantage compared to classical cryptography utilizing just mathematical encryption. The probability that an attacker will guess the correct encrypted text is considerably low under such assumptions.

#### **4.4 Optical wireless communication (OWC), the underlying technology for 5G and IoT**

The availability of 5G communications and the Internet of Things (IoT) exponentially increase the number of devices connected to the internet, generating a huge volume of transmitted data [9]. The main features of the 5G communication services include high capacity, low latency, high security, vast device connectivity, low energy consumption, and high quality of experience (QoE). OWC seems to satisfy the derived requirements by its unique attributes: wide spectrum, high-data-rate, low latency, high security, low cost, and low energy consumption. OWC contains visible light communication (VLC), light fidelity (LiFi), optical camera communication (OCC), and free-space optics (FSO). Its technologies may play the role of sensing, monitoring, and resource sharing in comprehensive device connectivity of IoT, and meet 5G and IoT high-security requirements. Hence, OWC is the right fit for 5G and IoT.

The VLC uses light-emitting diodes (LEDs) or laser diodes (LDs) as transmitters and photodetectors (PDs) as receivers. Only visible light (VL) is used as the communication medium in the VLC. LiFi provides high-speed wireless connectivity along with illumination and uses LEDs or defuse LDs as transmitters and PDs as receivers. It uses VL for the forward path and infrared (IR) as the communication medium for the return path. The OCC uses a LED array as a transmitter and a camera as a receiver. FSO uses LD and PD as the transmitter and the receiver, respectively. It is normally operated using Appl. Sci. IR as the communication means but can also use VL and UV. There are several OWC technologies. The differences between these technologies are very specific. The unique characteristic of VLC is the use of visible light as a communication media. A LiFi system supports seamless mobility, bidirectional communication, and point-to-multipoint, as well as multipoint-to-point communications. The OCC system uses a camera or image sensor as a receiver among all the OWC technologies. The OCC uses an LED array or light as a transmitter and a camera or image sensor as a receiver. OCC normally uses VL or IR as the communication medium.

The transmission rate of the 5G mobile communication systems is expected to reach an average of 1 Gbps at a 10 Gbps peak rate. An external network hacker device cannot pick up the internal optical signal. The information can be exchanged in a highly secure manner. In summary, the OWC systems offer a higher level of security for the 5G/6G and IoT networks.

### **5. Unique implementations of OC under constraints**

The incorporation and spread out of OC technologies are dictated by the benefits and impact it is expected to achieve. Hence, most of the efforts are towards the

long-distance, high capacity, high bandwidth, and high data rate. However, some efforts are put towards local solutions and small-scale implementations. The following are two examples of such implementations.

### **5.1 OC for short distance high-speed data transmission**

Data-center networks have much shorter transmission distances but much higher transmitted data than common network topologies [10]. Therefore, traditional telecommunication components are redundant and costly. Consequently, VCSELs, active optical cables, and parallel fiber transmission are used by data centers. With the significant increase in traffic inside the data center, the required bandwidth is increasing dramatically. Broadband optical modulators such as electro-absorption modulators (EAMs) and Mach-Zehnder modulators (MZMs) in combination with colored distributed feedback laser arrays are combined to build and Ultra-high-bandwidth and low energy links based on WDM technology. To further increase to Tbps bandwidth, a large number of lasers are used.

Another improvement is gained by using Optical switches which are completely different from electronic packet switches but when combined they complement each other. Hence, optical switches and conventional electronic switches are combined in the same architecture generating improved performance. Optical switches are used to adapt the network to specific traffic patterns, such as pairs of nodes exchanging high traffic levels that can have more bandwidth when using optical networks. However, the reconfiguration of an optical switch requires phase-locking and modifications of the routing tables. To overcome this issue and improve performance, optical reconfigurations are fully automated. Improving the utilization of the resources by reconfiguration of disaggregated elements enables the reduction of components and energy consumption by putting underused components in a sleep mode. It is possible to mitigate network congestion resulting from intense communications between servers or rack pairs by overprovisioning the network.

### **5.2 Integrating OC and mobile devices used in the automotive and drone industry**

**Automotive:** Until a few years ago, only minor improvements have been implemented in the data networks used in vehicles. The introduction of autonomous vehicles and smart cities has increased the demand for automation of vehicles and inter-vehicle communication [11]. This involves the reliable transmission of data with high rates in real-time and secured from interfering signals and security attacks. Existing and vehicle-bus-communications are insufficient, and a replacement of the vehicle communication infrastructure is inevitable. Optical data communication has been implemented as it transmits high amounts of data, can multiplex several signals into a single fiber, and is robust against external effects, with little attenuation. This confirms that optical busses are very useful for automotive applications. The solution is based on a central processing unit CPU connected to the optical hybrid data bus, which comprises several fibers. To improve reliability, safety, and security, separate fibers are used for different applications and functionalities such as multimedia and sensors. The CPU forwards messages to the different fibers. In automotive applications assigning priorities to messages is required for accurate functionality. Therefore, SCTP is used as it supports ordering messages and it provides redundant paths to increase reliability. SCTP uses heartbeats to check if a connection is still valid. If a node fails, the connection will find another path, if available. The SCTP protocol also has additional security features and adaptability, which will support new vehicle communication requirements in the future.

**UAV:** [12] In recent years the availability and common use of drones have increased, especially the grouping of drones to perform a common task, which requires ongoing precise synchronization of the engaged drones in real-time. This is achieved by a platform of high speed and high capacity communication channels that virtually connect these drones. A technology that benefits from both, optical data rates and the mobility of drones is required. Free-space optical (FSO) communication supports the optical wireless signal transmission from the infra-red band spectrum in outdoor environments. This combined with the mobility-based outdoor communication system is the correct direction that should be considered. Optical Wireless Communications (OWC) embedded in Unmanned Aerial Vehicles (UAV) is the compound technology used.

## **6. Quantum key-distribution (QKD) using OC**

QKD uses light-paths via optical fibers to share encryption keys between two remote parties [13]. The key-updating process and the key adaptive routing have dedicated paths protected from link failures. Sharing quantum keys between satellites requires communication channels among microsatellites capable of transmitting keys within constellations of trusted satellites. Using optical links with 10-yard pointing accuracy allows QKD of an inter-satellite distance of 400 km. In entanglement based QKD, pairs of entangled photons are generated and sent to two separate parties, where each is sent one photon from each pair. The two parties independently make measurements on a preselected property of their polarization state. Once many such pairs have been distributed and measured, the two parties perform statistical tests and ask if the received photons were entangled. Provided the entanglement measured exceeds a predefined threshold and their hardware is free of vulnerabilities, they can be sure that the security of the protocol. Then they use their private knowledge of the quantum states as a common source of entropy to derive symmetric keying material for encryption schemes.

A Quantum Module (QM) is a polarization-entangled photon-pair source and single-photon detectors that can operate as a qubit transmitter or receiver. The transmitting QM locally measures and timestamps one of the photons in each pair and sends the other photon of each pair to the receiver, where it is detected and timestamped by a receiving QM. These timestamps and measurement outcomes are used to synchronize the detections and subsequently to create a symmetric encryption key. The QM contains a laser diode that initiates spontaneous-parametric-down-conversion in beta-barium-borate crystals generating pairs of photons with specific wavelengths. The photons in each pair are entangled such that their polarization states are undefined until a measurement is made, at which point they will have correlated polarizations. In the transmitter QM, “signal” photons are transmitted, and the “idler” photons are detected within the QM by silicon avalanche photodiodes. Both satellites have a QM and both can send and receive entangled signal photons. The two satellites use a beacon laser and a beacon detector to monitor the other satellite’s beacon and control the relative pointing between them. A beam pointing correction signal is provided to a two-axis fast steering mirror, which compensates for high-frequency beam misalignment between the two spacecraft and optimizes the optical link for the transmission of entangled photons. The optical bench provides thermal and mechanical isolations and it is attached to the spacecraft structure. The reaction wheels have been placed, so that their spin axes are as near as possible to the center of gravity to minimize jitter of the pointing stability of the telescope.

## **7. Secured key-distribution using optical communication**

Key distribution is a growing concern for symmetric cryptography. Most of the current key-distribution mechanisms assume the use of the Internet and WAN public networks, which are exposed to security risks. Robust cryptographic mechanisms, such as Diffie-Helman (DH) and RSA algorithms are used along with Certificate Authority (CA), which generates certificates and distributes them simultaneously to the sender and receiver via alternate channels. These existing solutions are limited. DH and RSA are at threat since the introduction of Quantum computing and PKI/CA are effective in relatively local cases. Hence, new ideas are required. This section introduces a new approach for a safe key transmission using high-speed optical camera communication (OCC), Visible light communication (VLC) is a type of wireless communication. The data is transmitted through modulating the visible light spectrum. The key transfer is done using VLC with blinking LED lights in a specific sequence and frequency, following a coding system. The receiver decodes the received blinks to a bit string using a corresponding image processing application. Optical communication ensures secure transfer without the ability to quote it. Experiment results show that this method is feasible, robust, efficient, and implementable.

### **7.1 Introduction**

In symmetric cryptography, the same key is used for encrypting and decrypting the exchanged data. Sharing the same key requires a key transmission between the sender and the receiver. To avoid key discovery while transmitted, several protocols have been proposed, such as the Diffie-Hellman protocol and Asymmetric Cryptography such as RSA. The evolution of Quantum Computing makes redundant any known cryptography. Using a reliable third-party able to generate certificates and encryption keys and simultaneously distributes it to the two parties who intend to exchange data. It is using alternate distributing channels different from the channel the two parties use for transferring the data. However, due to the growing globalization and growing distance among users and systems, and the introduction of cloud computing, this approach is complicated to manage and so became irrelevant over time. A secured key transition uses an optical communication platform.

### **7.2 Related work**

Optical communication is simple, low cost and secured signal transmission. One of the technics is based on under-sampled differential phase shift on-off keying that can encode binary data. Arai et al. [14] define a new framing approach for high-speed optical signals transmission for road-to-vehicle communication. Luo et al. [15] use dual LED to triple the data rate transmission. Roberts [16] proposes encoding/decoding, using camera-subsampling synchronized with the camera frame rate. Leu et al. [17] introduce a new modulation scheme where the phase difference between two consecutive samples represents one-bit data.

### **7.3 Optical camera communications (OCC)**

The optical communication technique called Optical Camera Communications (OCC) is described in [18]. OCC allows the use of huge unregulated bandwidth in the optical domain spectrally located between microwave and X-ray wavelengths, as shown in **Figure 1**. In such a system, an image sensor and a camera are used



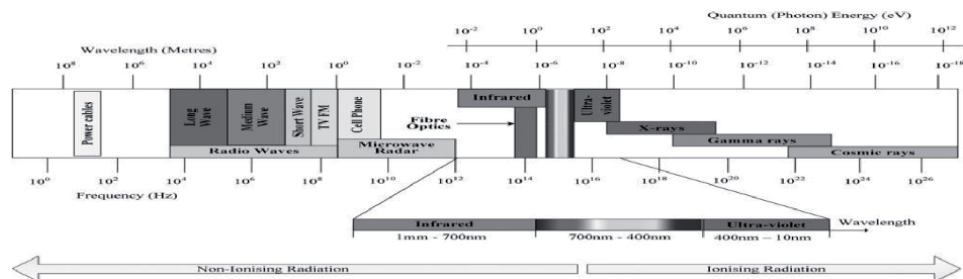
to demodulate the transmitted signal which has been modulated according to on-off keying (OOK). Currently available devices are smart devices equipped with LED flash and cameras. This provides a pragmatic form of an Optical Wireless Communication (OWC) where LED projectors provide the Visible Light spectrum (VLC) component and a camera as the receiving module, building a transceiver pair.

The OCC system uses commercial LED lighting sources that include, LED-based infrastructure lighting, LED flashes, LED tags, displays, laser diodes, image patterns, some current generation projectors. The major driving forces of OCC deployment are the widespread availability of visible light (VL) LEDs and the possibility of utilizing the camera in the smart devices to decode LED modulated data. Therefore, these LED infrastructures can be used for data transmissions using on-off keying (OOK).

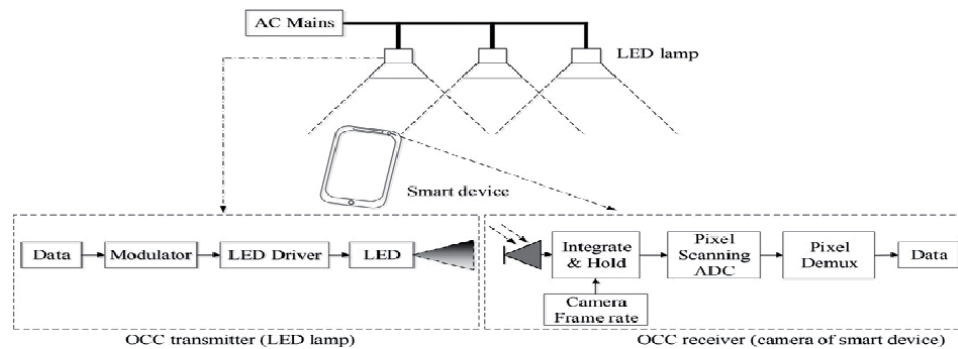
A typical OCC system is shown in **Figure 2**, where a camera is used as a receiver, which consists of an imaging lens, image sensor, and readout circuit.

### 7.4 Optical camera communication architecture

Optical communication comprises a LED, Infra-Red, or Laser projector and a high-speed camera embedded in a mobile phone. The projector projects a beam of light to the direction of the camera. The camera has an embedded CMOS image sensor capturing the projected beam. The beam on/off projection duration and frequency is according to an encoding pattern agreed with the receiving camera. The receiving camera records in a video the projection session and saves it in its internal storage. The recorded projection is decoded into bits, where for an "on" beam the corresponding decoding bit is set to "1", otherwise it is decoded as "0". The video in



**Figure 1.**  
 Electromagnetic spectrum range.



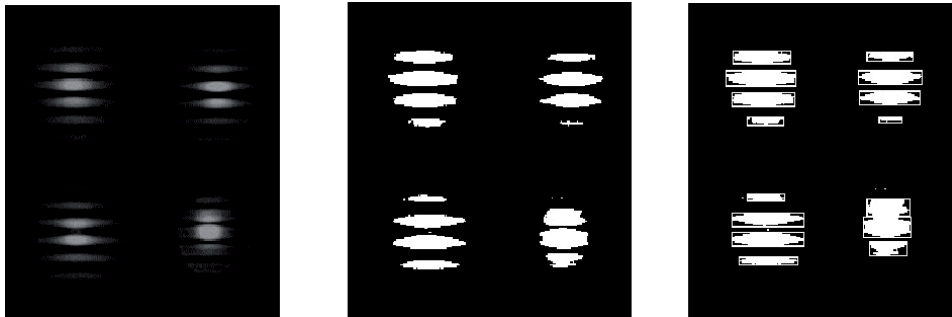
**Figure 2.**  
 A schematic view of the OCC system.

the camera can be further transmitted to the target receiver through a public network connection. The beam may be visible (normal lighting) or invisible (Infra-Red and Lazier). The illumination duration and frequency are so fast that a human eye is not able to follow and quote it. When the CMOS image sensor is operated, images are captured. These images are the source for extracting data by decoding it. **Figure 3** depicts the three phases of the received signal processing. The left image is the originally recorded beam impact, the image to the right is the original image after it was crystallized, and the third image to the right describes the final stage of the process. The third image is the input for decoding the beam stream into a bit string.

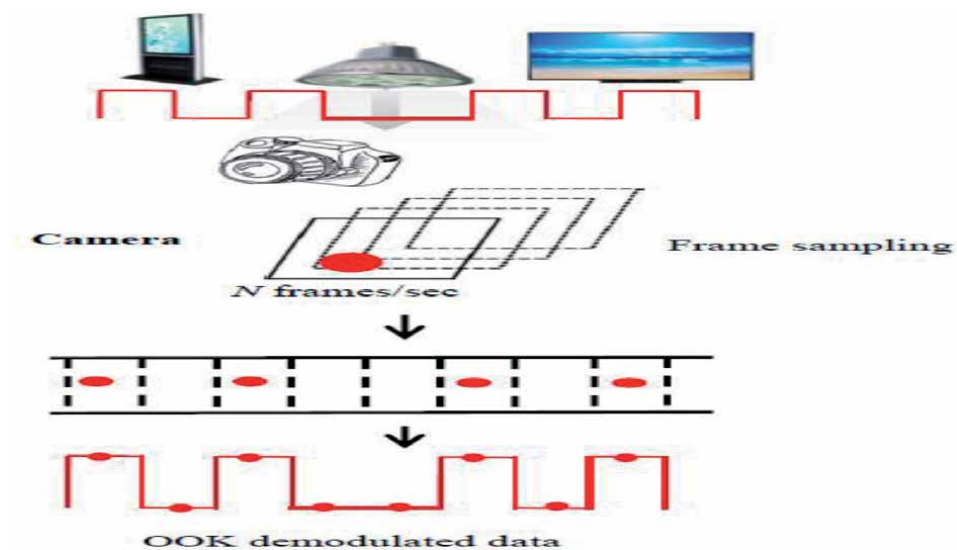
**Figure 4** depicts the encoding process, starting from processing the image and translating it into a sequence of a signal chart (the top chart). The bottom chart depicts the final bit sequence.

### 7.5 System architecture

The objective of this work is to securely exchange keys utilizing optical communication, where the LED transmits, and the camera collects it. The idea is to modulate the information in a way that cannot be decoded only by processing the received



**Figure 3.**  
*Three phases of fringe signal processing.*

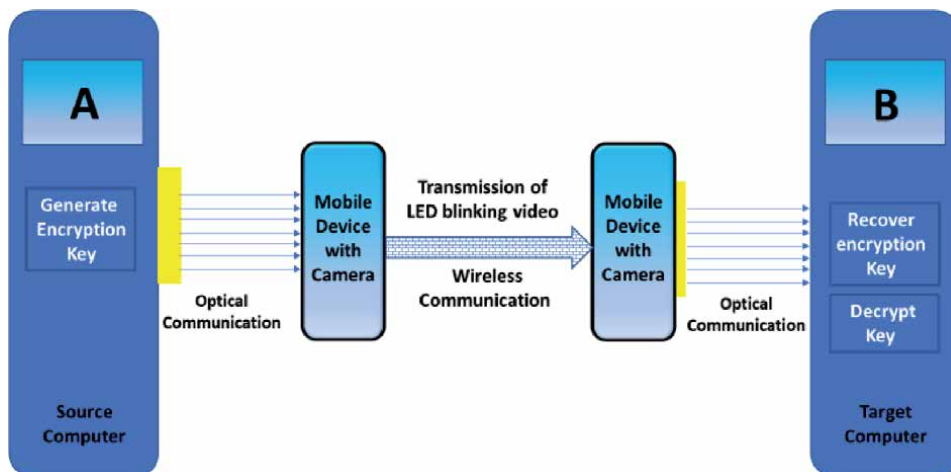


**Figure 4.**  
*Optical camera communication architecture.*

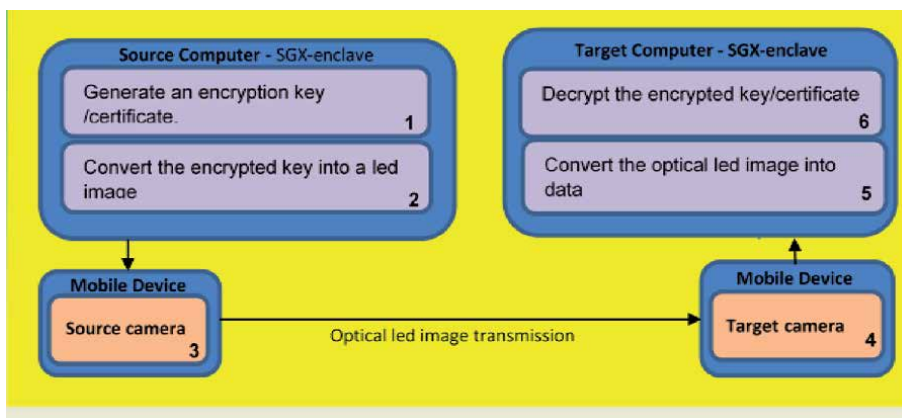
signals. **Figure 5** illustrates the basic idea of the optical-based communication approach. The source computer generates an encrypted key. The key is translated to optical signals, which are projected by the LED projector to the targeted camera, embedded into a mobile device. The camera captures the optical signals and records it as a video movie. For authentication and accuracy, the video movie is signed by a standard electronic signature and the signed video is encrypted and transmitted via VPN to the target mobile device, which then projects the original signed-video to the target computer. The target computer decrypts the received video signals into a sequence of bits and thus the encrypted key reaches the target computer. We may consider moving the mobile device itself towards the target computer avoiding the key transmission.

**Figure 6** outlines the 6 stage process. In stage 1, the key is generated and transformed into a LED code in stage 2, and then in stage 3, it is projected to the receiver camera. In stage 4, the received video is transferred to the target computer and in stage 5, the images are decoded into the encryption key. In step 6, the original key is discovered and forwarded for further use.

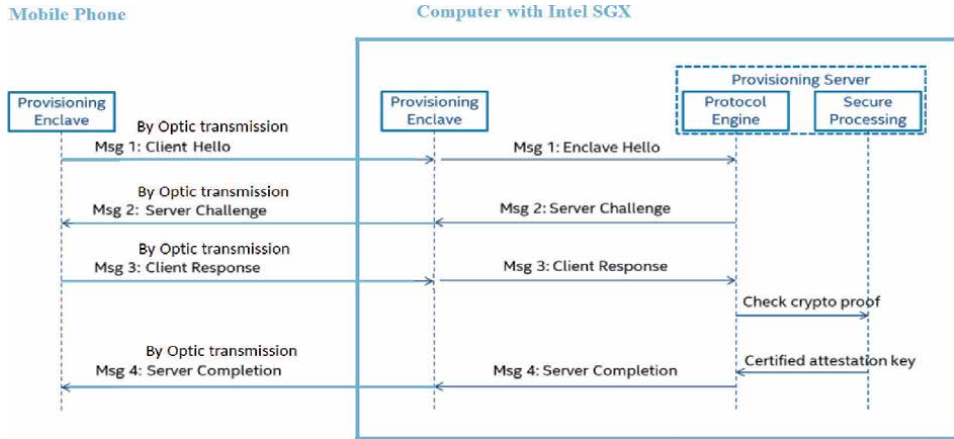
**Figure 7** depicts the messaging protocol between the mobile and the computer.



**Figure 5.**  
 High level secured key transmission system.



**Figure 6.**  
 Optical-based key transmission stages.



**Figure 7.** Provisioning message flow protocol.

This way of transmitting optical signals instead of a bit-string, adds to the key exchange security level comparing to other solutions. However, the transmitted content is much more than a bit string. The practical impact is reasonable based on a moderate frequency of key changes and the availability of high capacity and high-speed communication.

### 7.6 Experiment and results

For the experiment we used a USB connected blinking LED device controlled by an Arduino code and an embedded Linkit ONE hardware. The encoding/decoding is simple, “1” bit is set when the LED blinks, and “0” otherwise. The key is transmitted to the USB device, the *Serial.exe* program receives it and converts it into an ASCII code. Before starting the key transmission, a unique bit string is sent. A developed application accepts the sequence of the blinking LED, processes it to produce a bit sequence, and converted into an ASCII code. A lit LED is processed by the OpenCV image processing such that each non-white pixel turns to 0 while white remains 255. Then, all pixels are summed up. If the sum is 0, the LED remains “off”, and the output is a “0” bit. Otherwise, the output is a “1” bit.

We ran the entire cycle. The key was generated in a secured environment, then transmitted a bit string to the USB blinking device. The mobile phone camera recorded the video of the blinking sequence. The mobile phone signed, encrypted, and transmitted the blinking LED video, the receiver mobile device in the target location, accepted the blinking video, and transformed it into a bit string. We experimented with the “a b c d” key transferred between a host with an optical USB device and a smartphone with a camera. **Figure 8** depicts the output of the “abcd” transmission where lines 3, 6, 9, 12, and 15 represent the output “abcd” respectively.

**Figure 9** depicts the key transmission example “abcd” used in the experiment. The four images have been taken during the live key transmission stages.

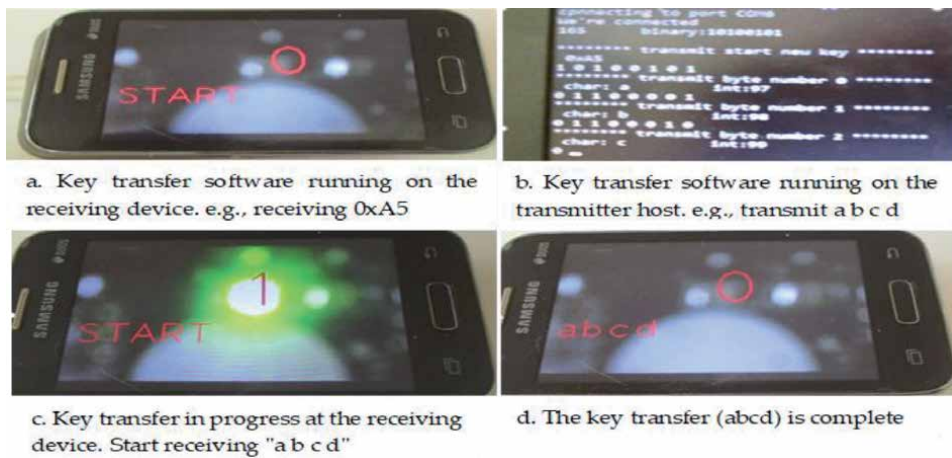
In image a, the starting special bit string has been accepted by the mobile device connected to the sending computer. Image b shows the sender computer screenshot during the key transmission to its associated mobile device. Image c is the mobile-screen accepting the “abcd” key, and image d depict the acceptance of the transmitted key.

In this section, we introduced a complete cycle of secured key exchange using a form of optical communication. We described the hardware components and

```

***** transmit start new key *****
0xA5
1 0 1 0 0 1 0 1
***** transmit byte number 0 *****
char: a int:97
0 1 1 0 0 0 0 1
***** transmit byte number 1 *****
char: b int:98
0 1 1 0 0 0 1 0
***** transmit byte number 2 *****
char: c int:99
0 1 1 0 0 0 1 1
***** transmit byte number 3 *****
char: d int:100
0 1 1 0 0 1 0 0
    
```

**Figure 8.**  
 Example of the key transmission.



**Figure 9.**  
 Captured images of the live key transmission stages.

software of the conducted experiment. This demonstrates the applicability of an Optical Communication (OC) assisted method for secured key distribution [18].

## 8. Summary and conclusions

In this chapter, we outlined advancements in the Optical Communications subject matter. We focused on OC main improvements, transmission channel, and method, bandwidth, speed, and security. We concluded the chapter with detailed unique use of OC for key transmission required for symmetric cryptography. OC technology is still at its development and growth stage. We expect it to continue its fast growth and be implemented in many more domains, transforming our lives to be much more convenient, safe, and automated.

**Comment:** Due to the comprehensiveness and wide-ranging scope, this chapter outlines just part of the advancements in OC leaving issues such as underwater OC [19] and Machine learning for OC [1] out of scope.


### **Author details**

Menachem Domb  
Computer Science Department, Ashkelon Academic College, Ashkelon, Israel

\*Address all correspondence to: [dombmnc@edu.aac.ac.il](mailto:dombmnc@edu.aac.ac.il)

### **IntechOpen**

---

© 2020 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

## References

- [1] F. Musumeci et al., "An Overview on Application of Machine Learning Techniques in Optical Networks," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1383-1408, Second quarter 2019, DOI: 10.1109/COMST.2018.2880039.
- [2] Mehtab Singh, Jyoteesh Malhotra, M.S.Mani Rajan Vigneswaran Dhasarathan Moustafa H. Alyc Performance evaluation of 6.4 Tbps dual-polarization quadrature phase-shift keying Nyquist-WDM super-channel FSO transmission link: Impact of different weather conditions, Elsevier, Alexandria Engineering Journal, Volume 59, Issue 2, April 2020, Pages 977-98
- [3] A.Mansour, R.Mesleh, M.Abaza, New challenges in wireless and free-space optical communications, Elsevier, Optics and Lasers in Engineering, Volume 89, February 2017, Pages 95-108
- [4] M. S. Bashir and M. R. Bell, "The Impact of Optical Beam Position Estimation on the Probability of Error in Free-Space Optical Communications," in *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 3, pp. 1319-1333, June 2019, DOI: 10.1109/TAES.2018.2869506
- [5] Alien wavelength technique to enhance Garr optical network, Paolo Bolletta, Massimo Carboni, Andrea Di Peo, Americo Gervasi, Lorenzo Puccio, Gloria Vuagnin, Cornell University, arXiv:1805.05811v1 [cs.NI], 2018
- [6] Alan E.Willner<sup>1</sup>, Yongxiong Ren<sup>1</sup>, Guodong Xie<sup>1</sup>, Yan Yan<sup>1</sup>, Long Li<sup>1</sup>, Zhe Zhao, JianWang, Moshe Tur, Andreas F. Molisch and Solyman Ashrafi, High-capacity free-space optical and radio-frequency communications using orbital angular momentum multiplexing, [doi.org/10.1007/978-3-030-26118-4\\_26](https://doi.org/10.1007/978-3-030-26118-4_26), ISBN978-3-030-26117-7,
- ISBN978-3-030-26118-4, Springer, Cham, 2019
- [7] S. Donati and V. Annovazzi-Lodi, "From order to chaos and back: Recent advances in optical cryptography of transmitted data," 2013 International Conference on Advanced Optoelectronics and Lasers (CAOL 2013), Sudak, 2013, pp. 1-6, DOI: 10.1109/CAOL.2013.6657507.
- [8] F. Futami, K. Tanizawa, and K. Kato, "Y-00 Quantum-Noise Randomized Stream Cipher Using Intensity Modulation Signals for Physical Layer Security of Optical Communications," *J. Lightwave Technol.* 38, 2774-2781 (2020)
- [9] Chowdhury, M.Z.; Shahjalal, M.; Hasan, M.K.; Jang, Y.M. The Role of Optical Wireless Communication Technologies in 5G/6G and IoT Solutions: Prospects, Directions, and Challenges. MDPI and ACS, Appl. Sci. 2019, 9, 4367
- [10] Celik, A., Shihada, B., & Alouini, M.-S. (2019). Optical wireless data center networks: potentials, limitations, and prospects. *Broadband Access Communication Technologies XIII*. DOI:10.1117/12.2507643
- [11] D. Kraus, E. Leitgeb, T. Plank and M. Löschnigg, "Replacement of the Controller Area Network (CAN) protocol for future automotive bus system solutions by substitution via optical networks," 2016 18th International Conference on Transparent Optical Networks (ICTON), Trento, 2016, pp. 1-8, DOI: 10.1109/ICTON.2016.7550335.
- [12] Petkovic M., Narandzic M. (2019) Overview of UAV Based Free-Space Optical Communication Systems. In: Ronzhin A., Rigoll G., Meshcheryakov R. (eds) *Interactive*

Collaborative Robotics. ICR 2019. Lecture Notes in Computer Science, vol 11659. Springer, Cham. [https://doi.org/10.1007/978-3-030-26118-4\\_26](https://doi.org/10.1007/978-3-030-26118-4_26)

[13] Denis P. Naughton, Robert Bedington, Simon Barraclough, Tanvirul Islam, Doug Griffin, Brenton Smith, Joe Kurtz, Andrey S. Alenin, Israel J. Vaughn, Arvind Ramana, Igor Dimitrijevic, Zong Sheng Tang, Christian Kurtsiefer, Alexander Ling, Russell Boyce, Design considerations for an optical link supporting inter-satellite quantum key distribution, *Optical Engineering*, 58(1), 016106 (2019). <https://doi.org/10.1117/1.OE.58.1.016106>, 9 January 2019

[14] S. Arai, S. Mase, T. Yamizato, T. Yendo, T. Fujii, M. Tanimoto, and Y. Kimura, Feasible Study of Road-to Vehicle Communication System using LED Array and High-Speed Camera, 15th World Congress on Intelligent Transport Systems and ITS America's 2008 Annual Meeting, Nov. 2008, pp. 1-12.

[15] P. Luo, Z. Ghassemlooy, H. L. Minh, X. Tang, H-M. Tsai, Undersampled Phase Shift ON-OFF Keying for Camera Communication, WCSP 2014, Oct 2014, pp. 1-6. IEEE

[16] R. D. Roberts, Space-time forward error correction for dimmable undersampled frequency shift ON-OFF keying camera communications (CamCom), Fifth International Conference on Ubiquitous and Future Networks (ICUFN), pp: 459-464, July 2013.

[17] N. Liu, J. Cheng, J. F. Holzman, Undersampled differential phase shift on-off keying for optical camera communications with phase error detection, 13th International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE Xplore, July 2017

[18] Domb, M.; Leshem, G. Secured Key Distribution by Concatenating Optical Communications and Inter-Device Hand-Held Video Transmission. *MDPI and ACS Style Appl. Syst. Innov.* 2020, 3, 11.

[19] Schirripa Spagnolo, G.; Cozzella, L.; Leccese, F. Underwater Optical Wireless Communications: Overview. *Sensors* 2020, 20, 2261



---

Section 2

# Security Analysis

---



# Survey and Analysis of Lightweight Authentication Mechanisms

*Adarsh Kumar and Deepak Kumar Sharma*

## Abstract

Interconnection of devices through Radio Frequency Identification (RFID) brings enormous applications that are increasing constantly day by day. Due to the rapid growth of such applications, security of RFID networks becomes crucial and is a major challenge. Classical or lightweight cryptography primitives and protocols are the solutions to enhance the security standards in such networks. Authentication protocols are one of the important security protocols required to be integrated before exchange of secured information. This work surveyed the recently developed authentication protocols. Further, classifications, security challenges, and attack analysis are explored. A comparative analysis of different types of authentication protocols explains their applications in resourceful and resource constraint Internet of Things (IoT). Authentication protocols are categorized into: symmetric, asymmetric, lightweight, ultra-lightweight and group protocols. Symmetric and asymmetric protocols are more suitable for resourceful devices whereas lightweight and ultra-lightweight protocols are designed for resource constraint devices. Security and cost analysis shows that asymmetric protocols provide higher security than any other protocol at a reasonable cost. However, lightweight authentication protocols are suitable for passive RFID devices but do not provide full security.

**Keywords:** authentication, authorization, cost analysis, cybersecurity, lightweight cryptography, primitives, protocols

## 1. Introduction

Kevin Ashton in 2009 proposed an interconnected network of uniquely identifiable objects, devices, and different types of systems called IoT [1]. Some of the important features of IoT are self-configuration, sensing, ad-hoc networking, automatic identification, etc. [2]. In IoT, each object has a unique address and identification. Here, mostly RFID is preferred for assigning an address and unique object identification. The information, captured by IoT objects, is propagated through the internet to other objects. The information communicated captures the current events and responses. The revealed information further requires human intervention to control the results [3]. Several objects are involved to form the interconnected network: RFID devices, sensors, mobiles, back end storage, etc. Resourceful and resource constraints are the types of IoT devices. In resourceful devices, there are sufficient software and hardware resources. There are some hardware and software resource limitations in resource constraint devices. The role

of the devices changes with the condition. For example, a metro smart card authenticates the passenger at the entry point, the same card authenticates exit after deducting a charge for the travel. Using the same smart card, information of daily passenger traveling systems is stored in a database server and helps in train counting. Library management, supply chain management, and inventory control systems are some of the applications of RFID enabled things. Here, users are validated using authentication protocols. Unauthenticated users are disallowed to enter into the system. The observation system is maintained to analyze the possibilities of intrusions by unauthenticated users.

There are different types of authentication protocols. Cryptographic primitives, like AES, RSA, SHA, etc. are used in resourceful devices for authentication and authorization. Lightweight primitives and lightweight protocols are the different types of lightweight cryptography [4]. Stream cipher, hash function, block cipher, pseudo-random number generation, etc. are included in symmetric primitives whereas asymmetric primitives include discrete logarithmic constructions, number based systems, and curve based cryptosystems. Authentication, yoking, identification, tag ownership protocols, distance bounding, etc. are some classes of lightweight protocols. Up to 30% of gate equivalents (GEs) can be used in resource constraint devices for cryptographic [5, 6]. With the advancement of technology, the GEs also increase [7].

Tags, readers, and data centers are the three types of RFID devices. Information is written over tags and readers are used to read the information. If required, data center is used for storing the information; otherwise, it is communicated to other objects to increase the information availability. The behavior of readers is similar to duplex links. These devices use different procedure for storing data. The tags get power from these devices and have longer information availability range. Tags, passive, semi-passive, active follows the cryptography procedures as implemented [8]. Passive tags do not have their source of power. These tags have low costs and low memory. These are more suitable for short range. Information on these devices is read many times after writing it for once [9–11]. Active tags are more costly, have their battery source, limited battery and communication range. Active or Semi-passive tags show economical to active tags and costlier to passive tags [12, 13]. These three tags are used in different applications. Semi-passive tags are mainly used in applications such as alarm systems, thermostats, etc. Active tags are used in applications meant for animal or person tracking, health care systems, etc. Supply chain management, smart cards, etc. are some applications of passive tags [14–29].

## **1.1 Chapter organization**

The rest of the chapter is organized as follows: Section 2 states the important security parameters required to analyze the authentication protocols. Section 3 introduces the classifications of recently developed authentication protocols [30]. Lightweight authentication protocols are discussed in section 4. Section 5 presents group authentication protocols. In this section, authentication protocols are classified, explained and analyzed from important attacks. Comparative security and cost analysis of surveyed authentication protocol is presented in section 6. Finally, conclusive and future scope remarks are given in section 7.

## **2. Security challenges**

RFID is a pervasive system. Security of this system is equally important. An attacker can harm at various points including information eavesdropping at end

user sites, obstructing physical access, controlling the devices and stealing the information etc. Protection from these threats demands strong mechanism for confidentiality, integrity, authentication, availability and non-repudiation [31–35]. This protection mechanisms should addresses major security concerns in RFID system like [36, 37]:

- *Privacy*: No one is interested to reveal personnel information to others without being part of authentic process. This privacy leakage could bring up many frauds. For example, if some item is equipped with tag and store name, price, area and other item information then a robber can easily fetch the information that how much he can earn with one or more robberies in a particular area. Similarly, unauthentic reader can scan the information written on e-passport to locate the important persons or count the gathering in an area [38–40]. This could result in planning of some terrorist activities. Thus, privacy of personnel or correspondence information leakage through RFID system is a major concern.
- *Tracking*: Objects, persons, animals etc. tracking through RFID readers and tags increases the information vulnerabilities also. This information availability helps to create profiles and important information can be leaked from these profiles [41]. This information can be used in various unauthentic or uninterested activities like: advertisement, etc. For example, if customer is buying items from a shop on a regular interval and each item is equipped with RFID tag then customer profile can be created in a database. This profile helps to put similar interest customers in a group. An advertisement can be floated of special interests for these groups which may not be interest to customers. Equipments used to track items, people or animal attached with RFID tags are not expensive thus data collection for these advertisements, promotions or gathering future requirements to earn profits is much easier. As compared to other tracking techniques like: video surveillance, RFID system based technique is much cheaper and faster. Thus, it is beneficial to both authentic and unauthentic users. Hence, it demands strong security mechanism to protect the information at any stage of system. Protected information results in wide applications of RFID technology.
- *Eavesdropping*: This is one of the most common forms of attack in networks where there is use of radio frequency for data communication. An eavesdropper can deploy an antenna to collect the information transmitted between reader and tag. Tags and readers communicate at different frequency bands like: low, high, ultrahigh and microwave. Thus, distance and location of eavesdropper from reader or tag is important. An attacker eavesdrop information in reader to tag (forward eavesdropping), tag to reader (backward eavesdropping), operation zone of reader and randomly selected distance directions. Since, it is easily feasible to fetch the information at longer distance and without any difficulty hence this attack should be handled properly. In real time applications, if an attacker deploy antenna to eavesdrop the information then information from RFID systems like e-passports, payment systems, identity cards, tickers etc. is on stake [42–44]. This information could reveal personnel data.
- *Skimming*: Eavesdropping is intercepting the information during its transit whereas skimming is reading the information from its store stage. Like eavesdropping, skimming attack can fetch the information from real time

applications like: e-passports, identity cards, traveling tickers or passes, consumer products etc. This could again reveal the personnel information like: name, birth date, financial account details, photo etc. Anti-skimming devices designed to protect against this attack uses reverse electromagnetic field. Anti-skimming devices are lightweight, persistent and easy to carry.

- *Cloning*: Resource constraint RFID devices are easy to clone because high security classical primitives cannot be implemented on these devices. RFID passive devices are cost effective as it does not require battery source. These devices gain power from reader thus easy to clone. Similarly, cloning devices could be passive and gain power from reader. Passive cloning devices are put closer to original device. Passing a cloning device closer to original device and making a copy of the data for cloning purpose may just take few seconds or minutes. This could be more dangerous for those devices which do not provide strong protection like: employee ID cards, train or bus ticket passes, product vouchers in supply chain management etc. Several solutions have been proposed to protect tags from cloning. Authentication is one of them. In authentication based mechanism, a random number is generated and exchanged. Response to this random number exchange uses cryptography primitives like digital signature, hashing, encryption/decryption, message authentication code etc. Verification of this response is performed at other side. If response is verified then tag is considered to be authentic else unauthentic or cloned. A new random number is generated every time a tag is read. This process further protects the tags from cloning.
- *Replay attacks*: In RFID system, one reader scans multiple tags and one tag could be associated with multiple readers. Replay attacks occur when freshness and aliveness of messages are not handled properly. If traceability is not a major concern then random number or nonce help to stop replaying of messages. A sequence number synchronizes the information between tag and reader. Count of numbers generated is limited in fixed length sequence number. Thus, an attacker can play old sequence number in new session. In order to avoid replaying an old sequence number in new session, aliveness of message is important [4, 45–47]. A computational challenge aliveness of message along with freshness hinders the attacker to play a replay attack. This attack is common among ultra-lightweight protocols where bitwise logical operators are only allowed [46, 48]. These operators are easy to break because of least computational breaking challenge.
- *Relay attack*: In this type of attack, RFID tags and readers are misled by providing false information. For example, if some reader is interested to scan a tag then attacker tag claims that it is the targeted tag [49]. Whereas, attacker tag fetches the information from another attacker reader which is close to authentic tag [50]. Thus, one reader and one tag attacker provide false information to authentic reader and tag [51, 52]. These authentic reader and tag are not in range of each other but attacker readers and tags mislead them to be close [53]. Attackers tries to prove the reader that the destination tag is nearby which is not in actual.
- *Denial of Service (DoS)*: Radio signal blocks, active and passive jamming, packet overflows etc. are the signs of DoS attack. Low cost passive devices are resource constraint devices thus this attack easily blocks the services and it is more dangerous. An attacker floods the packets towards specific or set of

nodes. This results to blockage in services. Many solutions are proposed to observe this attack through graphs, behaviors, trusts, performance, quality of service etc. Detection of this attack is easier as compared to removal of attack in resource constraint networks [54].

- *Spoofing Attack*: This attack modifies the identity, address or naming services to provide false information. For example, an attacker claims to have certain IP address, MAC address or domain name which is not true. Here, attacker aims to eavesdrop or modify the information during its transit [55, 56].
- *Secret disclosure attacks*: In this attack, vulnerabilities of key updating, data centre processing, reader or tag computing etc. reveal the identity or key information [57]. This attack is common in ultra-lightweight authentication protocols where some secret information is known to adversary. Secret disclosure attack could result to other attacks like: de-synchronization, impersonation, eavesdropping etc. Since, algebraic computing is main cause of this attack thus it is dangerous for low cost passive RFID devices [58].

### 3. Authentication protocols, classifications and security issues

Recently developed RFID authentication protocols in classical, lightweight, ultra-lightweight and grouping proof protocols are discussed in this section. This section also discusses the latest attacks found on recently developed authentication protocols.

#### Authentication Protocols in Classical Cryptography Primitives Category.

This work discusses authentication protocols that uses classical cryptography [59]. Symmetric and asymmetric are two major types of classical cryptosystems. Protocols in these categories are as follows:

#### Symmetric Cryptography Primitives based Authentication Protocols.

**Protocol (A1):** Cheng et al. Protocol [60].

**Premise:** Let 'R', 'T' and 'DC' represent the reader, tag and data centre respectively. Let  $r_i$ ,  $e_i$  and  $dc_i$  are the random numbers. Every tag selects its unique identification (ID) with its hash as  $H(\text{ID})$ .  $K_{\text{Session}}^{\text{Old}}$  and  $K_{\text{Session}}^{\text{Current}}$  are the old and current session key between R and T respectively.  $P(\cdot)$  represents the enhanced chebyshev polynomial.

**Step 1:- R → T** :  $r_1$   
**Step 2:- T** :  $\text{temp}_1 = H(\text{ID}) \oplus e_1 \oplus r_1$   
 :  $\text{temp}_2 = P_{r_1, e_1}(K_{\text{Session}}^{\text{Current}})$   
 :  $\text{temp}_3 = K_{\text{Session}}^{\text{Current}} \oplus e_1$   
**T → R** :  $\text{temp}_1, \text{temp}_2, \text{temp}_3$   
**Step 3:- R → DC** :  $r_1, \text{temp}_1, \text{temp}_2, \text{temp}_3$   
**Step 4:- DC** : Computes  $H(\text{ID}) \oplus K_{\text{Session}}^{\text{Current}} = \text{temp}_1 \oplus \text{temp}_3 \oplus r_1$   
 :  $\text{temp}_4 = H(\text{ID}) \oplus K_{\text{Session}}^{\text{Current}}$   
 : if  $\text{temp}_4$  record exist in data centre then fetch  $H(\text{ID})$ ,  
 $K_{\text{Session}}^{\text{Current}}, K_{\text{Session}}^{\text{Old}}$  :  $\text{temp}_5 = \text{temp}_1 \oplus H(\text{ID}) \oplus r_1$   
 :  $\text{temp}_6 = H(\text{ID}) \oplus r_1 \oplus dc_1$   
 : if  $\text{temp}_2$  equals to  $P_{r_1}(P_{e_1}(K_{\text{Session}}^{\text{Current}}))$  then  
 :  $\text{temp}_7 = P_{dc_1, e_1}(K_{\text{Session}}^{\text{Current}})$ ,  $K_{\text{Session}}^{\text{Old}} = K_{\text{Session}}^{\text{Current}}$  and  
 $K_{\text{Session}}^{\text{Current}} = K_{\text{Session}}^{\text{Current}} \oplus (e_1 || dc_1)$

: else if temp<sub>2</sub> equals to  $P_{r_1}(P_{e_1}(K_{Session}^{Old}))$  then  
 : temp<sub>7</sub> =  $P_{dc_1, e_1}(K_{Session}^{Old})$  and  $K_{Session}^{Current} = K_{Session}^{Old} \oplus (dc_1 || e_1)$   
 : else tag is unauthentic  
 : Now, if tag is authentic then  
 DC → R : temp<sub>6</sub>, temp<sub>7</sub>  
 Step 5:- R → T : temp<sub>6</sub>, temp<sub>7</sub>  
 Step 6:- T : dc<sub>1</sub> = temp<sub>6</sub> ⊕ H(ID) ⊕ r<sub>1</sub>  
 : if temp<sub>7</sub> equals to  $P_{dc_1, e_1}(K_{Session}^{Current})$  then  $K_{Session}^{Current} = K_{Session}^{Current} \oplus (e_1 || dc_1)$

**Explanation:** Cheng et al. proposed random number and hash based authentication protocol in 2013 [60]. In this protocol, reader starts the authentication process. It selects a random number and sends it to tag (step 1). Tag computes three responses temp<sub>1</sub>, temp<sub>2</sub> and temp<sub>3</sub> with the help of random numbers, H(ID),  $K_{Session}^{Current}$  and P(.). Now, tag sends r<sub>1</sub> and three responses to reader (step 2). Reader forwards this information to datacentre (step3). Data centre verifies the tag entry record in database. Further, if tag is authentic then datacentre computes two responses for reader: temp<sub>6</sub> and temp<sub>7</sub> (step4). Reader forwards these responses to tag (step5). Tag verifies the authenticity of reader by comparing temp<sub>7</sub> with  $P_{dc_1, e_1}(K_{Session}^{Current})$ . If both are equal then reader is considered to be authentic and symmetric session key is generated [36, 37, 46, 61, 62].

**Protocol (A2):** Single Entity-Single Communication based Unilateral Authentication Protocol.

**Premise:** Let ‘R’ and ‘T’ represents reader and tag respectively. Suppose, r<sub>i</sub> and e<sub>i</sub> are the i<sup>th</sup> random numbers. A symmetric key ‘K’ is shared between reader and tag. E<sub>K</sub>(.) and D<sub>K</sub>(.) are the encryption and decryption functions [63].

**Version 1:**

Step 1:- R → T : E<sub>K</sub>{ID<sub>T</sub>}  
 Step 2:- T : Verify {D<sub>K</sub>{ID<sub>T</sub>}}

**Version 2:**

Step 1:- T → R : E<sub>K</sub>{ID<sub>T</sub>}  
 Step 2:- R : Verify {D<sub>K</sub>{ID<sub>T</sub>}}

**Explanation:** In single entity-single communication based unilateral authentication protocol, two variations of protocols are possible. In first variation, reader sends an encrypted identification based message to tag (step 1) and tag verify its identity (step 2). In second version, tag sends its encrypted entity to reader (step 1) and reader authenticates it by decryption and verification (step 2) [64].

**Protocol (A3):** Single Entity-Two Communications based Unilateral Authentication Protocol.

**Premise:** Let ‘R’ and ‘T’ represents reader and tag respectively. Suppose, r<sub>i</sub> and e<sub>i</sub> are the i<sup>th</sup> random numbers selected by reader and tag respectively. A symmetric key ‘K’ is shared between reader and tag. E<sub>K</sub>(.) and D<sub>K</sub>(.) are the encryption and decryption functions.

**Version 1:**

Step 1:- R → T : {r<sub>1</sub>}  
 Step 2:- T → R : E<sub>K</sub>{r<sub>1</sub>}  
 Step 3:- R : Verify E<sub>K</sub>{r<sub>1</sub>}



**Version 2:**

- Step 1:-** T → R : {e<sub>1</sub>}  
**Step 2:-** R → T : E<sub>K</sub>{e<sub>1</sub>}  
**Step 3:-** T : Verify E<sub>K</sub>{r<sub>1</sub>}

**Explanation:** There are two version of single entity two communications based unilateral authentication protocol. In first version of protocol, reader initiates the authentication process by sending a random number challenge (step 1). Tag encrypts the received random number with symmetric key shared between tag and reader, and forwards it to reader (step 2). Now, reader re-encrypts its own random number challenge and verifies by comparing with the received data (step 3). If both are equal then tag is considered to be authentic. Similarly in second version, tag initiates the authentication process by sending a random number challenge (step 1). Reader encrypts the challenge with symmetric key and sends it to tag (step 2). Tag verifies the response for authentication (step 3) [65].

**Asymmetric Cryptography Primitives based Authentication Protocols.**

Like symmetric cryptography, asymmetric cryptography primitives based protocols are also designed to enhance the security of system. Major of recently developed asymmetric protocols are based on elliptic curve cryptography. This section discusses the recently developed elliptic curve cryptography based authentication protocols. Recently analyzed attacks on some of the authentication protocols are also explored.

**Elliptic Curve Cryptography (ECC) based Authentication Protocols.**

**Protocol (B1):** Authentication mechanism with ECC Encryption/Decryption for end users.

**Premise:** Let ‘R’ and ‘T’ represents reader and tag respectively. Suppose, r<sub>i</sub> is the i<sup>th</sup> random number selected by reader or tag. Let C<sub>j</sub> and P<sub>j</sub> represent the ciphertext and plaintext generated at i<sup>th</sup> side. Where, j ∈ {R, T}. Encryption and decryption functions at j<sup>th</sup> side are represented by E<sub>j</sub>(.) and D<sub>j</sub>(.). Unique identification of tag and reader is represented by ID<sub>T</sub> and ID<sub>R</sub> respectively. Let ‘h’ is the hash function used to generate the digest.

- Step 1:-** R : Selects ‘r<sub>1</sub>’ ∈ Z<sub>n</sub>  
 : Calculate (i) H = h(r<sub>1</sub>)  
 (ii) C<sub>R</sub> = E(r<sub>1</sub>, ID<sub>T</sub>)  
 R → T : C<sub>R</sub>, ID<sub>T</sub>, H  
**Step 2:-** T : (y, ID<sub>T</sub>) = D(C<sub>R</sub>)  
 : Verify [h(y) == H] and [decrypted ID<sub>T</sub>]  
 T → R : y  
**Step 3:-** R : if y == r<sub>1</sub> then ‘T’ is authentic else unauthentic.

**Explanation:** This is random number generation based authentication protocol. Here, reader selects a random number and computes the ciphertext of tag identification with this random number. Reader sends the ciphertext, tag identification and hashing over random number to tag (step 1). After receiving the data, tag decrypt the encrypted information and fetches the random value and tag identification. Here, tag verifies the received hash value with regenerated hash value. If both are verified then tag sends the decrypted random number value to reader (step 2). Reader verifies the received random value with its own generated random value in step 1. If it matches then user associated with tag is considered to be authentic otherwise unauthentic (step 3). This protocol was developed by taking consideration that protocol is protected from replay, reflection and chosen-text attacks due

to encryption/decryption and hash functions. Use of encryption/decryption and hash functions is the major cause that this protocol is not suitable for resource constraint devices.

**Protocol (B2):** ECC based signature-based mechanism for authenticating end users.

**Premise:** - Let 'R' and 'T' represents reader and tag respectively. Suppose,  $r_i$  and  $e_i$  are the  $i^{\text{th}}$  random number selected by reader and tag respectively,  $ID_r$  represents the identification of reader,  $CERT_{TAG}$  represents the certificate pre-shared between tag and reader, and SIGN and VERIFY represents the digital signature based signing and verification processes.

- Step 1:-** R  $\rightarrow$  T :  $r_1$   
**Step 2:-** T :  $y = \text{SIGN}(r_1, r_2, ID_r)$   
 T  $\rightarrow$  R :  $r_2, ID_r, y, CERT_{TAG}$   
**Step 3:-** R : VERIFY  $CERT_{TAG}$  and VERIFY  $y$   
 : if verified then consider that tag is valid.

**Explanation:** Reader starts the authentication process by sending a random challenge to tag (step 1). Tag selects another challenge and digitally signs both challenges along with the identification of reader. This signature message, random challenge, identification of reader and tag's certification is sent towards tag (step 2). Now, reader verifies both the certificate and digital signature. If both are verified then tag is considered to be authentic else unauthentic (step 3). Author claims that this protocol prevents existential forgery attack.

**Protocol (B3):** Schnorr Identification scheme and end-user verification with ECC [55].

**Premises:-** Let 'R' and 'T' represents reader and tag respectively. Suppose,  $r_i$  and  $e_i$  are the  $i^{\text{th}}$  random number selected by reader and tag respectively. Tag's public key is represented by Z and P is the base point selected on elliptic curve E.

- Step 1:-** T : Computer  $X = r_1P$   
 T  $\rightarrow$  R : X  
**Step 2:-** R  $\rightarrow$  T :  $e_1$   
**Step 3:-** T : Compute  $y = ae_1 + r_1$   
 T  $\rightarrow$  R : y  
**Step 4:-** R : if  $yP + e_1Z = X$  then authentic else unauthentic

**Explanation:** Tuyls proposed schnorr identification protocol based on elliptic curve discrete logarithmic problem in 2006. In this protocol, tag starts the communication by sending  $X = r_1P$  to reader (step 1). Reader receiver the message X. To verify this message and tag, it sends a random number to tag (step 2). Now, tag responds with 'y' to the reader (step 3). Reader verifies the message 'X' with the help of tag's public key. If it matches then tag is considered to be authentic else unauthentic. In this protocol, an attacker reader can easily trace the tag by acting as a middle entry between tag and reader. Attacker reader function is explained in attack 1.

**Attack 1:** Tag tracing by attacker reader on ECC and Schnorr Identification scheme.

**Premises:** In addition to premises of protocol, let  $R_{\text{attacker}}$  is the eavesdropper that want to trace the tag.

- Step 1:-** T  $\rightarrow$   $R_{\text{attacker}}$  : X  
**Step 2:-**  $R_{\text{attacker}}$   $\rightarrow$  R : X  
**Step 3:-** R  $\rightarrow$   $R_{\text{attacker}}$  :  $e_1$

- Step 4:-**  $R_{\text{attacker}} \rightarrow T$  :  $e_1$   
**Step 5:-**  $T \rightarrow R_{\text{attacker}}$  :  $y = ae_1 + r$   
 : Now,  $R_{\text{attacker}}$  is knowing  $X$ ,  $e_1$  and  $y = ae_1 + r$ .  
**Step 6:-**  $T \rightarrow R_{\text{attacker}}$  :  $X'$   
**Step 7:-**  $R_{\text{attacker}} \rightarrow T$  :  $e_2 (=e_1)$   
**Step 8:-**  $T \rightarrow R_{\text{attacker}}$  :  $y' = ae_2 + r'$   
 : computes  $y'P + e_2Z = X'$

**Explanation:** Now, attacker reader can easily trace the tag by checking whether  $(y'-y)P$  equals  $(X'-X)$ . In this attack,  $R_{\text{attacker}}$  communicates with 'T' and 'R' to trace 'T'. Here, 'T' communicates with  $R_{\text{attacker}}$  instead of 'R' (step 1).  $R_{\text{attacker}}$  does not generate a challenge by itself but forwards the  $e_1$  received from 'R' to 'T' (step 2 to step 4). In continuation, 'T' responses to challenge but it go to  $R_{\text{attacker}}$  instead of 'R' (step 5). Later, 'T' communicates again with  $R_{\text{attacker}}$ . 'T' and ' $R_{\text{attacker}}$ ' again generate new challenges and responses (step 6 and step 8). Now,  $R_{\text{attacker}}$  can keep trace of the 'T' by computing whether  $(y'-y)P$  equals  $(X'-X)$ .

**Attack 2:** If attacker reader knows the public key 'Z' of tag then it can easily compute the message by computing  $y'P + e_1Z = X$ . Thus, this mechanism is not considered to be secure against forward secrecy.

In addition to attack 1 and attack 2, this protocol is having scalability issues. Cost of computation at reader side is high since increase in number of tags handled per reader requires most of the public keys to be accessed from database by the reader. This increases the computational cost of reader. Increase in computational cost reduces the power of reader to handle more tag. Thus, scalability of network reduces gradually.

#### 4. Lightweight authentication protocols

Lightweight authentication protocols are less powerful as compared to classical cryptography based protocols. Lightweight cryptography is integrated with protocols to achieve confidentiality, integrity, availability, authentication and non-repudiation. Apart from security, communication and computational cost at reader and tag is another factor taken into consideration for selecting the lightweight authentication protocol.

**Protocol (C1):-** Yu et al. Protocol [49].

**Premises:-** Let 'R' and 'T' represents reader and tag respectively. Suppose,  $r_i$  and  $e_i$  are the  $i^{\text{th}}$  random number selected by reader and tag respectively. Let 'm' represents the m-bit map in form of non-volatile memory. This non-volatile memory is used to store random number information to protect from tracking attack.

- Step 1:-**  $R \rightarrow T$  :  $r_1$   
**Step 2:-**  $T$  : Compute  $j = h(k_i, r_1) \bmod m$   
 : if  $\text{map}[j]$  is zero then  
 :  $\text{map}[j] = 1$  and  
 $T \rightarrow R$  :  $h(k_i, r_1)$   
 : else if  $\text{map}[j]$  is non-zero then  
 $T \rightarrow R$  :  $h(k_i, e_1)$   
**Step 3:-**  $R \rightarrow DC$  :  $h(k_i, r_1)$  or  $h(k_i, e_1)$ .  
**Step 4:-**  $DC$  : find entry for  $h(k_i, r_1)$  or  $h(k_i, e_1)$  in database. If entry found then  
 : Compute  $h(k_i + 1, r_1)$  or  $h(k_i + 1, e_1)$   
 : Update  $k_i$  with  $h(k_i)$  and hash value with  $h(k_i, r_2)$

DC → R :  $h(k_i + 1, r_1)$  or  $h(k_i + 1, e_1)$   
 : if entry does not found in database then  
 DC → R : DENY  
**Step 5:-** R : if response from DC is DENY then  
 R → T :  $r_3$   
 : else  
 R → T :  $h(k_i + 1, r_1)$  or  $h(k_i + 1, e_1)$   
**Step 6:-** T : Compute  $h(k_i + 1, r_1)$  or  $h(k_i + 1, e_1)$  again  
 : Compare received message with computed message. If they  
 are equal then  
 : Update its key with  $h(k_i)$  and all bits of map equals to zero.

**Explanation:** This is a random number based authentication protocol. Reader starts a process of authentication by selecting a random number and sending towards tag (step 1). Tag computes its position and search the corresponding bit position on map. If bit position is zero on map then it sends its position to reader else selects a new random number and send towards tag (step 2). Reader sends the received value to data centre (step 3). Data centre searches the record in database. If entry found in database then it updates key and hash values. Updated information is forwarded to reader (step 4). If entry is not found in database then a DENY message is replied. Reader checks the received message. If received message is not DENY message then it forwards the received message to tag (step 5). Now, tag re-computes the hash value. If new hash value is equal to received value then tag also updates its hash value. It sets all bits of map to zero (step 6).

**Protocol (C2):-** Mitra et al. protocol [51].

**Premises:-** Let 'R' and 'T' represents reader and tag respectively. Suppose,  $r_1$  and  $e_i$  are the  $i^{\text{th}}$  random number selected by reader and tag respectively.

**Step 1:-** R → T<sub>i</sub> : {request}  
**Step 2:-** T : Compute  $IDS = e_1 * K + ID_T$   
 T → R : IDS  
**Step 3:-** R :  $ID'_T = IDS \text{ mod } K$

**Explanation:** Mitra proposed authentication protocol to protect against traceability and cloning in 2008 [51]. Reader to tag or tag to reader eavesdropping in communication is feasible in this protocol. In this protocol, reader starts the process by sending a random number (step 1). Tag computes the identification pseudonym and sends it to reader (step 2). Reader extracts the identification from received data (step 3).

**Attack:-** Cloning attack on Mitra Protocol.

**Step 1:-** R → T : {request}  
**Step 2:-** T : Compute  $IDS_1 = e_1 * K_1 + ID_T$   
 T → R<sub>Attacker</sub> :  $IDS_1$   
**Step 3:-** R<sub>Attacker</sub> → R :  $IDS_1$   
**Step 4:-** R :  $ID'_T = IDS_1 \text{ mod } K_1$   
 R → T : {request}  
**Step 5:-** T → R<sub>Attacker</sub> :  $IDS_2 = e_2 * K_2 + ID_T$   
**Step 6:-** R<sub>Attacker</sub> → R :  $IDS_2$   
 ...  
 ...  
**Step n-2:-** T → R<sub>Attacker</sub> :  $IDS_n = e_n * K_n + ID_n$

**Step n-1:-**  $R_{\text{Attacker}} \rightarrow R$  :  $IDS_n$   
**Step n:-**  $R$  :  $ID'_T = IDS_n \bmod K_n$   
**Step n + 1:-**  $R_{\text{Attacker}}$  : Collects  $IDS_1, IDS_2, \dots, IDS_n$ .  
 : Compute  $temp_1 = (IDS_2 - IDS_1) * K_1$ ,  $temp_2 =$   
 $(IDS_3 - IDS_2) * K_2, \dots, temp_{n-1} = (IDS_n - IDS_{n-1}) * K_{n-1}$ .  
 : Compute  $K_i = \text{GCD}(temp_1, temp_2, \dots, temp_{n-1})$

**Explanation:** In this attack, an attacker observes the communication between tag and reader [52]. Attacker observes and record  $IDS_1$  to  $IDS_n$  values (step 2, step 5, step n-2). This attacker again calculates  $temp_1$  to  $temp_{n-1}$  values and greatest common divisor (GCD) of these values (step n + 1). This GCD value is the secret key of tag in communication. Here, an attacker can start the message exchange with tag by collecting  $temp_1$  and sending  $IDS_i + r_i * temp_i$  to tag. This is an easy way to clone.

**Attack:-** Traceability attack in Mitra's protocol.

Step 1:-  $R_{\text{Attacker}} \rightarrow T$  : {request}  
 Step 2:-  $T \rightarrow R_{\text{Attacker}}$  :  $IDS_1$   
 ...  
 ...  
 Step i:-  $R_{\text{Attacker}} \rightarrow T$  : {request}  
 Step i + 1:-  $T \rightarrow R_{\text{Attacker}}$  :  $IDS_i$   
 Step i + 2:-  $R_{\text{Attacker}} \rightarrow T$  : {request}  
 $R_{\text{Attacker}} \rightarrow T'$  : {request}  
 Step i + 3:-  $T \rightarrow R_{\text{Attacker}}$  :  $IDS_n$   
 Step i + 4:-  $T' \rightarrow R_{\text{Attacker}}$  :  $IDS_{n+1}$   
 Step i + 5:-  $R_{\text{Attacker}}$  : accept  $IDS_n$  if  $b=0$ , accept  $IDS_{n+1}$  if  $b=1$   
 : Compute  $temp_1 = IDS_1 - IDS_i$   
 : Compute  $temp_2 = \begin{cases} IDS_1 - IDS_n & \text{if } b == 0 \\ IDS_n - IDS_{n+1} & \text{if } b == 1 \end{cases}$   
 : Select  $\begin{cases} d = 0 & \text{if } \text{GCD}(temp_1, temp_2) \geq 2^{L/2} \\ d = 1 & \text{if } \text{GCD}(temp_1, temp_2) < 2^{L/2} \end{cases}$

**Explanation:** Traceability attack in this protocol start with two requests from reader to tag (step 1 to step i + 1). In response to these requests, tag receives encrypted messages:  $IDS_1$  and  $IDS_i$ . Attacker again sends two requests to associated identifications ( $ID_T, ID'_T$ ) based tags (step i + 2). These tags return encrypted messages:  $IDS_n$  and  $IDS_{n+1}$  (step i + 3 and i + 4). Attacker accepts these messages from different tags in different form. It accepts  $IDS_n$  and  $IDS_{n+1}$  from tags with identification  $ID_T$  and  $ID'_T$  respectively. It uses  $b = 0$  for  $ID_T$  and  $b = 1$  for  $ID'_T$  to distinguish between tags and further necessary computations. Attacker computes  $temp_1$  and  $temp_2$  from received encrypted messages (step 5). Now, attacker guesses the bit based on length decision rule. Peris-Lopez found a success probability of guessing equal to 1 and this result in traceability with 50% probability [52].

**Attack:-** Full disclosure attack on Mitra's protocol

**Explanation:** As seen in cloning attack, attacker observes the messages exchange between tags and reader. This results in obtaining the secret key of tag with the help of GCD computations. After getting the secret of tag, attacker can easily reveal the stored and transmitted information. Peris-Lopez calculated the probability of revealing the secret using Riemann zeta function [52]. Authors found

a success rate of 60 to 100% of this attack and claim that it is most dangerous among all discussed attacks.

**Protocol (C3):** Qingling et al.'s protocol [51]

**Premises:** Let 'R', 'T' and 'DC' represents the reader, tag and data centre respectively. Suppose  $r_i$ ,  $e_i$  and  $dc_i$  are the random numbers selected by reader, tag and data centre respectively. MSB and LSB represents the most and least significant bits of a unique identifier ( $UID^T$ ) and access password ( $PASSWD^T$ ).

**Step 1:-**  $R \rightarrow T_i$  :  $r_i$

**Step 2:-**  $T_i$  :  $Message^{T_i} = Message_{LSB}^{T_i} || Message_{MSB}^{T_i}$   
 $Message_{LSB}^{T_i} = CRC(UID_{LSB}^{T_i} \oplus r_i \oplus e_i) \oplus PASSWD_{LSB}^{T_i}$   
 $Message_{MSB}^{T_i} = CRC(UID_{MSB}^{T_i} \oplus r_i \oplus e_i) \oplus PASSWD_{MSB}^{T_i}$

$T_i \rightarrow R$  :  $\{Message^{T_i}, e_i^{T_i}\}$

**Step 3:-**  $R$  : Verify  $Message^{T_i} \oplus PASSWD^{T_i}$  equals to  $CRC(UID_{LSB}^{T_i} \oplus r_i \oplus e_i) || CRC(UID_{MSB}^{T_i} \oplus r_i \oplus e_i)$ . If this condition holds for any tag in data centre then tag is authentic and process continues else unauthentic.

: Compute  $Message^R = Message_{LSB}^R || Message_{MSB}^R$ , Where,  
 $Message_{LSB}^R = CRC(UID_{LSB}^{T_i} \oplus r_i^{T_i}) \oplus PASSWD_{LSB}^{T_i}$  and  
 $Message_{MSB}^R = CRC(UID_{MSB}^{T_i} \oplus r_i^{T_i}) \oplus PASSWD_{MSB}^{T_i}$ .

$R \rightarrow T_i$  :  $Message^R$

**Step 4:-**  $T$  : Verify  $Message^R \oplus PASSWD^{T_i}$  equals to  $CRC(UID_{LSB}^{T_i} \oplus r_i^{T_i}) || CRC(UID_{MSB}^{T_i} \oplus r_i^{T_i})$ . If condition holds then reader is authentic else unauthentic.

**Explanation:** Qingling et al. [66] proposed a lightweight authentication protocol based on password challenge [51]. Reader starts the authentication process by sending a random number challenge to tag (step 1). Tag constructs most significant and least significant part of message to generate response for reader. Most significant and least significant parts are XORed with passwords before sending it to reader (step 2). Reader verifies the received messages and generates new challenge for tag to prove its authenticity (step 3). Tag verifies the received message for reader authenticity (step 4).

**Attack:-** Attack on Qingling et al.'s protocol.

**Premise:-** An attacker eavesdrops one session between 'R' and 'T'.

**Step 1:-**  $R_{Attacker} \rightarrow T_i$  :  $Message_{LSB}^{T_i} \oplus CRC(\alpha) || Message_{MSB}^{T_i} \oplus CRC(\alpha), e_i^{new}$ .  
 Where,  $\alpha = \delta + \gamma$ .  $\delta = e_i^{new} \oplus e_i$ ,  $\gamma = r_i^{new} \oplus r_i$ .

**Step 2:-**  $R_{Attacker} \rightarrow R$  :  $Message_{LSB}^R \oplus CRC(\delta) || Message_{MSB}^R \oplus CRC(\delta)$ .  
 Where,  $\delta = e_i^{new} \oplus e_i$ .

**Explanation:** Peris-Lopez et al. discovered impersonation of tag and reader in two communications [52]. This is possible by passively observing the one session between tag and reader. This impersonation helps the attacker to send a message with new random values ( $e_i^{new}$  and  $r_i^{new}$ ). Now, verification of this message at tag side is easy (step 1). Similarly, an attacker can supplant the reader with a message containing new random variables ( $e_i^{new}$ ). This message authenticates the attacker as a genuine reader. Tag can not detect this attack easily (step 2).

**Attack:-** Traceability attack on Qingling et al. protocol.

**Step 1 (Learning):**

$R_{Attacker}$  : Acquire  $r_1$ ,  $e_1$  and  $Message^{T_0} = Message_{LSB}^{T_0} ||$   
 $Message_{MSB}^{T_0}, Message_{LSB}^{T_0} = CRC(UID_{LSB}^{T_0} \oplus r_1 \oplus e_1)$   
 $\oplus PASSWD_{LSB}^{T_0}, Message_{MSB}^{T_0} = CRC(UID_{MSB}^{T_0} \oplus r_1 \oplus e_1)$   
 $\oplus PASSWD_{MSB}^{T_0}$ .

**Step 2 (Challenge):**

$R_{Attacker}$  : Selects two tags with  $UID^{T_0}$  and  $UID^{T_1}$ . It execute a test query that result to return two random numbers  $r_1^{new}$  and  $e_2^{T_i}$ , and message  $Message^{T_i} \in \{Message^{T_0}, Message^{T_1}\}$ . Selection of message is dependent on random bit  $b \in \{0,1\}$ .  $\{CRC(UID_{LSB}^{T_0} \oplus r_1^{new} \oplus e_2^{T_0}) PASSWD_{LSB}^{T_0} ||$   
 $CRC(UID_{MSB}^{T_0} \oplus r_1^{new} \oplus e_2^{T_0}) \oplus PASSWD_{MSB}^{T_0}$  if  $\{b==0\}$  or  
 $\{CRC(UID_{LSB}^{T_0} \oplus r_1^{new} \oplus e_2^{T_1}) PASSWD_{LSB}^{T_1} ||$   
 $CRC(UID_{MSB}^{T_1} \oplus r_1^{new} \oplus e_2^{T_1}) \oplus PASSWD_{MSB}^{T_1}$  if  $b==1\}$

**Step 3 (Guessing):**

$R_{Attacker}$  : An attacker obtains constant 1 and constant 2 values from step 1 and step 2 respectively. These values are associated to  $T_0$ .  $Constant1_{LSB} = Message_{LSB}^{T_0} \oplus CRC(r_1) \oplus$   
 $CRC(e_1) = CRC(UID_{LSB}^{T_0}) \oplus PASSWD_{LSB}^{T_0}$ .  $Constant1_{MSB} =$   
 $Message_{LSB}^{T_0} \oplus CRC(r_1) \oplus CRC(e_1) =$   
 $CRC(UID_{MSB}^{T_0}) \oplus PASSWD_{MSB}^{T_0}$ .  $Constant1 = Constant1_{LSB} ||$   
 $Constant1_{MSB}$ .  $\{CRC(UID_{LSB}^{T_0}) \oplus PASSWD_{LSB}^{T_0} ||$   
 $CRC(UID_{MSB}^{T_0}) \oplus PASSWD_{MSB}^{T_0}$  if  $\{b==0\}$  or  
 $\{CRC(UID_{LSB}^{T_1}) \oplus PASSWD_{LSB}^{T_1} ||$   
 $CRC(UID_{MSB}^{T_1}) \oplus PASSWD_{MSB}^{T_1}$  if  $b==1$ . An attacker calculate value of output bit  $d = \{0$  if constant1 equals to constant2, 1 if constant 1 not equals to constant 2}.

**Explanation:** Peris-Lopex et al. calculated the probability to distinguish between tags in order to interact for traceability [52]. This probability is high because it is easy to distinguish between tags. Thus, it is easy to implement traceability attack with above sequence of steps. There are three stage of observation: learning, challenge and guessing. Learning state observe the transactions between reader and tag to collect the secret parameters. Challenge step put random number based challenges to tag through attacker. Finally guessing state finds the probability of receiving 0 or 1.

**Protocol (C4):** LRAP (Lightweight RFID Authentication protocol) [67]

**Premises:-** Let 'R', 'T' and 'DC' represents the reader, tag and data centre respectively. Suppose  $r_i$ ,  $e_i$  and  $dc_i$  are the random numbers selected by reader, tag and data centre respectively. Further,  $IDS$ ,  $C_i$ ,  $K_E$ ,  $K_D$  are the identification pseudonym,  $i^{th}$  ciphertext, encryption and decryption keys respectively.

**Step 1:-**  $R \rightarrow T$  : {Hello}

**Step 2:-**  $T \rightarrow R$  : {IDS}

**Step 3:-**  $R$  : Compute ciphertext,  $(C_1, C_2, C_3) = E_{K_E}(r_1, r_2)$ ,  $C_3 = r_3P$ ,  
 $(temp_1, temp_2) = r_3K_E$ ,  $C_1 = temp_1 \cdot r_1 \text{ mod } N$ ,  $C_2 = temp_2 \cdot$   
 $r_2 \text{ mod } N$ ,  $temp_3 = (IDS + r_1 + r_2) \oplus K_E$ .

$R \rightarrow T$  :  $(C_1, C_2, C_3) || temp_3$

**Step 4:-**  $T$  : Extract  $(r_1, r_2)$  from  $(C_1, C_2, C_3)$ ,  $(temp_1, temp_2) = K_D.C_3$ ,  
 $r_1 = C_1 \cdot temp_1^{-1} \text{ mod } N$ ,  $r_2 = C_2 \cdot temp_2^{-1} \text{ mod } N$ , Compute

$temp'_3 = (IDS + r_1 + r_2) \oplus K_{DP}$  and verifies whether  $temp'_3$  equals to  $temp_3$ . If both are equal then compute  $temp_4 = (r_1 \oplus r_2) + ID$ .

T → R :  $temp_4$   
 : Updation  $IDS^{old} = IDS$ ,  $IDS^{new} = (IDS^{old} + r_1) + (ID+r_2)$

**Step 5:-** R : Computes  $temp'_4 = (r_1 \oplus r_2) + ID$ , Verifies  $temp'_4$  equals to  $temp_4$ . If both are equal then tag is authentic else unauthentic.  
 : Updation  $IDS = (IDS + r_1) \oplus (ID + r_2)$ .

**Explanation:** LRAP is elliptic curve based lightweight authentication protocol proposed by Liu et al. in 2013 [67]. Reader starts the authentication process by sending a hello request (step 1). Tag responds with its identification pseudonym (step 2). Reader response to tag includes the ciphertexts append with identification pseudonym (step 3). These ciphertexts are generated by encrypting the reader generated random numbers with encryption key. After receiving the response from reader, tag extracts the random numbers and verifies it. If these are verified then compute a new identification and random number based response to reader (step 4). After this communication, tag initiates the identification pseudonym updating process. On receiving the response, reader verifies it for authenticity and initiated the identification pseudonym updating process (step 5).

## 5. Grouping/yoking authentication protocols

This section discusses the protocols that allows the multiple tags to authentication simultaneously with same reader. Multiple tag authentication constructs groups with unique group identifications. Group construction is possible through collaborations of tag to jointly request the reader for authentication. Following are the important group authentication protocols [68].

**Protocol (E1):** Juels Yoking Protocol [69, 70].

**Premise:-** Let 'R', 'T' and 'DC' represents the reader, tag and data centre respectively. Let  $r_i$  and  $e_i$  are the random number selected by reader and tag respectively. Suppose, ' $K_i$ ' is the shared key between reader and  $i^{th}$  tag, MAC is the message authentication code.

**Step 1:-** R →  $T_1$  : {hello}  
**Step 2:-**  $T_1$  → R :  $ID_{T_1}, e_1$   
**Step 3:-** R →  $T_2$  :  $e_1$   
**Step 4:-**  $T_2$  → R :  $ID_{T_2}, e_2, temp_1=MAC_{K_2}[e_1]$   
**Step 5:-** R →  $T_1$  :  $e_2$   
**Step 6:-**  $T_1$  → R :  $temp_2=MAC_{K_1}[e_2]$   
**Step 7:-** R → DC :  $\{ID_{T_1}, e_1, temp_2, ID_{T_2}, e_2, temp_1\}$

**Explanation:** Juel's grouping protocol is the first group authentication protocol [71, 72]. This is the simplest protocol to understand and implement. Reader starts the authentication process by sending a random number based challenge (step 1). Tag responds with its identification mark and another random number challenge (step 2).

**Protocol (E2):** Saito and Sakurai's Protocol [73].

**Premise:-** Let 'R', 'T' and 'DC' represents the reader, tag and data centre respectively. Suppose, ' $K_i$ ' is the shared key between reader and  $i^{th}$  tag, MAC is the message authentication code. PT is the pallet tag.



- Step 1:-** DC  $\rightarrow$  R : {timestamp}  
**Step 2:-** R  $\rightarrow$  T<sub>i</sub> : {timestamp}, Where  $i \in \{1, n\}$   
**Step 3:-** T<sub>i</sub>  $\rightarrow$  R : temp<sub>i</sub> = MAC<sub>K<sub>i</sub></sub>[timestamp]  
**Step 4:-** R  $\rightarrow$  PT : {timestamp}, temp<sub>i</sub>,  
**Step 5:-** PT  $\rightarrow$  R : E<sub>K</sub>[{timestamp}, temp<sub>i</sub>]  
**Step 6:-** R  $\rightarrow$  DC : {timestamp, E<sub>K</sub>[{timestamp}, temp<sub>i</sub>], ID<sub>T<sub>1</sub></sub>}

**Explanation:** Saito and Sakurai protocol tried to remove replay attack from juel's protocol [74]. Data centre initiated the group authentication proof protocol by sending a timestamp message to reader (step 1). Reader forwards the timestamp to all tags (step 2). All tags then send a message authentication code of timestamp to reader (step 3). There is use of pallet tag in this protocol. This tag is assumed to have abundance of resources as compared to any existing tag. Reader forwards the timestamp message and message authentication code of all tags to pallet tag (step 4). Pallet tag encrypts the received message and sends it to reader (step 5). Reader forwards this message to data centre for storage (step 6). This stored entry is a grouping proof.

**Attack:** Secret disclosure attack on Kazahaya.

**Explanation:** Bagheri et al. found that it is possible for an attacker to retrieve tag's secret parameters at cost of  $O(2^{16})$  offline random number evaluations [75]. In this attack, an attacker eavesdrops one session between tag and reader. Further, at cost of  $O(2^{16})$  operations, it fetches private key of tag, identification of tag and group identification. These secret disclosure parameters increase the chance of tag and reader impersonation, and traceability. An attack can forge proofs at any time. It is found that verification of forged proofs is possible at cost of one session eavesdropping. Thus, forgery attack is another threat to this protocol and probability of this attack is '1'.

## 6. Comparisons

Security and cost analysis of authentication protocols is presented in this section. Security analysis is performed based on parameters selected in Section 3. Similarly, cost estimation is analyzed through communication and computational cost parameters. This analysis is performed to find authentication protocol suitable for resource constraint or resourceful devices in IoT.

### 6.1 Security analysis

Possibilities of attacks on surveyed authentication protocols are analyzed in security analysis. This comparison of authentication protocols is made through infeasible, strong, medium and weak possibilities of attacks. Authentication protocol attacks and their chance on studied protocols are searched from literature. If a direct attack is found then possibility of attack is considered to be strong (S). Otherwise, attacker's dependency on existing attack is searched. For example, man-in-the-middle and denial of service attacks lead to de-synchronization and traceability attacks. Hence, if chances of man-in-the-middle and denial of service attacks is strong then de-synchronization and traceability attacks provide medium (M) chances. Similarly, eavesdropping leads to secret disclosure attack. Chances of indirect attacks are considered to be medium because extra computational and communication cost is required to perform these attacks. Further, chances of indirect attacks with high computational and communication cost are considered to be weak

(W). Overall, it is analyzed that the recent trends is to design authentication protocols based on asymmetric key based cryptosystem because such protocol provide high security and low communicational cost as compared to symmetric key cryptosystem based protocols. Symmetric or asymmetric cryptosystem based authentication protocols are suitable for resourceful devices such as active RFID devices. These devices can afford the computational cost of protocols. Lightweight and ultra-lightweight protocols are designed for resource constraint devices like: passive RFID devices. These devices cannot afford high computations or storage. Security of such protocols is a major concern. It is impossible to fully secure such protocols from attacks. Protocol with higher attack resistant probability is considered to be more reliable. Hence protocol like C4, D2 and D3 are more reliable. Further, these authentication protocols can be extended to create groups called grouping or yoking protocols.

### 6.2 Cost analysis

Communication and computational cost of studied authentication protocols is analyzed in **Table 1**. Communication cost is measured in terms of number of transactions made between reader and tag. Different levels to measure the cost are Low (L), Medium (M) and High (H). If number of transactions is between 1 and 3 then communication cost is considered to be low. If it varies from 4 to 6 then communication cost is medium. Communication cost is considered to be high if number of transactions is more than 6. It is found that communication cost of asymmetric cryptography primitives based authentication protocols is much lower than any other type of authentication protocols. Although lightweight and ultra-lightweight protocols claim to be efficient for resource constraint devices but asymmetric cryptography based protocols can also be designed to reduce the overhead through reduction in communication cost. For example, protocol C4 is based on elliptic curve cryptosystem based asymmetric cryptography and it is efficient than any other lightweight protocol. Like communication cost, computational cost is also

Possibility of Attacks on Authentication Protocols															Cost Analysis	
Protocol	P <sub>r</sub>	T <sub>r</sub>	FS	BS	E <sub>a</sub>	S <sub>k</sub>	C <sub>l</sub>	R <sub>p</sub>	R <sub>L</sub>	DoS	S <sub>p</sub>	S <sub>D</sub>	D <sub>E</sub>	M <sub>M</sub>	C <sub>omm</sub>	C <sub>omp</sub>
<b>Symmetric Cryptography Primitives Based Authentication Protocols</b>																
A1 [60]	S	M	M	M	M	M	M	W	M	M	M	S	S	S	M	H
A2	M	S	S	M	M	M	M	S	S	S	M	M	S	M	L	H
A3	S	S	S	M	S	M	M	S	S	S	S	S	S	S	L	H
<b>Asymmetric Cryptography Primitives Based Authentication Protocols</b>																
B1	S	S	S	M	W	M	M	M	M	M	M	M	M	M	L	H
B2	S	S	S	M	W	M	M	M	M	M	M	M	M	M	L	H
B3	S	S	S	M	W	M	S	S	S	S	S	S	S	S	L	M
<b>Lightweight Authentication Protocols</b>																
C1	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	H
C2 [51]	M	S	M	M	M	M	S	M	M	M	M	S	S	S	L	L
C3 [51]	M	S	M	M	S	M	M	M	M	M	S	M	S	S	L	L
C4 [67]	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	L

Possibility of Attacks on Authentication Protocols															Cost Analysis	
Protocol	P <sub>r</sub>	T <sub>r</sub>	FS	BS	E <sub>a</sub>	S <sub>k</sub>	C <sub>l</sub>	R <sub>p</sub>	R <sub>L</sub>	DoS	S <sub>p</sub>	S <sub>D</sub>	D <sub>E</sub>	M <sub>M</sub>	C <sub>omm</sub>	C <sub>omp</sub>
<b>Ultra-lightweight Authentication Protocols</b>																
D1 [36]	S	S	S	S	S	S	S	S	S	S	S	S	S	S	M	L
D2 [76]	M	S	M	M	M	M	M	M	M	M	M	M	S	M	L	H
D3 [77]	M	M	M	M	M	M	M	M	M	M	M	M	M	M	H	L
<b>Group Authentication Protocols</b>																
E1 ([71]; [72])	W	W	M	M	W	W	W	W	W	W	W	W	W	W	H	L
E2 [74]	W	W	M	M	W	W	W	W	W	W	W	W	W	W	M	L
E3 [37]	M	M	W	W	M	W	W	M	W	W	M	W	M	M	M	L

*P<sub>r</sub>* = Privacy, *T<sub>r</sub>* = Tracking, *FS* = Forward Secrecy, *BS* = Backward Secrecy, *E<sub>a</sub>* = Eavesdropping, *S<sub>k</sub>* = Skimming, *C<sub>l</sub>* = Cloning, *R<sub>p</sub>* = Replay, *R<sub>L</sub>* = Relay, *DoS* = Denial of Service, *S<sub>p</sub>* = Spoofing, *S<sub>D</sub>* = Secret Disclosure, *D<sub>E</sub>* = De-synchronization, *M<sub>M</sub>* = Man-in-the-middle, *W* = Weak, *M* = Medium, *S* = Strong, *C<sub>omm</sub>* = Communication Cost, *C<sub>omp</sub>* = Computational Cost, *L* = Low, *H* = High.

**Table 1.**  
 Security and cost analysis of authentication protocols.

divided into three levels: Low, Medium and High. A high cost authentication protocol includes encryption, decryption, hashing or high computational functions. Medium cost based protocols include mathematical functions like elliptic curve based addition, multiplication or inverse, shift or permutation operations etc. A low cost protocol affords simple mathematical functions like: logical operations (AND, OR, NOT etc.), simple permutation, rotation random number generator etc. Lightweight and ultra-lightweight protocols are especially designed to count these low computational cost factors into considerations. Computational cost of these protocols is much lower than any classical cryptography based symmetric or asymmetric authentication protocols.

## 7. Conclusion

In this work, RFID authentication protocols from different categories are studied and compared on security requirements and cost. Authentication protocols are categorized as: symmetric, asymmetric, lightweight, ultra-lightweight and group based authentication based protocols. It is found that asymmetric cryptography based protocols are gaining popularity day-by-day and provide enough security. Symmetric and asymmetric cryptography based authentication protocols are suitable for resourceful devices. Passive RFID devices are resource constraint devices thus lightweight or ultra-lightweight protocols are more suitable. Security in lightweight protocols is a major challenge. Hardware limitations restrict the implementation of full security on these devices. Thus, these devices can not be fully protected. Integration of asymmetric key cryptography based lightweight authentication protocols is contemporary topic of research. These unilateral or mutual authentication protocols can be extended for group authentication. Multiple tags authenticate itself with reader and store group information in data centre. This concept of group authentication is important for IoT. Authenticated devices in IoT increase the chances of secure communication in a network. Future work demands

to construct a secure grouping proof protocol that is not affected with relay, replay or de-synchronization attacks.

## **Key terms and definitions**

Active attacks	an illegal act of modifying the information or operation to affect the system
Asymmetric key cryptography	a cryptosystem that uses public and private keys for encryption and decryption process is known as asymmetric key cryptosystem
Authentication	a process to confirm the attributes of message/ user is known as message or user authentication
Lightweight cryptography	a least computational cost based cryptosystem designed to provide security for resource constraint devices
Passive attacks	an illegal use of using the important system information using affecting the resources
Symmetric key cryptography	a cryptosystem that uses same or symmetric key for encryption and decryption operation
Yoking protocol	a group of participants authenticates each other for constructing a secure environment

## **Author details**

Adarsh Kumar<sup>1\*</sup> and Deepak Kumar Sharma<sup>2</sup>

1 Department of Systemics, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India

2 Department of Informatics, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India

\*Address all correspondence to: [adarsh.kumar@ddn.upes.ac.in](mailto:adarsh.kumar@ddn.upes.ac.in)

## **IntechOpen**

© 2020 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

## References

- [1] Ashton, K. (2009). That 'Internet of Things' Thing, in the real world things matter more than ideas, *RFID Journal*, Retrieved July 15, 2014, from <http://www.rfidjournal.com/articles/view?4986>
- [2] Uckelman D., Harrison M. and Michahelles F. (2011) Architecturing the Internet of Things. Springer-Verlag Berlin Heidelberg.
- [3] Aggarwal, C. C., Ashish, N. and Sheth, A. (2013). The Internet of Things: A Survey from the data-centric Perspective. In Aggarwal, C (Ed.), *Managing and Mining Sensor Data* (pp. 383–428). Springer-Verlag.
- [4] Abyaneh, M. R. S. (2012). Security Analysis of Lightweight Schemes for RFID Systems. Ph. D.Thesis, University of Bergen, Norway.
- [5] Juel A. and Weis S. (2005). Authenticating Pervasive Devices with Human Protocols. In V. Shoup, editor, *Advances in cryptology-Crypto 05*, LNCS 3126, pp. 293–298, Springer-Verlag.
- [6] Peris-Lopez, P., Hernandez-Castro, J. C., Esteveze-Tapiador, J. M. and Ribagorda, A. (2006). RFID Systems: A Survey on Security Threats and Proposed Solutions, *International Conference on Personal Wireless Communication- PWCA'06*, LNCS 4217, pp. 159–170, Albacete, Spain.
- [7] Moore, G. E. (1965), Cramming More Components onto Integrated Circuits. Electronics: <http://www.intel.com>, (1965).
- [8] Lopez, P. P. (2008). Lightweight Cryptography in Radio Frequency Identification (RFID) Systems, Ph. D. THESIS, UNIVERSIDAD CARLOS III DE MADRID. Madrid, Spain.
- [9] Oren, Y. and Feldhofer, M. (2009). A Low-Resource Public-Key Identification Scheme for RFID Tags and Sensor Nodes, Proceedings of the second ACM conference on Wireless network security (WiSec '09) (pp. 59–68), NY, USA.
- [10] Rabin, M. (1979). Digitized signatures and public key functions as intractable as factorization. Technical report, MIT, Cambridge, MA, USA.
- [11] Shamir, A. (1995) Memory efficient variants of public key schemes for smart card applications. In A. D. Santis (Ed.), *Advances in Cryptology, EUROCRYPT'94*, LNCS, vol. 950, page 445–449, Springer-Verlag, Perugia, Italy.
- [12] McEliece, R. (1978). A public key cryptosystem based on algebraic coding theory. *The Deep Space Network Progress Report*, (pp. 114-116), DSN PR 42–44.
- [13] Niederreiter, H. (1986). Knapsack-type cryptosystems and algebraic coding theory, *Problems of Control and Information Theory*, 15(2), pp. 159–166.
- [14] Bringer, J., Chabanne, H. and Icart, T. (2008). Cryptanalysis of EC-RAC, a RFID Identification Protocol, In M. K. Franklin, L. C. K. Hui, and D. S. Wong, (Ed.), *CANS 2008*(pp. 149–161), LNCS 5339 Springer, Hong-Kong, Chiana.
- [15] Bringer, J., Chabanne, H. and Icart, T. (2009). Efficient Zero-Knowledge Identification Schemes which respect Privacy, In W. Li, W. Susilo, U. K. Tupakula, R. Safavi-Naini, and V. Varadharajan (Ed.), *Proceedings of the 4<sup>th</sup> International Symposium on Information, Computer, and Communications Security, ASIACCS* (pp. 195–205), Sydney, Australia.
- [16] Cayrel, P. L., Veron, P. and Alaoui, S. M. E. Y. (2011). A Zero-Knowledge Identification Scheme Based on the q-ary Syndrome Decoding Problem, In A.

- Biryukov, G. Gong and D. R. Stinson (Eds.), *SAC 2010* (pp. 171–186), LNCS 6544, Ontario, Canada.
- [17] Faugere, J.-C., Otmani, A., Perret, L. and Tillich, J.-P. (2010). Algebraic cryptanalysis of McEliece variants with compact keys, In: Gilbert, H. (ed.) *EUROCRYPT 2010* (pp. 279–298), LNCS 6110, Springer, Heidelberg, France.
- [18] Fiat, A. and Shamir, A. (1986). How to prove yourself: Practical solutions to identification and signature problems, In Andrew M. Odlyzko (Ed.), *Advances in Cryptology-CRYPTO'86*, (pp. 186–194), Santa Barba, California, USA.
- [19] Fiat, A. and Shamir, A. (1987). Unforgeable proofs of identity, *Securicom 87* (pp. 147–153). Paris, France.
- [20] Feige, U., Fiat, A. and Shamir, A. (1988). Zero-knowledge proofs of identity, *J. Cryptology*, vol. 1(2), pp. 77–94.
- [21] Gauthier Umana, V. and Leander, G. (2009). Practical key recovery attacks on two McEliece variants, *IACR ePrint Archive*, <http://eprint.iacr.org/2009/509.pdf>
- [22] Guilion, L. C. and Quisquater, J. J. (1988). A “paradoxical” identity-based signature scheme resulting from zero knowledge, In Shafi Goldwasser, (Ed.), *Advances in Cryptology CRYPTO '88*(pp. 216–231). *8<sup>th</sup> Annual International Cryptology Conference*, Santa Barba, California, USA.
- [23] Micali, S. and Shamir, A. (1988). An improvement of the Fiat-Shamir identification and signature scheme. In Shafi Goldwasser, (Ed.). *Advances in Cryptology CRYPTO '88, 8<sup>th</sup> Annual International Cryptology Conference* (pp. 244–247). Santa Barba, California, USA.
- [24] Peters, C. (2009). Information-set decoding for linear codes over  $F_q$ , *ICAR Archive*: <http://eprint.iacr.org/2009/589>.
- [25] Quisquater, J. J. and Guilion, L. (2000). The new Guilion Quisquater Scheme, *In Proceedings of the RSA 2000 conference*.
- [26] Shamir, A. (1987). The search for provably secure identification schemes, *Proceedings of the International Congress of Mathematicians*(pp. 1488–1495), Berkeley, CA, USA.
- [27] Stern, J. (1989a). A method for finding codewords of small weight. In Wolfmann, J., Cohen, G. (eds.), *Coding Theory and Applications 1988* (pp. 106–113), LNCS 388, Springer, Heidelberg, Toulon, France.
- [28] Stern, J. (1989b). A method for finding codewords of small weight. In Wolfmann, J., Cohen, G. (eds.), *Coding Theory and Applications 1988* (pp. 106–113), LNCS 388, Springer, Heidelberg, Toulon, France.
- [29] Stern, J. (1994). A new identification scheme based on syndrome decoding, In: Stinson, D. R. (ed.) *CRYPTO 1993* (pp. 13–21), LNCS 773, Springer, Heidelberg, Santa Barbara, California, USA.
- [30] Aguilar, C., Gaborit, P. and Schrek, J. (2011). A new zero-knowledge code based identification scheme with reduced communication, *CoRR abs/1111.1644*.
- [31] Chiang, J. T., Haas, J. and Hu, Y. C. (2009). Secure and Precise Location Verification Using Distance Bounding and Simultaneous Multilateration, *Proc. Second ACM Conf. Wireless Network Security (WiSec '09)* (pp. 181–192), Zurich, Switzerland.
- [32] Hancke, G. and Kuhn, M. (2005). An RFID Distance Bounding Protocol, *In Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm)* (pp. 67–73), Athens.

- [33] Molnar, D., Soppera, A. and Wagner, D. (2006). A scalable delegatable pseudonym protocol enabling ownership transfer of RFID tags, *In Selected Areas in Cryptography* (pp. 276–290), Kingston, ON, Canada.
- [34] Saito, J., Imamoto, K. and Sakurai, K. (2005). Reassignment scheme of an RFID tags key for owner transfer, *Embedded and Ubiquitous Computing* (pp. 1303–1312), Nagasaki, Japan.
- [35] Tippenhauer, N. and Capkun, S. (2009). Id-Based Distance Bounding and Localization, *Proc. 14<sup>th</sup> European Conf. Research in Computer Security (ESORICS '09)* (pp. 621–636), Saint-Malo, France.
- [36] Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M. and Ribagorda, A. (2011a). Attacking RFID Systems, In Harold F., Nozaki K., Tipton, M. (Ed.), *Information Security Management Handbook* (pp. 313–334), Auerbach Publications.
- [37] Peris-Lopez, P. Orla, A., Hernandez-Castro, J. C. and Lubbe, J. C. (2011b). Flaws on RFID grouping-proofs. Guidelines for future sound protocols, *in Journal of Network and Computer Applications*, 34(3), pp. 833–845.
- [38] Chandran, N., Goyal, V., Moriarty, R. and Ostrovsky, R. (2009). Position Based Cryptography, *Proc. Int'l Cryptology Conf. (CRYPTO'09)* (pp. 391–407), Santabarbara, CA, USA.
- [39] Shmatikov, V. and Wang, M. H. (2007). Secure Verification of location claims with Simultaneous Distance Modification, *Proc. 12<sup>th</sup> Ann. Asian Computing Science Conf. (Asian '07)* (pp. 181–195), Doha, Qatar.
- [40] Wei, Y. Yu, Z. and Guan, Y. (2013). Location verification algorithms for wireless sensor networks, *IEEE Transactions on Parallel and Distributed Systems*, 24(5), pp. 938–950.
- [41] Gaborit, P. and Girault, M. (2007). Lightweight code-based identification and signatures, *IEEE International Symposium on Information Theory 2007, ISIT 2007* (pp. 191–195), Nice.
- [42] Burmester, M. and Munilla, J. (2011). Lightweight RFID Authentication with Forward and Backward Security, *ACM Transactions on Information and System Security*, 14 (1), pp. 11:1–11:26.
- [43] Cao, T., Bertino, E. and Lei, H. (2009). Security analysis of the SASI protocol, *IEEE Transactions on Dependable and Secure Computing*, 6 (1), pp. 73–77.
- [44] Sun, H.-M., Ting, W. C., and Wang, K. H. (2011). On the security of Chien's ultralightweight RFID authentication protocol, *IEEE Transaction on Dependable and Secure Computing*, 8 (2), pp. 315–317.
- [45] Juels A. (2005). RFID security and privacy: A research survey, *IEEE Journal on Selected Areas in Communication*, 24 (2), pp. 381–394.
- [46] Koh, R., Schuster, E. and Chackrabarti, I. (2003). A Bellman, Securing the pharmaceutical supply chain, White Paper, Auto-ID Labs, Massachusetts Institute of Technology.
- [47] Takaragi, K. Usami, M., Imura, R., Itsuki, R. and Satoh, T. (2001). An ultra small individual recognition security chip, *IEEE Micro*, 21(6), pp. 43–49.
- [48] Lehtonem, M., Staake, T., Michahelles, F. and Fleisch, E. (2007). From Identification to Authentication-A Review of RFID Product Authentication Techniues, *Networked RFID Systems and Lightweight Cryptography*, P. H. Cole, D. C. Ranasinghe (Ed.), pp. 169–187.
- [49] Yu, S., Ren, K. and Lou, W. (2007) A Privacy-preserving Lightweight

Authentication Protocol for Low-Cost RFID Tags. *Military Communication Conference, MILCOM 2007* (pp. 1–7), Orlando, FL, USA.

[50] Burmester, M., Le, T. V. and Medeiros, B. D. (2009). Universally Composable RFID Identification and Authentication Protocols, *ACM Transaction on Information and Systems Security*, 2(4), pp. 21:1–21:33.

[51] Mitra, M. (2008). Privacy for RFID systems to prevent tracking and cloning, *International Journal of Computer Science and Network Security*, 8(1), pp. 1–5.

[52] Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., Li, T. and Lubbe, J. C. A. van Der, (2010). Weaknesses in Two Recent Lightweight RFID Authentication Protocols, *Information Security and Cryptology* (pp. 383–392), Beijing, China.

[53] Tian, Y., Chen G. and Li, J. (May 2012). A New Ultralightweight RFID Authentication Protocol with Permutation, *IEEE Communications Letters*, 16(5), pp. 702–705.

[54] Haber, S. and Stornetta, W. (1991). How to time-stamp a digital document, *Journal of Cryptology*, 3(2), pp. 99–111.

[55] Deursen TV and Radomirovie S. (2010). EC-RAC: Enriching a Capacious RFID Attack Collection, *RFIDSec 2010* (pp. 75–90), Istanbul, Turkey.

[56] Fan, J., Hermans, J. and Vercauteran, F. (2010). On the claimed privacy of EC-RAC III, *RFIDSec 2010* (pp. 66–74), Istanbul, Turkey.

[57] Chien, H. Y. and Liu, S. B. (2009). Tree-Based RFID Yoking Proof, *International conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC'09)*, pp. 550–553.

[58] Due, D. N. and Kim, K. (2009). Grouping-proof protocol for rfid tags: Security definition and scalable construction, *Cryptology ePrint Archive*, Report 2009/609, <http://eprint.iacr.org/>

[59] Burmester, M., de Medeiros, B. and Motta, R. (2008). Provably Secure Grouping Proofs for RFID Tags, *Proceedings of the 8th Smart Card Research and Advanced Applications-CARDIS 2008*(pp. 176–190), Springer, Royal Holloway University of London, UK.

[60] Cheng, Z. Y., Liu, Y., Chang, C. C. and Chang, S.C. (2013). Authenticated RFID security mechanism based on chaotic maps, *Security and Communication Networks*, 6(2), pp. 247–256.

[61] Akgun, M. and Caglayan, M. U. (2013). Weaknesses in a Recently Proposed RFID Authentication Protocol, *IACR Cryptology ePrint Archive*: <https://eprint.iacr.org/2013/855>.

[62] Biasi, F. P., Barreto, S. L. M. B., Misoczki, R. and Ruggiero, W. V. (2012). Scaling efficient code-based cryptosystems for embedded platforms, *CoRR*, <abs/1212.4317>

[63] Mujahid, U., Najam-ul-islam, M., Ahmed, J. and Mujahid, Us. (2013). Cryptanalysis of ultralightweight RFID authentication protocol, *Cryptology ePrint Archive*, Report 2013/385.

[64] Pearson, J. (2005). Securing the pharmaceutical supply chain with RFID and public key infrastructure (PKI) technologies, *Texas instruments White Paper*, Available from: <http://www.ti.com/rfid/docs/docntr.shtml>

[65] Nochta, Z., Staake, T. and Fleisch, E. (2006). Product Specific Security Features Based on RFID Technology, *International Symposium on Applications and the Internet*



- Workshops (SAINTW'06), 2006 (pp. 72-75).Phoenix, AZ.
- [66] Qingling, C., Yiju, Z. And Yonghua, W. (2008). A minimalist mutual authentication protocol for RFID system and BAN logic analysis. *CCCM 2008* (pp. 449–453), Guangzhou.
- [67] Liu, Y., Qin, X., Wang, C. and Li, B. (2013). A Lightweight RFID Authentication Protocol based on Elliptic Curve Cryptography, *Journal of Computers*, 8(11), pp. 2880–2887.
- [68] Cho, J.-S., Yeo, S.-S, Hwang, S., Rhee, S.-Y. And Kim, S. K. (2008). Enhanced yoking proof protocols for RFID tags and tag groups. *International Conference on Advanced Information Networking and Applications- Workshop-AINAW 2008* (pp. 1591–1596), IEEE Computer Society, Okinawa, Japan, pp. 1591–1596.
- [69] Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M. and Ribagorda, A. (2007). Solving the Simultaneous Scanning Problem Anonymously: Clumping Proofs for RFID Tags, In *IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing-SecPerU 2007*(pp. 55–60), IEEE, IEEE Computer Society Press, Istanbul, Turkey.
- [70] Piramuthu, S. (2006). On Existence Proofs for Multiple RFID Tags, *IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing –SecPerU 2006*, IEEE, IEEE Computer Society Press, Lyon, France.
- [71] Juels, A. (2004). Yoking-Proofs for RFID Tags, In: Sandhu, R., Thomas, R. (Eds.), *International Workshop on Pervasive Computing and Communication Security- PerSec 2004* (pp. 138–143), IEEE, IEEE Computer Society, Orlando, Florida, USA.
- [72] Juels, A. (2006). RFID Security and Privacy: A Research Survey, *IEEE Journals on Selected Area in Communications*, 24(2), pp. 381–394.
- [73] Lin, E.-C., Lai, Y.-C., Tygar, J. D., Yang, C.-K. and Chiang, C.-L. (2007). Coexistence proof using chain of timestamps for multiple RFID tags, In: Chang, K. C.-C., Wang, W., Chen, L., Ellis, C. A., Hsu, C.-H., Tsoi, A. C., Wang, H. (Eds.), *International Workshop on DataBase Management and Application over Networks – DBMAN 2007* (pp. 634–643), LNCS 4537, Springer-Verlag, Huang Shan, China.
- [74] Saito, J. and Sakurai, K. (2005). Grouping Proof for RFID Tags, *International Conference on Advanced Information Networking and Applications-AINA*, (pp. 621–624), Taiwan.
- [75] Bagheri, N. And Safkhani, M. (2013). Secret Disclosure attack on Kazahaya, a Yoking-Proof For Low-Cost RFID Tags, *IACR Cryptology ePrint Archive 2013*: 453. <https://eprint.iacr.org/2013/453.pdf>
- [76] Hung-Yu Chein and Chen-Wei Huang. (2007). A lightweight RFID protocol using substring, In *Embedded and Ubiquitous Computing (EUC 2007)* (pp. 422–431), Taipei, Taiwan.
- [77] Ahmadian, Z., Salmasizadeh, M. and Reza Aref, M. (2013). Desynchronization Attack on RAPP Ultralightweight Authentication Protocol, *Information Processing Letters*, 113(7), pp. 206–209.



# Security and Privacy of PUF-Based RFID Systems

*Ferucio Laurențiu Țiplea, Cristian Andriesei  
and Cristian Hristea*

## Abstract

The last decade has shown an increasing interest in the use of the physically unclonable function (PUF) technology in the design of radio frequency identification (RFID) systems. PUFs can bring extra security and privacy at the physical level that cannot be obtained by symmetric or asymmetric cryptography at the moment. However, many PUF-based RFID schemes proposed in recent years do not even achieve the lowest privacy level in reputable security and privacy models, such as Vaudenay's model. In contrast, the lowest privacy in this model can be achieved through standard RFID schemes that use only symmetric cryptography. The purpose of this chapter is to analyze this aspect. Thus, it is emphasized the need to use formal models in the study of the security and privacy of (PUF-based) RFID schemes. We broadly discuss the tag corruption oracle and highlight some aspects that can lead to schemes without security or privacy. We also insist on the need to formally treat the cryptographic properties of PUFs to obtain security and privacy proofs. In the end, we point out a significant benefit of using PUF technology in RFID, namely getting schemes that offer destructive privacy in Vaudenay's model.

**Keywords:** Radio Frequency Identification (RFID), Physically Unclonable Function (PUF), security, privacy

## 1. Introduction

Although the roots of the *Radio Frequency Identification* (RFID) technology can be traced back to World War II, the ancestor of modern RFID technology was introduced by Cardullo and Parks in 1973 [1] when the two proposed a passive radio transponder with memory. In recent years, RFID technology has become increasingly popular and its applicability has expanded to more and more diverse and complex domains and systems. It is worth mentioning here process automation, tracking and identification, toll collection, public transportation, national IDs and passports, medical healthcare systems, pharmaceutical systems, and so on.

From a scientific point of view, RFID has become a well-defined research field, counting more than fifteen thousand scientific papers and books indexed by IEEE, Springer, and Elsevier, and more than twenty-two thousand patents or patent applications indexed by the most essential three regional patent databases (USA, Europe, and Japan) [2]. All of these highlight a rich palette of research directions in RFID technology, such as: system implementation, design principles, chipless implementations, IoT integration, security, and so on.

An interesting aspect is that most of the RFID references cover technical aspects, applications, and protocol design, very few addressing security and privacy issues. The conclusion is that very few research papers dealing with RFID implementation or application start with security and privacy in mind. Obviously, there are RFID applications for which security and privacy are not so vital, such as human activity recognition (e.g., smart gym), environmental corrosive monitoring, soil monitoring, and so on. However, for other fields like people identification or healthcare systems [3, 4], security and privacy are crucial issues.

Attempts to improve the authentication process in RFID systems or make them resistant to physical attacks (tag corruption, for example) have led to the need to insert unclonable or tamper-evident physical objects into tags. Unclonability offers unique fingerprints to tags, while the tamper-evidence property would protect against corruption. Thus, physically unclonable functions (PUFs) [5–7] have found themselves a suitable application in RFID technology and the researchers have already proposed a large spectrum of PUF-based RFID systems. However, the inclusion of PUFs in RFID systems (especially on tags) raises two key questions:

1. Are PUFs more efficient in implementation than ordinary cryptographic primitives?
2. Do PUFs provide security and privacy that standard cryptographic primitives cannot provide?

As with respect to the first question it is worth noting that an RFID implementation with strong security properties comes with increased cost for the final RFID product. This is the reason why some authors take into account the concept of *cost-effective protocol* [8]. As discussed in [9], the installation costs of current RFID solutions, not necessarily with improved hardware security, are not cheap at all, many different costs being involved when installing an RFID system (including maintenance and training).

As with respect to the second question, PUFs certainly offer security features that standard cryptographic primitives cannot provide. But if these security features are not used in a corresponding way, the result may be worse than if PUFs are not included. The lack of understanding of such issues has led many authors to propose PUF-based RFID schemes that are insecure or not at all private [10, 11] when analyzed in reputable models such as Vaudenay's security and privacy model [12, 13].

In this chapter, we want to highlight:

- The need to use PUFs in the construction of secure and private RFID schemes;
- The need to formalize the properties of PUFs to achieve provable security;
- The erroneous use of PUFs that does nothing but lead to insecure schemes and a lack of privacy.

The whole discussion is conducted on Vaudenay's security and privacy model. This model is currently considered one of the best RFID security and privacy models, offering a classification of the privacy of RFID schemes into eight classes. It is known that the strong privacy class cannot be obtained in this model, while the destructive privacy class can be obtained by using the PUF technology. This gives us an excellent example that justifies the opportunity to use PUFs in RFID technology.

## 2. RFID schemes and systems

An RFID system [14, 15] consists of a *reader*, a set of *tags*, and a *communication protocol* between reader and tags. The reader is a transceiver<sup>1</sup> that is connected through a secure channel with a back-end server, which is a powerful device that maintains a database with tag information. The reader's task is to identify *legitimate tags* (that is, tags with information stored in its database) and to reject all other incoming communication. The reader and its database are trusted entities, and the communication between them is secure. Many RFID protocols proposed so far do not make any separation between the reader and the back-end server. For this reason, the back-end server functions are considered to be taken over by the reader and, as a result, the reader is considered a powerful device not computationally restricted that can perform any cryptographic operation.

Opposite the reader, tags are small transponder<sup>2</sup> devices that are considered to be resource constrained. Depending on their class, they can perform only logical operations, symmetric encryption, or even public key cryptography. In practical scenarios, tags are attached to various items or carried by persons in order to facilitate some services when they are identified by readers.

The memory of a tag is typically split into *permanent* (or *internal*) and *temporary* (or *volatile*). The permanent memory stores the state values of the tag, while the temporary memory can be viewed as a set of *temporary variables* used to carry out the calculations required by the communication protocol. There are two types of temporary variables:

1. *local temporary variables*, used by tags only to do computations in a given protocol step;
2. *global temporary variables*. These get values in a given protocol step to be used in another protocol step.

From a formal point of view, an RFID scheme is defined as follows. Let  $\mathcal{R}$  be a *reader identifier* and  $\mathcal{T}$  be a set of *tag identifiers* whose cardinal is polynomial in some *security parameter*<sup>3</sup>  $\lambda$ . An *RFID scheme over*  $(\mathcal{R}, \mathcal{T})$  [12, 13] is a triple  $S = (\text{Setup}_R, \text{Setup}_T, \text{Ident})$  of *probabilistic polynomial time* (PPT) *algorithms*<sup>4</sup>, where:

1.  $\text{Setup}_R(\lambda)$  inputs a security parameter  $\lambda$  and outputs a triple  $(pk, sk, DB)$  consisting of a key pair  $(pk, sk)$  and an empty database  $DB$ .  $pk$  is public, while  $sk$  is kept secret by reader;
2.  $\text{Setup}_T(pk, ID)$  initializes the tag identified by  $ID$ . It outputs an initial tag state  $S$  and a tag specific secret  $K$ . The pair  $(ID, K)$  is stored in the reader's database  $DB$ ;

---

<sup>1</sup> Contraction from transmitter and receiver.

<sup>2</sup> Contraction from transmitter and responder.

<sup>3</sup> A security parameter usually specifies a minimum security value, such as the minimum length of an encryption key.

<sup>4</sup> A probabilistic (or randomized) algorithm is an algorithm that uses uniformly random bits as an auxiliary input to guide its behavior, in the hope of achieving good performance in the "average case" over all possible choices of random bits. A polynomial time algorithm is an algorithm that runs in polynomial time with respect to the size of its input.

3.  $Ident(pk; \mathcal{R}(sk, DB); ID(S))$  is an interactive protocol between the reader identified by  $\mathcal{R}$  (with its private key  $sk$  and database  $DB$ ) and a tag identified by  $ID$  (with its state  $S$ ) in which the reader ends with an output consisting of  $ID$  or a special symbol  $\perp$ . The tag may end with no output (*unilateral authentication*), or it may end with an output consisting of  $OK$  or  $\perp$  (*mutual authentication*).

By calling  $SetupR(\lambda)$  one should understand that a reader identified by  $\mathcal{R}$  is created, initialized, and some public parameters of the system are also established. We simply refer to the reader such created as being  $\mathcal{R}$ . By calling  $SetupT(pk, ID)$ , a tag identified by  $ID$  is created, initialized, and registered with the reader by storing some information about it in  $DB$ . We denote this tag by  $\mathcal{T}_{ID}$ . The meaning of the reader's output  $ID$  ( $\perp$ ) is that it authenticates (rejects) the tag. Similarly, the tag outputs  $OK$  ( $\perp$ ) when it authenticates (rejects) the reader.

The *correctness* of an RFID scheme means that regardless of how the system is set up, after each complete execution of the interactive protocol between the reader and a legitimate tag, the reader outputs the tag's identity with overwhelming probability. For mutual authentication, correctness asks for one more requirement, namely that the tag outputs  $OK$  with overwhelming probability.

An *RFID system* is an instantiation of an RFID scheme. This is done by a trusted operator  $\mathcal{F}$  who runs the RFID scheme over a reader identifier  $\mathcal{R}$  and a set  $\mathcal{T}$  of tag identifiers. In a given setting, the reader is initialized exactly once, while each tag at most once. Thus, the reader's database does not store multiple entries for the same tag. However, different settings with the same RFID scheme may initialize the reader and the tags in different ways.

We close the section by an example of a fundamental RFID scheme, namely the PRF-based RFID scheme proposed in [13]. To describe the scheme, let us assume that  $\lambda$  is a security parameter,  $\ell_1(\lambda)$  and  $\ell_2(\lambda)$  are two polynomials, and  $F = (F_K)_{K \in \mathcal{K}}$  is a *pseudo-random function*<sup>5</sup> (PRF), where  $F_K : \{0, 1\}^{2\ell_1(\lambda)} \rightarrow \{0, 1\}^{\ell_2(\lambda)}$  for all  $K \in \mathcal{K}$ .

Each tag is equipped with a random key  $K$  and has the capacity to compute  $F_K$ . The reader maintains a database  $DB$  with entries for all legitimate tags. Each entry is a vector  $(ID, K)$ , where  $ID$  is the tag's identity and  $K$  is its random key.

The protocol is given in **Figure 1** (the use of " $\leftarrow$ " specifies a random selection of an element from a set). As we can see, the reader sends initially a random

	Reader ( $DB$ )	Tag ( $K$ )
1	$x \leftarrow \{0, 1\}^{\ell_1(\lambda)}$	$\underline{x}$
2		$\underline{y, z} \quad y \leftarrow \{0, 1\}^{\ell_1(\lambda)}, z = F_K(x, y)$
	If $\exists (ID, K) \in DB$ s.t. $z = F_K(x, y)$ then output $ID$ (tag auth.) else output $\perp$	

**Figure 1.**  
PRF-based RFID scheme.

<sup>5</sup> A pseudo-random function is a collection  $F = (F_K)_K$  of efficiently-computable functions with the property that no efficient algorithm can distinguish (with significant probability) between a function chosen randomly from this family and a random function (a function whose outputs are fixed at random).

$x \leftarrow \{0, 1\}^{\ell_1(\lambda)}$  to the tag. On receiving it, the tag generates a random  $y \leftarrow \{0, 1\}^{\ell_1(\lambda)}$ , computes  $z = F_K(x, y)$ , and answers with  $(y, z)$ . The reader checks its database for a pair  $(ID, K)$  such that  $z = F_K(x, y)$ . If such a pair is found, it outputs  $ID$  (that is, authenticates the tag); otherwise, outputs  $\perp$ .

### 3. Security and privacy models for RFID

The design of an RFID scheme must start from consistent motivations for its usefulness and the desired security and privacy level, in a particular model of security and privacy, for the scheme to be proposed. The second desideratum requires that proofs of security and privacy accompany the proposed scheme. Ideally, the scheme designer should know in advance security and privacy models for RFID schemes and thus to offer his scheme in such a model. However, the practice shows that, although various fairly good security and privacy models have been proposed over time, many authors propose RFID schemes for which they study security and privacy in an ad hoc way without referring to the existing models. It is not surprising then that many of these schemes, analyzed in reputable models, do not reach the lowest level of security or privacy [11].

In this section, we aim to discuss one of the most critical security and privacy models for RFID, namely Vaudenay's model. We argue that this model falls into the class of gray-box models, and then make a consistent analysis of the corruption oracle in this model. The emphasis on this oracle is more than necessary, both for ordinary tags and for tags endowed with physically unclonable functions.

The discussion in this section can also be rephrased for other models that offer the corruption ability to the adversary, such as the model based on indistinguishability proposed in [16]. However, the choice of Vaudenay's model for the discussion in this chapter is a matter of the authors' scientific taste and their belief that it is one of the fundamental models for studying security and privacy properties of RFID schemes.

#### 3.1 Security and privacy models

A *security* or *privacy model* for a cryptographic construction consists of an *attack model* and a *security* or *privacy goal*, respectively. The attack model specifies the adversary's power, while the security or privacy goal specifies the property we are interested to be achieved by the cryptographic construction. Nowadays, researchers differentiate between three attack models [17]:

1. The *black-box model*: this is the traditional model where the adversary can only observe the response of the cryptographic construction when it is queried by inputs of the adversary's choice (the adversary may know the algorithms used in the cryptographic construction);
2. The *gray-box model*: this includes the black-box model and supplementary the adversary may use side-channel information such as power consumption, electro-magnetic radiation, or timing information;
3. The *white-box model*: this has been introduced in particular for software implementation of the cryptographic constructions. In this model, the adversary is assumed to have full control over the implementation and its execution environment.

For instance, the security model IND-CCA means that the security goal is *indistinguishability (semantic security)* and the attack model is the *chosen ciphertext attack* [18]. The power of the adversary in this model is specified by giving him access to an *encryption and decryption oracles* that assists the adversary to collect a polynomial size set of (plaintext,ciphertext) pairs.

The black-box model does not depend on the software or hardware implementation, platform, and so on. In contrast to it, the gray-box model of attack exploits the algorithm/protocol implementation. For instance, the side-channel analysis that can be used with this model may take into account fluctuations in timing delays, power consumption, or emitted signals and radiation [19]. The result of such an analysis varies depending on the implementation, the platform on which it is implemented, the measuring devices. Side-channel analysis is local and not global.

### 3.2 Vaudenay's RFID security and privacy model

One of the most influential security and privacy model for RFID is *Vaudenay's model* [12, 13]. In this model, the adversary is a PPT algorithm that is allowed to interact with the RFID scheme. This means that the adversary may create tags to play with them as being the reader (but without having direct access to the reader's database). The adversary may also play with the reader as being any of the tags created by it. Depending on the adversary, it may or may not have access to the tags' internal memory. From a formal point of view, the adversary interacts with the RFID scheme by means of a set of oracles. Before describing these oracles, we mention that each tag in Vaudenay's model is either *free* (i.e., outside the interaction area of the adversary) or *drawn* (i.e., in the interaction area of the adversary). When a tag is created, it is free. The adversary may draw a free tag at any time and, in the end, to free it.

Now, the oracles in Vaudenay's model are the following:

1. *CreateTag<sup>b</sup>(ID)*: When the adversary queries this oracle by *ID* for some bit *b*, the oracle calls the algorithm *SetupT(pk, ID)* to generate a pair  $(K, S)$  and create a tag  $\mathcal{T}_{ID}$  with the identifier *ID* and initial state *S*. If  $b = 1$ ,  $(ID, K)$  is added to *DB* and the tag is considered *legitimate*; otherwise ( $b = 0$ ), the tag is considered *illegitimate*. The tag thus created is considered *free*;
2. *DrawTag( $\delta$ )*: By this oracle, the adversary is allowed to interact with free tags according to some probability distribution  $\delta$  (on these tags). Therefore, this oracle chooses a number of free tags according to  $\delta$ , let us say *n*, generates *n* temporary identities  $vtag_1, \dots, vtag_n$ , and outputs  $(vtag_1, b_1, \dots, vtag_n, b_n)$ , where  $b_i$  specifies whether the tag  $vtag_i$  is legitimate or not. All these tags are considered now *drawn*.

As one can see, *DrawTag* provides the adversary with access to some free tags by means of temporary identifiers, and gives information on whether the tags are legitimate or not (but no other information);

3. *Free(vtag)*: By this oracle, the adversary may free the drawn tag *vtag*. The identifier *vtag* will no longer be used. We assume that when a tag is freed, its temporary state is erased. This is a natural assumption that corresponds to the fact that the tag is no longer powered by reader;



4. *Launch()*: When the adversary queries this oracle, it means that it wants to launch a new protocol instance. Therefore, the oracle returns to it a unique identifier to be used with this protocol instance;
5. *SendReader*( $m, \pi$ ): By this oracle, the adversary gets the reader's answer when the message  $m$  is sent to it as part of the protocol instance  $\pi$ . When  $m$  is the empty message, abusively but suggestively denoted by  $\emptyset$ , this oracle outputs the first message of the protocol instance  $\pi$ , assuming that the reader does the first step in the protocol. We emphasize that the reader's answer is conceived as the message sent to the tag by the communication channel and not as the reader's decision output (tag identity or  $\perp$ ). Therefore, if the reader does not send anything to the tag, the output of this oracle is empty;
6. *SendTag*( $m, vtag$ ): This oracle outputs the tag's answer when the message  $m$  is sent to the tag referred to by  $vtag$ . When  $m$  is the empty message, this oracle outputs the first message of the protocol instance  $\pi$ , assuming that the tag does the first step in the protocol. As in the case of the *SendReader* oracle, we emphasize that the tag's answer is conceived as the message sent to the reader by the communication channel and not as the tag's decision output (*OK* or  $\perp$ ). Therefore, if the tag does not send anything to the reader, the output of this oracle is empty;
7. *Result*( $\pi$ ): By this oracle, the adversary is allowed to know the reader's decision with respect to the authentication of the tag in session  $\pi$ . More precisely, the oracle outputs  $\perp$  if in session  $\pi$  the reader has not yet made a decision on tag authentication (this also includes the case when the session  $\pi$  does not exist), 1 if in session  $\pi$  the reader authenticated the tag, and 0 otherwise (this oracle is both for unilateral and mutual authentication);
8. *Corrupt*( $vtag$ ): This oracle outputs the current permanent (internal) state of the tag referred to by  $vtag$ , when the tag is not involved in any computation of any protocol step (that is, the permanent state before or after a protocol step).

It is customary to assume that the RFID tags can be corrupted to reveal not only their permanent memory but also the global temporary variables [20]. When the *Corrupt* oracle is considered in such a way, we will refer to Vaudenay's model as being *Vaudenay's model with temporary state disclosure*. We emphasize that "corruption with temporary state disclosure" means corruption of the permanent state and of the global temporary variables, but not of the local temporary variables (more details are provided in Section 3.4).

Now, the adversaries are classified into the following classes, according to the access they get to these oracles:

- *Weak adversaries*: they do not have access to the *Corrupt* oracle;
- *Forward adversaries*: if they access the *Corrupt* oracle, then they can only access the *Corrupt* oracle;
- *Destructive adversaries*: after the adversary has queried *Corrupt*( $vtag$ ) and obtained the corresponding information, the tag identified by  $vtag$  is destroyed and the temporary identifier  $vtag$  will no longer be available. The database *DB* will still keep the record associated to this tag (the reader does not know the tag was destroyed). As a consequence, a new tag with the same identifier cannot be

created (in this approach, the database cannot store multiple records for the same tag identifier);

- *Strong adversaries*: there are no restrictions on the use of oracles.

If we further restrict the adversary to access the *Result* oracle, we obtain four new classes: *narrow weak*, *narrow forward*, *narrow destructive*, and *narrow strong*.

Now we are ready to introduce the *tag* and *reader authentication* properties as proposed in [12, 13], simply called the *security* of RFID schemes.

An RFID scheme has the property of *tag authentication* if no strong adversary has more than a negligible advantage in causing the reader to authenticate an uncorrupted legitimate tag in a protocol instance where the reader had no conversation with that tag to lead upon its authentication.

An RFID scheme has the property of *reader authentication* if no strong adversary has more than a negligible advantage in causing an uncorrupted legitimate tag to authenticate the reader in a protocol instance where the tag had no conversation with the reader to lead upon its authentication.

*Privacy* in Vaudenay's model generalizes anonymity (which means that the tag ID cannot be inferred) and untraceability (which means that the equality of two tags cannot be inferred). Thus, privacy requires that no adversary can infer non-trivial tag ID relations from the protocol messages. The information provided by a protocol is trivial when the adversary may learn it without making effective use of the protocol messages. To formalize this, Vaudenay's model introduces the concept of a *blinder* that simulates the protocol for adversary without knowing any secret information of the tags or the reader. If this simulation does not change the adversary's output compared to the case when the adversary plays with the real protocol, then the protocol achieves privacy.

A *blinder* for an adversary  $\mathcal{A}$  that belongs to some class  $V$  of adversaries is a PPT algorithm  $\mathcal{B}$  that:

1. simulates the *Launch*, *SendReader*, *SendTag*, and *Result* oracles for  $\mathcal{A}$ , without having access to the corresponding secrets;
2. passively looks at the communication between  $\mathcal{A}$  and the other oracles allowed to it by the class  $V$  (that is,  $\mathcal{B}$  gets exactly the same information as  $\mathcal{A}$  when querying these oracles).

When the adversary  $\mathcal{A}$  interacts with the RFID scheme by means of a blinder  $\mathcal{B}$ , we say that  $\mathcal{A}$  is *blinded* by  $\mathcal{B}$  and denote this by  $\mathcal{A}^{\mathcal{B}}$ . We emphasize that  $\mathcal{A}^{\mathcal{B}}$  is allowed to query the oracles *Launch*, *SendReader*, *SendTag*, and *Result* only by means of  $\mathcal{B}$ ; all the other oracles are queried in the standard way.

Given an adversary  $\mathcal{A}$ , an RFID scheme  $S$ , and a blinder  $\mathcal{B}$ , define the following experiment (privacy game) that a challenger sets up for  $\mathcal{A}$ :

Privacy experiment  $RFID_{\mathcal{A},S,\mathcal{B}}^{prv}(\lambda)$

- 1:  $b \leftarrow \{0, 1\}$ ;
- 2: Set up the reader;
- 3:  $\mathcal{A}^b$  gets the public key  $pk$ ;
- 4:  $\mathcal{A}^b$  queries the oracles;
- 5:  $\mathcal{A}^b$  gets the secret table of the *DrawTag* oracle;
- 6:  $\mathcal{A}^b$  outputs a bit  $b'$ ;
- 7: Return 1 if  $b = b'$  and 0, otherwise,

where  $\mathcal{A}^0$  stands for  $\mathcal{A}$  and  $\mathcal{A}^1$  stands for  $\mathcal{A}^B$ .

An RFID scheme achieves privacy for a class  $V$  of adversaries if for any adversary  $\mathcal{A} \in V$  there exists a blinder  $\mathcal{B}$  such that  $\mathcal{A}$  has a negligible advantage over  $1/2$  to distinguish between the *real privacy game* (the bit  $b$  is 0 in  $RFID_{\mathcal{A},S,\mathcal{B}}^{prv}(\lambda)$ ) from the *blinded privacy game* (the bit  $b$  is 1 in  $RFID_{\mathcal{A},S,\mathcal{B}}^{prv}(\lambda)$ ).

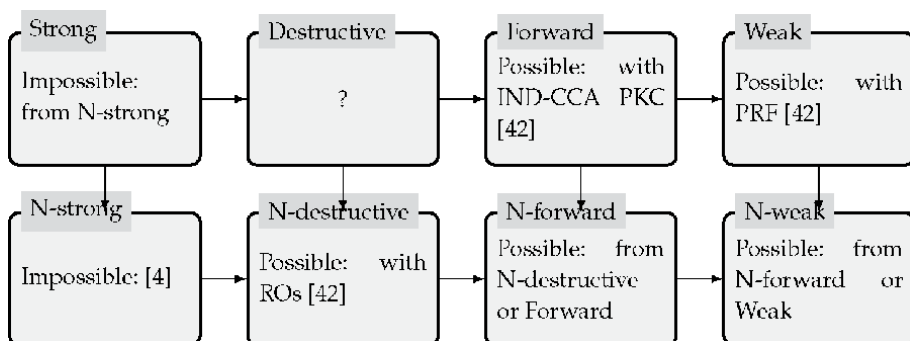
We thus obtain eight concepts of privacy: *strong privacy*, *narrow strong privacy*, *destructive privacy*, and so on. The diagram in **Figure 2** shows the relationship between the eight privacy concepts in Vaudenay’s model in the context of unilateral authentication. In this diagram, “N-x” is a shortcut for “narrow x”. An arrow from  $A$  to  $B$  means that  $A$ -privacy implies  $B$ -privacy.

### 3.3 Vaudenay’s model is a gray-box model

Let us take one last look at Vaudenay’s model to fit it into one of the three classes presented at the beginning of Section 3. The attack model associated with it falls in the class of gray-box models. Indeed, all the oracles except *Result* and *Corrupt* are specific to the black-box model because they do not output anything about the internal components of the algorithm implementation.

The *Result* oracle facilitates non-invasive side-channel analysis. Obviously, there may be situations in which the adversary can see the final result of the reader (the reader signals non-authentication of the tag, a gate opens, etc.). But, just as well, there are situations in which the adversary cannot see the final result of the reader without use of a specialized oracle. The analysis of Vaudenay’s model clearly shows that the *Result* oracle makes a big difference between protocols that ensure privacy against an adversary that has the possibility to use this oracle and protocols that ensure privacy against an adversary that does not have the possibility to use this oracle.

The *Corrupt* oracle provides the adversary with information about the internal memory of the tag. Although data stored in the internal memory of the tag (such as symmetric keys, public keys) does not depend on implementation or platform, it is internal information of the tag. The need for this oracle results from the fact that tags are devices with poor physical protection. For low-cost tags, corruption could be accomplished and thus the information stored in the permanent tag memory can be retrieved. Temporary (volatile) memory loses its data when the power is interrupted. However, the memory remanence effect may allow to recover some data. As a result, we can say that it is natural to consider the possibility of obtaining the information from the tag memory by various techniques called generically “corruption”. Once this information is obtained, the analysis is a theoretical one, abstracting the implementation.



**Figure 2.** Privacy and mutual authentication of RFID schemes in Vaudenay’s model without temporary state disclosure (PKC stands for public-key cryptography and RO for random oracle).

As a conclusion:

1. Vaudenay's attack model falls in the category of gray-box models. It provides the adversary with general information, including a limited amount of side-channel information that does not depend on the implementation or implementation platform;
2. Side-channel analysis that is not covered by Vaudenay's model comes as an additional analysis. It depends on the implementation of the protocol, implementation platform, measuring devices, etc.

### 3.4 Corruption with temporary state disclosure

When Vaudenay's model was proposed [13], it was somewhat unclear whether the *Corrupt* oracle returns the full (i.e., permanent and temporary) tag state or only the permanent one. This has also remained unclear in Paisie and Vaudenay's next year paper [12] on mutual authentication. While the distinction between full and permanent state did not have a negative impact on the results already obtained in the case of unilateral authentication, it highlighted several wrong results in the case of mutual authentication [21]. Thus, one of the results in [21], namely Theorem 1, says that there is no RFID scheme that achieves both reader authentication and narrow forward privacy in Vaudenay's model with temporary state disclosure. The argument is as follows. Given a blinder  $\mathcal{B}$ , one may construct an adversary  $\mathcal{A}_{sec}^{\mathcal{B}}$  against reader authentication so that, if the scheme is narrow forward private then  $\mathcal{A}_{sec}^{\mathcal{B}}$  has non-negligible advantage to authenticate itself as a valid reader. Going inside the proof, we remark that it is crucial the *Corrupt* oracle returns the full state of a tag in order to allow an adversary to perform the test by which the tag authenticates the reader. By this test, the adversary distinguishes with non-negligible probability between the real privacy game and the blinded one.

## 4. Physically unclonable functions

Purely cryptographic and mathematical techniques can provide security in a black-box or partially gray-box model. As we argued in the previous section, Vaudenay's model is a gray-box model. Within this model, no RFID scheme is known, built only on symmetric or asymmetric cryptographic primitives, which would offer destructive privacy. No one has indeed proved the non-existence of such a scheme, but we firmly believe that there is no such scheme. However, if we add physical security objects to the RFID schemes, then we can obtain RFID schemes that are destructive private [22].

Physically unclonable functions (PUFs) are possible candidates that can provide physical security in that they can ensure the secure generation and storage of the cryptographic keys [5–7]. A PUF can be seen as a *physical object* that evaluates a *noisy functions*: when queried with a challenge  $x$  it generates a response  $y$  that depends on both  $x$  and its unique and specific properties which are hard to *clone*. The PUFs are noisy because their specific properties can change with the operating conditions such as supply voltage or ambient temperature. So, PUFs may return slightly different responses when queried with the same challenge multiple times.

During the last years, the PUF concept attracted the attention of the research community and industry. Many research papers and patents focusing on

implementing distinct PUF architectures, larger systems employing PUFs as separate units or protocols dedicated to PUF-based implementations were proposed.

#### **4.1 PUF construction**

In principle, PUFs can be constructed with any physical entity or structure as long as an intrinsic mismatching or nonlinear behavior, inherent to such entity when implementing multiple alike, could be exploited.

For instance, two identical transistors designed in the same technology and on the same mask will show slightly different performances after implementing their layout (real physical circuit). The main difference will be noticed for the threshold voltage,  $V_{TH}$  in the case of CMOS process, different for both transistors. As such, a simple CMOS PUF could be obtained when implementing an array of identical transistors, this being also the first architecture reported in literature for chip identification [23] and disclosed in a patent application filed in 1989 [24]. Based on how challenges are applied to the circuit input and the great number of distinct responses (keys) that can be obtained, this particular PUF architecture is a strong PUF, at least according to PUF properties reiterated in [25]. A similar approach, yet implemented with bipolar transistors, was disclosed in a European patent application filed in 2013 [26].

Another example, even simpler, is that of a discrete electronic part, be it through-hole or surface-mount resistor or capacitor. It is well known that there are no two identical resistors or capacitors even though they have, theoretically, the same value and tolerance and are produced by the same manufacturer. Tolerance gives us valuable information about how much less or more the resistance or capacitance value is different of its nominal value. This sort of uncertainty favors PUF applications even though is not good from design perspective. And this is how the first RC PUF came into existence [27, 28].

Looking back, many PUF architectures have been proposed during the last two decades, various intrinsic properties being exploited, with many distinct classes identified [25]. This field encompasses so many implementations, technologies and design principles that two different perspectives to classify PUF architectures were used in that review. However, taking into account the scope and field of our study, i.e. RFID, we consider that the second classification (PUF tree), based on mechanism and evaluation parameter, is more relevant. In this regard, the PUF implementations fall into four classes: electronic, optical, radio frequency and magnetic PUFs. Furthermore, since RFID tags have limited chip area and (power) design constraints, it is obvious that electronic PUF architectures, known also as silicon-PUF, are of interest for our study.

Silicon-based PUFs involve conventional integrated circuit design techniques. Two essential design hints are identified regarding the implementation of a particular silicon-based PUF architecture:

1. A PUF architecture should generate at its output a unique sequence, useful either for authentication or cryptographic key generation, developed based on silicon intrinsic (physical) particularities. Therefore, no memory cells are allowed to store such a (PUF response) sequence. However, a (SRAM or DRAM) memory cell could be used to implement a PUF cell and thus generate a single bit of the PUF response because we are not interested in the binary value memorized in that cell but rather of the transition speed and delay, which are specific to that particular cell;

2. When it comes to intrinsic behavior, PUF construction starts either at transistor or system level. In the first case, it exploits certain anomalies in transistor functionality that could identify a particular circuit similar to a fingerprint, such implementation being reported in some references as analog PUF. In the second case, it uses specific differences that appear when connecting identical logic gates, as it is the case of ring oscillators or SRAM/DRAM cells array. In such implementation, the randomness property is based on intrinsic variations, at gate level, but the property is exploited and adjusted by digital designers in such manner that the spread of generated patterns (responses) is extended as much as possible. This is the reason why, such class of PUF architectures is reported in literature as digital PUF. The system-level approach favors FPGA based PUF implementations, the FPGA having all digital gates already manufactured, hence it lacks access to the transistor level. The most part of the PUF articles published during the last decade make use of FPGA. Either way, silicon PUF implementation is uniquely favored by the tolerance inherent to manufacturing process, the leading cause of device mismatching. It seems that what deteriorates the real performances of a particular silicon product, becomes quite useful for chip identification/cloning detection and key generation.

Silicon PUFs are still the most appealing ones because they occupy a very small chip area, especially when implemented in smaller technologies ( $\leq 65$  nm CMOS process), therefore they can be integrated into larger electronic units and systems (such as RFID). In addition, their design and preliminary testing on FPGA development boards ensure their proof of concept reproducibility, feasibility and success, before going deeper to implement a dedicated chip. A selection of representative silicon PUF architectures reported in literature is given below (for more details the reader may consult [6, 20, 29]):

- 2000:** Threshold voltage (TV) PUF [24];
- 2002:** Ring oscillator (RO) PUF [30];
- 2004:** Arbiter PUF (APUF) [31];
- 2007:** SRAM PUF [32], LATCH PUF [33];
- 2008:** Butterfly (B) PUF [34], D Flip-Flop (DFF) PUF [35];
- 2009:** Power distribution (PD) PUF [36], CNN PUF [37];
- 2010:** Super High Information Content (SHIC) PUF [38], Glitch PUF [39];
- 2011:** Pseudo-LFSR (PL) PUF [40];
- 2012:** Buskeeper PUF [41];
- 2013:** Micro-electrico-mechanical system (MEMS) PUF [42];
- 2014:** Transient effect RO (TERO) PUF [43];
- 2015:** Dynamic random access memory (DRAM) PUF [44], SA\_PUF [?];
- 2016:** D-PUF [45];
- 2017:** Aging-resistant Current-starved RO (ACRO) PUF [46];
- 2018:** Cryptanalysis/Robust Multiplexer-based PUF (cMPUF/rMPUF) [47].

## 4.2 Cryptographic properties of PUFs and idealization

In cryptography and security we typically build a cryptographic system and prove its security under the assumption that we have used secure ingredients (building blocks) such as *collision-resistant hash functions* (CRHF), *pseudo-random generators* (PRGs), or *pseudo-random functions* (PRFs). These secure ingredients are a kind of “ground truth” of applied cryptography. “Provable security” typically starts only above the level of these secure ingredients. A proof based on

experiments and simulations may only show that the scheme is secure with respect to those experiments and simulations. A proof based on ideal primitives has a major advantage: if a cryptographic primitive is assumed ideal and later is proved (by experiments) insecure, we may change it by another one of the same type that we believe is secure. The entire scheme remains unchanged and the security analyses is moved to the cryptographic primitives.

When a cryptographic construction is deployed in practice, the secure (ideal) primitives that underlie it are replaced by algorithms for which we do not have a theoretical proof of security. Instead, these algorithms are subjected to intense scrutiny by cryptographers to see if they resist all known classes of attacks and to get evidence supporting the assumption that they are secure.

PUFs have been introduced to physically supplement specific security properties that cannot be satisfactorily obtained at the software implementation level alone. The security properties offered by PUFs can only be highlighted through experiments and simulations. To be able to apply provable security to cryptographic constructions that include PUFs, it is necessary to formalize their security properties. The major problem that arises in this context is to maintain a balance between formalization and the real physical properties. The difficulty of maintaining this balance comes from the fact that it is quite challenging to capture the behavior of a physical object through a mathematical formula that is accurate or that approximates it well enough. Without such a balance, we can reach situations such as those in which either the formalization is not useful or is too strict and has no practical equivalent. As a result, the formalization must be sufficiently realistic and, at the same time, allow its use in provable security.

Among the basic properties we want from a PUF class we mention: [left=.5cm]

**Constructability** – this means that it is “easy” to construct a random instance of a given PUF class;

**Evaluability** – this includes constructability and further requires that any random instance of a given PUF class can be easily evaluated on any random challenge;

**Reproducibility** – this includes evaluability and further requires that the responses resulting from evaluating the same challenge on the same PUF instance should be similar (in some distance metric) with high probability;

**Uniqueness** – this includes evaluability and further requires that the responses resulting from evaluating the same challenge on different PUF instances should be dissimilar (in some distance metric) with high probability;

**Identifiability** – this means both reproducibility and uniqueness;

**Physical unclonability** – this includes evaluability and further requires that it is hard to create a new PUF instance that is more alike to a given PUF instance than expressed by the uniqueness property;

**Unpredictability** – this means evaluability and further requires that no PPT algorithm can predict the answer of a given PUF instance for a given challenge, except with negligible probability, even if it could have previously learned the PUF’s answer for a polynomial number of challenges (different from the challenge in question);

**One-wayness** – this includes evaluability and further requires that it is hard to invert the answer of a given PUF instance;

**Tamper-evidence** – this includes evaluability and further requires that it is hard to physically alter a given PUF instance without having a noticeable effect on its challenge-response behavior.

The choice of the PUF type to be included in a cryptographic system depends on the security properties we want to achieve, and which cannot be obtained through software techniques, as well as on the production costs. For example, the tamper-evidence feature can be handy for constructing destructive private RFID schemes. However, today’s technological development shows that only optical [48] and coating PUFs [49] can provide this property. Besides, such PUFs have high production

costs, which requires a careful analysis of the environment of the utilization of the RFID schemes that would use such PUFs.

## 5. PUF-based RFID systems

PUFs have proven to be suitable for integration into RFID systems to ensure their security in gray or white box models. So far, two significant directions for the use of PUFs in RFID systems have emerged. We dedicate this section to a discussion of the two directions and the issues that arise regarding them.

### 5.1 Endowing RFID tags by PUFs

The vulnerability of RFID systems to corruption consists in the fact that an adversary with corruption abilities can extract the information from the tag's memory and, thus, can impersonate it or, at least, destroy the privacy property. Without having a concrete proof at the moment, the researchers' opinion is that, in Vaudenay's model but not only, destructive privacy cannot be achieved only by using symmetric or asymmetric cryptographic primitives. Storing a private key in the tag's memory is useless when the adversary has corruption capabilities and can use the information obtained through corruption. The use of a public key system in which the private key is stored on the reader side is also useless in Vaudenay's model when destructive privacy is desired.

This discussion naturally leads to the idea of using a tamper-evident mechanism embedded in the tag to help the process of identifying and authenticating it. In this context, PUFs seem to be a good choice and the newest technologies show that it is possible to embed PUFs into tags. These kind of tags, with PUFs embedded into them, will be called *PUF tags*, while the standard tags will sometimes be referred to as *ordinary tags*. A PUF-based RFID scheme is an RFID scheme with PUF tags.

How PUF tags can be built can be very important in terms of tag corruption. This aspect will be touched on in the next section.

Two significant directions have emerged on the authentication protocol of PUF-based RFID schemes. The first direction treats PUFs as fingerprints [50–54]. This approach requires an initial configuration phase in which a PUF model or a large set of PUF challenge-and-response (CR) pairs is pre-computed and stored in the reader's database. To identify a PUF tag, the reader queries it by some challenge, the tag evaluates its PUF on the challenge, and then the reader compares the tag's response with the pre-computed response it already has stored in the database. There are several variants of this scenario, but regardless of these, special attention must be paid to the modeling attacks of PUFs [55]. This is because the adversary might get sufficient CR pairs in order to simulate the tag's PUF. Anyway, the authors of this paper are not aware of any PUF-based RFID schemes based on this approach, and that would provide destructive privacy in Vaudenay's model. Moreover, we believe that it is not possible to achieve this level of privacy through this approach because the set of CR pairs is generally polynomial in size. Then, a strong enough adversary may run the authentication protocol with a tag until it exhausts all CR pairs stored in the database. In such a situation, either a CR pair will be reused, or a reset mechanism has to be used. Regardless of the case, the privacy property might be compromised.

A second direction for the authentication protocol of PUF-based RFID schemes starts from the idea of using PUFs as cryptographic key generators or as storage methods [10, 22, 56, 57]. That is, the tag evaluates its PUF only to generate or extract a cryptographic key. Thus, the PUF is evaluated for a minimum number of challenges. This fact eliminates the shortcoming that the adversary can model the



PUF, but if the PUF is noisy, then an additional overhead may be incurred by using fuzzy extractors. Assuming PUFs are tamper-evident, this second approach produces schemes that achieve destructive privacy in Vaudenay's model (please see Section 5.3).

## 5.2 Tag corruption and PUFs

In order to adapt Vaudenay's model (with or without temporary state disclosure) to PUF-based RFID schemes, we have to clarify what corruption means in this case. At least two main scenarios are possible:

1. By corrupting a PUF tag, the adversary gets the state of the tag, according to the type of the attack model (with or without temporary state disclosure). Besides, the tag is destroyed, but its PUF can still be evaluated. This variant does not show significant differences compared to the case of corruption of ordinary tags, because the PUF of the tag can now be seen as a public function that the adversary can evaluate as he wishes;
2. By corrupting a PUF tag, the adversary gets the state of the tag, according to the type of the attack model (with or without temporary state disclosure). Besides, the tag and its PUF are destroyed (in this case, the PUF cannot anymore be evaluated).

The second scenario is the most significant. Within it, the PUF tag is seen as a tamper-evident device (circuit), such as a tamper-evident PUF [58, 59]. Working in this scenario, Theorem 1 in [21], at least in its present form, cannot be applied to PUF-based RFID schemes. This leaves open the invitation to PUF-based design RFID schemes that achieve mutual authentication and higher privacy levels than narrow forward in Vaudenay's model with temporary state disclosure. As we have already said, such schemes cannot be based on ordinary tags. A good choice is to use PUF tags, as it was done in [10, 22, 56, 57, 60]. However, the use of PUF tags does not mean that the schemes are immune to corrupting adversaries. This is because an adversary might not need the entire tag state to attack the scheme. An example in this sense is provided in [10] where it was shown that the RFID schemes proposed in [56, 57] do not achieve mutual authentication and (narrow) destructive privacy in Vaudenay's model with temporary state disclosure, as it was claimed by authors, although they use PUF tags. The proof exploits the fact that these schemes use volatile variables to carry values between protocol steps.

As we have seen, the corruption attack in Vaudenay's model may provide the adversary with the full state of the tag. However, this state does not include the values of the local temporary variables. The varied range of side-channel attacks includes other types of attacks, such as those called cold-boot attacks, through which the tag's memory can be frozen. Thus the adversary can obtain the value of the local variables at a given time. This type of attack has also been discussed in RFID-oriented papers, such as [56, 57, 61]. We are not aware of any formal treatment of this scenario in Vaudenay's model. To implement it in Vaudenay's model, the *Corrupt* oracle should be changed to return snapshots of the tag's state during its computation (recall that the standard *Corrupt* oracle returns the tag's state before or after a protocol step). A formal and complete treatment of such a corruption seems hard to reach; on the other side, such a corruption is very strong and probably no PUF-based RFID scheme may achieve a privacy level higher than (narrow) weak under such a corruption. However, special cases may be relevant. One of them is the cold boot attack mentioned

	Reader ( $DB$ )	Tag ( $P, s$ )
1	$x \leftarrow \{0, 1\}^{\ell_1(\perp)}$	$\xrightarrow{x}$
2		$y \leftarrow \{0, 1\}^{\ell_1(\perp)}, K = P(s)$ $z = F_K(0, x, y)$
3	If $\exists (ID, K) \in DB$ s.t. $z = F_K(0, x, y)$ then output $ID$ (tag auth.) else output $\perp$ ; $K \leftarrow \mathcal{K}_\lambda$ ; $w = F_K(1, x, y)$	$\xrightarrow{w}$ $w' = F_K(1, x, y)$ If $w = w'$ then output OK (reader auth.) else output $\perp$

**Figure 3.** PRF- and PUF-based RFID scheme that achieves destructive privacy and mutual authentication

above [56, 57, 61]. To defeat it, a PUF double evaluation technique was proposed in [61], which consists of two evaluations in a row of the same PUF. If the attack is applied immediately after the first PUF evaluation, the second PUF evaluation is lost, and vice-versa. This technique was implemented in [56, 57] too. Unfortunately, the authors did not pay much attention to the temporary variables, which made their schemes not to achieve even the narrow forward privacy level [10].

### 5.3 Destructive privacy by PUF-based RFID schemes

When the Vaudenay [12, 13] model was proposed, finding an RFID scheme to provide destructive privacy remained an open issue (please see the diagram in **Figure 2**). This problem was later solved by a PUF-based RFID scheme [22, 60]. The scheme, which provides unilateral authentication, is obtained from the PRF-based RFID scheme presented in Section 2, adding tamper-evident PUFs to tags to generate the key  $K$ . If the adversary corrupts the tag, its PUF is destroyed and cannot be evaluated. Thus, the adversary cannot get the key  $K$ . The scheme was extended later to ensure mutual authentication [10]. We present it in **Figure 3**. As one can see, the main difference between the scheme in **Figure 1** and this new one is that the domain of the PRF function  $F$  is extended with one more bit and the tag is endowed with a tamper-evident PUF  $P$  and a seed  $s$  for it. Whenever the tag needs to evaluate its PRF, it first computes the key  $K = P(s)$  and then uses it. It has to be understood that after using it, the variable  $K$  is erased. If the adversary corrupts the tag, the seed  $s$  he gets is useless because the PUF can no longer be evaluated (please see [10] for details regarding the security and privacy proofs).

As corruption with temporary state disclosure is a real threat in practice, the most natural question is how to extend the above schemes, or how to design new ones, secure and private in Vaudenay’s model under such a corruption. It is clear that ordinary tags (i.e., tags that only implement cryptographic primitives) do not help if one wants to achieve both mutual authentication and privacy (Theorem 1 in [21]). Endowing tags with PUFs is a potential solution but it is not a guarantee. It turns out that the subtlety is how to use temporary variables. This has been missed in some recently proposed RFID schemes [56, 57], which made these schemes not to achieve the privacy level claimed by authors [10]. It seems that the use of temporary variables in connection with mutual authentication and privacy is not really very well understood, especially under corruption with temporary state disclosure.

## **6. Conclusions**

The significant impact of PUF technology in the construction of RFID systems is demonstrated by the great diversity of scientific articles and patents proposed in the last decade. The use of PUFs in the construction of RFID schemes can bring extra security and privacy at the physical level that cannot be obtained by symmetric and asymmetric cryptography at the moment. However, this requires an adequate understanding and analysis of security and privacy models for RFID to consider PUFs only if existing standard techniques cannot lead to the desired security and privacy level. Unfortunately, the literature shows us enough PUF-based RFID schemes proposed in recent years that do not even reach the weak privacy level in Vaudenay's model. In contrast, weak privacy in this model can be achieved through standard RFID schemes that use only symmetric cryptography. This fact clearly shows that a sustained effort is needed to consolidate the understanding of the concept of security and privacy model and adapt it accordingly to PUF technology.

In this chapter, we highlighted the aspects mentioned above and emphasized the need to use formal models in the study of security and privacy properties of (PUF-based) RFID schemes. Achieving the level of destructive privacy in Vaudenay's model through PUF-based RFID schemes clearly shows us the potential of using PUF technology in the construction of RFID systems. Even if the security and privacy proofs on PUF-based RFID schemes make use of ideal PUFs, this is not a negative aspect as long as there is practically reasonable support for idealization, and this is in the trend of technology evolution.

### **Authors contribution**

This chapter (structure and content) was proposed by F.L. Țiplea, who also supervised its complete realization. Section 4.1 was prepared by C. Andriesei, as well as the second and third paragraphs of the introductory section. All the other sections of the chapter were prepared in an equal contribution by F.L. Țiplea and C. Hristea. All authors have read and agreed to the published version of the manuscript.

## **Author details**

Ferucio Laurențiu Țiplea<sup>1,3\*</sup>, Cristian Andriesei<sup>2,4</sup> and Cristian Hristea<sup>3</sup>

1 Alexandru Ioan Cuza University of Iasi, Iasi, Romania

2 Gheorghe Asachi Technical University, Iasi, Romania

3 Simion Stoilow Institute of Mathematics of the Romanian Academy, Bucharest, Romania

4 SC AT&C Technology SRL, Iasi, Romania

\*Address all correspondence to: [fltiplea@gmail.com](mailto:fltiplea@gmail.com)

## **IntechOpen**

---

© 2020 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

## References

- [1] Marion Cardullo and William Parks. Transponder apparatus and system, Jan 1973. US Patent 3713148
- [2] FPO. Free Patents Online, 2020. <http://freepatentsonline.com>
- [3] Haddara M, Staaby A. RFID applications and adoptions in healthcare: A review on patient safety. *Procedia computer science*. 2018;**138**: 80-88
- [4] Antti Lahtela. A short overview of the RFID technology in healthcare. In *2009 Fourth International Conference on Systems and Networks Communications*, pages 165–169. IEEE, 2009
- [5] Halak B. *Physically Unclonable Functions: From Basic Design Principles to Advanced Hardware Security Applications*. Springer International Publishing; 2019
- [6] R Maes. *Physically Unclonable Functions: Constructions, Properties and Applications*. Springer-Verlag Berlin Heidelberg; 2013
- [7] Christian Wachsmann and Ahmad-Reza Sadeghi. *Physically Unclonable Functions (PUFs): Applications, Models, and Future Directions*. Number 12 in *Synthesis Lectures on Information Security, Privacy, & Trust*. Morgan & Claypool Publishers, Dec 2014
- [8] Jones EC, Chung CA. *RFID and Auto-ID in Planning and Logistics: A Practical Guide for Military UID Applications*. CRC Press; 2016
- [9] Ustundag A. *The Value of RFID: Benefits vs. Costs*. Springer-Verlag, London; 2013
- [10] Cristian Hristea and Ferucio Laurențiu Țiplea. Destructive privacy and mutual authentication in Vaudenay's RFID model. *Cryptology ePrint Archive*, Report 2019/073, 2019. <https://eprint.iacr.org/2019/073>
- [11] Cristian Hristea and Ferucio Laurențiu Țiplea. Privacy of stateful RFID systems with constant tag identifiers. *IEEE Transactions on Information Forensics and Security*, 15: 1920–1934, Nov 2019.
- [12] Radu-Ioan Paise and Serge Vaudenay. Mutual authentication in RFID: Security and privacy. In *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security, ASIACCS '08*, pages 292–299, New York, NY, USA, 2008. ACM
- [13] Vaudenay S. On privacy models for RFID. In: *Proceedings of the Advances in Cryptology 13th International Conference on Theory and Application of Cryptology and Information Security, ASIACRYPT'07*. Berlin, Heidelberg: Springer-Verlag; 2007. pages 68-87
- [14] Klaus Finkenzeller. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*. Wiley Publishing, 3rd edition, 2010
- [15] Yingjiu Li H. Robert Deng, and Elisa Bertino. *RFID Security and Privacy*. *Synthesis Lectures on Information Security, Privacy, and Trust*. In: Morgan & Claypool Publishers. 2013
- [16] Hermans J, Peeters R, Preneel B. Proper RFID privacy: Model and protocols. *IEEE Transactions on Mobile Computing*. Dec 2014;**13**(12): 2888-2902
- [17] Pascal Sasdrich, Amir Moradi, and Tim Güneysu. White-box cryptography in the gray box. In *Revised Selected Papers of the 23rd International Conference on Fast Software Encryption - Volume 9783*, FSE 2016, pages 185–203, Berlin, Heidelberg, 2016. Springer-Verlag

- [18] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman & Hall/CRC, 2nd edition, 2014
- [19] Peeters E. *Advanced DPA Theory and Practice: Towards the Security Limits of Secure Embedded Circuits*. Incorporated: Springer Publishing Company; 2013
- [20] M. Al-Haidary and Q. Nasir. Physically unclonable functions (PUFs): A systematic literature review. In *2019 Advances in Science and Engineering Technology International Conferences (ASET)*, pages 1–6, 2019
- [21] Armknecht F, Sadeghi A-R, Scafuro A, Visconti I, Wachsmann C. Impossibility results for RFID privacy notions. In: Gavrilova ML, Tan CJK, Moreno ED, editors. *Transactions on Computational Science XI*. Berlin, Heidelberg: Springer-Verlag; 2010. pp. 39-63
- [22] Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann. PUF-enhanced RFID security and privacy. In *Workshop on secure component and system identification (SECSI)*, volume 110, 2010
- [23] K. Lofstrom, W. R. Daasch, and D. Taylor. IC identification circuit using device mismatch. In *2000 IEEE International Solid-State Circuits Conference. Digest of Technical Papers (Cat. No.00CH37056)*, pages 372–373, 2000
- [24] K. Lofstrom. System for providing an integrated circuit with a unique identification. US patent no. 6161213, Dec 2000
- [25] McGrath T, Bagci IE, Wang ZM, Roedig U, Young RJ. A PUF taxonomy. *Applied Physics Reviews*. 2019;6(1): 011303
- [26] Vanhoucke T and Nguyen V. A PUF method using and circuit having an array of bipolar transistors. European patent no. 2833287A1, July 2013
- [27] Lee S, Oh M-K, Kang Y, Choi D. Design of resistor-capacitor physically unclonable function for resource-constrained IoT devices. *Sensors*. 2020;20(2), pages 326-337
- [28] Sangjae Lee, Mi-Kyung Oh, Yousung Kang, and Dooho Choi. RC PUF: A low-cost and an easy-to-design PUF for resource-constrained IoT devices. In Ilsun You, editor, *Information Security Applications*, pages 275–285, Cham, 2020. Springer International Publishing
- [29] Herder C, Yu M, Koushanfar F, Devadas S. Physical unclonable functions and applications: A tutorial. *Proceedings of the IEEE*. 2014;102(8): 1126-1141
- [30] Blaise Gassend, Dwaine E. Clarke, Marten van Dijk, and Srinivas Devadas. Silicon physical random functions. In Vijayalakshmi Atluri, editor, *ACM Conference on Computer and Communications Security*, pages 148–160. ACM, 2002
- [31] Jae W. Lee, Daihyun Lim, Blaise Gassend, G. Edward Suh, Marten van Dijk, and Srinivas Devadas. A technique to build a secret key in integrated circuits for identification and authentication applications. In *2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525)*, pages 176–179, 2004
- [32] Jorge Guajardo, Sandeep S. Kumar, Geert-Jan Schrijen, and Pim Tuyls. FPGA intrinsic PUFs and their use for IP protection. In *Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 07*, pages 63–80, Berlin, Heidelberg, 2007. Springer-Verlag
- [33] Y. Su, J. Holleman, and B. Otis. A 1.6pJ/bit 96% Stable Chip-ID Generating Circuit using Process Variations. In *2007 IEEE International*

*Solid-State Circuits Conference. Digest of Technical Papers*, pages 406–611, 2007

[34] S. S. Kumar, J. Guajardo, R. Maes, G. Schrijen, and P. Tuyls. Extended abstract: The butterfly PUF protecting IP on every FPGA. In *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, pages 67–70, 2008

[35] Maes R, Tuyls P, Verbauwhede I. Intrinsic PUFs from flip-flops on reconfigurable devices. In: *3rd Benelux workshop on information and system security (WISec 2008)*. 2008

[36] Ryan Helinski, Dhruva Acharyya, and Jim Plusquellic. A physical unclonable function defined using power distribution system equivalent resistance variations. In *2009 46th ACM/IEEE Design Automation Conference*, pages 676–681. IEEE, 2009

[37] Csaba G, Xueming J, Chen Q, Porod W, Schmidhuber J, Schlichtmann U, et al. On-chip electric waves: An analog circuit approach to physical unclonable functions. *IACR Cryptology ePrint Archive*. 2009;2009:246

[38] Ulrich Ruehrmair, Christian Jaeger, Christian Hilgers, Michael Algasinger, Gyoergy Csaba, and Martin Stutzmann. Security applications of diodes with unique current-voltage characteristics. In *Proceedings of the 14th International Conference on Financial Cryptography and Data Security, FC'10*, page 328–335, Berlin, Heidelberg, 2010. Springer-Verlag

[39] Daisuke Suzuki and Koichi Shimizu. The Glitch PUF: A new delay-PUF architecture exploiting glitch shapes. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 366–382. Springer, 2010

[40] Yohei Hori, Hyunho Kang, Toshihiro Katashita, and Akashi Satoh.

Pseudo-LFSR PUF: A compact, efficient and reliable physical unclonable function. In *2011 International Conference on Reconfigurable Computing and FPGAs*, pages 223–228. IEEE, 2011

[41] Peter Simons, Erik van der Sluis, and Vincent van der Leest. Buskeeper PUFs, a promising alternative to D flip-flop PUFs. In *2012 IEEE International Symposium on Hardware-Oriented Security and Trust*, pages 7–12. IEEE, 2012

[42] Patrick Koeberl, Ünal Kocabas, and Ahmad-Reza Sadeghi. Memristor PUFs: a new generation of memory-based physically unclonable functions. In *2013 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 428–431. IEEE, 2013

[43] Bossuet L, Ngo XT, Cherif Z, Fischer V. A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon. *IEEE Trans. Emerg. Top. Comput.* 2014;2(1):30-36

[44] Fatemeh Tehranipoor, Nima Karimian, Kan Xiao, and John Chandy. DRAM based intrinsic physical unclonable functions for system level security. In *Proceedings of the 25th edition on Great Lakes Symposium on VLSI*, pages 15–20, 2015

[45] S. Sutar, A. Raha, and V. Raghunathan. D-PUF: An intrinsically reconfigurable DRAM PUF for device authentication in embedded systems. In *2016 International Conference on Compilers, Architectures, and Synthesis of Embedded Systems (CASES)*, pages 1–10, 2016

[46] Liu CQ, Cao Y, Chang CH. ACRO-PUF: A low-power, reliable and aging-resilient current starved inverter-based ring oscillator physical unclonable function. *IEEE Transactions on Circuits and Systems I: Regular Papers*. 2017; 64(12):3138-3149

- [47] Sahoo DP, Mukhopadhyay D, Chakraborty RS, Nguyen PH. A multiplexer-based arbiter PUF composition with enhanced reliability and security. *IEEE Transactions on Computers*. 2018;**67**(3):403-417
- [48] Pappu Srinivasa Ravikanth. Physical One-Way Functions. PhD thesis, USA, 2001
- [49] Pim Tuyls, Geert-Jan Schrijen, Boris Škorić, Jan van Geloven, Nynke Verhaegh, and Rob Wolters. Read-proof hardware from protective coatings. In *Proceedings of the 8th International Conference on Cryptographic Hardware and Embedded Systems, CHES'06*, pages 369–383, Berlin, Heidelberg, 2006. Springer-Verlag
- [50] Pier Francesco Cortese, Francesco Gemmiti, Bernardo Palazzi, Maurizio Pizzonia, and Massimo Rimondini. Efficient and practical authentication of PUF-based RFID tags in supply chains. In *2010 IEEE International Conference on RFID-Technology and Applications*, pages 182–188. IEEE, 2010
- [51] Devadas S, Suh E, Paral S, Sowell R, Ziola T, Khandelwal V. Design and implementation of PUF-based unclonable RFID ICs for anti-counterfeiting and security applications. In: *2008 IEEE international conference on RFID*, pages 58–64. IEEE. 2008
- [52] Gope P, Lee J, Quek TQS. Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions. *IEEE Transactions on Information Forensics and Security*. Nov 2018;**13**(11):2831-2843
- [53] Öztürk E, Hammouri G, Sunar B. Towards robust low cost authentication for pervasive devices. In: *2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pages 170–178. IEEE. 2008
- [54] Anthony Van Herrewege, Stefan Katzenbeisser, Roel Maes, Roel Peeters, Ahmad-Reza Sadeghi, Ingrid Verbauwhede, and Christian Wachsmann. Reverse fuzzy extractors: Enabling lightweight mutual authentication for PUF-enabled RFIDs. In *International Conference on Financial Cryptography and Data Security*, pages 374–389. Springer, 2012
- [55] Ulrich Rührmair, Frank Sehnke, Jan Sölter, Gideon Dror, Srinivas Devadas, and Jürgen Schmidhuber. Modeling attacks on physical unclonable functions. In *Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS '10*, pages 237–249, New York, NY, USA, 2010. Association for Computing Machinery
- [56] Mete Akgün and M. Ufuk Çağlayan. Providing destructive privacy and scalability in RFID systems using PUFs. *Ad Hoc Netw.*, 32(C):32–42, September 2015
- [57] Süleyman Kardas, Serkan Çelik, Muhammet Yildiz, and Albert Levi. PUF-enhanced offline RFID security and privacy. *J. Netw. Comput. Appl.*, 35 (6):2059–2067, November 2012
- [58] Dmitry Nedospasov, Jean-Pierre Seifert, Clemens Helfmeier, and Christian Boit. Invasive PUF analysis. In *Proceedings of the 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC '13*, pages 30–38, USA, 2013. IEEE Computer Society
- [59] Pim Tuyls and Lejla Batina. RFID-tags for anti-counterfeiting. In *Cryptographers' Track at the RSA Conference*, pages 115–131. Springer, 2006
- [60] Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann. *Enhancing RFID Security and Privacy by Physically Unclonable Functions*, pages 281–305. Springer Berlin Heidelberg, 2010



[61] Süleyman Kardas, Mehmet Sabir Kiraz, Muhammed Ali Bingöl, and Hüseyin Demirci. A novel RFID distance bounding protocol based on physically unclonable functions. In Ari Juels and Christof Paar, editors, *RFID. Security and Privacy*, pages 78–93, 2012. Springer Berlin Heidelberg



# The Security of Cryptosystems Based on Error-Correcting Codes

*Ahmed Drissi*

## Abstract

Quantum computers are distinguished by their enormous storage capacity and relatively high computing speed. Among the cryptosystems of the future, the best known and most studied which will resist when using this kind of computer are cryptosystems based on error-correcting codes. The use of problems inspired by the theory of error-correcting codes in the design of cryptographic systems adds an alternative to cryptosystems based on number theory, as well as solutions to their vulnerabilities. Their security is based on the problem of decoding a random code that is NP-complete. In this chapter, we will discuss the cryptographic properties of error-correcting codes, as well as the security of cryptosystems based on code theory.

**Keywords:** McEliece cipher, hash function, syndrome decoding, correcting codes, random code

## 1. Introduction

Like all asymmetric cryptographic systems, the idea is to base security on the difficulty of reversing a one-way function with a trap door. The theory of error-correcting codes contains well-structured and difficult problems to solve, more or less suitable for use in cryptography. The first who had the idea of using error-correcting codes for cryptographic purposes was McEliece in 1978 and he proposed an asymmetric encryption algorithm. In 1986, Niederreiter proposed another cryptographic system equivalent to that of McEliece [1]. The two systems of McEliece and Niederreiter are of equivalent security against a passive attack; however, they are not against an active attack [2]. In the following paragraph, we give an overview of the theory of error-correcting codes. In the third paragraph, we will only deal with the basic systems based on this theory. The last paragraph is devoted to the discussion of security settings and the most well-known attacks. In what follows we note.

$F_{2^m}$ : a finite field of  $2^m$  elements.

$K[x]$ : the ring of polynomials with an indeterminate.

$K[x]/(P)$ : the quotient ring  $K[x]$  de modulo  $P$ .

$K^*$ : a private set of the element 0.

$dQ(x)$ : the degree of the polynomial  $Q(x)$ .

$F_2^m$ : the set of length vectors  $m$  and components 0 and 1.

$F^n$ : the scalar product  $n$  times of the set  $F$ .

$[x]$ : the integer part of  $x$ .

$A^t$ : the transpose of the matrix  $A$ .

$I_k$ : the identity matrix of order  $k$ .

$gcd$ : greatest common divisor.

$C_n^t$ : the combination of  $t$  elements among  $n$  elements.

## 2. Error-correcting codes

### 2.1 Finite fields

Finite fields are the basis of many error-correcting codes and cryptographic systems, it is therefore essential to recall the theory of finite fields in order to understand the functioning of linear codes. In this paragraph we present some properties of finite fields and a method of representing them for later use. We are interested in constructing finite fields  $F_{2^m}$  and the calculations on these fields. Finite fields are generally constructed from primitive polynomials [3].

Definitions

The minimal polynomial of an element  $\beta$  on a finite field  $F$  is the unit polynomial with coefficients in  $F$  smaller degree and its value in  $\beta$  is zero.

Proposition

1. The ring  $K[x]/(P)$  is a field if and only if the polynomial  $P(x)$  is irreducible on the field  $K$ .
2. If  $P(x)$  is irreducible of degree  $m$  and  $K$  a finite field of  $q$  elements then  $K[x]/(P)$  is field of  $q^m$  elements.

This proposition gives us a way to build a finite field: Take a polynomial  $P$  irreducible over a field  $K$  et former le quotient  $K[x]/(P)$ .

Theorem (the primitive element)

If  $K$  is a finite field of order  $q$ , then the multiplicative group  $K^*$  is cyclic generated by an element  $\alpha$  called primitive element of  $K$  and we write  $K^* = \{\alpha^i, i = 1 \dots q-1\}$ . Any generator of this group is called a primitive element of  $K$ .

Definition (primitive polynomial)

We say that a polynomial  $P \in F_2[x]$  of degree  $m$  is primitive if it is the minimal polynomial of a generator of  $F_{2^m}^*$ .

Lemma

Let  $F_2[x]^{(m)} = \{Q(x) \in F_2[x], dQ(x) \leq m-1\}$ ,  $P(x) \in F_2[x]^{(m)}$  primitive and  $\alpha$  a root of  $P(x)$ , so we have:  $F_2^m \approx F_2[x]^{(m)} \approx F_2[x]/(P(x)) \approx F_{2^m} \approx \{0\} \cup \{1, \alpha, \dots, \alpha^{2^m-1}\}$ .

It follows from this lemma that we can represent the nonzero elements of a finite field  $F_{2^m}$  by nonzero vectors of  $F_2^m$  and that the  $\alpha^i$  have representatives of  $x^i \text{ mod } P(x)$  and consequently  $\alpha^i = x^i \text{ mod } P(x)$ . In what follows we denote by  $\alpha$  a primitive element of  $F_{2^m}$ .

### 2.2 Principle of error-correcting codes

In order to transmit a message, it must be coded, it consists in temporarily giving it a certain form, the coding mode depends on the means of transmission, it can be disturbed by noise, hence the need for coding which allows the receiver to find the initial message even if it has been altered. Such coding is called channel coding.

The principle of error-correcting codes is to add to a message to be transmitted additional information called redundant or control information, so that transmission errors can be detected and corrected. This operation is called coding and its result is a code word, each message is associated, therefore a code word of length greater than that of the message.

The code is the set of code words thus obtained. We assume that all messages are words of the same length  $>0$ , written using an alphabet  $F$  of  $q$  elements. Each message  $(x_0, x_1, \dots, x_{k-1})$  is an element of the set of  $F^k$  (message space). We then have  $q^k$  possible messages. We assume that all the code words are of the same length  $n > k$ . Encode  $m$  messages of length  $k$ , ( $m \leq q^k$ ) consists in choosing an integer  $n > k$ , and associate with each message from  $F^k$  a word from  $F^n$  (injectively). The coding introduces a redundancy equal to  $n - k$ . Decoding consists of receiving a word  $x$  of  $F^n$  to determine if  $x$  is a code word and if not correct it thanks to the redundancy. This is done using the Hamming distance.

Definition (hamming distance)

let  $x = (x_0, x_1, \dots, x_{n-1}) := x_0x_1\dots x_{n-1}$  and  $y = (y_0, y_1, \dots, y_{n-1}) := y_0y_1\dots y_{n-1}$  of  $F^n$ . We call the Hamming distance between words  $x$  and  $y$ , and we note  $d_H(x, y) = d(x, y)$  the number of index  $i \in \{0, 1, 2, \dots, n-1\}$  such as  $x_i \neq y_i$ , we call Hamming's weight of a word  $x$  the number of nonzero components of  $x$ , we note  $w(x) = d(x, 0)$ .

Definitions

We call the minimum distance of a code  $C$  an integer  $d$  such as  $d = \min \{d(m, m'), m \in C, m' \in C, m \neq m'\}$ . We call the weight of a word  $x$  of code  $C$  on integer  $w(x) = d(x, 0)$ .

Proposal (correction capacity)

Let  $C$  a minimum distance code  $d$ , and  $x \in F^n$  a received message assigned to  $r$  errors, with  $r \geq 1$ .

1. If  $2r < d$  that is to say that  $r \leq \lfloor \frac{d-1}{2} \rfloor$ , the code  $C$  correct  $r$  errors.
2. If  $\lfloor \frac{d-1}{2} \rfloor < r = \lfloor \frac{d}{2} \rfloor$ , the  $C$  code detects the existence of  $r$  errors but cannot always correct them.
3. If  $\lfloor \frac{d}{2} \rfloor < r \leq d - 1$ , the  $C$  code detects the existence of  $d'$  errors but risk of making an erroneous correction.

The integer  $t = \lfloor \frac{d-1}{2} \rfloor$  is called code correction capability, we also say that  $C$  is a  $t$ -corrector code.

Proof

Let  $m$  the code word transmitted and  $x$  the message received and assigned from  $r$  errors then  $d(m, x) = r$ .

1. We show that the code word  $m$  is the only code word such as  $d(m, x) \leq r$ .

Otherwise it exists  $m'$  of  $C$  such as  $d(m', x) \leq r$ , we are  $d(m, m') \leq d(m, x) + d(x, m') \leq 2r < d$ , then  $m = m'$ .

2. There is no code word  $m'$  of  $C$  such as  $d(x, m') < d(m, x) = r$ , but the code word  $m$  is not necessarily the only one to check  $d(m, x) = r$ . Indeed be  $m = m_1m_2\dots m_n$  and  $m' = m'_1m'_2\dots m'_n$  two code words and if we receive the message  $x = m_1m_2\dots m_r m'_1\dots m'_r$ , we'll have  $d(x, m) = d(x, m') = r$ .

3. We know there is an error because  $x \notin C$ , but there may be a code word  $m' \notin C$  such as  $d(m', x) < d(m, x) = r$ .

The most used codes are the linear codes which we discuss in the next part.

### 2.3 Linear codes

#### Definitions

A linear code  $C$  of size  $n$  and dimension  $k$  on the finite field  $F_q$  is a vector subspace of  $F_q^n$ . We note it  $[n, k, d]_q$  with  $d$  its minimum distance.

Linear codes are codes in which each code word  $y$  is obtained by linear transformation of the components of the initial word (information)  $x$ .

A linear code is characterized by its generator matrix  $G$ , we have

$$C = \left\{ y = xG / x \in F_q^k \right\}.$$

let  $H$   $(n - k) \times n$  matrix with coefficients in  $F_q$ .  $H$  is called the parity control matrix of  $C$  if " $x \in C \Leftrightarrow Hx^t = 0$ ".

$F_q^k$ : the message space.

The systematic code

The matrix  $G$  defines a bijective function  $F_q^k \rightarrow C$  by  $x \rightarrow xG$  which we represent  $q^k$  messages, its length  $k$  by code words, of length  $n$ .

The generator matrix  $G$  of a  $C$  code is not unique;  $G$  can be transformed into  $G' = (I_k | A)$  with  $I_k$  the identity matrix with  $k$  order and  $A$  the matrix of  $k$  lines and  $n - k$  columns.

$G$  and  $G'$  generate the same  $C$  subspace;  $G'$  is called canonical generator matrix and if the generator matrix of a code is of the form  $G = (I_k | A)$ , this code is said systematic.

Theorem

Let  $C$  a  $[n, k]_q$  linear code.

1. If  $G$  is a generator matrix of  $C$  and  $H$  a parity control matrix of  $C$  then  $GH^t = 0$ .
2. If  $G$  is a  $k \times n$  matrix of rank  $k$  and  $H$  is a  $(n - k) \times n$  matrix of rank  $n - k$  such as  $GH^t = 0$  then we have:

$H$  is a parity control matrix of  $C$  if and only if  $G$  is a generator matrix of  $C$ .

Proof

1. We know that  $H^t = 0, \forall x \in C$ , in particular we have  $G_i H^t = 0$  for all  $i = 1 \dots k$  with  $G_i$  is line of  $G$ . It follows that  $GH^t = 0$ .
  2.  $\Rightarrow$ ) Since  $GH^t = 0$ , then we have  $G_i H^t = 0$ . For all  $i = 1 \dots k$ . And since  $H$  is a parity control matrix of  $C$ , we have the  $G_i$  belong to  $C$ .  $\text{rg}(G) = k$ , then  $\{G_i, i = 1 \dots k\}$  constitute a basis of  $C$ . It follows that  $G$  is a generator matrix of  $C$ .
- $\Leftarrow$ ) we have  $y \in C$  if and only if it exists  $x \in F_q^k$  such as  $y = xG$ . Then  $y \in C$  if and only if  $yH^t = xGH^t = 0$ . Then  $H$  is a parity control matrix of  $C$ .

In the case of systematic code, we have the following corollary.

Corollary

Let  $C$  a  $[n, k]_q$  linear code

1. If  $G = (I_k|A)$  a canonical generator matrix of  $C$  then  $H = (-A^t|I_{n-k})$  is a parity control matrix of  $C$ .
2. If  $H = (B|I_{n-k})$  is a parity control matrix of  $C$  then,  $G = (I_k|-B^t)$  is a generator matrix of  $C$ .

Proof

By applying the preceding theorem

1. we have  $GH^t = (I_k|A)(-A^t|I_{n-k})^t = -A + A = 0$ , if  $G$  is a generator matrix of  $C$  then,  $H$  is a parity control matrix of  $C$ .
2. we have  $GH^t = (I_k|-B^t)(B|I_{n-k})^t = B^t - B^t = 0$  then if  $H$  is a parity control matrix of  $C$  we will have  $G$  is a generator matrix of  $C$ .

Encoding and decoding

The coding is obtained by applying the generator matrix. Decoding consists in applying the control matrix to the message; if the result is 0 then the message is valid otherwise look for errors and correct them.  $Hx^t$  is called syndrome. Suppose the word  $x$  is sent through a noisy channel and the word received is  $y$  so the error vector is  $e = y - x$ .

Given  $y$ , the decoder must decide which word of the code  $x$  has been transmitted (which error vector?). For a vector  $u$  and a code  $C$  we call coset class of  $C$ , the set  $u + C = \{u + c, c \in C\}$ . A representative of a class of  $C$  of minimum weight is called a leader of this class.

Theorem

Let  $C$  a  $[n, k, d]_q$  linear code then,

1.  $u$  and  $v$  are of the same coset class of  $C$  if and only if  $u - v \in C$ .
2. Any vector of  $F_q^n$  is in a coset of  $C$ .
3. Given two coset classes, they are either disjoint or identical.

Proof

1. If  $u, v \in x + C$  then, it exists  $y, z \in C$  such as  $u = x + y$  and  $v = x + z$ , then  $u - v = y - z \in C$ , because  $C$  is a vector subspace of  $F_q^n$ .

If  $u - v \in C$  it exists  $x \in C$  such as  $u - v = x$  then  $u = v + x \in v + C$  and we have  $v = v + 0 \in v + C$ .

2. Let  $a \in F_q^n$ , on a  $0 \in C$  then  $a = a + 0 \in a + C$ .

3. Suppose that  $(a + C) \cap (b + C) \neq \emptyset$ , the nit exists  $v \in F_q^n$  such as  $(a + C) \cap (b + C)$  contains the element  $v$ , the nit exists  $x, y \in C$  such as  $v = a + x = b + y$  hence  $b = a + (x - y)$  and  $a = b + (y - x)$ .  $\forall b + c \in b + C$  we have  $b + c = a + (x - y) + c \in a + C$  (then  $b + C \subset a + C$ ).  $\forall a + c \in a + C$  We have  $a + c = b + (y - x) + c \in b + C$  (then  $a + C \subset b + C$ ), hence  $b + C = a + C$ .

Principle

We construct the standard array of  $C$  which is a matrix of  $q^{n-k}$  lines and  $q^k$  columns. It contains all the vectors of  $F_q^n$ ; its first line corresponds to the words of  $C$  with vector  $0$  on the left. The other lines represent the cosets  $u_i + C$  with the class leader  $u_i$  to the left. The procedure is as follows:

1. We list the words of  $C$  starting with  $0$  on the first line.
2. We choose a vector  $u_1$  of minimum weight that does not belong to the first line and we list in the second line the elements  $u_1 + C$ , by entering below  $0$  the class leader  $u_1$  and below each element  $x \in C$  the element  $u_1 + x$ .
3. We choose  $u_2$  in the same way and we repeat the same operation.
4. We iterate this process until all the side classes are listed and all the vectors of  $F_q^n$  appear only once.

When the word  $y$  is received, we look for its position in the standard table. The decoder then decides that the error vector  $e$  corresponds to the class leader who is located in the first column of the same row of  $y$  and decode  $y$  like  $x = y - e$ , by choosing the code word of the first line on the same column of  $y$ .

Remark

The standard table provides nearest neighbor decoding. Note that this process is too slow and too expensive in memory for large codes. In practice each code has by its structure a decoding algorithm.

**2.4 The hamming code**

A Hamming code with  $r \leq 2$  redundancy is a linear code  $[2^r - 1, 2^r - 1 - r]_2$  its parity control matrix  $H$ , with  $H$  is a matrix of  $r$  lines and  $2^r - 1$  columns that correspond to the set of all nonzero vectors of  $F_2^r$ .

Theorem

The minimum distance of the Hamming  $[2^r - 1, 2^r - 1 - r]_2$  code is  $d = 3$  (it therefore corrects a single error).

Proof

This code does not contain any element of weight 1 and 2 otherwise we would have a column of  $H$  which would be zero or two columns of  $H$  would be identical.

It exists  $x \in C$  such as  $w(x) = 3$ , indeed by definition of the parity control

matrix  $H$ , the first 3 columns are  $\begin{pmatrix} 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \dots \\ 0 & 0 & 0 & \dots \\ 0 & 1 & 1 & \dots \\ 1 & 0 & 1 & \dots \end{pmatrix}$  then the vector

$x = (1 \ 1 \ 1 \ 0 \dots \ 0)$  its weight  $w(x) = 3$  and belongs to  $C$  because  $Hx^t = 0$ .

Decoding

The vector syndrome  $x$  of which only the  $j$ th component is nonzero is none other than the transpose of the  $j$ th column of  $H$ . If the columns of  $H$  are ordered in increasing order of binary numbers, the  $j$ th column corresponds to the binary writing of  $j$ , hence the following decoding algorithm:

Let  $y$  a message received, we calculate  $Hy^t$ . If  $Hy^t = 0$  then,  $y$  corresponds to the message transmitted. If  $Hy^t \neq 0$  and assuming there is only one error,  $Hy^t$  directly



gives the position of the error written in binary in the form  $\dots b_3 b_2 b_1 b_0$ . We can then correct  $y = y_1 \dots y_n$  like  $x + e_j$  for  $j = \sum_{i=1}^n b_i 2^i$  and  $e_j$  the vector of which only the  $j$ th coordinate is nonzero.

## 2.5 The Reed-Solomon codes

Let  $n = q - 1$  with  $q = 2^m$  et  $F_q[x]^{(k)}$  The set of polynomials of degree strictly less than  $k$  on  $F_{2^m}$ . Let us build a length code  $n$  and dimension  $k$ . Let  $L = (\alpha_1, \alpha_2, \dots, \alpha_n, )$  a vector formed of distinct elements of  $F_{2^m}^* = \{\alpha^i, i = 1 \dots n\}$ , with  $\alpha$  primitive of  $F_{2^m}$ . Each word of the code is the evaluation of a function  $f$  of  $F_q[x]^{(k)}$  on  $L$  then, we have a length code  $n$  and dimension  $k$  and generator matrix

$$G = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \dots & \dots & \dots & \dots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_n^{k-1} \end{pmatrix}.$$

By its structure, this code has a minimum distance of at least  $n - k + 1$ , because two polynomials of degrees less than  $k$  distinct cannot be equal in addition to  $k - 1$  positions. This distance is exactly equal to  $n - k + 1$ , since the evaluation of a polynomial of the form  $\prod_{i=1}^{k-1} (x - \alpha_i)$  his weight is  $n - k + 1$ . So we have a code on  $F_{2^m}$  of the form  $[n, k, n - k + 1]_q$  which can have both good transmission rate and good correction ability.

Remark

Reed-Solomon codes represent a special case of a slightly more general class called generalized Reed-Solomon codes GRS whose definition is as follows.

Definition

Let  $(v_1, v_2, \dots, v_n)$  a vector of length  $n$  in  $F_{2^m}^*$  et  $(\alpha_1, \alpha_2, \dots, \alpha_n, )$  a vector of length  $n$  in  $F_{2^m}^*$ , with the  $\alpha_i$  are distinct two by two.

The set of codes with the generator matrix  $G$  of the form

$$G = \begin{pmatrix} v_1 & v_2 & \dots & v_n \\ v_1 \alpha_1 & v_2 \alpha_2 & \dots & v_n \alpha_n \\ \dots & \dots & \dots & \dots \\ v_1 \alpha_1^{k-1} & v_2 \alpha_2^{k-1} & \dots & v_n \alpha_n^{k-1} \end{pmatrix} \text{ is called the family of generalized Reed-}$$

Solomon codes.

## 2.6 The classical Goppa codes

Definition

Let  $L = (\alpha_1, \alpha_2, \dots, \alpha_n)$  a suite of  $n$  distinct elements of  $F_{2^m}$  and  $g(z) \in F_{2^m}[z]$  a unit polynomial of degree  $r$  irreducible in  $F_{2^m}[z]$ . The irreducible binary Goppa code, its support  $L$  (generator vector) and its generator polynomial  $g$  noted  $\Gamma(L, g)$  is the set of words  $a = (a_1, \dots, a_n) \in F_2^n$  such that one of the following equivalent characterizations is verified:

$$1. R_a(z) = \sum_{i=1}^n \frac{a_i}{z - \alpha_i} = 0 \text{ mod } g(z).$$

$$2. \text{Ha}^t = 0 \text{ with } H = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \dots & \dots & \dots & \dots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \dots & \alpha_n^{r-1} \end{pmatrix} \begin{pmatrix} g(\alpha_1)^{-1} & & & \\ & \dots & & \\ & & \dots & \\ & & & g(\alpha_n)^{-1} \end{pmatrix}$$

parity check matrix.

3.  $g(z)$  divided  $\frac{d\sigma_a(z)}{dz}$  with  $c \sigma_a(z) = \prod_{i=1}^n (z - \alpha_i)^{a_i}$  locator polynomial.

The construction of a code Goppa:

Goppa's code is a linear code on the field  $F_2$ , its construction requires the use of an extension  $F_{2^m}$ . Each element of the matrix  $H$  is then broken down into  $m$  elements of  $F_2$  placed in columns, using a projection of  $F_{2^m}$  in  $F_2^m$ ; we go from a size matrix  $r \times n$  on  $F_{2^m}$  to a matrix of size  $rm \times n$  on  $F_2$  so it is a length code  $n = |L|$  and dimension  $k = n - mr$  and has a minimum distance at least equal to  $d = r + 1$ . Indeed the parity check matrix  $H$  is written as the product of a Vandermonde matrix and an invertible matrix therefore all under a square matrix  $r \times r$  of  $H$  is invertible, then there are no code words with a weight less than or equal to  $r$ .

The decoding of a Goppa code:

Several techniques exist to decode Goppa codes but they work by the same principle. Let  $c' = c + e$  and  $w(e) < \frac{r}{2}$ . We start by calculating the syndrome  $R_{c'}(z)$  on  $F_{2^m}$ ; from this syndrome we will write a key equation, and we will finish the decoding by solving the key equation to find  $e$ .

If  $R_a(z) = 0$  the word will belong to the code.

The key equation

Let  $\sigma_e(z) = \sum_{i=1}^n (z - \alpha_i)^{e_i}$  of degree  $< \frac{r}{2}$ . On introduit le polynôme  $w_e(z) = \sigma_e(z)R_e(z) \text{ mod } g(z)$  called evaluator polynomial.

$$\sigma_e(z)R_e(z) = \sum_{i=1}^n \frac{e_i}{z - \alpha_i} \prod_{j=1}^n (z - \alpha_j)^{e_j} \text{ mod } g(z) = \sum_{i=1}^n e_i \prod_{\substack{j=1 \\ j \neq i}}^n (z - \alpha_j)^{e_j} \text{ mod } g(z).$$

We can solve the key equation in two different ways: Berlekamp Massey's algorithm and the extended Euclidean algorithm. The latter has the advantage of being easier to present. Indeed we seek to find  $w_e$  and  $\sigma_e$  of degree  $< \frac{r}{2}$  such as  $w_e(z) = \sigma_e(z)R_e(z) \text{ mod } g(z) = \sigma_e(z)R_e(z) + k(z)g(z)$ . If we try to calculate the gcd of  $(g, R_e)$  with the extended Euclidean algorithm, we will calculate at each step the polynomials  $u_i, v_i, r_i$  checking  $R_e u_i + g v_i = r_i$ . At each step the polynomials  $u_i$  and  $v_i$  will be of degree  $< i$  and the degree of  $r_i$  is equal to  $r - i$ . There is therefore a step at which if we stop the algorithm we will find a solution of the equation  $\sigma_e = u_{i_0}$  and  $w_{i_0} = r_{i_0}$  to a scalar coefficient.

### 3. Encryption/decryption systems

#### 3.1 The basic system (McEliece)

We start by generating a code  $[n, k, d]_q$  linear of a well-chosen family and its generator matrix  $G$ . We are going to mix this matrix to make it indistinguishable from a random matrix, so we need a permutation matrix  $P$  her size is  $n \times n$  (having 1 in each row and column and 0 everywhere) and an invertible matrix  $S$  her size

$k \times k$  ( $S$  is jammer). The public key will be  $G' = SGP$  which is indistinguishable from a random matrix (The definition of a random matrix comes from the definition of random code which be introduced in section four). The knowledge of  $S$ ,  $P$  and  $G$  allows us to find the structure of the design code and provides us with the decoding algorithm.

### 3.1.1 The algorithms of the McEliece system

We cite the component algorithms of the McEliece cryptosystem [4].

The generation of keys

Input

A family of linear codes  $[n, k, d]_q$  chosen for design.

Procedure

Choose a generator matrix  $G$  in systematic form of the design code.

Choose an invertible matrix  $S$  her size  $k$  with coefficients in  $F_q$ .

Choose a permutation matrix  $P$  her size is  $n \times n$ .

Calculate  $G' = SGP$ .

Output

The public key  $G'$ .

The private key  $(S, G, P)$ .

Encryption of the plaintext.

Input

The public key  $G'$ .

The plaintext  $x \in F_q^k$ .

Procedure

Choose a vector  $e \in F_q^n$  (an error) his weight less than or equal to the design code correction capacity.

Calculate  $y = xG' + e$ .

Output: The cipher text  $y$ .

Decryption of cipher text

Input: the cipher text  $y$ , The private key  $(S, G, P)$ .

Procedure

Calculate  $u = yP^{-1}$ .

Calculate  $x' = f_G(u)$  with  $f_G$  the design code decoding algorithm, whose generator matrix is  $G$ .

Calculate  $x = x'S^{-1}$ .

Output: the plaintext  $x$ .

Remark

The use of binary Goppa code as a secret key is initially proposed by McEliece in its original version. Where he took the following parameters:  $m = 10$ ,  $n = 2^m = 1024$ ,  $r = 50$ ,  $k = n - mr = 524$ . So far it seems that this choice is perfectly safe, but it is not used in practice because the size of its public key is very large.

Example

We use the Hamming code with its generator matrix  $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$

and parity check matrix  $H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$

The generation of keys

Let the private key S, G, P.

$$S = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} = S^{-1}, P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix},$$

$$P^{-1} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

The public key:  $G' = SGP = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$

Encryption

Let the plaintext  $x = (0110)$  and let error vector  $e = (0010000)$ .

The cipher text is  $y = xG' + e = (0111000) + (0010000) = (0101000)$ .

Decryption

We decipher the text received  $y = (0101000)$ . We have  $y = xG' + e = xSGP + e$

then  $P^{-1}y = xSG + eP^{-1} = (1100000) = y'$ .  $Hy'^t = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ , so the error is in the third

position hence  $u = (1110000) = xSG$ . And since G is generator matrix of the systematic system then  $xS = (1110)$  then  $x = (1110)S^{-1} = (0110)$ . x. Then the plaintext sought.

### 3.2 The Niederreiter variant

Let C a linear t-corrector code of length  $n$  and dimension  $k$ . Let H a parity check matrix of C her size is  $(n - k) \times n$ . We randomly choose an invertible matrix S and P a permutation matrix. We calculate  $H' = SHP$ . We will have  $H'$  a public key and  $(S, H, P)$  the private key, with the knowledge of a syndrome decoding algorithm in C. Let  $x$  a plaintext of length  $n$  and weight  $t$ , we calculate the cipher text  $y = H'x^t$ . The recipient receives  $y$  knowing the secret key, he can calculate  $S^{-1}y = HPx^t$ . Using the syndrome decoding algorithm of C, he can find  $Px^t$  and applying  $P^{-1}$  the plaintext  $x$  is found.

The algorithms of the Niederreiter cryptosystem [5]

The generation of keys

Input

A linear code  $[n, k, d]_q$  is chosen for the design, of which we know a decoding algorithm by syndrome.

Procedure

Choose a parity check matrix  $H$  of design code.

Choose a matrix  $S$ , invertible of size  $k$  with coefficients in  $F_q$ .

Choose a permutation matrix  $P$  of size  $n \times n$ .

Calculate  $H' = SHP$ .

Output

The public key  $H'$ .

The private key  $(S, H, P)$ .

Encryption

Input

The public key  $H'$ .

The plaintext  $x \in F_q^n$  of weight less than or equal to the correction capacity.

Procedure

Calculate  $y = H'x^t$ .

Output

The cipher text  $y$ .

Decryption

Input

The private key  $(S, H, P)$ .

The cipher text  $y$ .

Procedure

Calculate  $y' = S^{-1}y$ .

Calculate  $x' = f_H(y')$  with  $f_H$  the code syndrome decoding algorithm, its parity check matrix is  $H$ .

Calculate  $x = x'P^{-1}$ .

Output

The plaintext  $x$ .

Remark

Reed-Solomon codes were originally proposed by Niederreiter as a family of codes that could be considered by his cryptosystem. In 1992 Sidelnikov and Shestakov have shown that it is easy to attack this cryptosystem [2].

#### 4. The security of cryptosystems based on correcting codes

The security of cryptosystems based on error-correcting codes is based on the problem of distinguishing the design code (hidden) from a random code. We first give the following definitions:

- Code equivalence

Two codes are said to be equivalent if their generator matrices (respectively parity) are deduced from each other by permutation of columns.

- Random code

A random code is a linear code of which the  $k$  linearly independent lines of the generator matrix (or the  $n$  linearly independent columns of the parity matrix) have been generated randomly.

The main parameters for securing an McEliece cryptosystem and its variants are then the structure of the code family chosen for the design, which it is desirable that it will be difficult to find an equivalent code. Since the robustness of such a system lies in the difficulty of decoding and the hidden structure of the design code, then

the attacker can attempt to attack the system by two methods: decoding attack and structural attack. The resistance of the system to these two attack methods depends on the family of codes chosen for the design. The choice of code family is the essential point in the design of the cryptosystem.

#### 4.1 Decoding attack

The attacker directly attempts to decode the cipher text in the  $C$  code (generator matrix  $G$  or public key parity  $H$ ); the principle consists of decoding the intercepted cipher text relative to the public code using general decoding algorithms. We cite two decoding problems in a random code:

Problem 1

Given  $G$  a random binary matrix of size  $k \times n$ , generator of a  $C$  code of dimension  $k$ .  $x$  a random word of  $F_2^n$  and  $t$  a positive integer, find if there is an error word  $e$  of  $F_2^n$  such as  $w(e) \leq t$  and  $x + e \in C$ .

Problem 2

Given  $H$  a binary random parity matrix; her size  $(n - k) \times n$  of a  $C$  code its dimension  $k$ ,  $s$  a random vector of  $F_2^{n-k}$  and  $t$  a positive integer, find if there is a word  $x$  of  $F_2^n$  such as  $w(x) \leq t$  and  $Hx^t = s$ .

Decoding in random code is behind the following attacks:

- Algorithme de décodage par ensemble d'information

The principle is based on two steps: the selection of a set of information and the search for low-weight word. There are several variants which propose to optimize one or the other of these two steps.

Definition

Let  $C$  a linear code of generator matrix  $G$  and length  $n$ . A set of information  $I$  is a subset of  $\{1, 2, \dots, n\}$  such as  $G_I$ , her size  $k \times k$  formed of columns of  $G$  labeled by the elements of  $I$ , is invertible.

Remark

The matrix  $(G_I|G_J)$  with  $I \cup J = \{1, 2, \dots, n\}$  is equivalent to  $G$ .

Algorithm

Input

$G$ : a matrix generating of a code  $C$ .

$t$ : a positive integer.

$y$ : a word of  $F_2^n$  such as  $d(y, C) \leq t$ .

Output

The couple  $(x, e)$  such as  $y = xG + e$  where  $w(e) \leq t$ .

Procedure

Randomly draw a set of information  $I$  of the code  $C$  (let  $J$  such as  $I \cup J = \{1, 2, \dots, n\}$ ).

Calculate  $R = G_I^{-1}G_J$ .

Write  $y = (y_I|y_J)$ .

Calculate  $e_j = y_j - y_I R$ .

Repeat the previous operations until you find  $e_j$  such as  $w(e_j) \leq t$ .

Returne  $= (0|e_j)$ .

Determine the word  $x$  such as  $y - e = xG$ .

Proof

We have a  $y = xG + e$  and  $y = (y_I|y_J) = x(G_I|G_J) + (e_I|e_J)$ . Hence  $e_I = y_I - xG_I$  and  $e_J = y_J - xG_J$ .

If the set of information I does not contain an error position ( $e_i = 0$ ) and like  $G_I$  is invertible, we obtain  $y_1 = xG_I$ ,  $e_j = y_j - y_1G_I^{-1}G_j$ . Then  $e = (0|y_j - y_1G_I^{-1}G_j)$  is the solution sought.

Remark

We have  $C_n^k$  possibilities to choose  $k = |I|$  positions of  $\{1, 2, \dots, n\}$  ( $|I|$  is a cardinality of I). And we have  $C_{n-t}^k$  possibilities to choose  $k = |I|$  positions among  $n - t$  positions where  $e_i = 0$ . So the probability of getting the set of information I with  $e_i = 0$  is  $p = \frac{C_{n-t}^k}{C_n^k}$  and the average number of iterations will be  $\frac{1}{p}$ .

Example

Let us try to attack the following system by this method: We

$$\text{have } G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

The cipher text  $y = (10101011)$  et  $t = 1$ .

looking  $(m, e)$  such as  $mG + e = y$ .

$$\text{Let } I = \{1, 5\} \subset \{1, 2, \dots, 8\} \text{ then } G_I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = G_I^{-1}$$

$$\text{and } G_j = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

$y_1 = (1, 1)$  and  $y_j = (0, 1, 0, 0, 1, 1)$ . Then  $e_j = y_j - y_1G_I^{-1}G_j = (001000)$ , it follows that  $(e_1|e_j) = (00001000)$ .

$$\begin{aligned} (y_1|y_j) + (e_1|e_j) &= (11010011) + (00001000) = (11011011) = m(G_I|G_j) \\ &= m \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \end{aligned}$$

then  $m = (11)$ .

- Decoding by paradox of birthdays

Consider an instance of problem 2. For a parity check matrix  $H$  of size  $r \times n$ , a syndrome  $s$  and a weight  $t$ . If the weight  $t$  is even, let us separate the columns of  $H$  in two sets of the same size  $H_1$  and  $H_2$  such as  $H = (H_1|H_2)$ .

Let us build  $L_1 = \{H_1e_1^t, e_1 \text{ of length } \frac{n}{2} \text{ and the weight } \frac{t}{2}\}$  et  $L_2 = \{s + H_2e_2^t, e_2 \text{ of length } \frac{n}{2} \text{ and the weight } \frac{t}{2}\}$ . Common elements of  $L_1$  and  $L_2$  are such that  $H_1e_1^t = s + H_2e_2^t$ , that is to say  $(e_1|e_2)$  is solution of problem 2.

The probability that one of the solutions splits into two equal parts of the parity

matrix is  $p = \frac{\binom{C_{n/2}^{t/2}}{C_n^t}}{C_n^t}$ ; to solve problem 2 you have to repeat these operations  $\frac{1}{p}$  on different permutations of the public code.

- The recovery of a plaintext encrypted twice by the same McEliece system

This is an active attack that only applies to the McEliece encryption system (because it is not deterministic) and does not apply to the Niederreiter system. Suppose the plaintext  $x$  is encrypted in two different ways. We will have  $y_1 = xG + e_1$ ,  $y_2 = xG + e_2$  où  $e_1$  et  $e_2$  sont deux vecteurs d'erreur distincts de poids  $t$ . We get the word  $y_1 - y_2 = e_1 - e_2$  which is less than or equal to  $2t$ . Once an attacker has detected that the two cipher texts  $y_1$  and  $y_2$  correspond to the same plaintext, this information will reduce the number of iterations of the decoding algorithm set

of information. Message forwarding is detected by observing the weight of the two cipher texts. If the two plaintexts are identical then, the weight of the sum of the two numerical texts remains less than  $2t$  in general ( $t$  the correction capacity).

Algorithm

Input

$G$ : The public key of size  $k \times n$ .

Two words  $y_1$  and  $y_2$  such as  $y_1 = xG + e_1$ ,  $y_2 = xG + e_2$  where  $e_1$  and  $e_2$  are two distinct error vectors of weight  $t$ .

Output

The plaintext  $x$ .

Procedure

Calculate  $y_1 - y_2$ .

Randomly draw a set of information  $I \subset \{1, 2, \dots, n\}$  which label the zero positions of  $y_1 - y_2$ .

Calculate  $e_j = y_j - y_1 G_I^{-1} G_j$  où  $y_1 = (y_1 | y_j) \text{ et } I \cup J = \{1, 2, \dots, n\}$ .

Repeat the previous operations until the weight of  $e \leq t$ .

Return  $x = y_1 G_I^{-1}$ .

Example

Let us try to attack by this method the system of the previous example.

Either plaintext encrypted two ways in which the public key is

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

$$y_1 = mG + e_1 = (11) \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} + (00010000) = (10101011)$$

$$y_2 = mG + e_2 = (11) \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} + (00100000) = (10011011)$$

$$y_1 + y_2 = (00110000).$$

Draw a set of information that labels the zero positions of  $y_1 + y_2$  let  $I = \{7, 8\}$ .

$$G_I = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = G_I^{-1}, G_j = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix};$$

$$y_1 = (10101011), y_I = (11), y_j = (101010).$$

$$e_j = y_j - y_I G_I^{-1} G_j = (101010) - (11) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} = (000100).$$

$$\begin{aligned} (y_I | y_j) + (e_I | e_j) &= (11101010) + (00000100) = (11101110) \\ &= m \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \end{aligned}$$

So we extract  $m = (11)$ .

## 4.2 Structural attack

The attacker tries to find a decomposition of the key  $G' = S_1 G_1 P_1$ , which allows it to develop its own decoding algorithm. Succeeding in a structural attack generally amounts to finding a code equivalent to the public code for which we know a decoding algorithm. This attack depends exclusively on the structure of the space of



the keys used. We quote here a successful attack on an McEliece system with the Reed-Solomon code as the design code.

- The attack of Sidelnikov and Shestakov

Sidelnikov and Shestakov showed [6] that generalized Reed-Solomon codes were so structured that one could find a decoder of the public code in polynomial time. The systematic form of the matrix generating a GRS code can be obtained from the following proposition:

Proposal

$$\text{Let } G = \begin{pmatrix} v_1 & v_2 & \dots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \dots & v_n\alpha_n \\ \dots & \dots & \dots & \dots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \dots & v_n\alpha_n^{k-1} \end{pmatrix} \text{ a matrix generating a Reed-Solomon}$$

code generalized on  $F_{q^m}$  then there is a matrix  $k \times k$  invertible  $S$  coefficient in  $F_{q^m}$  and a matrix  $R = (R_{ij})_{\substack{i=1\dots k \\ j=k+1\dots n}}$  such that  $(I|R) = SG$  and  $R_{ij} = \frac{v_i}{v_j} \prod_{\substack{s=1 \\ s \neq i}}^k \frac{\alpha_j - \alpha_s}{\alpha_i - \alpha_s}$

Proof

For  $i = 1, 2, \dots, k$  we define the following interpolation polynomial  $f_i(x) = \prod_{\substack{s=1 \\ s \neq i}}^k \frac{\alpha_j - \alpha_s}{\alpha_i - \alpha_s} = \sum_{j=1}^k f_{ij} x^{j-1}$  of degree  $k - 1$  such that  $f_i(\alpha_i) = 1$ ,  $f_i(\alpha_j) = 0$  for

$j = 1, 2, \dots, k$  and  $j \neq i$ . We note  $S = \left( \frac{f_{ij}}{v_i} \right)_{\substack{i=1\dots k \\ j=1\dots k}}$ .

The  $i$ th row of the matrix produces  $SG$  is  $\left( f_i(\alpha_1) \frac{v_1}{v_i}, f_i(\alpha_2) \frac{v_2}{v_i}, \dots, f_i(\alpha_n) \frac{v_n}{v_i} \right)$

By construction of polynomials  $f_i$ , the  $k$  first columns of the matrix  $SG$  form the identity matrix, therefore  $S$  is invertible and  $SG = (I|R)$  where  $R = R_{ij}$  and  $R_{ij} = f_i(\alpha_j) \frac{v_j}{v_i}$ .

Corollary

Let  $I$  the identity matrix its order  $k$  and  $R = (R_{ij})_{\substack{i=1\dots k \\ j=k+1\dots n}}$  where

$R_{ij} = \frac{v_i}{v_j} \prod_{\substack{s=1 \\ s \neq i}}^k \frac{\alpha_j - \alpha_s}{\alpha_i - \alpha_s}$ . Alors la matrice  $(I|R)$  is the generator matrix in systematic form

$$\text{of the generator matrix GRS code } G = \begin{pmatrix} v_1 & v_2 & \dots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \dots & v_n\alpha_n \\ \dots & \dots & \dots & \dots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \dots & v_n\alpha_n^{k-1} \end{pmatrix}.$$

Proof

Can be deduced from the definition of the generalized Reed-Solomon code and the latest proposal.

Algorithm

Input

A family of generalized Reed-Solomon code of length  $n$ , of dimension  $k$  constituting the key space.

The public key  $G'$ .

Results

The matrix  $G = (v_j \alpha_j^i)_{\substack{i=0, \dots, k-1 \\ j=1 \dots n}}$  and  $S$  invertible matrix its size  $k \times k$  such that

$$G' = SG.$$

Procedure

Put the matrix  $G'$  in form  $(I|R)$  by Gaussian elimination.

Determine the matrix  $G = \left( v_j \alpha_j^i \right)_{\substack{i=0, \dots, k-1 \\ j=1, \dots, n}}$  such that  $\alpha_1, \dots, \alpha_n$  et  $v_1, \dots, v_n$  check the equations  $R_{ij} = \frac{v_j}{v_i} \prod_{s=1}^k \frac{\alpha_j - \alpha_s}{\alpha_i - \alpha_s}$ ,  $s \neq i$ .

Determine the matrix  $S$  such that  $G' = SG$ .

## 5. Conclusion

In conclusion, the security of cryptosystems based on error-correcting codes is strongly linked to the family of code used in the design of the system. The cryptosystem based on the Reed-Solomon code was broken by Sidelnikov and Shestakov in 1992. The version of McEliece using Goppa codes has been studied for 40 years and it seems perfectly secure from a cryptographic point of view; but it is not used in practice because the size of its public key is much larger than we know how to do with systems from other fields (RSA for example), hence the importance of finding a way to reduce the size of their public key. In the end, the McEliece system based on Goppa's code remains a preferred system as a post-quantum cryptosystem. We have not covered in this chapter other cryptographic applications of error-correcting codes, including hash functions [3, 7–11], pseudo-random generators, identification protocols, etc.

## Author details

Ahmed Drissi

National School for Applied Sciences, ENSA, Abdelmalek Essaadi University, Tangier, Morocco

\*Address all correspondence to: idrissi2006@yahoo.fr

## IntechOpen

© 2020 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

## References

- [1] Cayrel PL. Nouveaux résultats en cryptographie basée sur les codes correcteurs d'erreurs.
- [2] Loidreau P. Etude et optimisation de cryptosystèmes à clé publique fondés sur la théorie des codes correcteurs [doctoral dissertation]; Thèse de doctorat. ENSTA Paris. 2001
- [3] Drissi A. Formation doctorale [doctoral dissertation]. Thèse de doctorat. Université Ibn Zohr; 2014
- [4] McEliece RJ. A Public-Key Cryptosystem Based on Algebraic Coding Theory, 42441978. pp. 114-116
- [5] Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*. 1986;15(2): 159-166
- [6] Sidelnikov VM, Shestakov SO. On insecurity of cryptosystems based on generalized Reed-Solomon codes. *Discrete Mathematics and Applications*. 1992;2(4):439-444
- [7] Drissi A, Asimi A. One-way hash function based on goppa codes «OHFGC». *Applied Mathematical Sciences*. 2013;7(143):7097-7104
- [8] Dallot L. Sécurité de protocoles cryptographiques fondés sur les codes correcteurs d'erreurs [doctoral dissertation]; France: Université de Caen/Basse-Normandie; 2010
- [9] Merkle R. One way hash functions and DES. In: *Crypto 1989, LNCS*. Vol. 435. 1990
- [10] Pretzel O. *Error-Correcting Codes and Finite Fields*. Student ed. Oxford University Press, Inc.; 1996
- [11] Kumar R, Naidu AS, Singh A, Tentu AN. McEliece cryptosystem: Simulation and security vulnerabilities. *International Journal of Computing Science and Mathematics*. 2020;12(1): 64-81



# Tradeoff Attacks on Symmetric Ciphers

*Orhun Kara*

## Abstract

Tradeoff attacks on symmetric ciphers can be considered as the generalization of the exhaustive search. Their main objective is reducing the time complexity by exploiting the memory after preparing very large tables at a cost of exhaustively searching all the space during the precomputation phase. It is possible to utilize data (plaintext/ciphertext pairs) in some cases like the internal state recovery attacks for stream ciphers to speed up further both online and offline phases. However, how to take advantage of data in a tradeoff attack against block ciphers for single key recovery cases is still unknown. We briefly assess the state of art of tradeoff attacks on symmetric ciphers, introduce some open problems and discuss the security criterion on state sizes. We discuss the strict lower bound for the internal state size of keystream generators and propose more practical and fair bound along with our reasoning. The adoption of our new criterion can break a fresh ground in boosting the security analysis of small keystream generators and in designing ultra-lightweight stream ciphers with short internal states for their usage in specially low source devices such as IoT devices, wireless sensors or RFID tags.

**Keywords:** symmetric cipher, block cipher, stream cipher, tradeoff attack, keystream, keystream generator, Hellman table, rainbow table, one-way function, preimage

## 1. Introduction

In general, bulk encryption is performed through symmetric ciphers; that is, block ciphers or stream ciphers. Hash functions, message authentication codes and authenticated encryption schemes are also based on the quite similar design and security principles. All these cryptographic primitives are examples of one-way functions for which it must be computationally infeasible to find a preimage. Indeed, the only generic method to invert a given output is exhaustively searching for one of its inputs.<sup>1</sup> This may be embodied as brute force attacks on block ciphers and stream ciphers, internal state recovery attacks on keystream generators, preimage attacks on hash functions or constructing valid messages to given tag values for message authentication codes.

The brute force attacks can be expedited significantly by utilizing very large tables that have been already prepared during the offline phase. This phase is called the precomputation phase also and is usually equivalent to exhaustive search. Nevertheless, once it is executed, the prepared tables can be used several times.

---

<sup>1</sup> Permutations as one-way functions are out of scope of this chapter.

It may be possible to further improve a tradeoff attack by exploiting large amount of data (plaintext/ciphertext pairs). Biryukov-Shamir attack on keystream generators can be considered as a typical example of a tradeoff among time, memory and data [1]. One of the internal states of a long keystream sequence is recovered. However, it is still unknown how to use data to improve the tradeoff attacks on block ciphers.

The state sizes of block ciphers are not of security concern against tradeoff attacks, enabling to design ultra-lightweight block ciphers. In fact, we encounter several such block cipher designs in the literature during the last decades [2–9]. However, it seems to be almost impossible to design ultra-lightweight stream ciphers due to their strict security criterion on the lower bound of their internal state sizes to resist tradeoff attacks.

The tradeoff attacks can be quite effective against some real world cryptographic primitives. The tradeoff tables can be used in practical applications to break real life ciphers such as A5/1 for the GSM encryption [10–12] or to crack passwords by finding preimages to hash functions [13–17]. In this chapter, we introduce briefly how to use tradeoff tables to invert small sized one-way functions. Moreover, we evaluate the state of art of the applications, raise some open problems and come up with a discussion on the countermeasures against tradeoff attacks on keystream generators.

We argue that it is possible to loosen the lower bound for the state size without sacrificing the security against tradeoff attacks and this can enable designing ultra-lightweight stream ciphers. We claim that the lower bound for the internal state size can be diminished to  $4n/3$  bits from  $2n$  bits where  $n$  is the key length. It is possible to design a keystream generator of size  $4n/3$  bits, which remains still secure against tradeoff attacks and which presents a great advantage in low cost applications. Indeed, such ciphers are in real world demand due to the confidentially issues of lightweight devices such as RFID tags, wireless sensors or IoT devices.

It is straightforward that resistance against tradeoff attacks is not sufficient for security. Unfortunately, the security of small stream ciphers has not been studied sufficiently so far. We still do not know how to design secure and small stream ciphers. This is due to fact that almost all the stream ciphers in the literature have internal state sizes at least twice as large as their key sizes. Hence, there is almost no example in the literature to analyze. The recent small keystream generators such as Sprout [18] or Plantlet [19] are analyzed intensively in a short while and several weaknesses are discovered [20–26].

The tradeoff attacks on block ciphers so far are limited to the tradeoff between only time and memory. It is an open problem how to construct a tradeoff curve between memory and data or among memory, data and time for a single key recovery attack. We phrase the problem of *inverting one-way function with data*, the problem of *mutual inverting of multiple one-way functions* and the problem of *inverting only one of the several independent one-way functions*. Moreover, we address these problems with block ciphers and raise a question about the hierarchical relationships between any pair of them.

The outline of the chapter is as follows. We briefly overview the tradeoff attacks on symmetric ciphers, give some recent applications of these attacks and evaluate them in Section 2. Then, we assess the tradeoff attacks on stream ciphers and keystream generators in Section 3. We also introduce the tradeoff attacks on block ciphers, discuss the differences from those on stream ciphers and state some open problems in Section 4. We assess the internal state recovery tradeoff attacks and make an argument about the internal state sizes of keystream generators in Section 5. Finally, we introduce our concluding remarks in Section 6.

## 2. Inverting a one-way function through tradeoff

Let  $f : GF(2)^m \rightarrow GF(2)^n$  be a one-way function of  $m$ -bit input and  $n$ -bit output. That is, it is easy to compute the output,  $f(x) = y$ , of a given input  $x \in GF(2)^m$ ; but computationally infeasible to find a preimage  $x \in f^{-1}(y)$  for a given output  $y \in GF(2)^n$ .

The phrase "computationally infeasible" is not a formal or a precise statement. Indeed, we mean that the fastest algorithm of finding a preimage  $x \in f^{-1}(y)$  must be exhaustively searching for  $x$ , either online or offline. This definition is valid for random one-way functions which are generally not permutations. The one-way functions deduced from symmetric ciphers are examples and we consider them only throughout the chapter. The time complexity of recovering one preimage of a given value  $y \in GF(2)^n$  is about  $T = 2^n$  calls of the  $f$ -function (simply  $2^n$ ) for a one-way function  $f$ . There is almost no memory or data complexity. Hence this can be considered as one of the extreme cases where only the time complexity dominates.

The time complexity may be substituted by the memory complexity if we compute all the  $(x, f(x))$  values in advance during the offline phase (which we call precomputation phase) and save them in a sorted table with respect to the second column,  $f(x)$ . Then, the time complexity of the precomputation phase is  $2^n$  and the memory complexity is  $M = 2^n$ . On the other hand, the time complexity of finding a preimage  $x \in f^{-1}(y)$  for a given  $y$  during the online phase is relatively negligible in comparison to the memory complexity. One needs to search for  $y$  in the second column of the table and this search takes roughly  $n$  steps since the table is sorted. This is also one of the extreme cases where only the memory complexity dominates.

In general, we can regard the tradeoff attacks as the attacks searching for a preimage of a one-way function by utilizing a significant memory prepared in the precomputation phase to reduce the time complexity from  $2^n$ . A tradeoff curve between memory and time is introduced with possibly some restrictions. The time complexity is decreased by increasing the memory complexity or vice versa. But the ratio of increase/decrease depends on the tradeoff curve. In general, the optimum point on the curve is considered as the point where  $T = M$  if the restrictions permit to choose this point. Let us remark that the precomputation phases of these attacks must be the whole exhaustive search to provide significantly high success rates. But, since this offline phase is run only once, its complexity can be ignored in some applications where one uses the tables several times to invert enormous number of outputs. The Hellman tables or the rainbow tables for the GSM encryption algorithm A5/1 are typical real world applications [10, 12].

It is possible to ease the problem of inverting a one-way function  $f$  by introducing large number of data. Then the corresponding tradeoff attacks can be further improved by constructing better tradeoff curves with the addition of the amount of data used.

We can define the problem of *inverting one-way function with data* as follows. Let  $y_1, \dots, y_D \in GF(2)^n$  be given. Then, find a preimage for one of them. That is, find  $x_i$  such that  $f(x_i) = y_i$ . This problem is easier than finding a preimage of only one given element  $y \in GF(2)^n$ . Indeed, it is possible to prepare a sorted list of  $y_1, \dots, y_D$  and then search for  $x$  such that  $f(x)$  is in this sorted list. It is clear that the time complexity of the exhaustive search is  $2^n/D$ . Hence, the time complexity of the default attack for inverting one-way function with data is reduced by a factor of  $D$ .

It is possible to address the problem of inverting one-way function with data in stream ciphers and mount some tradeoff attacks for single key setting. We introduce these attacks in Section 3. However, it is not known in the literature yet how to

associate a single key recovery attack for a block cipher as a problem of inverting one-way function with data (see Section 4 for details of the tradeoff attacks in the case of block ciphers).

## 2.1 Hellman and rainbow tables

One very well known way of inverting a one-way function is using Hellman tables [27]. Initially, Hellman introduced the tables only for recovering the DES keys in his original work in [27] but it can be used to invert any one-way function.

Let us assume that the input and the output sizes of a one-way function,  $f$ , are equal. That is,  $f : GF(2)^n \rightarrow GF(2)^n$ . The general cases may easily be deduced by the reduction or enlargement techniques as Hellman applied for the DES encryption by reducing its block size to 56 bits. Let  $x \in GF(2)^n$  be an input. Then, compute  $f(x), f^2(x), \dots, f^t(x)$  and save the pair,  $(x, f^t(x))$ .

If a given value  $y \in GF(2)^n$  is equal to  $f^i(x)$  for some  $i \in \{1, \dots, t\}$  then we can find a preimage for  $y$  easily:  $f^{i-1}(x)$  will be a preimage since  $f(f^{i-1}(x)) = y$ . We can check if  $y = f^i(x)$  for some  $i$  by checking the equality  $f^{t-i}(y) = f^t(x)$ . Indeed we have

$$f^{t-i}(f^i(x)) = f^t(x) = f^{t-i}(y). \quad (1)$$

Therefore, it is highly probable that  $y = f^i(x)$ . It may be possible that  $y \neq f^i(x)$  even though  $f^{t-i}(y) = f^t(x)$  since  $f$  is not a permutation. This case is considered as a false alarm. The probability of the false alarms should be taken into account for the success rate of the attack. Gildas *et al.* introduce an efficient way of ruling out the false alarms, particularly in the perfect tables [28].

Choosing  $m$  different  $x$  points and preparing a table of  $m$  pairs  $(x, f^t(x))$  sorted with respect to  $f^t(x)$  (which is called a Hellman table), it is possible to find a preimage of a given output  $y \in GF(2)^n$  if  $y = f^i(x)$  for some  $x$  in these  $m$  pairs by calling the  $f$  function and checking if the result is among the second (sorted) values of the pairs  $(x, f^t(x))$  at most  $t$  times. Therefore, examining if  $y$  is in the set  $\{f^i(x)\}$  with  $m \cdot t$  elements, costs  $t$  calls of  $f$  and the memory amount we need is  $m$  since we save  $m$  pairs for one table of  $m \cdot t$  elements. These  $m$  pairs consist of the initial and the final columns of the table.

The most significant disadvantage of Hellman tables is the high propagation of the collisions throughout the rows. If  $f^i(x) = f^j(x')$  for some  $1 \leq i, j < t$  and different starting points  $x \neq x'$ , then the collision is going to merge to the rest of the rows as  $f^{i+k}(x) = f^{j+k}(x') \forall k = 1, \dots, \min\{t-i, t-j\}$ . This restricts the capacity of a Hellman table. Indeed, we should choose the number of the rows and the columns  $m$  and  $t$  such that  $mt^2 \leq 2^n$  to optimize the probability of collisions according to the birthday paradox [27]. Therefore, we need roughly  $t$  tables since one table can contain at most  $mt$  different elements and each Hellman table must be prepared by using a different function deduced from a slight derivation of the  $f$ -function so as to ensure the independence of the tables.

The time complexity is  $T = t^2$  since examining through one table costs  $t$  calls of the  $f$ -function and we have  $t$  tables. Similarly, we need  $M = mt$  memory to save  $t$  tables. As a corollary, the tradeoff curve  $M^2T = 2^{2n}$  is deduced with  $mt^2 = 2^n$ . The optimum point on the curve is  $T = M = 2^{2n/3}$ . The precomputation phase for



preparing the tables is equivalent to the exhaustive search and hence its complexity is  $2^n$ .

Oechslin introduces another kind of tables to invert one-way functions, which he calls rainbow tables [29]. He proposes to use a different function for the computation of each column and hence each row is constituted as

$$f_1(x), f_2(f_1(x)), \dots, f_t(f_{t-1}(\dots f_1(x))) \quad (2)$$

instead of  $f(x), f^2(x), \dots, f^t(x)$  for a chosen starting point  $x$  where  $f_i$ s are derived from  $f$  by slight modifications. Only the initial point  $x$  and its final evaluation  $f_t(f_{t-1}(\dots f_1(x)))$  are saved as in the case of Hellman tables.

Rainbow tables have a significant advantage over Hellman tables: The collisions in different columns do not propagate in rainbow tables. So, it is possible to use only one rainbow table for covering majority of the space  $GF(2)^n$ . The table contains  $t$  columns and  $mt$  rows. However, tracing through a rainbow table costs much more. For a given output  $y$ , check if it is in the last column. If not then check  $f_t(y)$  and then  $f_t(f_{t-1}(y))$  and then,  $f_t(f_{t-1}f_{t-2}(y))$  and so on are in the last column one by one.

Both the Hellman tables and the rainbow tables have the same tradeoff curve. But, the time complexity is  $t(t-1)/2$  for a rainbow table which is roughly twice less than  $t^2$ . This makes rainbow tables more popular in practical applications.

Barkan *et al.* compares these two methods and combine them in a general model based on stateful random graphs [30]. They also improve the time complexity of the rainbow tables [30]. Lu *et al.* use the unified rainbow tables to break GSM A5/1 algorithm and recover an A5/1 key in 9 s with a success rate of 81% by using general purpose GPUs with 3 NVIDIA GeForce GTX690 cards [12]. There are also FPGA implementation versions of tracing through the rainbow tables of the A5/1 states [10, 11]. The success rates of the rainbow tables for A5/1 are improved in [12]. Rainbow tables are commonly used to invert hash functions and crack passwords [13–17]. Even though rainbow tables are ubiquitously used in the real world applications, Biryukov *et al.* show that Hellman tables are superior to rainbow tables in multiple data scenario [31].

### 3. Tradeoff attacks on stream ciphers

The main building blocks of (synchronous) stream ciphers are keystream generators. The most general design principle of keystream generators make use of a state update function  $\phi : GF(2)^s \rightarrow GF(2)^s$  and an output function  $g : GF(2)^s \rightarrow GF(2)^r$  producing  $r$ -bit output from each  $s$ -bit internal state. An internal state  $S_t$  is updated to the next internal state  $S_{t+1}$  via  $\phi$ . The initial internal state  $S_0$  is called the seed and produced from a key  $K$  and an initial vector  $IV$  through an initialization algorithm *InAlg*:

$$\begin{aligned} InAlg : GF(2)^n \times GF(2)^l &\rightarrow GF(2)^s \\ (K, IV) &\mapsto S_0. \end{aligned} \quad (3)$$

The objective of the attacks on stream ciphers is twofold in general. They aim at either recovering the key or an internal state. The same approach is adopted for tradeoff attacks. The state recovery attacks are conventional examples of the problem of inverting one-way function with data in a single key attack scenario. Indeed, it is enough to recover one of the internal states occurred during the encryption process.

Babbage [32] and Golić [33] independently introduce a natural way of recovering one of the internal states by using data. They define a one-way function by extending the output function which produces enough number of output bits by calling  $\phi$  and  $g$  certain number of times consecutively to identify the input state from its keystream piece uniquely. One can compute  $M$  pairs of the states and their outputs during the precomputation phase and save them as sorted with respect to the outputs. Then, it is highly probable to recover one of the states which produce  $D$  data when  $MD \geq 2^s$  during the online phase. The optimum point on the tradeoff curve  $MD = 2^s$  is  $M = D = 2^{s/2}$ . So,  $s/2$  is supposed to be larger than the key length to ensure that the Babbage-Golić attack is slower than the exhaustive search. This imposes a well known and highly adopted security criterion on stream ciphers: The internal state size must be at least twice as large as the key size. It was one of the main security requirements for the stream ciphers in both the NESSIE project [34] and the eSTREAM project [35, 36].

Another tradeoff attack on keystream generators using data is introduced by Biryukov and Shamir [1]. They propose to use Hellman tables to recover one of the internal states which produce  $D$  data. It is nothing but finding a preimage for one of the data. The optimum online complexity is achieved when only one Hellman table is constructed. So,  $mt^2 = 2^s$  and  $D = t$  with  $M = m, T = tD$ . Hence, we have the tradeoff curve given as  $M^2D^2T = 2^{2s}$  with the restriction  $D \leq \sqrt{T}$ . The optimum point on the curve is achieved when  $D^2 = T = M$  and this gives  $T = 2^{s/2}$ . Again, if  $s \geq 2n$  then the online phase of the Biryukov-Shamir attack will be slower than the exhaustive search, confirming the security criterion that the internal state size should be at least twice as large as the key size.

Both the Babbage-Golić attack and the Biryukov-Shamir attack aim at recovering one of the internal states. The online phases of these attacks are compared with the exhaustive search rather than the default tradeoff attacks. The attacks use multiple data since the one-way function they would like to invert has several outputs available. On the other hand, it is possible to define the one-way function as the function taking the  $n$ -bit main key as input and producing the keystream of  $n$ -bits for a chosen fixed  $IV$ . The internal state size has no significance for inverting this one-way function. So, we have the classical complexities  $T = M = 2^{2n/3}$ . However, we can not exploit the multiple data for this function. Therefore the Babbage-Golić attack and the Biryukov-Shamir attack are superior when the internal state size is too short. The tradeoff attacks on the GSM encryption algorithm A5/1 with its 64 bit internal state are mostly the applications of the Biryukov-Shamir attack [10–12].

Armknacht and Mikhalev examine the keyed update functions and show that the keystream generators with keyed state update functions are secure against conventional tradeoff attacks no matter how small the internal state sizes are [18]. They also introduce an example cipher they call Sprout [18]. A keyed state update function takes the main key as the second parameter of the input to produce the next internal state from the current internal state.

The cipher Sprout is analyzed intensively in a short while and some weaknesses are discovered [20, 22]. More interestingly, special tradeoff attacks are mounted [21, 23]. Then, Armknacht and Mikhalev present another keystream generator with keyed state update. They call it Plantlet [19]. This cipher also attains significant interests of cryptanalysts and several results are published including correlation attacks [24–26, 37, 38], some of them are even faster than exhaustive search [25]. It seems that it is indeed a challenging task for the crypto community to design keystream generators of small state sizes even if the tradeoff attacks are ignored in their security assessments.

#### 4. Tradeoff attacks on block ciphers

Let  $E : GF(2)^n \times GF(2)^m \rightarrow GF(2)^m$  be a block cipher of  $n$ -bit key and  $m$ -bit block size.  $E(K, P) = E_K(P)$  and  $E_K$  is a permutation for a fixed key  $K$ . We can define a one-way function  $f(x) = E(x, P_0) = E_x(P_0)$  for a chosen fixed plaintext  $P_0$ . Finding a preimage for a given ciphertext is nothing but finding a key candidate that encrypts the plaintext  $P_0$  to the given ciphertext.

It is possible to invert  $f(x)$  by using tradeoff tables. Hellman initially mounted the tradeoff attack on the block cipher DES in his original work [27]. The online time complexity is reduced to  $2^{2n/3}$ . But preparing the tables requires as many encryption calls as in the exhaustive search.

There is no known method of using multiple data to improve the tradeoff curve  $M^2T = 2^{2n}$  in the single key recovery setting for block ciphers yet. Choosing another plaintext will result in another one-way function to convert. So, using multiple data yields the following problem. Let  $f_1, \dots, f_D$  be  $D$  independent one-way functions of  $n$ -bit inputs and  $n$ -bit outputs. We call the problem of finding  $x$  as the problem of the *mutual inverting of multiple one-way functions* where

$$f_1(x) = y_1, f_2(x) = y_2, \dots, f_D(x) = y_D \quad (4)$$

and  $y_1, \dots, y_D$  are given.

Choosing  $D$  different plaintexts  $P_1, \dots, P_D$  for a block cipher  $E$  is an example of the problem of the mutual inverting of multiple one-way functions given as:  $f_1(x) = E_x(P_1), f_2(x) = E_x(P_2), \dots, f_D(x) = E_x(P_D)$ . Here  $x$  is the key and we have  $D$  chosen plaintexts encrypted with  $x$ . Then, finding  $x$  becomes a mutual inverting problem of multiple one-way functions.

The problem may further be generalized as inverting only one of the  $D$  independent one-way functions. Let

$$f_1(x_1) = y_1, f_2(x_2) = y_2, \dots, f_D(x_D) = y_D \quad (5)$$

be given for  $D$  independent one-way functions  $f_1, \dots, f_D$ . The goal is to find one of  $x_i$  for  $i = 1, \dots, D$ .

The problem of mutual inverting multiple one-way functions can be applied to stream ciphers also. Several one-way functions may be defined by choosing several IVs. Each IV determines a one-way function taking the key as the input and producing  $n$ -bit keystream. That is, each one-way function  $f_{IV} : GF(2)^n \rightarrow GF(2)^n$  is defined as

$$f_{IV}(K) = (z_1, \dots, z_n) \quad (6)$$

where  $K$  is an  $n$ -bit key and  $(z_1, \dots, z_n)$  is the first  $n$ -bit keystream segment produced by the pair  $(K, IV)$ . The function  $f_{IV}$  can be inverted by the conventional Hellman tables or rainbow tables. Finding preimage for one specific  $f_{IV}$  can be considered as the default tradeoff attack on stream ciphers and its online complexity is given as  $2^{2n/3}$ .

It may be still possible to use any number of IVs. For the single key attack scenario, the keystream generator is initialized by several different IVs and the corresponding  $n$ -bit keystream segments are produced. Then, the unknown inputs of the one-way functions will be mutual, namely the main key.

It seems that inverting only one specific one-way function once is not easier than the other two problems. One can use the algorithm of inverting a one-way function

to invert one of  $D$  one-way functions. So, an algorithm inverting a one-way function can be used to solve the problem of inverting at least one function among  $D$  one-way functions. Similarly, any algorithm inverting one of  $D$  one-way functions can straightforwardly be used to solve the mutual inverting problem.

It is not known yet if these three problems are of equal difficulty. It is an open problem if the mutual inverting problem is strictly easier than the problem of inverting one of the several one-way functions. It is also an open problem that inverting one of the several one-way functions is strictly easier than inverting only one one-way function. If there is an algorithm solving problem of mutual inverting problem but not solving the problem of inverting one-way function then the security levels and the key lengths for both block ciphers and stream ciphers must be assessed again. Because, the algorithms solving mutual inverting problems efficiently can be very powerful and serious attacks on symmetric ciphers.

## 5. Assessment of security criterion on state size

The online complexities of both the Babbage-Golić and the Biryukov-Shamir attacks are compared to the complexity of the exhaustive search and the security criterion on the state size of a stream cipher is imposed thereof. However, there is still a faster tradeoff attack even though the internal state size is larger than twice of the key size. It is possible to define a one-way function from a main key to its keystream piece of a stream cipher by choosing and fixing an  $IV$ . Then, one of the preimages of the keystream segment will be the main key. The attack complexity is derived from the key size rather than the internal state size. At the optimum point of the tradeoff curve, the online complexity is  $2^{2n/3}$  where  $n$  is the key length. This is the default Hellman or Oechslin tradeoff attacks and valid for block ciphers also. Note that the complexity is much smaller than  $2^n$ , the complexity of the exhaustive search.

Any tradeoff attack on symmetric ciphers should be compared with the default tradeoff attack with its complexity  $2^{2n/3}$ , instead of the exhaustive search. In this case, the strict criterion on the internal state size can be lightened, enabling to design ultra-lightweight stream ciphers. Indeed, a stream cipher of 128 bit key is required at least 256 bit internal state according to the conventional security criterion. If we assume one bit register is implemented by a flip flop of 6 GE (Gate Equivalent) area, we must allocate roughly 1.5 K GE only for the registers. This is why there is almost no stream cipher in the literature having a hardware implementation less than 1 K GE. However, there are several block cipher designs with hardware implementations less than 1 K GE such as Ktantan [9], PRINTCipher [39], SLIM [2] and LBlock [7].

Recall that we have the tradeoff curve  $MD = 2^s$  for the Babbage-Golić attack with the optimum point  $M = N = 2^{s/2}$  where  $s$  is the internal state size of a given stream cipher. The online time complexity is also equal to the data complexity. Then, we simply should consider the attack to be successful if  $2^{s/2} < 2^{2n/3}$ . Therefore, the internal state size must be at least  $4n/3$ . An attacker may prefer to choose much larger  $M$  on the curve  $MD = 2^s$ . For example, preparing a memory of  $M = 2^n$ , we have  $D = 2^{n/3}$  for the case  $s = 4n/3$ . However, it is possible to restrict the total number of the keystream bits produced per one key and force the users to change the key before completing encrypting the amount of  $2^{n/3}$  data.

Similarly, the optimum point of the tradeoff curve for the Biryukov-Shamir attack is  $D^2 = M = T = 2^{s/2}$  where  $M^2 D^2 T = 2^{2s}$ . Then, the attack will be slower than the default key recovery tradeoff attack if again  $2^{s/2} \geq 2^{2n/3}$ . Once more, we achieve the

same security bound that the minimum size for the internal state must be  $4n/3$ . If the precomputation phase is required to be not faster than the exhaustive search, then the amount of data encrypted per one key can be bounded above by  $2^{n/3}$ .

As a result, the tradeoff attacks aiming at the internal state recovery should be compared to the default tradeoff key recovery attack. Then, it is possible to loosen the restriction on the state size from  $2n$  to  $4n/3$ . This new criterion can enable novel designs of ultra-lightweight stream ciphers. However, stream ciphers with short internal states may be prone to several other attacks. The attacks on Plantlet and Sprout are the examples [20–26, 37, 38]. Therefore, it seems to be a fruitful challenge for the cryptography community to design secure stream ciphers having quite short internal states. On the other hand, the real world applications such as IoT devices, RFID tags or wireless sensors require ultra-lightweight stream ciphers for confidentiality.

## 6. Conclusions

We briefly introduce the tradeoff attacks on symmetric ciphers and initiate hopefully a fruitful discussion about how to assess the degree of precautions or countermeasure to be taken against these attacks.

The tradeoff attacks targeting at recovering one of the internal states producing a given keystream sequence are compared to the exhaustive search attack on the corresponding key used. However, a stream cipher key can be recovered much faster through the default tradeoff attack. Therefore, the internal state recovery tradeoff attacks should be compared to the default key recovery tradeoff attack. In this case, it is possible to loosen the bound for the countermeasure taken against state recovery tradeoff attacks.

The internal state size is supposed to be at least twice as large as the key size if the security threshold for tradeoff attacks is taken as the complexity of the exhaustive search. This is indeed a well known and worldwide adopted security criterion. We argue that it is indeed not necessary to allocate such large internal state just for the resistance against tradeoff attacks. The internal state size is enough to be at least  $4n/3$ -bits particularly for the lightweight applications where  $n$  is the key length. Besides, there are several other cryptanalytic techniques for internal state recovery that must be taken into account. It is an open problem how to design secure stream ciphers with short internal states. Such ciphers must be secure against other types of attacks such as divide-and-conquer attacks, guess and determine attacks or correlation attacks. It is interesting to study this generic problem.

We believe that it is a challenging task to design small stream ciphers and the industry requires such ciphers to use in lightweight applications such as IoT devices, wireless sensors or RFID tags.

## Acknowledgements

We would like to thank Mehmet Sabır Kiraz, Ali Aydın Selçuk and Sırrı Erdem Ulusoy for their helpful comments. We also would like to thank IntechOpen LIMITED for the grant.

## Conflict of interest

The authors declare no conflict of interest.

## **Author details**

Orhun Kara

Department of Mathematics, Faculty of Science, IZTECH Izmir Institute of Technology, Urla, Izmir, Turkey

\*Address all correspondence to: [orhunkara@iyte.edu.tr](mailto:orhunkara@iyte.edu.tr)

## **IntechOpen**

---

© 2021 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

## References

- [1] A. Biryukov and A. Shamir, “Cryptanalytic time/memory/data tradeoffs for stream ciphers,” in *Advances in Cryptology - ASIACRYPT 2000*, vol. 1976 of *LNCS*, pp. 1–13, Springer, 2000.
- [2] B. Aboushosha, R. A. Ramadan, A. D. Dwivedi, A. El-Sayed, and M. M. Dessouky, “SLIM: A lightweight block cipher for internet of health things,” *IEEE Access*, vol. 8, pp. 203747–203757, 2020.
- [3] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai, “Piccolo: An ultra-lightweight blockcipher,” in *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28–October 1, 2011. Proceedings* (B. Preneel and T. Takagi, eds.), vol. 6917 of *Lecture Notes in Computer Science*, pp. 342–357, Springer, 2011.
- [4] L. Li, B. Liu, and H. Wang, “QTL: A new ultra-lightweight block cipher,” *Microprocess. Microsystems*, vol. 45, pp. 45–55, 2016.
- [5] Z. Gong, S. Nikova, and Y. W. Law, “KLEIN: A new family of lightweight block ciphers,” in *RFID. Security and Privacy - 7th International Workshop, RFIDSec 2011, Amherst, USA, June 26–28, 2011, Revised Selected Papers* (A. Juels and C. Paar, eds.), vol. 7055 of *Lecture Notes in Computer Science*, pp. 1–18, Springer, 2011.
- [6] H. AlKhzaimi and M. M. Lauridsen, “Cryptanalysis of the SIMON family of block ciphers,” *IACR Cryptol. ePrint Arch.*, vol. 2013, p. 543, 2013.
- [7] W. Wu and L. Zhang, “Lblock: A lightweight block cipher,” in *Applied Cryptography and Network Security - 9th International Conference, ACNS 2011, Nerja, Spain, June 7–10, 2011. Proceedings* (J. López and G. Tsudik, eds.), vol. 6715 of *Lecture Notes in Computer Science*, pp. 327–344, 2011.
- [8] J. Guo, T. Peyrin, A. Poschmann, and M. J. B. Robshaw, “The LED block cipher,” in *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28–October 1, 2011. Proceedings* (B. Preneel and T. Takagi, eds.), vol. 6917 of *Lecture Notes in Computer Science*, pp. 326–341, Springer, 2011.
- [9] C. D. Cannière, O. Dunkelman, and M. Knezevic, “KATAN and KTANTAN - A family of small and efficient hardware-oriented block ciphers,” in *Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop, Lausanne, Switzerland, September 6–9, 2009, Proceedings* (C. Clavier and K. Gaj, eds.), vol. 5747 of *Lecture Notes in Computer Science*, pp. 272–288, Springer, 2009.
- [10] M. Kalenderi, D. N. Pnevmatikatos, I. Papaefstathiou, and C. Manifavas, “Breaking the GSM A5/1 cryptography algorithm with rainbow tables and high-end FPGAs,” in *22nd International Conference on Field Programmable Logic and Applications (FPL), Oslo, Norway, August 29–31, 2012* (D. Koch, S. Singh, and J. Tørresen, eds.), pp. 747–753, IEEE, 2012.
- [11] P. Papantonakis, D. N. Pnevmatikatos, I. Papaefstathiou, and C. Manifavas, “Fast, fpga-based rainbow table creation for attacking encrypted mobile communications,” in *23rd International Conference on Field programmable Logic and Applications, FPL 2013, Porto, Portugal, September 2–4, 2013*, pp. 1–6, IEEE, 2013.
- [12] Z. Li, “Optimization of rainbow tables for practically cracking GSM A5/1 based on validated success rate modeling,” in *Topics in Cryptology -*

- CT-RSA 2016 - *The Cryptographers' Track at the RSA Conference 2016, San Francisco, CA, USA, February 29–March 4, 2016, Proceedings* (K. Sako, ed.), vol. 9610 of *Lecture Notes in Computer Science*, pp. 359–377, Springer, 2016.
- [13] J. Bieniasz, K. Skowron, M. Trzepak, M. Rawski, P. Sapięcha, and P. Tomaszewicz, “Hardware implementation of rainbow tables generation for hash function cryptanalysis,” in *Information Systems Architecture and Technology: Proceedings of 36th International Conference on Information Systems Architecture and Technology - ISAT 2015 - Part II, Karpacz, Poland, September 20–22, 2015* (A. Grzech, L. Borzowski, J. Swiatek, and Z. Wilimowska, eds.), vol. 430 of *Advances in Intelligent Systems and Computing*, pp. 189–200, Springer, 2015.
- [14] G. Avoine, A. Bourgeois, and X. Carpent, “Analysis of rainbow tables with fingerprints,” in *Information Security and Privacy - 20th Australasian Conference, ACISP 2015, Brisbane, QLD, Australia, June 29–July 1, 2015, Proceedings* (E. Foo and D. Stebila, eds.), vol. 9144 of *Lecture Notes in Computer Science*, pp. 356–374, Springer, 2015.
- [15] J. Horalek, F. Holík, O. Horák, L. Petr, and V. Sobeslav, “Analysis of the use of rainbow tables to break hash,” *J. Intell. Fuzzy Syst.*, vol. 32, no. 2, pp. 1523–1534, 2017.
- [16] H. Ying and N. Kunihiro, “Decryption of frequent password hashes in rainbow tables,” in *Fourth International Symposium on Computing and Networking, CANDAR 2016, Hiroshima, Japan, November 22–25, 2016*, pp. 655–661, IEEE Computer Society, 2016.
- [17] G. Avoine, X. Carpent, and C. Lauradoux, “Interleaving cryptanalytic time-memory trade-offs on non-uniform distributions,” in *Computer Security - ESORICS 2015 - 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21–25, 2015, Proceedings, Part I* (G. Pernul, P. Y. A. Ryan, and E. R. Weippl, eds.), vol. 9326 of *Lecture Notes in Computer Science*, pp. 165–184, Springer, 2015.
- [18] F. Armknecht and V. Mikhalev, “On lightweight stream ciphers with shorter internal states,” in *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8–11, 2015, Revised Selected Papers* (G. Leander, ed.), vol. 9054 of *Lecture Notes in Computer Science*, pp. 451–470, Springer, 2015.
- [19] V. Mikhalev, F. Armknecht, and C. Müller, “On ciphers that continuously access the non-volatile key,” *IACR Trans. Symmetric Cryptol.*, vol. 2016, no. 2, pp. 52–79, 2016.
- [20] V. Lallemand and M. Naya-Plasencia, “Cryptanalysis of full sprout,” in *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16–20, 2015, Proceedings, Part I* (R. Gennaro and M. Robshaw, eds.), vol. 9215 of *Lecture Notes in Computer Science*, pp. 663–682, Springer, 2015.
- [21] B. Zhang and X. Gong, “Another tradeoff attack on sprout-like stream ciphers,” in *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29–December 3, 2015, Proceedings, Part II* (T. Iwata and J. H. Cheon, eds.), vol. 9453 of *Lecture Notes in Computer Science*, pp. 561–585, Springer, 2015.
- [22] S. Maitra, S. Sarkar, A. Baksi, and P. Dey, “Key recovery from state information of sprout: Application to cryptanalysis and fault attack,” *IACR Cryptol. ePrint Arch.*, vol. 2015, p. 236, 2015.



- [23] M. F. Esgin and O. Kara, "Practical cryptanalysis of full sprout with TMD tradeoff attacks," in *Selected Areas in Cryptography - SAC 2015 - 22nd International Conference, Sackville, NB, Canada, August 12–14, 2015, Revised Selected Papers* (O. Dunkelman and L. Keliher, eds.), vol. 9566 of *Lecture Notes in Computer Science*, pp. 67–85, Springer, 2015.
- [24] O. Kara and M. F. Esgin, "On analysis of lightweight stream ciphers with keyed update," *IEEE Trans. Computers*, vol. 68, no. 1, pp. 99–110, 2019.
- [25] S. Banik, K. Barooti, and T. Isobe, "Cryptanalysis of plantlet," *IACR Trans. Symmetric Cryptol.*, vol. 2019, no. 3, pp. 103–120, 2019.
- [26] Y. Todo, W. Meier, and K. Aoki, "On the data limitation of small-state stream ciphers: Correlation attacks on fruit-80 and plantlet," in *Selected Areas in Cryptography - SAC 2019 - 26th International Conference, Waterloo, ON, Canada, August 12–16, 2019, Revised Selected Papers* (K. G. Paterson and D. Stebila, eds.), vol. 11959 of *Lecture Notes in Computer Science*, pp. 365–392, Springer, 2019.
- [27] M. E. Hellman, "A cryptanalytic time-memory trade-off," *IEEE Transactions on Information Theory*, vol. 26, no. 4, pp. 401–406, 1980.
- [28] G. Avoine, P. Junod, and P. Oechslin, "Characterization and improvement of time-memory trade-off based on perfect tables," *ACM Trans. Inf. Syst. Secur.*, vol. 11, no. 4, pp. 17:1–17:22, 2008.
- [29] P. Oechslin, "Making a faster cryptanalytic time-memory trade-off," in *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17–21, 2003, Proceedings* (D. Boneh, ed.), vol. 2729 of *Lecture Notes in Computer Science*, pp. 617–630, Springer, 2003.
- [30] E. Barkan, E. Biham, and A. Shamir, "Rigorous bounds on cryptanalytic time/memory tradeoffs," in *Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20–24, 2006, Proceedings* (C. Dwork, ed.), vol. 4117 of *Lecture Notes in Computer Science*, pp. 1–21, Springer, 2006.
- [31] A. Biryukov, S. Mukhopadhyay, and P. Sarkar, "Improved time-memory trade-offs with multiple data," in *Selected Areas in Cryptography, 12th International Workshop, SAC 2005, Kingston, ON, Canada, August 11–12, 2005, Revised Selected Papers* (B. Preneel and S. E. Tavares, eds.), vol. 3897 of *Lecture Notes in Computer Science*, pp. 110–127, Springer, 2005.
- [32] S. Babbage, "Improved exhaustive search attacks on stream ciphers." Security and Detection 1995, European Convention IET, 1995.
- [33] J. D. Golić, "Cryptanalysis of alleged A5 stream cipher," in *EUROCRYPT '97*, vol. 1233 of *LNCS*, pp. 239–255, Springer, 1997.
- [34] B. Preneel, *NESSIE Project*, pp. 408–413. Boston, MA: Springer US, 2005.
- [35] M. Robshaw, "The estream project," in *New Stream Cipher Designs - The eSTREAM Finalists* (M. J. B. Robshaw and O. Billet, eds.), vol. 4986 of *Lecture Notes in Computer Science*, pp. 1–6, Springer, 2008.
- [36] V. Rijmen, "Stream ciphers and the estream project," *ISC Int. J. Inf. Secur.*, vol. 2, no. 1, pp. 3–11, 2010.
- [37] J. Copeland and L. Simpson, "Finding slid pairs for the plantlet stream cipher," in *Proceedings of the Australasian Computer Science Week*,

*ACSW 2020, Melbourne, VIC, Australia, February 3–7, 2020* (P. P. Jayaraman, D. Georgakopoulos, T. K. Sellis, and A. Forkan, eds.), pp. 7:1–7:7, ACM, 2020.

[38] S. Wang, M. Liu, D. Lin, and L. Ma, “Fast correlation attacks on grain-like small state stream ciphers and cryptanalysis of plantlet, fruit-v2 and fruit-80,” *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 763, 2019.

[39] M. J. Mihaljević, S. Gangopadhyay, G. Paul, and H. Imai, “Generic cryptographic weakness of  $k$ -normal boolean functions in certain stream ciphers and cryptanalysis of Grain-128,” *Periodica Mathematica Hungarica*, vol. 65, no. 2, pp. 205–227, 2012.



```
operation == "MIRROR_Y":  
mirror_mod.use_x = False  
mirror_mod.use_y = True  
mirror_mod.use_z = False  
if operation == "MIRROR_Z":  
mirror_mod.use_x = False
```

*Edited by Riccardo Bernardini*

Despite being 2000 years old, cryptography is still a very active field of research. New needs and application fields, like privacy, the Internet of Things (IoT), physically unclonable functions (PUFs), post-quantum cryptography, and quantum key distribution, will keep fueling the work in this field. This book discusses quantum cryptography, lightweight cryptography for IoT, PUFs, cryptanalysis, and more. It provides a snapshot of some recent research results in the field, providing readers with some useful tools and stimulating new ideas and applications for future investigation.

Published in London, UK

© 2021 IntechOpen  
© monsitj / iStock

**IntechOpen**

