UNIVERSITÉ DU BURUNDI
GRENIER DU SAVOIR DU BURUNDI
Dépôt institutionnel officiel
https://repository.ub.edu.bi

Post-Quantum Cryptography Based on Computational Assumption Securing Against Quantum Computer : Case of Random Number and Key Generation

Ndagijimana, Protais

2024
UB, Ecole doctorale
https://repository.ub.edu.bi/handle/123456789/1014

Document téléchargé depuis le **Grenier du Savoir du Burundi** — https://repository.ub.edu.bi



UNIVERSITY OF BURUNDI
Doctoral School

PhD thesis submitted to the Doctoral school-University of Burundi
in partial fulfillment of the requirements for the degree of Doctor of Science
Option: Information and Communication Technology
Speciality: Information Systems Security

By

Protais Ndagijimana

Post-Quantum Cryptography Based on Computational Assumption Securing Against Quantum Computer: Case of Random Number and Key Generation

Thesis defended publically, March 04, 2024, in front of the
Jury:

Prof. Jérémie NDIKUMAGENGE, University of Burundi (President)
Dr. Roméo NIBITANGA, University of Burundi (Repporter)
Dr. Michèle MUKESHIMANA, University of Burundi (Member)
Prof. Juma SHABANI, University of Burundi (Co-supervisor)
Prof. Fulgence NAHAYO, University of Burundi (Co-supervisor)
Prof. M. Kokou ASSOGBA, EPAC of Abomey-calavi, Benin (Co-supervisor)
Prof. Vincent HAVYARIMANA, ENS, Burundi (Member)

Bujumbura, February 2024

Dedicate

To all those who fight for scientific research and human dignity,

To my lovely wife KIBUGA Asha,

To all my family and friends.

I dedicate this thesis !

Protais Ndagijimana © Doctoral school - University of Burundi

Acknowledgements

Grateful acknowledgement to my Supervisors distinguished Professor Juma SHABANI Director of Doctoral School of University of Burundi, Professor Fulgence NAHAYO Director of Agence Universitaire de la Francopfonie "AUF-Burundi" and founder member of LURMISTA-ISTA as research center, Professor Marc Kokou ASSOGBA from Abomey-calavi University of Benin, Professor Vincent HAVYARIMANA from Ecole Normale Superieure "ENS" member of suport committee and to all the members of the Jury of this thesis for their availability, recommendations, advices and encouragement that helped me to achieve the outcome of this research work. My gratitude to Prof. Peter A. Okebukola of Lagos State University for his facilitation through different courses and platforms. Many thanks to the Doctoral School of University of Burundi for giving me the admission and support to well conduct this research. Special thanks to the General Direction of Ecole Nationale d'Administration "ENA" for authorizing me to follow this doctoral research. Sincere gratitude to the autorities of the Institut Superieur de Mathématiques et de Sciences Physiques of Univerisity of Abomey-Calavi "IMSP-UAC" of Benin who accepted me to conduct the research to their Laboratory without forgetting lecturers and experts in department of computer sciences at IMSP for their guidance during my research mobility. I shall not forget to thank la Direction régionale Afrique centrale et Grands Lacs de l'Agence Universitaire de la Francopfonie "AUF" for the research mobilities financial support in specialised Laboratories of different countries.

Protais Ndagijimana © Doctoral school - University of Burundi

Abstract

The emergence of practical Quantum computers poses a significant threat to the most popular public key cryptographic schemes in current use. This would seriously compromise the confidentiality and integrity of digital communications on the internet and elsewhere. Quantum technologies will revolutionize computation, communication, and sensing, including the way information is secured. Unlike traditional classic cryptography which employs various mathematical techniques to restrict eavesdroppers from learning the contents of encrypted message, Quantum cryptography is focused on the physic of information. Thus, the implementation of new cryptographic primitives is essential. They must follow the breakthroughs and properties of quantum calculators which make vulnerable existing cryptosystems. In this work, we described the evolution of cryptography and the theory related to computational performance and predictive modeling of quantum computers to improve the life of new quantum universe. We proposed a random number generation model based on evaluation of the thermal noise power of the given number of volume elements of an electronic or embedded system. We proved, through the sampling of the temperature of each volume, that it is very difficult for an attacker to carry out an exploit. We generated a stream of key that will be used to encrypt and decrypt messages.

Keywords: Quantum computer, Post-quantum cryptography, True random number generation, volume element, key and algorithm.

Protais Ndagijimana © Doctoral school - University of Burundi

Resumé

L'émergence d'ordinateurs quantiques fonctionnels constitue une ménace importante pour les systèmes cryptographiques à clé publique les plus populaires et actuellement utilisés. Cela compromettrait gravement la confidentialité et l'intégrité des communications numériques sur l'internet et ailleurs. Les technologies quantiques vont révolutionner les methodes de calcul, la communication et la sensibilité y compris la manière dont l'information est sécurisée. Contrairement à la cryptographie classique qui utilise diverses techniques mathématiques pour empêcher les espions de découvrir le contenu d'un message crypté, la cryptographie quantique est axée sur la qualité physique de l'information. La cryptographie quantique, en tant que branche de la physique et de la cryptologie, elle utilise des corrélations de phénomènes quantiques pour protéger la distribution de la clé cryptographique. Ainsi, la mise en oeuvre de nouvelles primitives cryptographiques est essentielle. Dans ce travail, nous avons décri l'évolution de la cryptographie et la théorie liée aux performances de calcul et à la modélisation prédictive des ordinateurs quantiques pour contribuer à la compréhension en rapport avec l'existance de l'univers quantique. Nous avons proposé un modèle de génération de nombre aléatoire basé sur l'évaluation de la puissance du bruit thermique des éléments de volume d'un système électronique ou système ambarqué proposé qui est Arduino Uno ATMega 328p en lui déployant des capteurs de temperature de type LM 35. Nous avons prouvé par échantillonnage de la température de chaque élément volume qu'il est tellement difficile pour un attaquant de réaliser un exploit. Nous avons finalement généré un flux de clé qui sera utilisé pour chiffrer et déchiffer les messages.

Mots clés: Ordinateur Quantique, Cryptographie Post-Quantique, Génération des nombres aléatoires, système ambarqué,élément de volume, clé et algorithme.

Protais Ndagijimana © Doctoral school - University of Burundi

Contents

Dedicate i

Acknowledgements ii

Abstract iii

Resumé iv

List of Abbreviations viii

List of Figures x

List of Tables xi

List of published papers related to this thesis xii

Declaration xiii

1 General Introduction 2

1.1 Introduction 2

1.2 Definitions and Terminologies 5

1.2.1 Definitions 5

1.2.2 Important Therminologies 6

1.3 Cryptographic Goals 7

1.4 Evolution of Cryptography 9

1.5 Current status of cryptography 11

1.6 Research objectives 13

Protais Ndagijimana © Doctoral school - University of Burundi

1.6.1 General objective 13
1.6.2 Specific objectives 13
1.7 Motivation for this work 13
1.8 Research problem statement 14
1.9 Research thesis Outline 14

2 Theoretical Backgroung and Related work 16
2.1 Introduction 16
2.2 Classical and Quantum Computers 18
2.3 Overview of Cryptography 21
2.4 Quantum Cryptography development 26
2.5 Post-Quantum Cryptography 28
2.5.1 Code-based cryptography 29
2.5.2 Hash-based cryptography 30
2.5.3 Multivariate cryptography 31
2.5.4 Lattice-based cryptography 32
2.5.5 Supersingular elliptic curve isogenies Cryptography 33
2.6 Time complexity and algoritms 34
2.6.1 Advanced Encryption Standard(AES) 37
2.6.2 Diffie-Hellman (DH) Algorithm 37
2.6.3 The RSA Scheme 38
2.7 Impact on quantum computing and modern Communication 41
2.7.1 Impact on quantum computing 41
2.7.2 Impact on modern communication 42

3 Innovative Predictive Quantum Computer Modeling 43
3.1 Introduction 43
3.2 Principles of Quantum Computing 46
3.3 Development of Quantum Computing 49
3.3.1 Initial ideas 50
3.3.2 Advantages and disadvantages of Quantum computing 51

3.4 Quantum Computer prototype Modeling 53
3.4.1 Qubits modeling 55
3.4.2 Qubit Logic Gates 57
3.4.3 Extraction of information from quantum states 57
3.5 Large scale Computer Prototype 58
3.6 Quantum Computer Efficiency proof 60
3.7 $\mathcal{R}2022\mathcal{A}^{+}$ Algorithm 62

4 Random Number and Key Generation 65
4.1 Introduction 65
4.2 The evolution of random number generation 67
4.2.1 True Random Number Generator 68
4.2.2 Pseudo-random Number Generator 72
4.3 Architecture of proposed mechanism 73
4.3.1 Logical structure 74
4.3.2 Security proof 77
4.4 Description of experimental environment 78
4.5 Results analysis and discussion 80

Research Contribution 84

5 Conclusion and Perspectives 89
5.1 General context 89
5.2 Achieved Results Briefings 90
5.3 Challenges and Perspectives 92

A Appendix 95

List of Abreviations

AES	Advanced Encryption Standard
AI	Artificial Intelligence
ATM	Automated Teller Machines
B.C	Before Christ
BB84	Bennet and Brassard(1984)
BIT	Binary Digit
CRYPTREC	Cryptography Research and Evaluation Commities
DES	Data Encryption Standard
DH	Diffie Hellman
DPS	Differential-phase-Shift
DSP	Digital Signal Processing
V-QKD	Discrete-Variable Quantum-Key-Distribution
EB	Entanglement-based
ECC	Elliptic Curve Cryptography
FIPS	Federation Information Processing Standard
FIRO	Fibonacci Ring Oscillator
GARO	Galois Ring Oscillator
HSM	Hardware Security model
I/O	Input/Output
IBC	Identity-based Cryptography
IBM	International Business Machine Corporation
ICT	Information and Communication Technology
IETF	Internet Engineering Task Force

Protais Ndagijimana © Doctoral school - University of Burundi

IoT	Internet of Things
ITSI	Internet Technology Service Intelligence
LO	Local Oscillator
MQ	Multivariate Quadratic
NIST	National Institute of Standars and Technology
NMR	Nuclear Magnetic Resonance
NP	Nondeterministic Polynomial
OQS	Open Quantum Safe
OTP	One-Time-Pad
PKC	Public-Key Cryptography
PKI	Public Key Infrastructure
PMD	Polarization Mode Dispersion
PQC	Post-Quantum Cryptography
PRNG	Pseudo random number generation
QC	Quantum Computer
QKD	Quantum Key Distribution
QLG	Quantum Logic Gate
QRA	Quantum-Resistant Algorithm
QSDC	Quantum Secure Direct Communication
QUBIT	Quantum Bit
RNG	Random Number Generation
RSA	Rivest,Shamir and Adleman
SSL	Secure Socket Layer
SSP	Six-state protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TRNG	True Random Number Generation
WDM	Wavelength-Division-Multiplexing

Protais Ndagijimana © Doctoral school - University of Burundi

List of Figures

1.1 Enigma machine, used by the German military sending secret codes during World War II. 10

2.1 A classical and quantum computer side by side 20
2.2 The entire alphabet shifted by three spaces. 24
2.3 Program implementation of Caesar cipher algorithm. 25
2.4 Caesar cipher output. 25
2.5 Example for error correction on an unreliable channel. 30
2.6 Example for lattice-based encryption in a two-dimensional lattice. . . . 33

3.1 Graphical representation of BITs alongside QUBITs. 54
3.2 Atoms. 56
3.3 Book searching from Library via q-Oracle. 61

4.1 Classification of random number generators 67
4.2 Volume elements. 78
4.3 Variation of temperature depending on volume elements. 81
4.4 Sampling the temperature for each volume element. 82
4.5 Variation of temperature depending on the power of thermal noise. . . 82

A.1 Illustration of a QKD-based cryptographic scheme. 98
A.2 The key exchange in the BB84 protocol implemented with the polarization of photons. 104
A.3 Illustration of five stages in the BB84 protocol. 106

Protais Ndagijimana © Doctoral school - University of Burundi

List of Tables

2.1 Tabula Recta 22

2.2 Vigenère example 23

3.1 Comparison between Quantum and Classical Computer 55

4.1 Comparative study of the mechanisms leading to true random numbers generation. 71

4.2 Power computation experment. 79

4.3 Integer/decimal parts retrieval. 79

4.4 Number of digits counted per volume element. 80

A.1 Polarization Basis and Encoding rule in the 4-state BB84 protocol. . . 103

A.2 Sample of grouped BB84 protocol with presence of Eve. 105

Protais Ndagijimana © Doctoral school - University of Burundi

List of published papers related to this thesis

This thesis is concerned with the study of protecting data during their transmission from a side to an other by cryptographic method particulary the mechanism for random number generation which can resist to attackers with quantum computer. The following are Published papers:

1) Ndagijimana P., Nahayo F., Assogba M.K., Ametepe A.F.-X. and Shabani J. (2020) "Towards Post-Quantum Cryptography Using Thermal Noise Theory and True Random Numbers Generation". Journal of Information Security , 11,149-160. https://doi.org/10.4236/jis.2020.113010

2) P. Ndagijimana , F. Nahayo , J. Shabani , M. Kokou Assogba and V. Havyarimana (2023)"An Innovative Predictive Quantum Computer Modeling;The Power of $\mathcal{R}2022\mathcal{A}^{+}$ Cryptography Technology". Contemporary Engineering Sciences, Vol. 16, 2023, no. 1, 43 - 54 HIKARI Ltd, www.m-hikari.com. https://doi.org/10.12988/ces.2023.93065

Protais Ndagijimana © Doctoral school - University of Burundi

Declaration

The content of this research thesis titled *"Post-Quantum Cryptography Based on Computational Assumption Securing Against Quantum Computer; Case of Random Number and Key Generation"* submitted in partial fulfillment of the requirements for the award of the degree of Doctor of Philosophy in Science is a record of original work, and any work done by others or by myself previously has been acknowledged and referenced accordingly !

Protais Ndagijimana © Doctoral school - University of Burundi

Chapter One

General Introduction

Contents

1.1 Introduction 2
1.2 Definitions and Terminologies 5
1.3 Cryptographic Goals 7
1.4 Evolution of Cryptography 9
1.5 Current status of cryptography 11
1.6 Research objectives 13
1.7 Motivation for this work 13
1.8 Research problem statement 14
1.9 Research thesis Outline 14

1.1 Introduction

Before the modern era[1], cryptography was used only to ensure secrecy in communications, i.e., to enable two people to communicate over an insecure channel so that any third party can neither understand nor change the message. The main idea is to modify the message such that nobody apart from the sender and receiver can understand its meaning; we call this new message the ciphertext. Nowadays, cryptography is the cornerstone[2] in data security and is used for many purposes: secrecy of data, anonymity ensuring, the authenticity of communications, digital signatures, etc[1]. Some examples of daily use of cryptography are the electronic commerce, e-banking, e-Learning,

[1]The period of human history that succeeds the Middle Ages.

[2]Cryptography is the foundation in data security.

Protais Ndagijimana © Doctoral school - University of Burundi

automated teller machine or ATM cards, Artificial Intelligence "AI", Internet of Things "IoT", computer password, etc. Cryptography is mainly divided in two types: symmetric cryptography and asymmetric or public-key cryptography. Let us assume that Alice wants to send a message to Bob through an insecure channel. In cymmetric case, Alice and Bob agree on a secret key. This key is used in the encryption and the decryption process. In the asymmetric case, there exist two different keys: the public key, used in the encryption process, and the secret key used to decrypt the ciphertext. Bob is the only one who is able to find the original message, since he is the only one who knows the secret key. In a public-key cryptosystem "PKC" we need a function that is easy to compute in one way, anybody can encrypt the message, and that is hard to invert unless we have an additional information called a trapdoor[3]. These functions are called trapdoor one-way functions.
Nowadays, many strong, and standardized public key encryption schemes are available. Nevertheless, the security of the public-key cryptosystems used in practice depend dangerously on only the two following problems:

a) The factoring problem: Given $n = pq$, where p and q are different primes, find p and q. This is a hard problem.

b) The discrete logarithm problem: Given α, m and $\beta = \alpha$ a mod m, find a. This is a hard problem if the involved numbers are large.

Today the Advanced Encryption Standard "AES", based on an algorithm called Rijndael, is the standard for symmetric encryption [2], while Elliptical curve cryptography "ECC" and "RSA" proposed by Rivest, Shamir and Adleman in 1977, are among the most popular approaches to asymmetric encryption for data transmission and digital certificates. In both cases one has to be careful with the choice of the values since there are some ease cases. Peter Shor "1994" found a polynomial-time [4] algorithm [3] which

[3]In theoretical computer science and cryptography, a trapdoor function is a function that is easy to compute in one direction, yet difficult to compute in the opposite direction without special information.

[4]In theoretical computer science, the time complexity is the computational complexity that describes the amount of computer time it takes to run an algorithm.An algorithm is said to be of

solves these two problems using quantum computers. Therefore, public key cryptosystems based on these problems would be broken as soon as quantum computers of an appropriate size could be built. The public key cryptosystems that remain secure even when the adversary has access to a quantum computer are called Quantum Resistant[5] or post-quantum cryptosystems.

Grover's algorithm [4], is another quantum algorithm that may lead to some attacks, but it is not too dangerous since cryptographers can avoid the attack by a simple change of parameters it means that the algorithm has exponential complexity. However, according to security proof, the safety of post-quantum cryptography based on Euclidean networks, errors correction, multivariate polynomial, isogeny and hash function will be compromised if a powerful enough quantum computer is implemented.

The main contribution in this thesis consist of describing the evolution of cryptography and the theory related to computationnal performance, efficiency, prototype and predictive modeling of a quantum computer. It consist also of proposing a random number generation model based on evaluation of the thermal noise power of different volume elements of a given electronic system, this fundamentals of thermal noise theory is a random phenomenon.

For tests and experiments, we used an Arduino Uno ATMega 328p microcontroller as a solid space that generated volume elements. We sampled the temperature from those volume elements to determine the power of thermal noise for each of them. Thus, we have obtained for seven volume elements, a serie of random numbers which, after its conversion into binary system, represented the cryptographic key.

The analysis proved the difficulty for an attacker to sample the same temperature from each volume element and to determine the generated sequence numbers from the volumes and it was then very complicated for an attacker to carry out an exploit.

polynomial time "space" complexity if its time "space" complexity function $f(n)$ satisfies $f(n) \leqslant p(n)$ for some polynomial p.

[5]Quantum resistance refers to algorithms that withstand code-breaking efforts from quantum computers.

1.2 Definitions and Terminologies

According to this research fied , the terms have just the related meaning except that here, definition means a statement of the meaning of a term "a word, phrase, or other set of symbols". Definitions can be classified into two large categories, intensional definitions which try to give the sense of a term and extensional definitions which try to list the objects that a term describes; while terminology is a general word for the group of specialized words or meanings relating to a particular field, and also the study of such terms and their use. This is also known, in cryptography, as terminology science.

1.2.1 Definitions

The term *cryptography* usually refers to the study of designing cryptosystems, while *cryptanalysis* refers to the science of breaking them. *Cryptology* is the name given to the field which includes both cryptography and cryptanalysis. In this work, however, we adhered to the common practice of using the term cryptography to mean cryptology. *Quantum cryptography*, on the other hand, is the actual use of quantum technology to protect messages. The term *post-quantum cryptography* refers generally to cryptographic algorithms that are believed to be secure against attacks by quantum computers. A *quantum computer* is a computer that takes advantage of the quantum properties of Quantum Bits(Qubits) to perform certain types of calculation extremely quickly compared to conventional or classical computers while *cyber-attack* is any type of offensive action that targets computer information systems, it would have the power to unlock encryption algorithms and expose protected data. A *Qubit*, short for quantum bit, is the basic unit of information in quantum computing and counterpart to the *Bit*, short for binary digit, in classical computing. A qubit plays a similar role as a bit, in terms of storing information, but it behaves much differently because of the quantum properties on which it's based. To define key terms related to security in quantum and post-quantum cryptography is important when we want to well understand the existing cryptographic issues in the post-quantum era. An *algorithm* is a set

of commands that must be followed for a computer to perform calculations or other problem-solving operations.According to its formal definition, an algorithm is a finite set of instructions carried out in a specific order to perform a particular task.

1.2.2 Important Therminologies

Cryptography comes from Greek words "kryptos" meaning "Secret" and "graphein" meaning "writing", so cryptography is known as the art/science of secret writing. The modern day cryptography uses the following terminologies:

a) Encryption: The process of encoding the message with help of key is called *encryption*. In this the simple text is converted into unreadable text;

b) Decryption: The process of decoding the encoded message with the help of key is called *decryption*: It is the reverse of encryption process;

c) Plaintex: The message or data which need to be secured for various reasons is called *plaintext*;

d) Ciphertext: The unreadable form of data which is produced at the end of encryption process is called *ciphertext*;

e) Communication channel: Device that conveys a digital bit stream, from: one or several senders to one or several receivers;

f) Key: It is a parameter that determines what will be the final output of a cryptographic process. The key length plays a significant role in encryption process; As long as the communication needs to remain secret, the key must remain secret. Encryption and decryption with a symmetric algorithm are denoted by:

$$E_k(M) = C \; and \; D_k(C) = M \tag{1.1}$$

with:
$E = encryption$, $M = message(plaintext)$, $C = ciphertext$, $D = decryption$, $k = key$

g) Key establishment: Before any communication, both the sender and the receiver need to agree on a secret key. It requires a secure key establishment mechanism in place;

h) Trust Issue: Since the sender and the receiver use the same key, there is an implicit requirement that the sender and the receiver "trust" each other. For example, it may happen that the receiver has lost the key to an attacker and the sender is not informed; These last two challenges are highly restraining for modern day communication. Today, people need to exchange information with non-familiar and non-trusted parties. For example, a communication between online seller and customer;

i) Network protocol: Set of rules for formatting data so that all connected devices can process it.

1.3 Cryptographic Goals

Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. The various goals of Cryptography are:

1. Confidentiality: To ensure that no one other than the receiver is able to read the message. This is also known as privacy or secrecy.

2. Data integrity: Making assure that the message received by the receiver is not manipulated, it means the message is not altered and is in its original form.

3. Authentication: It is process related to user's identification. It is really important that the two parties "sender and receiver" engaged in communication should

identify each other.

4. Non-repudiation: It is a mechanism to check or prove that the message received by the receiver is really send by the sender itself.

In the 19^{th} century, a Dutch cryptographer A. Kerckhoff furnished the requirements of a good cryptosystem. Kerckhoff stated that a cryptographic system should be secure even if everything about the system, except the key, is public knowledge. The design principles defined by Kerckhoff for cryptosystem are:

a. Encryption and decryption transformation must be efficient for all keys;

b. The system must be easy to use;

c. The key should be easily communicable, memorable, and changeable;

d. The security of the system must depend only on the secrecy of the key and not on the secrecy of the algorithm E or D;

e. It should be computationally infeasible for a cryptanalyst to determine the deciphering transformation D_k from intercepted ciphertext C , even if the corresponding plaintext M is known.

In modern era, Kerckhoff principles became essential guidelines for designing algorithms in modern cryptography.
In cryptography, we start with the unencrypted data, referred to as plaintext. Plaintext is encrypted into ciphertext, which will in turn be decrypted back into usable plaintext. The encryption and decryption is based upon the type of cryptography scheme being employed and some form of key.

1.4 Evolution of Cryptography

There are records of cryptography being used by the Greeks and Persians as far back as the 5^{th} century B.C. [5].

Cryptography probably began in or around 2000 B.C. in Egypt, where hieroglyphics were used to decorate the tombs of deceased rulers and kings. These hieroglyphics told the story of the life of the king and proclaimed the great acts of his life. The ancient Chinese used the ideographic nature of their language to hide the meaning of words. Messages were often transformed into ideographs for privacy, but no substantial use in early Chinese military conquests is apparent. In India, secret writing was apparently more advanced, and the government used secret codes to communicate with a network of spies spread throughout the country.[6]

During the Middle Ages, cryptography started to progress. Venice created an elaborate organization in 1452 with the sole purpose of dealing with cryptography. Leon Battista Alberti is known as "The Father of Western Cryptology" in part because of his development of polyalphabetic substitution. The next major step was taken in 1518, by Trithemius, a German monk who had a deep interest in the occult. In 1553, Giovan Batista Belaso extended this technique by choosing a keyword that is written above the plaintext, in a letter to letter correspondence. In 1628, a Frenchman named Antoine Rossignol helped his army defeat the Huguenots by decoding a captured message.

In the 1700^s, every European power had established its own "Black Chamber", a center for deciphering messages and gathering intelligence. By World War II, mechanical and electromechanical cipher machines such as Enigma[6] were in wide use [7]. The codes sent by these machines were famously broken by Alan Turing and his team at Bletchley Park, as dramatized in "The Imitation Game." This particular machine, built in 1943, was expected to sell for between £50,000 and £70,000 at Sotheby's in London[8].

In the 1970^s, due to the increased use of cryptography by businesses, the Data Encryption Standard "DES" was created.

[6]The Enigma machine is a cipher device developed and used in the early- to mid-20^{th} century to protect commercial, diplomatic, and military communication.



Figure 1.1: Enigma machine, used by the German military sending secret codes during World War II.

The 1970^s also saw the introduction of public key cryptography. Communication is a process that people have used, developed, and improved since ancient times. In the majority of cases, it is necessary to make sure that information remains protected. The examples of ancient leaders, kings and queens in the Middle Ages, and modern generals show that privacy and confidentiality cannot be ignored to enhance efficient relationships[9]. The desire for secrecy provokes the necessity to create some new codes and specific languages. Cryptography is one of such practices where the techniques of secret writing are developed with the purpose of hiding a message's meaning. It is characterized by a list of specific goals and methods "algorithms" that were firstly introduced by Egyptians and have gained high importance today. The evolution of cryptography is a unique topic for discussion because it touches upon all the spheres of human life, including politics, economics, society, and religion. In this thesis, attention will be paid to the progress of cryptography through ancient, technical, and paradoxical periods, the worth of common encryption methods, and the impact of coding on modern communication.

As it has already been mentioned in the discussion of cryptography evolution, each century is a new achievement with a possibility to learn from mistakes and make necessary adjustments. The period of the 1930^s was known for its military ciphers and the necessity to break them and find out the required information. A distinctive feature of 1930^s cryptography was the impact of the German Enigma machine. Many attempts were made to break the code, understand the interests of Germans and their tactics,

and change the situation in the world. The art of cryptography was politically (war) driven in order not to invent some new techniques but to crack the already existing system. However, the decision of the Japanese to create a new method known as Purple proved that the desire to win the war was a serious motive [9]. In both cases, encryption of the 1930^s has to be defined as a military practice with the ambitions of global leaders being underlined.

Compared to the 1930^s, the 1970^s was a period when people were challenged and inspired by a number of opportunities and discoveries. The emergence of digital data required the creation of a new encryption system and control devices to protect business and private life. Lucifer cipher was a technique with a secure cryptographic algorithm that was not as complex as DES but effective. The cryptography of the 1970^s was based on quantum states and the first steps to connect people via the world wide web. Cryptographers and researchers had limited knowledge about the Internet and its potential effects on codes and algorithms.In a series of experiments, participants who searched for information on the Internet believed they were more knowledgeable than a control group about topics unrelated to the online searches. In a result that surprised the researchers, participants had an inflated sense of their own knowledge after searching the Internet even when they couldn't find the information they were looking for. Therefore, unstable and unpredictable[7] studies occurred to check the system and choose the best options.

1.5 Current status of cryptography

Today, cryptography is a result of the most sophisticated mathematical algorithms checked by human experience and time. People have already discovered many methods to encrypt and decrypt information and continue improving their skills globally. Talking about modern applications and practices, one should mention the Cloud as

[7]Unpredictability as unforeseen new lines of research and discoveries When referring to a feature of the dynamic of a line of research, "scientific unpredictability" designates the occurrence of unexpected results in the course of the inquiry that open up new lines of research and discoveries.

one of the most captivating and dangerous things in technology. It is not a product or a service that belonged to one person or organization. It is a collective idea that remains uncontrolled today, and cryptography is the science that is used to understand and control such concepts as the cloud. Compared to the war-driven era of the 1930^s and a digitally challenged period of the 1970^s, today's cryptography is a combination of all the best and worst technological discoveries to gain power, enhance privacy, and promote security in the Information Age.

The growth of a quantum computer is marked through its capabilities of achieving entanglement over larger number of qubits and ability to perform large number of quantum gate operations in a noise-resilient manner.

Currently, the traditional cryptography has several types of algorithms that give High Security, but some of them not suitable for implementing in constrained environment. The Internet of Things introduces a plethora of new constraints and challenges that requires security to be focused on in another way than is usual in existing data systems[10].

Cryptography contains different algorithms and techniques functionally difficult to break since the complexity of these algorithms. Therefore, most security systems based on using cryptography [11], but traditional cryptography solutions focus on producing high level security, ignoring the conditions of constrained devices.

Current security that used in internet protocols depends on a popular broadly trusted suite of cryptographic algorithms which are a block cipher AES used to provide confidentiality, asymmetric algorithm RSA used to digital signatures and Key transport.

Today's systems use standard security algorithms that are easy to implement and work for most forms of communication and storage, there is no such standard solution that will work on every device within the Internet of Things, because of the varied constraints between different devices.

1.6 Research objectives

1.6.1 General objective

To develop a cryptographic system able to secure against quantum computers and interoperate with existing communications protocols and networks.

1.6.2 Specific objectives

- To descibe the quantum computer prototype and its computational or information processing efficience;
- To build a cryptosystem with resistant algorithms to both clasical and quantum attacks through random number and key generation mechanism.

1.7 Motivation for this work

When started research in cryptographic field in 2019, we got the impression that quantum cryptography was quite mature. There were several startup institutions that have been visited, like Burundi Central Bank, Burundi Revenue office and Telecommunications Regulation and Control Agency in Burundi, with quite general security proofs incorporated a wide array of imperfections. However, their security system were not yet covered by the nowadays existing cryptographic security proofs, but by other kinds of security systems. Therefore the motivation was that, practical quantum cryptography could deliver their provable unconditional security in the future. During the research, the opportunity to exchange with the IT responsable of each of those institutions to see if they actually comply with the assumptions in the security proofs with Quantum Cryptography has been presented. If Quantum Cryptography becomes too mature, it is crucial that the security of the practical devices would be tested by independent researchers, in order to obtain a reasonable level of security in more different institutions particularly those which store in their databases a big number and very sensitive data.

1.8 Research problem statement

Post-quantum cryptography refers to cryptographic algorithms that are thought to be secure against an attack by a quantum computer.

Therefore, the advent of quantum computer exposes classical cryptosystems whose semantic security is based on mathematical problems such as the discrete logarithm problem or the factorization of large number.

The appropriate algorithms for post-quantum cryptography must be identified before quantum computers become a practical reality.

For instance, the only possible strategy is to identify algorithmic problems for which the resistance to quantum computer attacks is strongly probable. Such a probability is currently based on two arguments. The first argument is that attempts of the scientific community to find polynomial time quantum algorithms for these problems have failed since a long time. The second argument is the belief that NP-hard[8] problems resist quantum attacks.

1.9 Research thesis Outline

The remainder of this thesis is organized as follow: After chapter one consisting of "General Introduction" of the work, the chapter two "Theoretical background and related works", is focused on review of the evolution of quantum computing where tremendous efforts and progress mark a significant milestone in solving real-world problems in recent years. Discuss the current situation according to classical and quantum computer, overview of cryptography, quantum cryptography development, post-quantum or quantum resistant cryptography and quantum algorithms. It talk also about "post-quantum cryptography",the field which provides cryptographic primitives that are secure against attacks using quantum computers. It is using mathematical problems that are believed to be hard to solve by both classical and quantum computers. As digital communication has become the backbone of our business collaboration,

[8]A problem is NP-hard if an algorithm for solving it can be translated into one for solving any NP-problem "nondeterministic polynomial time" problem.

secure transmission of data is essential. Post-quantum cryptography will be required when quantum computers are powerfull enough to perform algorithms and break the existing publick-key cryptography methods.

The Chapter three gives an overview of an "Innovative predictive quantum computer modeling", shows the evolution of cryptography and the theory related to computational performance, efficiency and predictive modeling of quantum computers.

Chapter four "Random Number and Key Generation", proposed a random number generation model to generate a key which haved been used to encrypt and decrypt a message before being transmited from source to destination. This chapter touched on different classes of generators, the entropy descraption, classification and technology, advantages and limites and then made comparative studie of mechanisms to describe good result for random number generation.

Chapter five "Conclusion and perspectives", summarized the work already done in previous chapters and provided suggestions about the further work in the domain of post-quantum cryptography.

The annexe part concerning of "Quantum Key Distribution", a cryptographic primitive that allows two remote users to generate an arbitrary amount of secret key even in the presence of an eavesdropper. This approach is particularly interesting in security because it relies on the laws of quantum physics, which state that qubits collapse as soon as they are measured. It means that if a third party eavesdrops on the exchange and measures the qubits to obtain the cryptographic key, they will inevitably leave a sign of their intrusion.

Chapter Two

Theoretical Backgroung and Related work

Contents

2.1 Introduction 16

2.2 Classical and Quantum Computers 18

2.3 Overview of Cryptography 21

2.4 Quantum Cryptography development 26

2.5 Post-Quantum Cryptography 28

2.6 Time complexity and algoritms 34

2.7 Impact on quantum computing and modern Communication 41

2.1 Introduction

Computers are getting smaller and faster day by day because electronic components are getting smaller and smaller. But this process is about to meet its physical limit. Electricity is flow of electrons. Since size of transistors is shrinking[1] to size of few atoms, transistors cannot be used as switch because electron may transfer themselves to the other side of blocked passage by the process called quantum tunnelling[2]. The field of quantum computing is actually a sub-field of quantum information science, which

[1]In 1965, Gordon Moore posited that roughly every two years, the number of transistors on microchips will double. Commonly referred to as Moore's Law, this phenomenon suggests that computational progress will become significantly faster, smaller, and more efficient over time.

[2]Quantum tunnelling is defined as a quantum mechanical process where wavefunctions can penetrate through a potential barrier. The transmission through the potential barrier can be finite and relies exponentially on the barrier width and barrier height.

Protais Ndagijimana © Doctoral school - University of Burundi

includes quantum cryptography and quantum communication[13][14]. The literature review shows that the studies derived aim at providing an insight of the advancements which have been made in the field of quantum safe algorithms and the research gaps which need to be reviewed so as to propose a framework for building systems which are quantum safe[3].

Brandon Rodenburg and Stephen P. Pappas published a research on vulnerabilities which need to be addressed by blockchain architecture as the world advances to a new technology known as quantum computers[15].

The second threat to blockchain which uses the asymmetric key security model at any point is by Shor's Algorithm which can factorize prime numbers by exponentially increasing the computations[16]. To counter the threats posed by these quantum algorithms, post quantum cryptographic methods along with some secure algorithms and security models have been discussed.

The development of quantum key distribution protocol in which a randomly generated random bit stream is used to encrypt a secret message, also known as OTP or One time password is recommended[17][18].

This generation of random key needs to establish by the sender and receiver and once that is achieved then the message is considered to be unconditionally secured.

The cryptographic community is working on post-quantum cryptography in order to provide alternatives using hard mathematical problems that cannot be broken by quantum computers.

This work focuses on Human-centered computing that shall facilitate various research level. This research is novel around the domain of design of quantum computing interfaces integrating science and technology. The systematic literature review has been conducted to find the current innovations that are either completely new or modification of existing approaches for the study on the evolution of quantum computing.

In this chapter, we reviewed the evolution of quantum computing where tremendous efforts and progress mark a significant milestone in solving real-world problems in recent years. We also presented the progress of various frameworks, tools, and protocol that

[3]Thought to be secure against a cryptanalytic attack by a quantum computer.

facilitate quantum computingparticularly in quantum key distribution. Finally, we discussed the current situation according to classical and quantum computer, overview of cryptography, quantum cryptography development, post-quantum or quantum resistant cryptography, quantum algorithms, challenges.

2.2 Classical and Quantum Computers

Quantum computers are computational devices that use the laws of quantum mechanics to perform calculations. The theory of quantum computing was first developed in the early 1980^s by pioneers including Paul Benioff, Richard Feynman, David Deutsch, and Peter Shor:

1. Paul Benioff, 1980: proposes the therethical concept of Hamiltonians as Turing Machines. He was honored for his pioneering work that first proved that quantum computing was a theoretical possibility[19];

2. Richard Feynman, 1982: " trying to find a computer simulation of physics, seems to me to be an excellent program to follow out and I'm not happy with all the analyses that go with just the classical theory, because nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem because it doesn't look so easy"[20];

3. David Deutsch, 1985: "Computing machines resembling the universal quantum computer could, in principle, be built and would have many remarkable properties not reproducible by any Turing machine. Complexity theory for, such machines, deserves further investigation"[21];

4. Peter Shor 1994, came up with a quantum algorithm to factor very large numbers in polynomial time[22];

5. Lov Grover 1997, develops a quantum search algorithm with $O(\sqrt{n})$ complexity; "A fast quantum mechanical algorithm for database search"[23].

In 1998, first 2 qubit quantum computing system developed, was only able to do some simple calculations by using the principle of nuclear magnetic resonance "NMR".

The motivation for quantum computing comes from the potential to perform calculations efficiently, which can only be performed inefficiently on a digital computer. Here, efficient means that the runtime is polynomial in the size of the problem.

Both classical and quantum computing process data. The difference lies in the methods and the speed of each type of computing. Although quantum computing is becoming more widely used, it will not replace classical computing; it can, however, do some things that classical computing cannot. Getting the computing power that many industries need is increasingly less possible with classical computing, which is where quantum computing comes in.

Quantum computation results from the link between quantum mechanics, computer science and classical information theorie[24]. It uses quantum mechanical effects, especially superposition, interfence and entanglement to perform new types of computation which show promise to be more efficient than classical computations. This is what makes quantum computing probabilistic[4].

The following elements are among those which make quantum computing different from conventional or classical computing[25].

-Classical computing calculates with transistors which can represent either 0 or 1 while quantum computation calculates with qubits, which can represent 0 and 1 at the same time.

-Classical computing encreases power in a 1:1 relationship with the number of transistors while for quantum computation power encreases exponantially in proportion to the number of qubits.

-Only specifically defined results are available, inherently limited[5] by algorithm's design while quantum answers are probabilistic because of suporposition and entanglement, multiple possible answers are considered in a given computation.

[4]When measuring a qubit, the result is a probabilistic output of a classical bit, therefore making quantum computers nondeterministic in general.

[5]Algorithm limitations are the postconditions or drawbacks that your algorithm produces or faces. For example, a limitation could be that your output data is approximate, incomplete, or sensitive.



Figure 2.1: A classical and quantum computer side by side

[26]

The current researches allow to better understand this quantum universe and more necessarily they open the life to a new technological revolution. The quantum computer might be the theoretician's dream, but as far as experimentalists are concerned, its realisation is a nightmare[27]. The problem is that while some prototypes of the simplest elements needed to build a quantum computer have already been implemented in the laboratory, it is still an open question how to combine these elements into scalable systems[28].

Quantum computers may be able to efficiently solve classically intractable problems[6], hence re-describe the abstract space of computational complexity[29], computational concepts and even computational kinds such as "an efficient algorithm" or "the class NP", become machine-dependent, and recourse to "hardware" becomes inevitable in any analysis thereof[30].

[6]Quantum computing can be used to solve problems that are intractable for classical computers by taking advantage of quantum parallelism and quantum algorithms. Classical computers work with bits, which are limited in storage capacity and speed of calculations.

2.3 Overview of Cryptography

Cryptography is the study and practice of techniques for secure communication in the presence of third parties called adversaries. It deals with developing and analyzing protocols that prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security. Secure communication refers to the scenario where the message or data shared between two parties can't be accessed by an adversary. In cryptography, an adversary is a malicious[7] entity, which aims to retrieve precious information or data thereby undermining the principles of information security. Data confidentiality, data integrity, authentication and non-repudiation are core principles of modern-day cryptography. In the field of cryptography there exist several techniques for encryption/decryption these techniques can be generally classified in to two major groups conventional and public key cryptography. Conventional encryption is marked by its usage of single key for both the process of encryption and decryption whereas in public key cryptography separate keys are used. Several classic encryption algorithms are available and used in information security[31] [32][33]. There are several algorithms that can be categorized as classical but out of many in this section we will be shedding some light on 3 such techniques: i) Vigenere Cipher, ii) Caesar Cipher and iii) Playfair Cipher.

(I) In the field of polyalphabetic substitution[8] and symmetric key cryptography, Vigenère cipher [34] is a traditional algorithm that makes use of the same keys for both encryption and decryption. This cipher uses a table called tabula recta[9], which is a 26x26 matrix comprising alphabet letters, to encrypt and decode data[35].

[7] In cryptography, an adversary is a malicious entity whose aim is to prevent the users of the cryptosystem from achieving their goal.

[8] A polyalphabetic cipher is a substitution, using multiple substitution alphabets. The Vigenère cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case.

[9] The tabula recta is often referred to in discussing pre-computer ciphers, including the Vigenère cipher and Blaise de Vigenère's less well-known autokey cipher.

KEY \ PLANTEXT	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Table 2.1: Tabula Recta

The Vigenère cipher's encryption and decryption can be understood in (2.1) and (2.2).

$$CT_i = (PT_i + K_{ey})\,\%26 \tag{2.1}$$

$$PT_i = (CT_i - K_{ey})\,\%26 \tag{2.2}$$

Where CT is the ciphertext, PT is the plaintext, K_{ey} is the Key. Alphabet ciphertext is the intersection of the ciphertext's plaintext and alphabet keys, and it is used to encrypt sensitive information. There are times when the key alphabet is less than the plaintext, hence the key will be repeated until the plaintext is equal to that of the key. Key repetition[10] is an issue when the length of the key is less than the length of the plaintext in Vigenère cipher because the algorithm most likely produces the same

[10]The idea is that you choose some secret key and then repeat it until it's the same length as the

PT	*C*	*R*	*Y*	*P*	*T*	*O*	*G*	*R*	*A*	*P*	*H*	*Y*
ID	2	17	24	15	19	14	6	17	0	15	7	24
Key	L	U	C	K	L	U	C	K	L	U	C	K
ID	11	20	2	10	11	20	2	10	11	20	2	10
CT	N	L	A	Z	E	I	I	B	L	J	J	I
ID	13	11	0	25	4	8	8	1	11	9	9	8

Table 2.2: Vigenère example

ciphertext for plaintexts of equal length. For example, an encryption of the message "C R Y P T O G R A P H Y" using the key "L U C K" gives ciphertext "N L A Z E I I B L J J I" as it declared in Table 2.2. There are certain disadvantages to the Vigenère cipher, such as a key length that is too short for the plaintext length. This means that the key will be repeated, which cryptanalysts can utilize this to decrypt the ciphertext. Vigenère cipher techniques were broken by the Kasiski method, which uses the same characters in the ciphertext to determine the distance to the key length. For an exhaustive key search, the next step is to identify the keywords that should be used [36].

According to the research, the classical algorithm Vigenère cipher appears to have a better degree of trust than the ordinary Vigenère cipher when the keys are reconfigured. This is because the keys are adjusted in such a way that when the length of the key exceeds the length of the plaintext, the key is not repeated but created by a function. As a result of not needing to repeat the key, more random keys are generated.

(II) An example of Caesar cipher: The Caesar Cipher is a famous implementation of early day encryption. It would take a sentence and reorganize it based on a key that is enacted upon the alphabet. It is a classical substitution cipher, and one of the simplest example of substitution ciphers which replaces the letter of alphabet with a letter that is 3 paces ahead of it, for example "ZULU" will be converted in to "CXOX" as one can see such an article[37].

plaintext you'd like to encrypt and for every char in your string you exclusive or (XOR) it with the corresponding char in the key.



Figure 2.2: The entire alphabet shifted by three spaces.

Also known as shift encryption, it simply consists of permuting each letter by another, by translating a certain number of positions in the alphabet[38].

If we shift the word "CESAR" three positions to the right, we get "FHVDU" (because C+3=F in the alphabet). While cryptography is a powerful tool for securing information, it also presents several challenges, including:

a) Key management: Cryptography relies on the use of keys, which must be managed carefully to maintain the security of the communication.

b) Quantum computing: The development of computing poses a potential threat to current cryptographic algorithms, which may become vulnerable to attacks.

c) Human error: Cryptography is only as strong as its weakest link, and human error can easily compromise the security of a communication.

In general, Caesar cipher is one of the simple methods in cryptography. This method requires two inputs a number and a plaintext. The time complexity and space complexity both are $O(N)$.

The encryption formula is:

$$E_n(x) = (x + n)\, mod\ 26 \tag{2.3}$$

and the Decryption formula is:

$$D_n(x) = (x - n)\, mod\ 26 \tag{2.4}$$

The following is an example of cryptography program and its implementation in Python language:

```
def encrypt(text,s):
result = ""

    # transverse the plain text
    for i in range(len(text)):
        char = text[i]

        # Encrypt uppercase characters in plain text
        if (char.isupper()):
            result += chr((ord(char) + s-65) % 26 + 65)

        # Encrypt lowercase characters in plain text
        else:
            result += chr((ord(char) + s - 97) % 26 + 97)

    return result

#check the above function
text = "CEASER CIPHER DEMO"
s = 4
print "Plain Text  : " + text
print "Shift pattern : " + str(s)
print "Cipher: " + encrypt(text,s)
```

Figure 2.3: Program implementation of Caesar cipher algorithm.

```
E:\Cryptography- Python>python caeserCipher.py
Plain Text  : CEASER CIPHER DEMO
Shift pattern : 4
Cipher: GIEWIVrGMTLIVrHIQS

E:\Cryptography- Python>
```

Figure 2.4: Caesar cipher output.

The plain text character is traversed one at a time. "For each character in the given plain text, transform the given character as per the rule depending on the procedure of encryption and decryption of text". After the steps is followed, a new string is generated which is referred as cipher text.

(III) The Playfair cipher is an example of a polyalphabetic cipher and it was Charles Wheatstone who invented the cipher in 1854 but was named after lord Playfair who promoted its usage[39] [40]. A polyalphabetic cipher treats a combination of two letters "digraphs" in the plaintext as a single unit and converts these digraphs into ciphertext digraphs using a key square. The key square is formed by writing a keyword horizontally with duplicate letters being removed. The rest of the square is filled with the remaining letters of the alphabet, in alphabetical orde.
Playfair cipher was a powerful cipher in the olden days but it is losing its potency nowadays because of the sophistication in computing devices which possess features that can make them break ciphers such as Playfair within a few seconds. Researchers have worked on and proposed several modified versions of the cipher but attention has been on modification of the key matrix sizes and perhaps different techniques to introduce diffusion and confusion properties into the cipher.

2.4 Quantum Cryptography development

Quantum cryptography is an emerging technology in which two parties can secure network communications by applying the phenomena of quantum physics[41]. The security of these transmissions is based on the inviolability of the laws of quantum mechanics.
Quantum cryptography was born in the early seventies(1970^s) when Steven Wiesner wrote "Conjugate coding"[42].The quantum cryptography relies on two important elements of quantum mechanics: the Heisenberg uncertainty principle and the principle of photon polarization. The Heisenberg uncertainty principle[11] states that, it is

[11]Formulated by the German physicist and Nobel laureate Werner Heisenberg in 1927, the uncertainty principle states that we cannot know both the position and speed of a particle, such as a photon

not possible to measure the quantum state of any system without distributing that system[43][44][45]. The principle of photon polarization states that, an eavesdropper can not copy unknown qubits i.e. unknown quantum states, due to no-cloning theorem which was first presented by *Wootters and Zurek in 1982*,[46].

Today, several companies like International Business Machines Corporation(IBM), Google LLC, Rigetti and Co, Inc., have already made quantum machines available to users. The devices are limited in the number of quantum bits "qubits" and the operations applied to qubits during the coherence time. At the time of writing, quantum computers have not posed a severe threat to public-key algorithms. However, there is an unignorable possibility that technological innovations will lead to ideal machines in the future, the timing of which is unpredictable. Furthermore, the migration of cryptographic algorithms may take several years in practice. Research and development of quantum cryptography for security against ideal quantum computers, have been in progress in order to update the existing algorithms.

The Cryptography Research and Evaluation Committees "CRYPTREC" established by the Japanese government has evaluated the impact of quantum computers on current cryptographic algorithms and considered adoption of Post-Quantum Cryptography "PQC" in the future[47]. In 2019, CRYPTREC set up a task force to follow the research trends regarding quantum computers and discuss how to deal with PQC.

In addition, the Open Quantum Safe "OQS" project aims to support the development and prototyping of post-quantum cryptography. The project implements the National Institute of Standards and Technology (NIST) candidate algorithms and evaluates their performance. If post-quantum cryptography replaces the existing algorithms in many devices, financial institutions and payment service providers will have to apply post-quantum cryptography to their Information Technology "IT" systems for online financial services. Thus, it will be necessary to consider how to prepare for the migration to post-quantum cryptography in the near future.

---

or electron, with perfect accuracy.

2.5 Post-Quantum Cryptography

Post-Quantum Cryptography refers to a familly of cryptographic algorithms that are secure against an attack by both a classical and a quantum computer[48]. Such cryptography will be required when quantum computers are powerfull enough to perform algorithms and break the existing publick-key cryptography methods. As digital communication has become the backbone[12] of our business collaboration, secure transmission of data is essential. Cryptographic algorithms employ generated and deciphered codes to conceal private information from unauthorized access when shared over the internet. Most of algorithms are based on the difficulty of solving mathematical computations within a limited timeframe[49][50].

This difficulty varies depending on whether classical computers or quantum computers are used. The research and technical challenges in integrating post-quantum cryptography with various area like Atltificial Intelligence, e-learning, Internet of Things "IoT" and more networks must be conducted to ensure the high standardization of performance and security in different areas. With this growth, a large amount of data will be generated. For example, IoT-based applications like smart homes, smart traffic light systems, smart transportation systems, automated traffic lights, automated vehicles, medical and healthcare services, and other supply chain management will generate huge data per second. It is expected that more and more devices will be interconnected to the Internet compared to people joining the Internet services. Post-quantum cryptography is developed to resist quantum computers and quantum computing-based attacks. Various post-quantum cryptography approaches are already implemented for information and communication technologies "ICTs". There are several classes of mathematical problems that are conjectured to resist attacks by quantum computers and have been used to construct public key cryptosystems, several of which date from the early days of public key cryptography[51][52].

[12] At the same time, the revolutionary workplace changes that emerged were enabled by the technological advances we have seen over the past decades and not least among them are the unified communications capabilities that connect business workers with colleagues, customers, and partners, regardless of where they may be physically located.

Those are:

1- code-based cryptography;

2- hash-based cryptography;

3- multivariate cryptography;

4- lattice-based cryptography and;

5- supersingular elliptic-curve isogenies cryptography.

Each of these families is based on different mathematical problems that are hard to solve both with traditional computers as well as quantum computers. They differ in efficiency, e.g., in the size of public and private keys, sizes of cipher texts and key-exchange messages, and computational cost, their maturity, and the amount of trust in their strength. Efficiency of post-quantum schemes is important because it determines how well the schemes can be used on current and future devices, in particular on devices with few resources or limited network bandwidth like embedded and handheld devices.

In general post-quantum schemes require more resources compared to traditional cryptography, in particular Elliptic Curve Cryptography "ECC", which is a public key cryptographic algorithm used to perform critical security functions, including encryption, authentication, and digital signatures. Therefore, security against quantum computer attacks comes at a cost.

2.5.1 Code-based cryptography

The McEliece public key encryption scheme [53] was one of the first public key schemes, and is based on error-correcting codes, in particular, the hardness of decoding a general linear code. Niederreiter [54] subsequently proposed a digital signature scheme based on error correcting codes; The error-correcting code enables the receiver to correct a certain number of bit-errors during decoding. The message $\vec{m}$ is converted into a code word $\vec{c}$ of the respective code (see Figure 4.2). This adds redundancy, i.e., the code

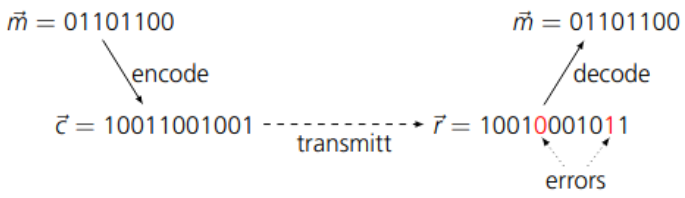


Figure 2.5: Example for error correction on an unreliable channel.

word is longer than the message. Then $\vec{c}$ is transmitted over the channel. During transmission several bits of $\vec{c}$ might be flipped, the receiver does not receive $\vec{c}$ but $\vec{r} = \vec{c} \oplus \vec{e}$ where $\vec{e}$ is an error vector of some weight w (w bits in $\vec{e}$ are 1, the other bits are 0). Now, the receiver maps $\vec{r}$ to the closest code word $\vec{c'}$ in the code. If the number of errors in $\vec{r}$ is smaller than the number of errors that can be corrected, i.e.,w $\leq t$, then $\vec{c'}$ is equal to the original code word $\vec{c}$ (otherwise decoding fails). Finally, the receiver applies the inverse of the encoding operation to $\vec{c'}$ and obtains the original message $\vec{m}$. However, decoding arbitrary "random" codes is computationally hard and can be infeasible depending on the code parameters. Nevertheless, there are specific codes for which efficient decoding algorithms are known. Therefore, in practice only such codes are used that have efficient decoding algorithms. The main security assumption of code-based cryptography is the hardness of decoding a random linear code [55].

2.5.2 Hash-based cryptography

The approach of hash-based cryptography is conceptually different from code-based and lattice-based cryptography. Hash functions are one-way functions that map bit-strings of an arbitrary length to relatively short, fixed-length bit strings called hash values. There are three properties that are required for a cryptographic hash function:

1. Preimage resistance: It must be hard to compute a preimage of a hash value, i.e., a bit string that once hashed results in a given hash value;

2. Second preimage resistance: Given a bit string, it must be hard to find a different bit string that has the same hash value;

3. Collision resistance: It must be hard to find two arbitrary bit strings that have the same hash value.

As a basic example for the functionality of hash-based signatures consider the following scenario using a hash function h: Alice wants to sign a single bit message. She creates a private signature key by randomly choosing two bit strings r_0 and r_1. She computes her public key as $\{s_0 = h(r_0)\ ,\ s_0 = h(r_0)\}$ and publishes $\{s_0,s_1\}$. Bob receives the public key and verifies that $\{s_0,s_1\}$ belongs to Alice. Eventually, when Alice wants to sign a one-bit message $m \in \{0,1\}$, she publishes r_m together with the message. For example, let 1 encode "true" and 0 encode "false". For signing the message "true", Alice publishes r_1 . Bob can easily verify the signature by computing $h(r_1)$ and comparing it to the public key element s_1. The signature must be from Alice since only she knew the preimage r_1 of s_1 and since it is computationally infeasible for an attacker to compute a preimage from s_1. However, this example describes a one time signature scheme: Alice can no longer use this private key since publishing the other value from her private key would reveal all private information to the public, Bob could no longer distinguish whether Alice or somebody else signed subsequent messages. Another obvious drawback of this basic scheme is the extremely limited length of the messages.

2.5.3 Multivariate cryptography

Multivariate cryptography is based on the hardness of the Multivariate Quadratic MQ-problem. Solving multivariate quadratic systems of equations over finite fields is NP-hard: As opposed to linear systems, there is no efficient algorithm for solving random multivariate polynomial systems. The hardness of solving a specific system depends on the size of the underlying finite field, the number of variables, and the degree of the system. However, the number of equations and variables is sufficiently large, even systems of quadratic equations "with degree two, smallest finite field" are hard to solve.

$$\begin{aligned} x_0x_3 + x_2x_3 + x_0 + 1 &= 0 \\ x_0x_1 + x_2x_3 + x_2 + 1 &= 0 \\ x_0x_1 + x_0x_3 + x_0 + x_1 + 1 &= 0 \\ x_1x_2 + x_2x_3 + x_3 &= 0 \end{aligned}$$

Here an example of a multivariate polynomial system of four equations in four variables x_0,....,x_3 (i.e., multivariate) of maximum degree two "i.e., quadratic".
This particular quadratic system is small and therefore easy to solve. A solution of this system is $x_0 = 1$,$x_1 = 0$, $x_2 = 1$, $x_3 = 0$.

2.5.4 Lattice-based cryptography

The name derives from the fact that this crypto scheme is built on mathematical problems around lattices. A lattice in this context resembles a grid of graph paper using a set of points located at the crossings of a lattice of straight lines. This grid is not finite in any way. Ajtai [56] proposed the first cryptographic schemes directly based on lattices. The underlying hard problem for lattice-based cryptography is the shortest vector problem: it is computationally hard to find the shortest vector in a high dimensional lattice.
Starting with a set of points, known as vectors, numbers are then added and subtracted in any integer multiples. The hard problem is finding points in the lattice that are close to 0 or close to some other point. These problems are quite simple in 2 dimensions, but they become extremely challenging in 400 dimensions, for example. Within the diagram bilow, an example would be that one set of points could be the private key and another set of points that are further away could be the public key. For encryption, the sender of a message maps the message to a point $\vec{m}$ in the lattice using the public scrambled base.
Then, the sender adds a random error to the lattice point such that the resulting point $\vec{c}$ is still closer to the original $\vec{m}$ than to any other point in the lattice. This distorted point $\vec{c}$ is the cipher text which is sent to the receiver. Since the receiver is in possession of the secret, well-formed basis s of the lattice, he can recover the original lattice point $\vec{m}$ (the lattice point that is closest to the distorted cipher point) with low computational effort and obtain the original message.
The secret, well-formed base is $\{\vec{s_0}, \vec{s_1}\}$; the public, "scrambled" base is $\{\vec{p_0}, \vec{p_1}\}$.
The sender uses $\{\vec{p_0}, \vec{p_1}\}$ and adds an error vector to obtain the point $\vec{c}$. The point $\vec{c}$ is closed to $\vec{m}$ than to any other lattice point.

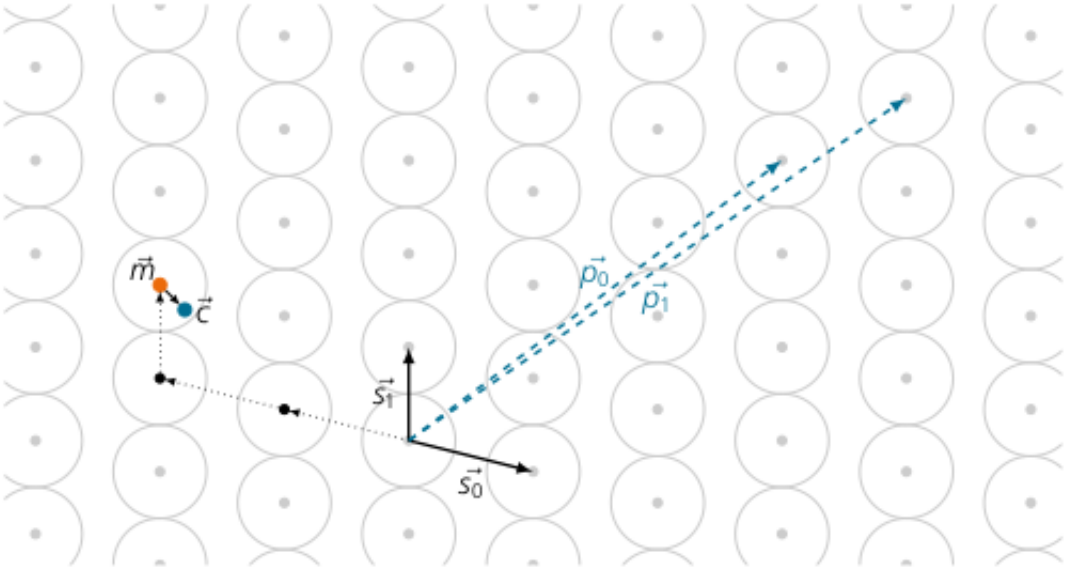


Figure 2.6: Example for lattice-based encryption in a two-dimensional lattice.

Therefore, the receiver can use the well-formed secret base $\{\vec{s_0}, \vec{s_1}\}$ to easily recover $\vec{m}$ this is a hard computation for an attacker who only has the scrambled base. For a secure scheme, the dimension of the lattice must be much higher than 2 as in this example

2.5.5 Supersingular elliptic curve isogenies Cryptography

One of the newest candidates for quantum-resistant public key cryptography is based on the difficulty of finding isogenies between supersingular elliptic curves [57]. Classical elliptic-curve cryptography "ECC" works on points on specific elliptic curves: operations like addition and scalar multiplication are performed on points and also the exchanged data structures in cryptographic protocols are coordinates of points. However, instead of computing on points of an elliptic curve, one can also define operations between different elliptic curves. Operations that map a curve onto another curve have different properties. Maps with certain properties are called isogenies. Using isogenies between elliptic curves for building cryptographic schemes is a relatively new approach compared to the schemes described previously.

In addition, quantum information can be used directly to create cryptosystems; this

is called quantum cryptography. For example, quantum key distribution allows two parties to establish a shared secret key using quantum communication and an authenticated classical channel. While this can provide very strong security, it is not yet a candidate for widespread usage since it requires physical infrastructure capable of transmitting quantum states reliably over long distances.

Finally, all of the four main families have their merits and deficits. It is hard to predict which family of quantum-resistant algorithms will prove to be the most efficient in the future. While lattice-based cryptosystems have been subject to most research, code-based algorithms remain a solid choice for the future cryptographic standards, whilst both hash-based and multivariate algorithms provide secure signature schemes. Based on the number of submissions, lattice-based algorithms seem to be favoured the most.

2.6 Time complexity and algoritms

A concept of polynomial time refers to the time complexity that describes the amount of computer time it takes to run an algorithm. In computer science, the time complexity is usually expressed using the big O notation. Linear time complexity is expressed as $O(n)$, where n is the size in bits that represents the input. The above mentioned polynomial time could be expressed as $O(n^c)$ or $poly(n)$, and its running time complexity is the polynomial expression with the degree of the complexity of the input. Computers perform mathematical operations of addition, subtraction, multiplication, division, square roots, powers, and logarithms in polynomial time.

The paradigm of time complexity is vastly important in the field of cryptography since it determines how safe an encryption scheme is. Any such scheme is designed to encrypt and decrypt a message in a short amount of time when the key is given and to make the decryption without a key infeasible. An encryption scheme would be useless if decryption without a key can be performed in a small amount of computational time. A strong encryption scheme requires years for a malicious third party to decrypt a single message. The time complexity of an algorithm is determined from its design:

sequential statements have constant time complexity[13] $O(1)$, loop statements have linear time complexity $O(n)$, conditional statements have linearithmic time complexity $O(n.log(n))$, recursive statements have exponential time complexity 2poly(n), trial and error "brute-force" statements have factorial time complexity $O(n!)$. The time complexity can be improved if the algorithm uses multithreading and other opti- mization techniques.

One-way functions are fundamental tools in cryptography, personal identification, authentication, and other areas of data protection. Although the existence of such functions remains unproven, there are one-way functions that have not been rejected yet. They are an integral part of most telecommunications systems, as well as e-commerce and online banking systems around the world since modern cryptography is heavily dependent on the use of such functions.

The main characteristic of one-way functions is that it is easy to compute the result of such functions but very difficult to compute the inverse of that result [58]. Even though we know the function, say $f(x)$, and we can easily calculate the result for any input, say $f(a) = b$ but finding the inverse $f^{-1}(b)$ of that function would take an unreasonable amount of computing time from the point of view of computational complexity theory. There are two types of one-way functions: those that produce a fixed-length output and those with a variable-length output.

Definition: (One-way Function).A function $f : \{0,1\}^* \to \{0,1\}^*$ is a one- way function if:

1) f can be evaluated in polynomial time;

2) f^{-1} cannot be found in polynomial time or, in other words, there is only a negligible probability that any efficient algorithm will solve the problem of inverting f in polynomial time.

One type of one-way function is a trapdoor function. If f is a trapdoor function, then

[13]Type of computational complexity that describes the time required to execute an algorithm. The time complexity of an algorithm is the amount of time it takes for each statement to complete.

there exists a secret y, such that given $f(x)$ and y, x can be computed easily [58]. RSA and Rabin cryptosystems use asymmetric encryption implemented as trapdoor functions, and their security is related to the complexity of factorization. They are presented as the exponentiation modulo a composite number and assumed that it is difficult to factorize a large composite number. Functions involving a discrete logarithm problem, such as modulo a prime, are not trapdoor functions since there is no secret that would allow their efficient computation.

Another type of one-way function is a cryptographic hash function. It transforms the input of any size into a hash value of a fixed size. Its main property is that such a function should be collision-free, meaning two different input sequences should not produce the same hash value [59]. A slight change in the input normally causes a drastic change in the hash value. This way, data can be protected from any modifications since its integrity is verified by comparing the hash values. An inverse of a hash function can be obtained using a brute-force search or a rainbow table of matched hashes. Examples of one-way hash functions include MD5 (currently unsuitable for most use cases due to collisions), SHA-1 (considered vulnerable due to collisions), SHA-2, SHA-3, where SHA stands for Secure Hash Algorithm, and the security of each new generation is more robust than the predecessor.

Symmetric algorithms[14], such as the Advanced Encryption Standard "AES", use shared keys and the same algorithm for both encryption and decryption, unlike asymmetric keys, which differ depending on the process[60],it is also known as the public key cryptography. There are two types of key first one is public key which is used for encryption and second is private key which is used for decryption. Only a particular user/device knows the private key whereas the public key is distributed to all users/devices taking part in the communication. Two popular asymmetric algorithms are Diffie-Hellman "DH" and Rivest-Shamir-Adleman "RSA".

[14]Symmetric algorithms are those where the decryption key can be calculated from the encryption key. The same key is usually used for encryption and decryption.

2.6.1 Advanced Encryption Standard(AES)

The Advanced Encryption Standard "AES", also known by its original name *Rijndael*. The AES specifies a Federal Information Processing Standard "FIPS" cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt "encipher" and decrypt "decipher" information. Information is confronted with various challenges primarily owing to the Internet, which has transformed the world into a small village, where numerous illegal methods are used to obtain information. Accordingly, the subject of security has become extremely critical for information protection, in which many security algorithms are used to achieve safety goals, and that the various aims of secure systems include authentication, confidentiality, and data integration [61].

2.6.2 Diffie-Hellman (DH) Algorithm

Diffie-Hellman "DH"[62] is one of the first practical implementations of asymmetric encryption or public-key cryptography "PKC". It was published in 1976 by Whitfield Diffie and Martin Hellman. Other contributors who are credited with developing DH include Ralph Merkle and researchers within the United Kingdom's intelligence services [63].

The DH Algorithm is a key-exchange protocol that enables two parties communicating over public channel to establish a mutual secret without it being transmitted over the Internet. DH enables the two to use a public key to encrypt and decrypt their conversation or data using symmetric cryptography.

Diffie-Helman is generally explained by two sample parties, Alice and Bob, initiating a dialogue. Each has a piece of information they want to share, while preserving its secrecy. To do that they agree on a public piece of benign information that will be mixed with their privileged information as it travels over an insecure channel[63]. Their secrets are mixed with the public information, or public key, and as the secrets are exchanged the information they want to share is commingled with the common secret. As they decipher the other's message, they can extract the public information

and with knowledge of their own secret, deduce the new information that was carried along. While seemingly uncomplicated in this method's description, when long number strings are used for private and public keys, decryption by an outside party trying to eavesdrop is mathematically infeasible even with considerable resources.

2.6.3 The RSA Scheme

RSA (Rivest-Shamir-Adleman)[64] is an asymmetric "public-key" encryption technique that is widely used for data transmission in computer systems. Its cryptographic security is based on the complexity of factoring large numbers or, in other words, on the exceptional difficulty of finding the secret key using the public key. It uses RSA numbers that are a set of large semiprimes "numbers with exactly two prime factors". The most secure systems use 2048-bit numbers that can store 2^{2048} or $3.23.10^{616}$. That is a number with 617 decimal digits, and the corresponding RSA-2048 method is considered as not factorizable in the near future.

Algorithm 1: "RSA Key Generation".

To generate the public and the private keys, we need to do the following:

1) Choose two distinct prime integers p and q. These numbers are chosen at random and are kept secret.

2) Define n as a result of multiplication of these numbers: $n = p.q$. It will be a part of the public key "the modulus", and its length represented in bits determines the key length for the RSA encryption.

3) Choose a random integer number e. This number must be coprime "have no common divisors except 1" with the result of multiplication $(p-1).(q-1)$. This number is also a part of the public key "the exponent".

4) Determine a number d for which the following relation is true:

$$d.e = 1 \ mod(p-1).(q-1) \tag{2.5}$$

This number is the private key exponent.

5) The public key consists of the modulus n and the public exponent e. The private key is comprised of the modulus n and the private exponent d.

Algorithm2:"RSA Encryption and Decryption".

In order to encrypt a message using the public key n,e, we need to perform the following operation:

1) Turn the message into a nonnegative integer m, such that $m < n$. If $m \geq n$, the message can be broken up into blocks, and each block is turned into a nonnegative integer.

2) Compute the ciphertext c as follows:

$$c = m^e \ mod \ n \tag{2.6}$$

In order to decrypt the message using the private key n,d, we have to do the following:

1) Recover the original integer from the following formula:

$$m = c^d \ mod \ n \tag{2.7}$$

2) Turn the recovered integer back into the text to obtain the original message. If the message consists of several blocks, reconstruct the message.

Proof. The correctness of the RSA can be proven using Euler's theorem:

$$\left(m^{e.d} = m \ mod \ n, \ n = p.q\right) \tag{2.8}$$

If e and d are positive integers such that $e.d = 1$ mod $\psi(n)$, then $ed = 1$+h.$\psi(n)$ for some nonnegative integer h. Since m is coprime to n,

$$m^{ed} = m^{1+h.\psi(n)} = m(m^{\psi(n)})^h = m(1)^h = m \ mod \ n, \tag{2.9}$$

due to Euler's theorem.

Knowing the algorithms of RSA key generation, encryption, and decryption, we can analyze the potential flaws of this encryption technique. The security of an RSA implementation depends on the following parameters[65]:

1) Prime selection.

   The security of RSA is based on the difficulty of factorizing a large number. This number is a product of two primes. These primes have to be selected in a way that their product cannot be factorized. To ensure the security of the algorithm, the primes have to be truly random and independent. If they share enough of their upper bits, their product can be factorized using Fermat's factorization method. If there are multiple certificates generated, there is a possibility of duplicate primes, which allows factoring the modulus using the Euclidean algorithm[15].

2) Public exponent.

   In some cases, in order to speed up the encryption time, the public exponent is chosen to be a small number which leads to lower security of the RSA encryption. When e is small, the Franklin-Reiter attack can be used to decrypt two RSA-encrypted messages that differ by a known fixed difference.

3) Private exponent.

   To improve the decryption performance, the value of d is sometimes chosen 1 to be small. In a case when d$< \frac{1}{3}n^{\frac{1}{4}}$, the private key can be recovered using Wiener's attack, and the RSA encryption will be compromised.

The above mentioned methods and attacks for decrypting a message without a private key or recovering the private key are efficient and can be performed in some cases. However, they are only applicable under certain circumstances when the RSA parameters are not chosen to be secure. For the RSA-2048, which is widely used today, the RSA numbers have been considered unfactorizable for many years.

[15]The Euclidean algorithm, a way to find the greatest common divisor of two positive integers, a and b. First let me show the computations for $a = 210$ and $b = 45$. Divide 210 by 45, and get the result 4 with remainder 30, so $210 = 4.45 + 30$.

2.7 Impact on quantum computing and modern Communication

Quantum computing holds immense promise for various fields, including cryptography, optimization, drug discovery, and simulation of quantum systems. The ability to tackle these problems more efficiently has the potential to revolutionize industries and drive scientific advancements. Quantum communication has the potential to secure communication networks, ensuring privacy and integrity in an increasingly interconnected world.

The impact of quantum theory on modern computing and communication cannot be overstated. From quantum computing's potential to solve complex problems at an unprecedented speed to quantum cryptography's role in securing our digital infrastructure, quantum theory has opened up new horizons for technology and scientific discovery. This allows quantum computers to perform certain types of calculations, such as factorizing large numbers, much faster than classical computers. The impact of quantum computing has the potential to have a significant impact on the field of mathematics, particularly in areas such as number theory and cryptography.

2.7.1 Impact on quantum computing

Quantum computer will have a major impact on cryptography, which relies up on hard-to-compute probleme to protect data. Shor's algorithm running on a large quantum computer will greatly reduce the required computation to extract a public key from a symmetric ciphers used to protect almost all internet traffic and stored encrypted data. Given a large risk a quantum computer poses to current protocols, there is an active effort to develop post-quantum cryptography, asymmetric ciphers that a quantum computer can not defeat.

While the potentiality utility of Shor's algorithm for cracking deployed cryptography was a major driver of early anthusiasm in quantum computing research, the axistance of an cryptographic algorithms that are believed to be quantum-resistant will reduce the usefulness of a quantum computer for cryptanalysis and thus will reduce extend to

which this application will drive quantum computing in the long term.

Key finding 1: Quantum computing is valuable for driving foundational research that will help humanity's understanding of the universe.

Key finding 2: Although the feasability of a large-scale quantum computer is not yet certain, the benefit of effort to develop a practical quantum computer, are likely to large, and they may continue to spill to over other nearer-term applications of quantum information technolohy, such as quibit-based sensing[16].

2.7.2 Impact on modern communication

Modern cryptography is a complex subject, and its effects and technologies are frequently discussed by researchers, theorists, and philosophers. On the one hand, cryptography is a means to protect people and make sure their communication remains private. There are many situations when people have to keep secrets in the presence of some third parties. They construct specific systems and analyze protocols in order to cover all the aspects of information security and content. Modern communication is full of codes and signs, and applications of cryptography turn out to be good money sources. Data privacy, authenticity, and integrity are the purposes of ciphers that enrich communication and human relationships. On the other hand, the use of ciphers means the presence of secretes and, as a result, some danger. Progress in developing of cryptographic components that can be used in control system communications and the risks anlysis still a need.

However, new quantum algorithms and implementations could lead to new quantum cryptanalytic technics, as with cybercecutity in general, post quantum resilience will require ongoing security research.

[16]sensitivity of a qubit can also be seen as unique feature, enabling the investigation of other systems by means of a very sensitive sensor.

Chapter Three

Innovative Predictive Quantum Computer Modeling

Contents

3.1 Introduction 43

3.2 Principles of Quantum Computing 46

3.3 Development of Quantum Computing 49

3.4 Quantum Computer prototype Modeling 53

3.5 Large scale Computer Prototype 58

3.6 Quantum Computer Efficiency proof 60

3.7 $\mathcal{R}2022\mathcal{A}^{+}$ Algorithm 62

3.1 Introduction

Due to the revolution of technology since the beginning of the 20^{th}century, it is considerable to develop efficient tools on the quantum level in order to improve confidentiality and interoperability of data. The quantum computer, with quantum mechanics as its basic principle, still promises to bring great surprises even though we are at the beginning of its development. Quantum computer is the only known model for computing that could offer exponential speedup classic computer. The current major challenges of the quantum computer include increasing or reducing the number of qubits for a given system, coherence management to preserve the properties of the superposition and entanglement state of a quantum system to perform data operation, of course through appropriate quantum algorithms.

Protais Ndagijimana © Doctoral school - University of Burundi

We admit the possibility of dealing with the principle of quantum superposition, it means to reduce the number of quantum binary digit(Qubits) needed to perform a computation, to adapt with a new concept convincing that one object could be in several places or states at the same time, even though reportedly, it seems to be impossible! When I am in Laboratory analyzing medical data, I cannot be at a beach enjoying the floating water and soft wind at the same time. According to the classical physics law, we all have a perfectly defined state[66]. When we are there, we cannot be anywhere else! But on the other hand, when we are in the infinitely small world at the level of atoms, then the rules of the day are completely different. It is not easy to be understood, even very difficult to conceive, however every thing could be possible in the quantum world. The quantum computer, a funny mechanic! How can a particle be in two places or two states at the same time? Example: a living and dead Cat at the same time, a key of our car in two places at the same time and two basketballs always on the same side. We should know that physicists have been trying to explain the phenomena they observed from the origins of quantum physics to the first computer prototype.

I cannot find the key of my car! You haven't seen it by chance? No, there you see, you will find it exactly where you left it. In short, everything that surrounds us has a well defined mass, position and velocity. For example, the key weighs 48 grams, you put it on the living room table and of course its velocity is zero. All these values define the physical state of your key. It has only one perfectly defined state. This vision of the world is clear, our daily objects are well described by the physics known as classical.

But in a world of science fiction, imagine your key being in several places at once, both in living room and in kitchen. This is usually seems impossible for objects on our scale, but it is common for microscopic objects. If we extract for example an atom from your key and isolate it in a free vacuum without light, we observe a situation that requires us to radically change our view of the world.

As answer to the previous question in the first paragraph of this section, the atom can of course be placed in 2 or 3 even an infinite number of places at the same time. The atom is then said to be in a quantum coherent superposition of states. This phe-

nomenon is a particular case of a basic principle of quantum physic, a branch of physics that describes well the microscopic world. At the microscopic scale, the atom has a property that is not equivalent to our everyday life! It behaves sometimes like an atom, sometimes like a wave. When it is not well observed, the atom must be assimilated to a wave. The same atom, is present everywhere at the same time in the same way as water is a fluid present everywhere along a surge.

The development of the quantum computer can be divided into three generation:[67]

i) First Generation: The first-generation quantum computers are developed at the early stage for non-commercial use. These models were built for proof of concept with low to medium complexity.

ii) Second Generation: Many organizations who got the breakthrough in their initial research and possessed the necessary hardware infrastructure could develop the quantum computer with a higher number of qubits and complexity. The second-generation quantum computers are solely designed and developed for commercial applications and high-end research focused on improved scalability and speed. These quantum computers can be rented out for higher computing demand just like cloud computing to serve on a demand basis.

iii) Third Generation: Third generation will be true quantum supremacy as the exponential growth and development will bring down the hardware cost. The quantum computer will be affordable and easily accessible to the mass. The third-generation quantum computer will bring the viable solution across a wide variety of non-commercial applications and it will outperform the classical computer and applications.

There are many technological challenges to the development of Quantum Computer with a higher number of qubits. Initially, the breakthrough research in quantum computing was considerably slow and took significant time to realize the working model. However, in the last few years, there is an unprecedented development[68][69]. Scientists around the world are addressing various challenging issues to develop an affordable quantum computer with higher accuracy.

3.2 Principles of Quantum Computing

Quantum computing is a new emerging field that has the potential to dramatically change the way we think about computation, programming, and complexity. The challenge for computer scientists and others is to develop new programming techniques appropriate for quantum computers. Quantum entanglement and phase cancellation introduce a new dimension to computation. Programming no longer consists of merely formulating step-by-step algorithms but requires new techniques of adjusting phases and mixing and diffusing amplitudes to extract useful output[70].

The computational process manipulates quantum states and obtains desired information by observing the states.

In principle, the power of quantum computing stems from parallel computing taking advantage of three aspects of quantum states: *superposition*, *entanglement*, and *interference*.

A. Superposition: As one of quantum computer fundamental properties leads on quantum mechanics to store, present and perfom operations on data in such away so that it can compute exponentially faster than any classical computer[71].

$$|x\rangle = a|0\rangle + b|1\rangle \tag{3.1}$$

Note that qubits are often written in the braket notation, where the variable name is between a "|" and a "⟩" symbol. The expression in relation 3.1 tells us that the qubit x is in a superposition of the $|0\rangle$ state AND the $|1\rangle$ state. This does not mean that it is in the $|0\rangle$ state OR the $|1\rangle$ state; we don't know its current state. It is really in both states simultaneously, and it can be manipulated as such. Once we measure the qubit, it will be in a single state though, either $|0\rangle$ or $|1\rangle$. In the above expression, there is the additional limitation that $a^2 + b^2 = 1$. The values of a and b are linked to probabilities: there is an a^2 chance that, when measured, the qubit $|x\rangle$ will contain the value $|0\rangle$, and there is a b^2 chance that, when measured, the qubit $|x\rangle$ will contain the value $|1\rangle$. Superposition in quantum computing refers to the ability of quantum system when quantum particule or Qubit can exist in two positions or say, in multiple states at the same time. Let's dig into the following expermentations:

In the first experment, the h gate makes a new state: $|+\rangle = H|0\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$ that is a uniform superposition of the $|0\rangle$ and $|1\rangle$ state. The measurement forces the system to be in ether the $|0\rangle$ state or $|1\rangle$ with an equal probability.

In the second experment, we made a new state: $|-\rangle = H|1\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$, that is still a uniform superposition of $|0\rangle$ and $|1\rangle$ with different sign.

In the last case, we can take the sum of two previous experments $H|0\rangle$ and $H|1\rangle$.

After adding the two experments together, the $|1\rangle$ state cancels out because of the minus sign.

From now , we can see the difference between classical probability p and the quantum amplitudes ψ, which can be positive, negative, or even complex. The relationship between classical probabilities and quantum amplitudes is $p = |\psi|^2$, and is known as Born rule.

Putting all this together gives: $|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$, $|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$, and using $|+\rangle = H|0\rangle$ and $|-\rangle = H|1\rangle$, uniquely defines the Hadamard gate in computational basis by the following matrix:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} \tag{3.2}$$

In many cases, an algorithm has a simple outcome "for example, "'yes' or 'no'", but requires lots of parallel computations. By keeping qubits in a superposition during computations, it is possible to take into account all different options at once. Rather than doing evaluations for every single combination, a quantum computer can execute an algorithm on all options in a single step.

Sum, from the previous relation, you see that qubits can be in the quantum superpositions, and these superpositions can have a sign that leads to interference. The given physical system in a definite state could still befave randomly.

B. Entanglement: Entanglement means that groups of particles are connected and can interact in ways such that the quantum state of each particle cannot be described independently of the state of the others even when the particles are separated by a large distance. One of the most important implications of entanglement is that qubits can be error-corrected, which will likely be necessary for the advent of universal quantum

computing. An application of quantum computing that is already available is certifiably random bits, a proven source of randomness, which is used in secure cryptography. The concept of entanglement may seem strange and abstract, but it plays a crucial role in quantum computing. In classical computing, information is processed using bits that can take on either a value of 0 or 1. In quantum computing, however, information is processed using quantum bits, or qubits, which can exist in a superposition of both 0 and 1 states at the same time. This allows quantum computers to perform certain calculations much faster than classical computers, and entanglement is a key ingredient that makes this possible.

To understand how entanglement enables quantum computing, it's important to first understand the basics of entanglement itself. The concept of entanglement is most easily illustrated using a pair of entangled qubits. Let's say we have two qubits, q1 and q2, and we prepare them in an entangled state. We can represent this state mathematically using the tensor product:

$$|\psi\rangle = (|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle / \sqrt{2} \tag{3.3}$$

Here, $|0\rangle$ and $|1\rangle$ represent the two possible states of a single qubit, and $\otimes$ represents the tensor product operation. The state $|\psi\rangle$ indicates that if we measure the state of q1 to be 0, we know with certainty that the state of q^2 will be 1, and vice versa. This is because the two qubits are entangled in a way that is stronger than any classical correlation.

C. interference: Interference is the situation where intervention from noise in the environment damages the quantum object, and also the possibility that the wave functions of particles can either reinforce or diminish each other.

To illustrate how quantum computers work, imagine that the bits in a computer are coins, and heads and tails are one and zero. In a classical computer, you would lay the coins out on a table, and by moving and flipping the coins according to definitive rules, you would get a final output. This is an example of an idealized Turing machine. In a quantum computer, though, you take the coins and the qubits and throw them in the air, where they spin. When the coins land, you check the heads and tails to get the

answer. Of course, throwing coins randomly in the air and getting random answers is not useful, so quantum computers have more tricks up their sleeves.
Now, imagine the coins are magnets and can stay spinning in the air indefinitely. While in the air, you can do several things to control the coins:

1. The coins can interact with each other, flipping one causes another to flip. This illustrates how quantum entanglement causes qubits to affect each other.

2. You can place other magnets around the coins to cause certain outcomes to be more likely than others. This illustrates how quantum interference can be used to direct outcomes toward the desired output.

3. You can use other magnets to cause certain coins to go through particular spins or have particular orientations. This is like how quantum gates cause changes in a qubit to program their state.

By combining entanglement, interference and gates, you can cause the coins to perform a calculation. When the coins land, they will most likely be in the correct outcome of heads and tails. But, because there is an element of probability present, you may only be 99.99% sure of the results, so you want to run the same process many times to increase your confidence.

3.3 Development of Quantum Computing

Quantum computers are being developed to increase the security rate in communication and computations via decreasing the computational time. The fusion of all the performance attributes in a single quantum computing technique is still ambiguous until now[72]. To build a quantum computer which can perform concurrent operations, it is essential to have a quantum computing technique that can allow quantum I/O with all the necessary classified features. While considerable progress is being made to move quantum computing in recent years, significant research efforts need to be devoted to move this domain from an idea to a working paradigm.

3.3.1 Initial ideas

In 1936 Birkhoff and Von Neumann proposed quantum logic, which is a set of rules for reasoning about propositions which takes the principles of quantum theory into account [73]. However, they did not work out the possibility of realizing a quantum computer. In the year 1980, Benioff wrote about the possibility of constructing a computer based on quantum theory [74]. He described a quantum mechanical computer model in the framework of a Turing machine and suggested using different spins of particles to represent the two binary digits. In 1982, Feynman examined the problem of what kind of computer would be required to simulate physics. He pointed out that quantum mechanical phenomena cannot be simulated by traditional computers and stated that a quantum computer would be required [75]. This is because although natural laws are reversible, classical computation isn't. For instance, if an AND gate gives output 1, it is impossible to determine based on the output the inputs that were originally fed into the AND gate. It can be said that Feynman's most important contribution is outlining the need for quantum computers.

By the late 1990s, most foundational research on quantum computing had been completed, and research on implementation had begun [76]. Gershenfeld and Chuang implemented the first quantum computer in the year 1998 [77]. It was based on nuclear magnetic resonance "NMR" and was limited to 2 quantum bits. In 2001, IBM demonstrated Shor's algorithm to factor the number 15 on a 7-quantum-bit NMR computer [78]. Following the two initial successful implementations described above, there were several breakthroughs with researchers publishing new possibilities for implementing quantum computer hardware and using Shor's algorithm to factorize larger numbers. In 2012, a team at the University of Bristol successfully factored 21 using a version of Shor's algorithm and later the same year Xu et al. factored 143 on a dipolar-coupling NMR system [79], although this used adiabatic quantum computation rather than Shor's algorithm. In 2014, it was discovered that the 2012 adiabatic quantum computation had also factored larger numbers, the largest being 56153 [80]. In subsequent work, issues in the scaling of adiabatic quantum factorization to larger numbers were

addressed, and the factorization of 291311 was achieved in 2017 [81]. One of the most significant challenges in the development of quantum computers is their high susceptibility to errors as compared to classical computers . For instance, errors can be caused by spontaneous emission where the state of a qubit changes spontaneously. An excited qubit representing a binary digit may decay into the ground state and now represent the other binary digit. Research is being conducted on error correction schemes for quantum computers.

Note that Quantum computing does not yet have its own high-level programming language. In the circuit model, the algorithms are processed by constructing quantum circuits which systematically apply available quantum gates or operations to find the desired solution.

3.3.2 Advantages and disadvantages of Quantum computing

Though the most advanced version of this technology is still far from being competitive with classical computers, there are a number of benefits and advantages that make it worth keeping an eye on. This section will list the main advantages and disadvantages of quantum computing.

A. Advantages of Quantum Computing

1. *Fastest Calculations:* A quantum computer is capable of solving problems faster than other computers. For instance, it can solve highly complicated mathematical problems in a matter of seconds that would take a classical computer thousands of years to do. This is what is meant by the term quantum speed-up. Quantum computers can break some of the most complex encryption codes.

2. *Storing and Retrieving Data:* A quantum computer can store, retrieve, and process large amounts of information in a fraction of the time needed by digital computers. It is possible to do this because a quantum computer deals with qubits instead of bits.

3. *High Privacy:* A quantum computer is highly confidential and secure. It uses the phenomenon of superposition to form the supercomputer that makes hacking impossible. They are also ideal for storing and managing passwords and cryptographic keys

without fear of being hacked or intercepted by hackers. Quantum computers will help to create new methods of Internet security, which is one of the main purposes of quantum computing.

4.*Used in Artificial Intelligence:* Recent developments in quantum physics show that quantum computers will play a crucial role in future artificial intelligence developments. Quantum computer systems can provide the basis for solving some of the most challenging problems in artificial intelligence.

5. *Machine Learning:* Quantum computers are used in machine learning. It is a computer science approach that's based on the idea of artificial intelligence. Computer scientists use this technology to perform image recognition, speech processing, computational linguistics, and pattern recognition.

6. *Healthcare:* Quantum computing can speed up making vaccines and medicines, help doctors figure out what's wrong with a patient sooner, and customize treatment. Scientists will be able to test molecules, though, if they have quantum computers. Scientists will be able to run simulations of even single molecules on quantum computers that are very accurate.

B. Disadvantages of Quantum Computing

1.*Cost:* The first disadvantage is that quantum computers are extremely expensive. The materials used to create them can be costly.

2.*The low Temperature Needed:* Quantum computers require extreme temperatures that are hard to keep. It can't be isolated from its environment because it has to interact with the environment. If it interacts with the environment, it will lose its quantum nature. This is why quantum computers need to operate at incredibly low temperatures.

3. *Fragility Problems:* Apart to extremely difficult to program and control, quantum computers are very fragile. They break easily because of their environment. The smallest amount of heat can destroy the computer, and this is an issue. When the information is saved and retrieved, it needs to be very accurate. If there is any change in the information, it needs to be rewritten because it won't work with the same

software.

4. *Difficult to Build:* It is difficult to build a quantum computer because the researchers need to find a way to get the qubits accurate. Quantum computers cannot be run on traditional computers. Software, algorithms, and programs are needed to work with these computers. There is a lot of work that needs to be done for the computer to run correctly.

Quantum computers will revolutionize almost every aspect of life. It will be used in many fields such as medicine, artificial intelligence, defense and so on. The changes that quantum computers will bring will completely change our view of the world.

3.4 Quantum Computer prototype Modeling

In this section we identified the gape between classical computer and the quantum one . Classic computers use binary code to operate. A quantum computer uses atoms to encode information. In quantum theory atoms behave differently when treated in certain ways. So the process known as superposition is based on the mind-boggling principles that an atom can be in two different places at the same time; The short quantum simulation algorithm has been also proposed.

This new invention allows actual quantum bits to be transmitted between individual modules in order to obtain a fully modular large-scale machine capable of reaching nearly arbitrary large computational processing powers.

Most classical computers operate on Boolean logic and algebra, and power increases linearly with the number of transistors in the system – the 1s and 0s. The direct relationship means in a classical computer, power increases 1:1 in tandem with the transistors in the system.

Since the quantum computer is based, as its name indicates, on quantum mechanics, we prefer to go back to the essential notions of quantum mechanics and quantum computing[82]. The power of quantum computing is estonishing and not many people benefiting from the full potentialities it has to offer. We look first at what makes quantum computing different from today's common place classical computing. Quan-

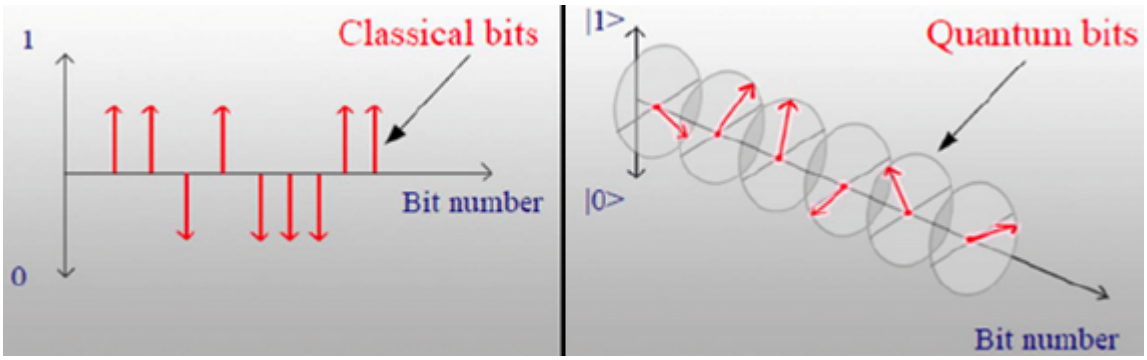


Figure 3.1: Graphical representation of BITs alongside QUBITs.

tum Computer uses quantum bits QUBITs and they are distinguished from classical BITs by their properties. The qubits obey all the rules of the quantum physics and ,in particular, principle of superposition $|0\rangle + |1\rangle$, that means they can take all the values at the same time. Quantum computers typically must operate under more regulated physical conditions than classical computers because of quantum mechanics. Classical computers have less compute power than quantum computers and cannot scale as easily. They also use different units of data.

In classical computers, algorithms need a lot of parallel computations to solve problems. Quantum computers can account for multiple outcomes when they analyze data with a large set of constraints. The outputs have an associated probability, and quantum computers can perform more difficult compute tasks than classical computers can.

Quantum programming languages are essential to translate complex ideas into instructions to be executed by a quantum computer. They facilitate the discovery and development of new quantum algorithms, as well as executing the existing ones[83]. Classical and quantum computers have many differences in their compute capabilities and operational traits. The following table shows what makes quantum computing different from conventional or classical computing [25]. .

Classical Computing	Quantum Computing
1. Calculates with Transistors which can represent either 0 or 1.	1. Calculates with Qubits,which can represent 0 and 1 at the same time.
2. Power encreases in a 1:1 relationship with the number of transistors.	2. Power encreases exponantially in proportion to the number of qubits.
3. Classical Computers can operate at room temperature.	3. Quantum Computers need to be kept ultracold.
4. Most every day processing is best hundled by classical Computers.	4. Well suited for tasks like optimization problems, data analysis and simulation.
5. Only specifically defined results are available, inherently limited by algorithm's design.	5. Quantum answers are probabilistic because of suporposition and entanglement, multiple possible answers are considered in a given computation.

Table 3.1: Comparison between Quantum and Classical Computer

The current researches allow to better understand this quantum universe and more necessarily they open the life to a new technological revolution.

3.4.1 Qubits modeling

(a) The Qubit (quantum binary digit): is the basic unit of quantum information. It is a quantum system with two states, which means that it evolves in a Hilbert space of dimension 2. While a classical bit can take the values 1 and 0, a Qubit can rather be, in an analogous way, in two states, but also in a superposition of both states: $|0\rangle$ and $|1\rangle$. This is what differentiates the *classical bit* from the *quantum bit*. Instead of just two values, we have a vector with two components, and single qubits operations:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{3.4}$$

The state of a qubit is generally noted as follows:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle; \tag{3.5}$$

where α and β are coefficients such that : $|\alpha|^2$ is the probability of being in the state$|0\rangle$ and $|\beta|^2$ that of being in the state $|1\rangle$. In the real world where bits are perceived as 0 or 1, only one of the four possible states 01 , 00 , 10 , 11 can exist at any time in space. However in a quantum superposition state, all four of the possible states can coexist in time and space simultaneously. It is in this principle of quantum superposition that the interest of quantum computation lies.

(b) With two Qubits: Qubits are the indivisible units "atoms" of quantum information. Let us examine the case of two qubits. Consider now electons in two hydrogen atoms.



Figure 3.2: Atoms.

Classically, the two electrons are in one of four states: 00, 01, 10, or 11 and represente two bits of classical information. But Quantum mechanically, they are in a superposition of those four states: $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle| + \alpha_{11}|11\rangle$; where $\sum_{ij} |\alpha_{ij}|^2 = 1$.

The two-qubits in the most general case where the qubits that are different from each other. The spectrum of the system in the ultrastrong-coupling regime is shown to converge to two forced oscillator chains by perturbation theory.
The imagery of atomism in modern physics moves from atoms of matter or energy via "atoms" *quanta* of action to "atoms" *qubits* of quantum information. This is a conceptual shift in the cognition of reality to terms of information, choice, and time.

3.4.2 Qubit Logic Gates

Since we know what qubits are, we need to know how to manipulate them. This means taking a quantum state as input and obtaining another quantum state as output, because this is what a computer does. To do this, we use Quantum Logic Gates which are the analogue of the logic gates which constitute quantum computers. Since our qubits $|0\rangle$ and $|1\rangle$ can be represented by column vectors as explained before, we can thus represent the NOT gate by a matrix X as follows:

$$X = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{3.6}$$

we then see directly that:

$$\alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \Leftrightarrow X \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \tag{3.7}$$

$|\psi\rangle = \alpha_{00}|\uparrow\uparrow\rangle + \alpha_{01}|\uparrow\downarrow + \alpha_{10}|\downarrow\uparrow\rangle|\alpha_{11}|\downarrow\downarrow\rangle\rangle;$

In fact, we can always represent a quantum logic gate by a matrix. This comes from the linearity of the equations determining quantum mechanics. In order to perform any algorithm in quantum system, there must be operations that correspond to some universal set of quantum gates. These criteria can be used to test the adequacy of realisation of a quantum computer.

3.4.3 Extraction of information from quantum states

To obtain desired information from qubits, the qubits must be observed. When a quantum state is observed, it converges to a classical state probabilistically, and the observer obtains the corresponding outcome.At this moment, the quantum state loses the information on other classical states and the observer can never retrieve them again. As this indicates, the amount of information obtained from qubits is limited in principle. For instance, in the case of a quantum state of n qubits in which each state shares the equal observation probability, only one of 2^n possible states can be obtained from a single observation. It should be noted that the amount of information obtained by a

single observation from qubits equals that from classical bits. Moreover, the observed state is randomly determined and cannot be selected arbitrarily by the observer. Thus, if there is only one state corresponding to a correct answer out of 2^n states and any of the states are observed with equal probability, then the probability of obtaining the correct answer by observation is $1/2^n$. This means that the efficiency of naive quantum computation does not necessarily exceed that of classical computation. Thus, quantum computations using only superposition do not accelerate calculations. Quantum computing accelerates computation by efficiently extracting information corresponding to the solution of a problem from qubits. Such efficient extraction is enabled by running quantum algorithms, which ingeniously amplify/attenuate the probability of observing the state corresponding to the desired/undesired information for arbitrary input quantum states. In the process of manipulating the observation probabilities, the "quantum entanglement" and the "quantum interference" play essential roles. The entanglement indicates that the entangled states correlate with each other in terms of their observed outcomes. The interference, which amplifies/attenuates the observation probabilities of multiple quantum states, takes advantage of the wave nature of the quantum states.

3.5 Large scale Computer Prototype

To build a large scale of quantum computing that can efficiently impliment quantum properties in its operation is a great challenge for researchers[84]. One of the most challenging problem is that the quantum information is quickly lost during operations due to the decoherence. So, it is not easy to construct a large scale of quantum computation with a large quantity of Qubits. The proposed solution to this problem is to find a way on how to minimize the total volum of physical hardware for topological quantum computation.

Today's quantum computers look like large containers suspended from the roof, cooled to near absolute zero (-273.14 °C), with hundreds of cables hanging from them[85],Fig.(a). Fugure(b) also describes the architecture of Quantum calculator and the implementation of its work in order to overcome its common technical problem. Especially, com-



Fig.(a): QC view

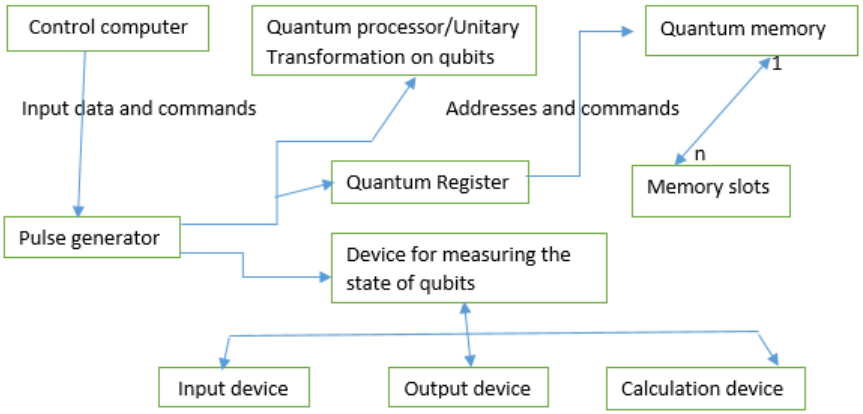


Fig.(b): Quantum computer architecture.

puter capability has the potential to challenge the way we use encryption to secure much of our digital life, whether it is the protection of confidential data, the privacy of our online communications.

The encryption and decryption system is composed of a quintuplet[86]; example:

$(P, C, C_k, D_{k'}, K)$ o:

-P is a set called clear text space(plain text)

-C is a set called space of cipher text

-K is a set called key space

-Gen_k a key generation algorithm (= the elements of K);

-C_k: $P \rightarrow C$ is a left invertible function called the encryption function and which depends on a parameter k called key;

-$D_{k'}$: $C \rightarrow P$ is a left invertible function of C_k (i.e $D_{k'}$ o $C_k(m) = m, \forall m \in P$) and is called the decryption function (depending on the key k') .

Unlike a classical computer, a quantum computer can therefore calculate several values at the same time

By Ecnrypting the Quibit in relation(3.3), we consider an operation where an attacker can not determine the probability emplitude of the number of measurements already performed[87]. Once the key generation procedure is defined, we can also define the qubit encryption procedure.

Suppose Alice wants to encrypt the qubit in the relation(3.3) for Bob. Encryption is

done as follows:

1) Alice generates randomly a set of r natural numbers ranging from 1 to n. This set is noted with R=$\{r_0$,r_1,...$r_n\}$, $1 \leqslant r_i \leqslant n$.

2) We denote with U_R, the composition with the transformations U_{r_1},U_{r_2},...U_{r_n}. Alice applies the transformation U_R to the Qubit in relation(3.3).

The Qubit new state (encrypted) is now $|\psi\rangle = U_R|\psi\rangle$. Alice sends then Bob via an unsafe channel the Qubit in its new state(encrypted).

Encryption of a qubit is a cryptographic operation that does not allow an attacker to access a probability amplitudes that define the superposition of the qubits. The encryption operation assures that the attacker can not reconstruct through quantum tomographic the content of message during its transmission.

3.6 Quantum Computer Efficiency proof

It is already known that quantum computer relies on Qubits[88] to run and solve multidimentional quantum algorithms to conduct measurements and observations. I am looking for the book. Don't you know where it is stored? No, but you have to find the answer with the computer in this library. Careful, I will tell you how it works! First of all, you must know that a classic computer uses a particular language "binary language" that is to say for image, sound, video issue, text, even the titles of books in this library. In short, all information stored and processed by a computer are translated into a sequence of 0 and 1, each 0 and each 1 is called a BIT, these sequences of 1^s and 0^s are filed in a numbered memory with specific addresses, as the address that indicates where you live for example.

But what does this computer do with these 1^s and 0^s at this or that address? Well, it adds them, multiplies them or even compares them via small electronic circuits called "Logic Gates" as seen before. These gates perform all sorts of simple logical operations; they deliver themselves as a result in form of a 1 and a 0. But, this still doesn't tell me how these logic gates will find the location of my book? To understand this, let's take the title of the book you are looking for:

-The computer saves it in a box in its memory;

-In other boxes the titles of the books are already recorded;

-Each one has an address corresponding to its place in the library;and

-The computer will use a network of logic gates to compare the Bits of any of each title in the list. This gate array is often called ORACLE.

An oracle gate in quantum gate is usually a "variable" gate. It enables the encoding of a problem instances and representes in this way the input of a quantum algorithm. By using a quantum type, it must be an intervention of quantum bits so called q-bits and they are distinguished of course from classical bits. These q-bits obey all the rules of quantum physics and in particular principle of superposition. With this new paradigm, our logic gate array is called q-Oracle. According to the following example, q-oracle will be responsble to find the location of the book in the Library. According to this quantum mechanic, the needed book has been found at the position number 2 on the first floor up of this Library(Fig.3.3). It is therefore very necessary to respect

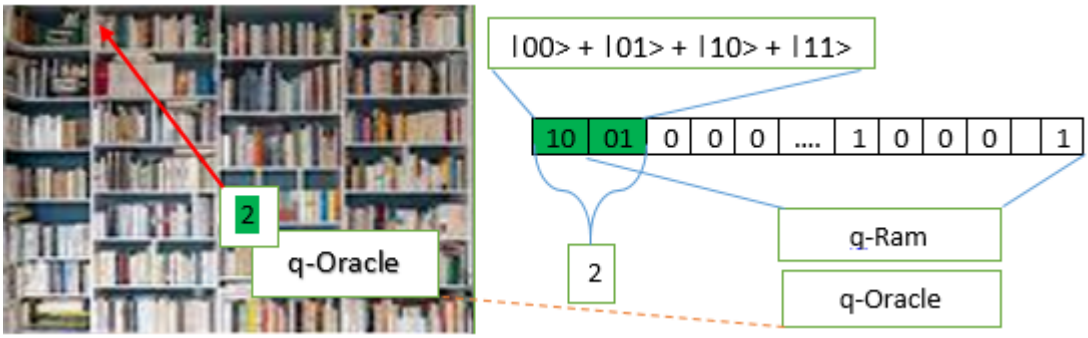


Figure 3.3: Book searching from Library via q-Oracle.

the algorithm if one wants to be totally certain of the answer. Anyway, the Quantum Computer remains efficient to solve some mathematical calculations which become impossible to solve using classical computers beyond a certain volume of data.

3.7 $\mathcal{R}2022\mathcal{A}^+$ Algorithm

The construction of quantum computers represents many challenges but also potential major contributions both technologically and theoretically. Most of the applications of quantum computers concern computer science and algorithms. Even in information security, encrypted data to be vulnerable to a quantum computer they must become first discoverable and exposed to a quantum cryptographic algorithm.

Quantum algorithms require a different way of thinking than a way one normally approaches programming. It is not possible to store quantum states on a working memory for accessing later in the algorithm[89][90]. This is due to the so called *no-cloning* principle of quantum physics. It is not possible to make a copy of quantum system. But it is possible to move the state of a set of qubits to an other set of qubits.

Quantum algorithms are already being applied in a variety of industries including healthcare, finance, manufacturing, cybersecurity, and blockchain. Optimization problems for scheduling and route planning, search algorithms, sampling and pattern matching, quantum encryption are a few of them.

Besides, advertisements strategy and product marketing, software verification, and validation are much easier with emerging quantum computing[91]. Quantum algorithm consists of thee basec steps:

a) Encording of data, which could be classical or quantum into the state of a set of input quibits;

b) A sequence of quantum states applied to this set of input quibits;

c) Meseaurement of one or more qubits at the end to obtain a classical interpretable results.

As with all types of quantum algorithm, an extra step is required in the processing to concentrate the information we want into the register for the final measurement. Particularly for quantum simulation, amassing enough useful information also typically requires a significant number of repetitions of the simulation. Classical simulations of quantum systems are usually "strong simulations" which provide the whole probability

distribution, and we often need at least a significant part of this, e.g., for correlation functions, from a quantum simulation. If we ask only for sampling from the probability distribution, a "weak simulation", then a wider class of quantum computations can be simulated efficiently classically, but may require repetition to provide useful results, just as the quantum computation would.

Through the $\mathcal{R}2022\mathcal{A}^{+}$ Algorithm quantum computer can perform the simulation of dynamic much more efficiently. Quantum simulation seems to be an important application of Quantum Computer.

A quantum computer similation means "*predicting*" the state of a system at some functional time t_f as efficientely as possible given an initial system state. Let the n-qubit $|\psi\rangle$ approximate a given system. Then, the quantum computer similation algorithm can be presented as follows:

Algorithm 1 : $\mathcal{R}2022\mathcal{A}^{+}$ Quantum Simulation

Input:

$\psi_0 = 10, \ \varepsilon_0 = 10^{-1000}$

maxiter $= N$

Time step size Δt , t_f

Output:

$|\psi_{t_f}\rangle$, t_f

Step1:

For $1 \leqslant$ j $\leqslant$ N *do*

$|\psi_{j+1}\rangle = \Delta t \ |\psi_j\rangle$;

$j = j + 1$;

Step2:

$if \ \ j\Delta t \leqslant t_f, \ \ \frac{|\psi_N - \psi_{N-1}|}{N+1} \leqslant \varepsilon_0$;

write $|\psi_{t_f}\rangle$;

End For

else

return to step 1.

The purpose of $\mathcal{R}2022\mathcal{A}^{+}$ algorithm was to give a proof of concept of how quantum computer perform based on how the state of its system at some functional time regarding to simulation state and the process . Each step presents the simulation in practice consistent with the theory and literature.

Quantum Computing and algorithms meet some specific requirements such as the number of qubits, fiting of hardware architecture and will have a brighter common future. Algorithms could be implemented so that they can run and be tested on quantum computer. Especially, a good quantum algorithm solves the order finding problem during data processing partucularly under a quantum system.

Chapter Four

Random Number and Key Generation

Contents

4.1 Introduction 65

4.2 The evolution of random number generation 67

4.3 Architecture of proposed mechanism 73

4.4 Description of experimental environment 78

4.5 Results analysis and discussion 80

4.1 Introduction

Randomness[1] is produced by generating a sequence of independent uniform variates and transforming them in an appropriate way. It is still with impotance to better examine practical ways of generating "nondeterministic approximations to" such non-uniform variates on a computer and compare them in terms of implementation, efficiency, theoretical support, and statistical robustness. We look in particular at several classes of generators, the entropy descraption, classification and technology, advantages and limites and make a comparative studies of mechanisms to describe good result for random numbers generation. Then, to mention other classes of generators like pseudo-random number generation, discuss other kinds of theoretical and empirical statistical tests, and finally analyse the results[92][93]. Random number generation(RNG) became important in cryptographic systems; it is used for the generation of session keys, challenges in cryptographic protocols or padding of plain text messages.

[1]In common usage, randomness is the apparent or actual lack of definite pattern or predictability in information.

Protais Ndagijimana © Doctoral school - University of Burundi

In this chapter, we propose a random number generation model using the thermal noise theory. The power is evaluated by sampling the temperature in non-equilibrium state according to Fourrier's law [94]. For a sampling period (t) with $t\varepsilon[0;+\infty[$, we will prove the diffuclty or impossibility for an attacker to determine exactly the variations of the temperature (ΔT_i); so the sequences of generated numbers. There are two main types of random number generators: true random number generators and pseudo random number generators.

A RNG that does not conform to this act may not be legally used for gambling business. These rules have been put forward in order to ensure fair game by providers and to prevent possibility that gamers manipulate the system by foreseeing outcomes.

Random number generators have been an occupation of scientists and inventors for a long time. Whole branches of mathematics have been invented out of a need to understand random numbers and way to obtain them. In early seventies, at the dawn of modern computing era, John von Neumann was one the first to note that deterministic Turing computers are not able to produce true random numbers and put it in his well-known statement that any one who considers arithmetical methods of producing random digits is, of course, in a well defined state. Random number generators are one of the hottest topics of research in the last decade[95].

There are very many constructions or true RNGs and research is still getting impetus[2], but in our view one can roughly classify the present art in four families[95]:

- noise based RNGs;
- tree running oscillator RNGs;
- chaos RNGs;
- quantum RNGs.

[2]catalyst impulse incentive momentum motivation stimulant.

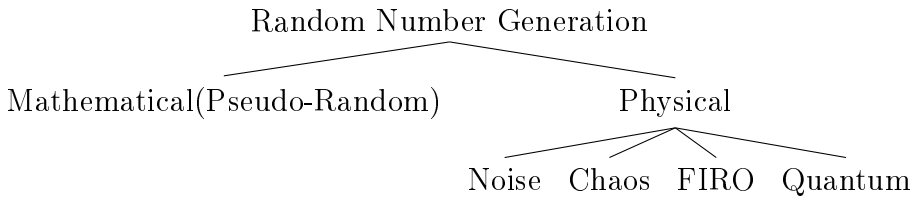


Figure 4.1: Classification of random number generators

Mathematically, pseudo random generators can also be divided into several categories depending on type of the algorithm used.

4.2 The evolution of random number generation

The evolution of random number generation has been a fascinating journey, marked by significant leaps in technological advancements. From classical methods to the contemporary quantum techniques, this evolution has been pivotal in various fields, including cryptography, simulations, and gaming.

In the classical era[3], random number generation was a physical process. It involved flipping coins, rolling dice, or drawing lots. These methods, though simple, were time-consuming and had limitations in generating large sequences of random numbers. With the advent of computers, pseudo-random number generators (PRNGs) were introduced. PRNGs are algorithms that use mathematical formulas or precalculated tables to produce sequences of numbers that appear random. They start from an arbitrary starting state using a seed state. Despite their efficiency and speed, PRNGs are deterministic in nature. Given the same initial seed, they will always produce the same sequence of numbers, which is a significant drawback in areas where unpredictability is crucial.

In the late 20th century, the development of true random number generators "TRNGs" marked a significant milestone. Unlike PRNGs, TRNGs generate random numbers from

[3]From classical methods to the contemporary quantum techniques, this evolution has been pivotal in various fields, including cryptography, simulations, and gaming. In the classical era, random number generation was a physical process. It involved flipping coins, rolling dice, or drawing lots.

a physical, rather than a deterministic[4] process. They utilize natural phenomena such as atmospheric noise or radioactive decay, which are fundamentally random. However, TRNGs are slower and more resource-intensive than PRNGs, and their output can be difficult to verify for randomness.

4.2.1 True Random Number Generator

A True Random Number Generator (TRNG) is a device able to produce a sequence of numbers for which there is no known deterministic link paradoxically to the pseudo-random number generator[96]. According to Stipcevic and Koç, it follows that a true random numbers is a sequence of numbers for which there is no deterministic algorithm[97].

In computer science, a hardware random number generator is a device that generates random numbers from a physical phenomenon rather than use of a computer program [98][99][100][101]. These systems are in most cases based on laws of quantum physics and proven random phenomena. Several techniques exist for the generation of these random numbers whose properties are widely used in cryptography.

TRNG is always important for information encryption and decryption, numerical simulations, lottery games and stochastic experiments. True Random Number generators are a fundamental resource in information security and can guarantee the absolute security of information in principle. Entropy[5] source is the most critical part of TRNGs, which provides the unpredictability and is the root of security for TRNGs. Electrical noise, which is inevitable and unpredictable in electronic systems, is always used as entropy source for TRNGs. This review discusses the different methods to harvest electrical noise in TRNGs, including the early amplify noise based on amplifier, phase jitter based on oscillator, the effect of electrical noise on the metastable behav-

[4] In mathematics, computer science and physics, a deterministic process is a process in which no randomness is involved in the development of future states of a given system. A deterministic model will thus always produce the same output from a given starting condition or initial state.

[5] The measure of a system's thermal energy per unit temperature that is unavailable for doing useful work.

ior and amplify noise based on chaos circuits. The emergence of quantum computers exposes classical cryptosystems. These cryptosystems whose semantic security is based on difficult mathematical problems and algorithmic complexity become vulnerables. This challenge to the fundamentals of symmetric and asymmetric cryptography worries the researchers. It leads to the rise of quantum and post-quantum cryptography [102]. However, post-quantum cryptography implemented through NP-complete problems[103] cannot guarantee perfect secrecy [104]. A promising related theory is the generation of random numbers associated to quantum physical phenomenon. The aim is to exploit the laws of quantum physics associated to basic principle of cryptology for the implementation of new cryptographic primitives.

Noise refers to all harmful signals that overlap with the useful signal at any point in a measurement chain or transmission system. The useful signal represents the information, while noise is a hindrance to understanding the information conveyed by the signal. In electronics, it presents interesting properties due to its randomness. According to Johnson-Nyquist work [105][106], we define thermal noise as the noise generated by the thermal agitation of charge carriers. In other words, that is electrons at thermal equilibrium in electrical resistance. It is expressed:

-when we evaluate the noise across resistor by:

$$\bar{\nu}_b^2 = 4KTR\Delta F; \tag{4.1}$$

with:

$\bar{\nu}_b^2$: Voltage variance across the resistor,

K: Boltzmann constant,$K = 1.3806 \times 10^{-23} J.K^{-1}$,

T: resistor absolute temperature expressed in kelvin,

R: resistance expressed in Ohms,

ΔF: bandwidth expressed in Hertz.

This application enables to predict the minimum noise in electronic system and its detection limit:

-when we evaluate the power of thermal noise by:

$$\eta_0 = KT\Delta F; \tag{4.2}$$

with:

K: Boltzmann constant, $K = 1.3806 \times 10^{-23} J.K^{-1}$,

T: conductor temperature expressed in Kelvin,

ΔF: bandwidth in Hertz,

η_0: thermal noise power, expressed in Watt.

Thermal noise is inevitable and unpredictable in electronic systems and has quite important characteristics when Shannon theory is associated it[107]. Indeed, by considering the noise as information source, it is possible to evaluate the quantity of derived information. In cryptography, this quantity of information is an entropic source for true random numbers generation.

As mentioned above, TRNGs are entirely based on a physical process yielding a significant degree of entropy that is captured and digitized. Three main techniques were reported in the literature for creating TRNGs:

- Oscillatory metastability: It can be exploited for a random number generation in different ways: e.g. capturing the transitional waveforms or just measuring the time till settling (by counting pulses).

- Direct amplification of the noise that is intrinsic in analog signals: this method relies on the amplification of the shot noise, the thermal noise, the atmospheric noise or the nuclear decay. The noise is amplified and then, using comparators and analog-to-digital converters, bits are then "extracted" from it;

- Chaos-based TRNGs: this method is based on a well-defined deterministic analog signal that exhibits chaos. Existing implementations exploit Markov's chaotic sources theory and use mixed analog-digital chips.

When building a cryptographic system, it is very important to make it tamper resistant. By combining an analog part with a digital one, its vulnerability to attacks increases; that is why, it is preferable to embed the whole TRNG in a single chip. Through Table 4.1: we make a comparative study of mechanisms of which entropy describe good results for true random numbers generation.

Classification		Technology	Advantages	Limits
Amplify Noise		Analog	Simple structure	High energy consumption
Oscillator	Couple Oscillator	Digital	Easy integration	Vulnerable to frequency attacks
	Ring Oscillator	Digital	Good portability	Hermetic
	FIRO/GARO	Digital	More sensitive to jitter	Vulnerable to feedback connections leading to arbitrary output
Metastability		Digital	Easy integration	Sensitive to physical phenomena and vulnerable to symmetry of metastability
Chaos	Continuous Time	Analog	High rate	High energy consumption
	Discret Time	Digital	High rate	Finite computable precision with a pseudo-random output

Table 4.1: Comparative study of the mechanisms leading to true random numbers generation.

Scott A. Wilber proposes a mechanism for non-deterministic random numbers generation[99]. It uses an electronic assembly of two oscillators producing output signals, of which one is multiplexed. The processor extracts the entropy resulting from the fluctuation during successive emission of signals by the two oscillators for true random numbers generation. The author mention that random number generators use physical sources of entropy evaluation. This value is then used as information source for true random numbers generation. Thus, it is possible to establish a hypothesis between the entropy and its evaluation sources. However, we estimate that Scott A. Wilber's approach inherits the limits of the oscillatory phenomena due to periodic properties of these phenomena. Indeed, study and determination of the frequencies of emitted signals by each oscillator influence the entropy. The device is therefore vulnerable to

side channel attacks. Let's consider g, as the fluctuation between two signals according to time t and respectively frequencies f_1, f_2, if:

$$\lim_{t \to +\infty} g(t) = 0; \tag{4.3}$$

an attacker who studies behavior of the system, could compute the entropy accurate values. Therefore, they are many theories and implementation for true random numbers generation[108][109]. Despite research efforts, the weaknesses persist and the semantic security still a great challenge due to advances in the implementation of quantum computers and side channel attacks. So, new theories need to be developed! Most of all, researchers hope that quantum computers will take artificial intelligences (AI) a big step forward. These could then safely and reliably take over tasks such as data evaluation or forecasting in the future.

4.2.2 Pseudo-random Number Generator

Pseudo random number generators (PRNGs) are initialized with an externally generated sequence and they produce a much longer sequence in a deterministic manner, i.e. if the generator is initialized with the same seed value, it will always produce the same result. PRNG are well known in the art. Surveys and individual examples of PRNGs can be found anywhere [110][111]. Pseudorandom number generator is nothing more than a mathematical formula, which produces deterministic, periodic sequence of numbers, which is completely determined by the initial state called seed[6]. By definition such generators are not provably random. In practice, PRNGs feature perfect balance between 0's and 1's "zero bias" but also strong long-range correlations, which undermine cryptographic strength and can show up as unexpected errors in Monte Carlo calculationsand modeling. While most modern PRNGs pass all known statistical tests, there are myths about some PRNGs being much better than the others.

In any case, due to strict determinism of PRNG algorithms, no PRNG is random

[6]Frequently, the initial seed is either a predetermined value or it is obtained from the built-in clock in the computer. Then, based on this seed, a process determines the next "random number". Using that number as the seed the next time, another random number is generated, and so forth.

by any reasonable definition of randomness. Let us illustrate this by the following example when Alice wanted to impress Bob. She claimed that the true random numbers would be produced, by asking him to test them. Bob agreed but asked a minimum of 1 Giga bytes of random data to be sent to him via e-mail. Alice produced the huge file but her mailing program refused to send such a big file. Cutting a file into small pieces and sending multiple e-mails was an option but too big a nuisance for both of them. Finally, Bob received from Alice a 1kilo byte e-mail containing the following short notice: Dear Bob, Please find attached a program in C++. Compile it, use the following seed: *12345678* and stop the program after producing 1Giga bytes of data. That is what I wanted to send you. Instead of reproducing the file and running on his computer very time consuming tests, Bob shortly answered: Dear Alice, if you think that 1Giga bytes of truly random data can, under any circumstances, be compressed without loss to just 1000 bytes, than I have nothing more to say to you !

4.3 Architecture of proposed mechanism

The true random number generators help to ensure the security of cryptographic and communication systems by the generation of different session keys. Every true random number generator follows generic architecture. Some correction techniques are usually used for approach real noise[7] source properties to ideal noise source properties. TRNGs are implemented into some miniaturized devices and therefore it is important to use noise source which is possible to implement on chip for analog non-deterministic signal generating. The aim of section was proposal and realization of the random number generator with direct amplification of analog noise that creates stable base for future research in the sphere of the true random number generators. This mechanism uses the fundamentals of thermal noise theory which is a random phenomenon[8].

[7] A noise generator is a circuit that produces electrical noise "i.e., a random signal",they are used to test signals for measuring noise figure, frequency response, and other parameters and are also used for generating random numbers.

[8] A physical random number generator can be based on an essentially random atomic or subatomic physical phenomenon whose unpredictability can be traced to the laws of quantum mechanics.

In this section, we present logical structure of the proposed true random number generation mechanism. Also we perform the tests.

4.3.1 Logical structure

The logic behind a random number generator involves ensuring that the generated numbers are statistically independent and uniformly distributed, meaning that each number has an equal chance of being selected.

Most computer generated random numbers use RNGs which are algorithms that can automatically create long runs of numbers with good random properties and eventually the sequence not repeats "or the memory usage grows with bound". These random numbers are fine in many situations and are as random as numbers generated from electromagnetic atmospheric noise used as a source of entropy. The series of values generated by such algorithms is generally nondetermined by a fixed number called a seed.

Let consider an embedded system in non-equilibrium state. Its density is given by:

$$\rho = \frac{m}{v}; \tag{4.4}$$

with:

ρ: density expressed in $kg\ m^{-3}$,

m: mass expressed in kg,

v: volume expressed in m^3 .

According to Fourier's law[94], this non-equilibrium state generates a variation in temperature and creates a heatflow defined by:

$$F = I \times S \times GradT; \tag{4.5}$$

with:

F: heatflow in Watts,

S: plane area expressed in m^2,

I: thermal conductivity expressed in $W.m^{-1}.k^{-1}$,

$GradT$: temperature gradient expressed in $k.m^{-1}$.

$Let's$ consider:

a volume element of embedded system defined by:

$$\nu = \iiint_{\sum} dxdydz; \tag{4.6}$$

T: the temperature according to time (t) and space (ν). We evaluate it considering two parameters:

-time(t): it is sampling period of temperature;

-volume element (ν): it is the volume element considered during temperature evaluation. The evaluation of thermal noise power in relation to its volume element is defined by:

$$P\nu = K\Delta T\Delta F; \tag{4.7}$$

with:

K: Boltzmann constant,K= 1.38 $\times 10^{-23} J.K^{-1}$,

ΔT: volume element temperature expressed in Kelvin,

ΔF: bandwidth expressed in Hertz,

Pν: thermal noise, expressed in Watt.

Let consider:

$P_e\nu$ and $P_d\nu$ respectively as the integer part and the decimal part of the thermal noise power.

TRNG as the concatenation of $P_e\nu$ and $P_d\nu$ ($P_e\nu||P_d\nu$)such as :

$$TRNG_i = P_e\nu_i||P_d\nu_i; \tag{4.8}$$

where $TRNG_i$: the sequence of random numbers generated and $i\ \epsilon[0;+\infty[$ the clock step of each temperature evaluation. Also, we describe through an algorithm, the proposed mechanism for true random numbers generation.

Algorithm 2 True Random numbers generation

Input:

$lenghtVariation$ dx,

$widthVariation$ dy,

$heighVariation$ dz,

$frequencyRange$ ΔF,

$samplingTime$ t

Output:

$volumeElement$ ν_i,

$temperatureVariation$ ΔT_i,

$thermalPower$ $P\nu_i$;

$trueRandomNumberGeneration$ $TRNG_i$,

$integerPart$ $P_e\nu_i$,

$decimalPart$ $P_d\nu_i$

Begin:

1. $\nu_i \leftarrow 0$; //Volume element initialization
2. $\Delta T_i \leftarrow 0$; //Temperature initialization
3. $For\ t\ \varepsilon[0; +\infty[\ ,\ i\ \varepsilon[0; n]i++$
4. $\nu_i \leftarrow d_x\ d_y\ d_z$; //Volume element determination
5. $While\ \nu_i > 0$
6. $P\nu_i \leftarrow K\Delta T_i\Delta F$; //Thermal power evaluation
7. $P_e\nu_i \leftarrow integer(P\nu_i)$; //retrieval of integer part
8. $P_d\nu_i \leftarrow P\nu_i - P_e\nu_i$; //retrieval of decimal part
9. $TRNG_i \leftarrow P_e\nu_i||P_d\nu_i$; //True random number generation
10. $End\ while$
11. $End\ for$

End

4.3.2 Security proof

We evaluate the robustness of the proposed mechanism through the notion of entropy derived from Shannon[112] and Yamamoto [113] and the constraints to which the model is subjected:
- the numbers are generated following the measured temperature (ΔT_i) within each volume element (ν_i) of the proposed device;
- the measured value determines the power ($P\nu_i$) of the thermal noise.

Letnote respectively: X,Y,Z the random variables associated to the sources ($P\nu_i$),(ΔT_i), (ν_i) and $H(X)$, $H(Y)$, $H(Z)$, their entropies.

Let consider the determination of the thermal noise power of a volume element as a source of information. Its probability and entropy follow respectively the relation:

$$P(X = x_i) = P(Y|Z); \tag{4.9}$$

$$\begin{aligned} H(X = x_i) &= -\sum_x P(X = x_i) log(P(X = x_i)); \\ &= -\sum_x P(Y|Z) log(P(Y|Z)) \text{ (By identification following to (4.10))}; \end{aligned} \tag{4.10}$$

with: $P(Y|Z) = \frac{P(Y \cap Z)}{P(Z)}$.

For an infinity of volume elements(z), $z \to +\infty$:

$P(Z = z_i) \to 0$ (equiprobability); (a)

$P(Y \cap Z) \to 0$ (nonequiprobable due to the source $(Y = y_i)$; (b)

$P(X = x_i) = P(Y|Z) \to 0$. (c)

From *(a)*, *(b)* and (c), we have:

$$\begin{aligned} H(X = x_i) &= -\sum_x P(X = x_i) log(P(X = x_i)) \\ &= -\sum_x P(Y|Z) log(P(Y|Z)) \to 0 \; bit. \end{aligned} \tag{4.11}$$

Thus, an attacker has none information to determine the thermal power of each volume element. We conclude that the proposed mechanism is efficient.

4.4 Description of experimental environment

We use an Arduino[9] Uno ATMega 328p as source of the thermal noise. It generates a solid ($\sum$) of space (ω).

We mention that the function which characterizes each volume element of the solid ($\sum$) is

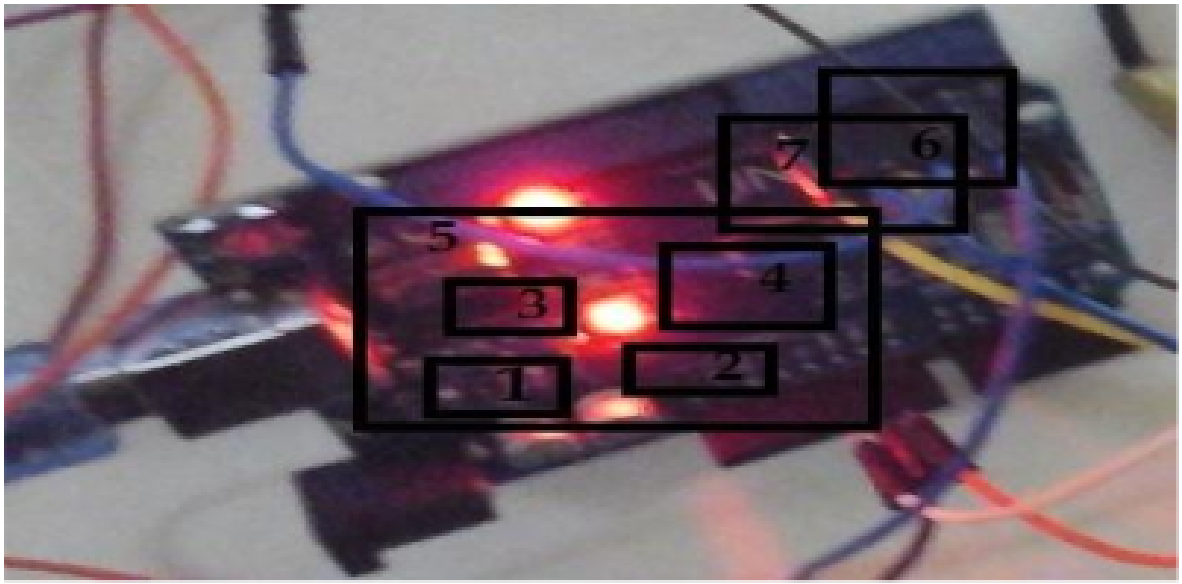


Figure 4.2: Volume elements.

defined by:

$$\nu = \iiint_{\sum} dxdydz; \tag{4.12}$$

We define by framing in black (figure 4.2) the considered volume elements during the temperature evaluation. They are referenced by numbering. We perform the tests on a set of seven volume elements.

For each volume element of the electronic system, we deploy a temperature sensor type LM 35. Then, we determine the power for each volume element according to the temperature values measured.

[9]Arduino is an Italian open-source hardware and software company, project, and user community that designs and manufactures single-board microcontrollers and microcontroller kits for building digital devices.

Index	Volume (cm^3)	Constant $J.K^{-1}$	Temperature (k)	Time (s)	Power (w)
ν_1	1.35	1.3806×10^{-23}	305.25	0	67428504×10^{-24}
ν_2	1.46	1.3806×10^{-23}	303.55	2	$670529808 \times 10^{-25}$
ν_3	1.08	1.3806×10^{-23}	305.85	4	$675610416 \times 10^{-25}$
ν_4	1.98	1.3806×10^{-23}	297.85	6	$657938736 \times 10^{-25}$
ν_5	22.2	1.3806×10^{-23}	304.75	8	67318056×10^{-24}
ν_6	1.2	1.3806×10^{-23}	296.45	10	$654846192 \times 10^{-25}$
ν_7	5.4	1.3806×10^{-23}	296.95	12	$655950672 \times 10^{-25}$

Table 4.2: Power computation experment.

Table 4.2 represents graph relating to the achieved results during the experiments. It is constant to note that the thermal noise computation power varies for each volume element. This variation happened due to changes of the temperature for each volume element over a given time.

Clock step	Time(s)	Volume(cm^3)	Power(w)	Integer part	Decimal part
1	0	1.35	67428504×10^{-24}	0	67428504×10^{-24}
2	2	1.46	$670529808 \times 10^{-25}$	0	$670529808 \times 10^{-25}$
3	4	1.08	$675610416 \times 10^{-25}$	0	$675610416 \times 10^{-25}$
4	6	1.98	$657938736 \times 10^{-25}$	0	$657938736 \times 10^{-25}$
5	8	22.2	67318056×10^{-24}	0	67318056×10^{-24}
6	10	1.2	$654846192 \times 10^{-25}$	0	$654846192 \times 10^{-25}$
7	12	5.4	$655950672 \times 10^{-25}$	0	$655950672 \times 10^{-25}$

Table 4.3: Integer/decimal parts retrieval.

We summarize through table 4.2 and table 4.3, the obtained results following the experiments.

4.5 Results analysis and discussion

We devote this section to the analysis of the results obtained during the tests. Thus, Tables 4.2, 4.3 and 4.4 represent graphs relating to the achieved results during the experiments. It is constant to note that the thermal noise power varies for each volume element at figure 4.3. This variation happened due to changes of the temperature for each volume element over a time. Thus, the thermal noise power in a volume element means the determination of the following parameters: Temperature (T), time (t), and volume element (ν). The power varies according to temperature, volume element and time. As a result, the generated numbers vary in time and space and do not follow any deterministic approach. Therefore, they are deemed to be true and random.

We generate a number by concatenation[10] of the integer and decimal parts of the thermal noise power obtained per volume element ignoring the decimal point. A sequence of generated numbers is equivalent to a sequence of concatenation of integer and decimal parts of the power of each volume element according to its assignment index j. So:

for$j \in [1;7] \Rightarrow \nu_j \in \{\nu_1, \nu_2, \nu_3, \nu_4, \nu_5, \nu_6, \nu_7\}$

$\Rightarrow P\nu_j \in \{P\nu_1, P\nu_2, P\nu_3, P\nu_4, P\nu_5, P\nu_6, P\nu_7\} \Rightarrow TRNG = \{P_e\nu_1||P_d\nu_1||P_e\nu_2||P_d\nu_2||P_e\nu_3||$
$P_d\nu_3||P_e\nu_4||P_d\nu_4||P_e\nu_5||P_d\nu_5||P_e\nu_6||P_d\nu_6||P_e\nu_7||P_d\nu_7\}$.

ν_i	$np_e\nu_i$	$np_d\nu_i$	$n\nu_i$
ν_1	1	25	26
ν_2	1	26	27
ν_3	1	26	27
ν_4	1	26	27
ν_5	1	25	26
ν_6	1	26	27
ν_7	1	26	27
		Total number of digits	**187**

Table 4.4: Number of digits counted per volume element.

[10]The action of linking things together in a series, or the condition of being linked in such a way.

For 7 volume elements, we get a sequence of random numbers of 187 digits distributed as follows:

Let note:

$n\nu_i$: number of digits for each volume element,

$nP_e\nu_i$: number of digits enumerated for the integer part of each volume ν_i,

$nP_d\nu_i$: number of digits enumerated for the decimal part of each volume element ν_i. The results are represented in Table 4.4.

Therefore, for z volume elements, $z\epsilon[0;+\infty[$, it is very difficult for an attacker to determine exactly the different temperatures within each volume element and:

$TRNG_z = P_e\nu_1||P_d\nu_1||P_e\nu_2||P_d\nu_2||P_e\nu_3||P_d\nu_3||P_e\nu_4||P_d\nu_4||P_e\nu_5||P_d\nu_5||P_e\nu_6||P_d\nu_6|$
$|P_e\nu_7||P_d\nu_7||.....||P_e\nu_{z-4}||P_d\nu_{z-4}.....||P_e\nu_{z-1}||P_d\nu_{z-1}||P_e\nu_z||P_d\nu_z.$

The obtained TRN is converted into binary and recovered as a keystream. This keystream will be transmitted from the transmitter to the receiver through quantum cryptography properties.

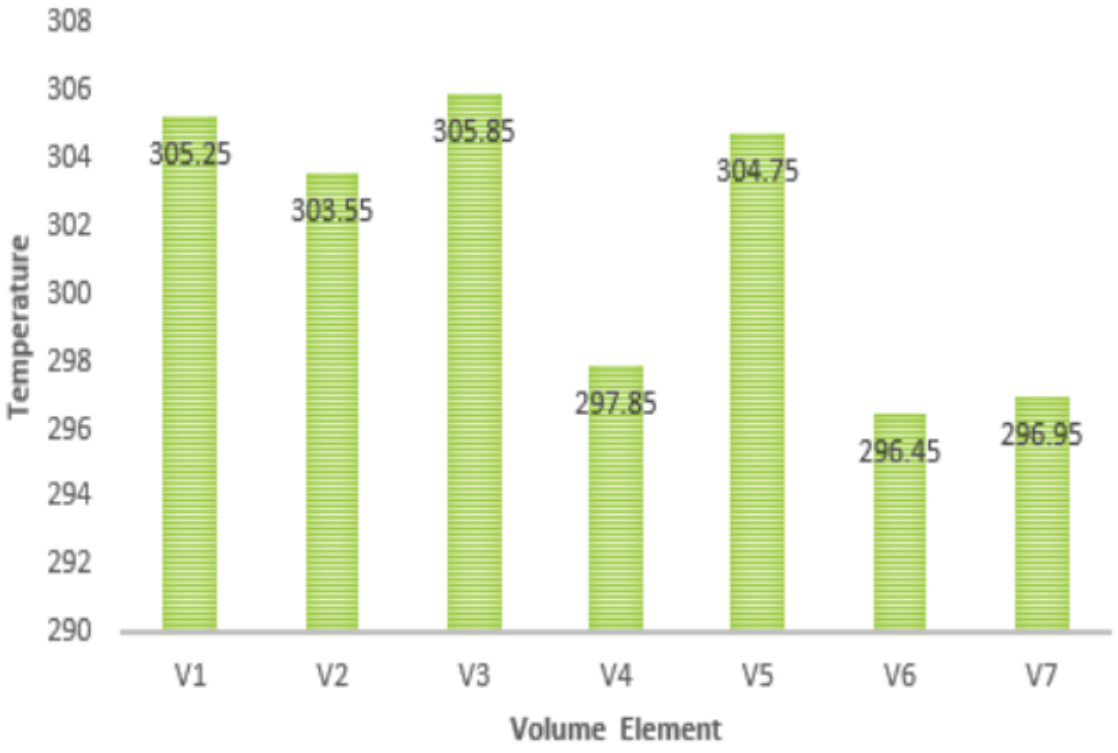


Figure 4.3: Variation of temperature depending on volume elements.

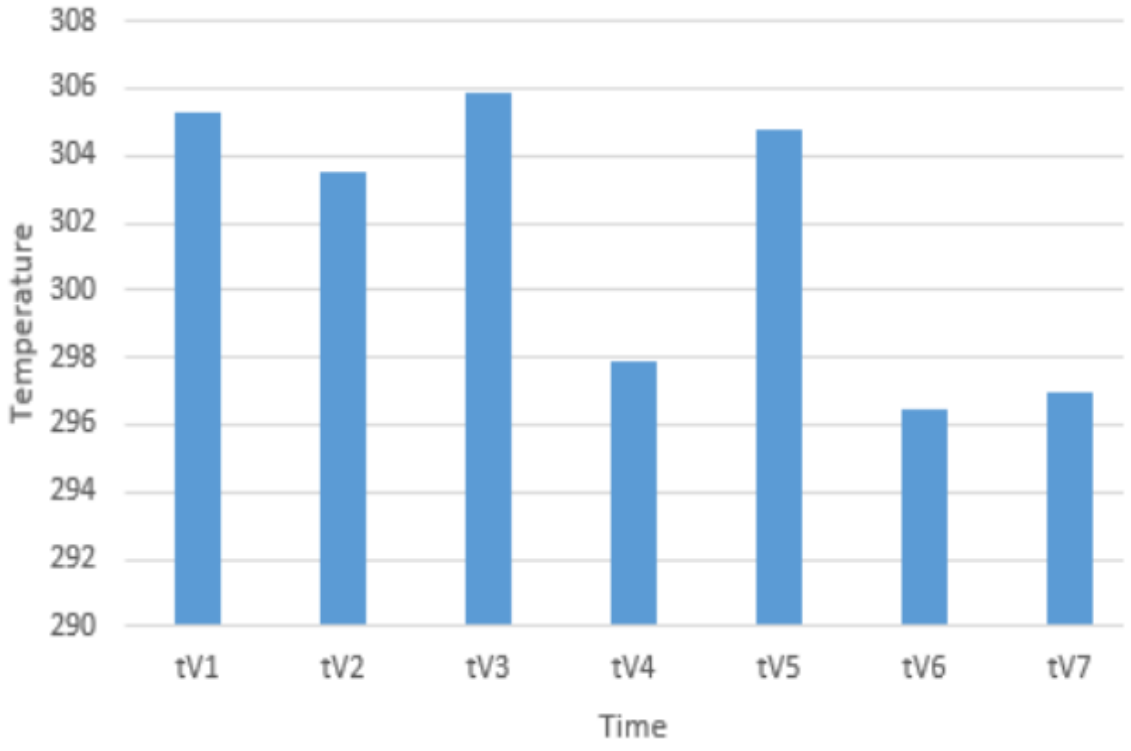


Figure 4.4: Sampling the temperature for each volume element.

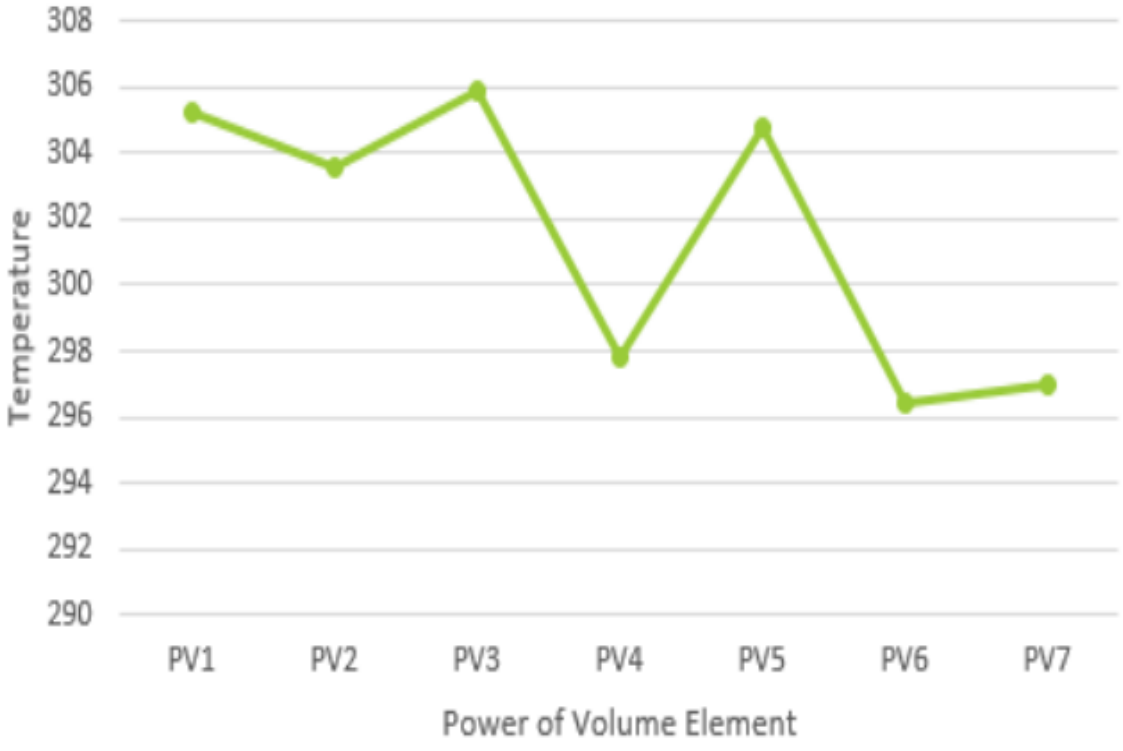


Figure 4.5: Variation of temperature depending on the power of thermal noise.

We have proposed a mechanism for true random number generation which can resist to an attacker with quantum computers. This mechanism uses the fundamentals of thermal noise theory which is a random phenomenon. For tests and experiments, we used an ATMega microcontroller as a solid space that generates volume elements.

We sample the temperature of these volume elements to determine the power of thermal noise for each volume element. Thus, we have obtained for 7 volume elements, a series of random numbers of 187 digits which conversion into binary represents the cryptographic key.

Our analysis shows that it is not possible for an attacker to determine the generated sequence numbers for infinity of volume elements.

Research Contribution

1. General Context

An online transaction occurs, such as a purchase or a bank transfer, users authenticate their identities with each other, verify permissions to access specific services and products, and communicate data entrusted to a secure encryption system. This process is enabled by secret passwords, communication protocols, and an encryption system based on mathematical problems believed to be too difficult for present-day computers to "crack." These systems protect us from security threats such as viruses, fraud, and identity theft. Staying on the cutting-edge of the next generation of cryptographic technologies and threats is critical to maintaining our security. Better to gain a deeper understanding of how quantum cryptography and conventional cryptography interact and combine systems resistant to quantum technologies can be developed and integrated into a larger cryptographic tools. This knowledge will allow us to recognize how to develop secure larger systems, such as global multi-user quantum networks, we have to cosider the following strategies: (a) undertand appropriated methods for guaranteeing security of systems using new quantum-safe tools and (b) understand how tools and protocols optimize network performance without compromising security. As a result, the difficulty in creating a secure encryption method now lies in developing a protocol that generates a cryptographic key with the desired properties. This goal cannot be achieved with purely classical algorithms because we have no private communication channel; this is where quantum theory comes into play. The unique features of quantum mechanics lend themselves extraordinarily well to the task of establishing a secret key between two parties.

Firstly, the intrinsic[11] randomness of quantum states and measurements can be exploited to generate truly random bits.

[11]Intrinsic quantum randomness is produced when a projective measurement on a given basis is implemented on a pure state that is not an element of the basis.

Protais Ndagijimana © Doctoral school - University of Burundi

Secondly, the phenomenon of entanglement allows the generation of the same set of random bits in two distant locations.
Thirdly, quantum states have the property that they cannot be perfectly copied, in contrast to classical bits. Even though it is impossible to make perfect copies of an unknown quantum state, it is possible to produce imperfect copies. This can be done by coupling a larger auxiliary system to the system that is to be cloned, and applying a unitary transformation to the combined system. If an adversary attempts to access information encoded in quantum states, he/she has to somehow interact with the quantum state, which in turn will lead to detectable changes in the state[12]. Consequently, the communicating parties will be alerted to the attack before confidential information has been exchanged.

Post-quantum cryptography, with its ability to provide secure communication channels using the principles of quantum mechanics, holds immense potential for revolutionizing various aspects of daily lives. While still in the early stages of development and deployment, there are several real-world applications where quantum cryptography could be explored and implemented. Here are some notable domains:

1. Artificial Intellience: Integrating Artificial Intelligence "AI" and quantum cryptography has led to remarkable advancements in sectors such as banking and e-commerce, facilitating the development of robust security protocols and bolstering users' trust in these sectors.

1. Secure Communication Networks: this thesis could motivate governments in creation of unbreakable encryption keys ensuring that sensitive information transmitted over networks remains confidential. This is particularly crucial for protecting classified communications and safeguard sensitive data.

2. Financial Services: With the advent of quantum computers, traditional cryptographic algorithms could be vulnerable to attacks. THis thesis could inspire governmental and non governmental institutions to implement quantum-resistant encryption methods to secure electronic money transactions, and protect against emerging threats.

3. Data Centers and Cloud Computing: This thesis could contribute, by using quantum-resistant encryption algorithms, to establish secure channels between data centers and

users, organizations can ensure the confidentiality and integrity of their data in cloud environments.

4. Internet of Things "IoT" Security: The proliferation of IoT devices brings about concerns regarding their security and vulnerability to cyber attacks. Quantum cryptography offers a potential solution by providing secure key distribution and encryption mechanisms for IoT devices. With quantum-resistant algorithms and secure communication channels, the integrity and confidentiality of IoT data can be preserved, mitigating potential risks.

5. Defense and National Security: Through this thesis, defense organizations could maintain secure and tamper-proof communication channels. Quantum cryptography could enhance their capabilities by enabling the secure transmission of classified information, protecting military communications.

6. Healthcare and Medical Data: This thesis can contribute in healthcare industry to deal with highly sensitive patient information and medical records. Quantum cryptography can provide an additional layer of security for protecting electronic health records, ensuring patient privacy, and preventing unauthorized access or tampering of medical data.

7. Authentication and Identity Management: Tis thesis can help to enhance authentication and identity management systems. Quantum cryptographic algorithms can be employed to secure digital identities, prevent identity theft, and ensure the integrity of user authentication processes.

8. Secure Elections and Voting Systems: This thesis cold contribute in encryption and secure communication channels, it is possible to prevent tampering, ensure the confidentiality of votes, and maintain the integrity of election results.

While these aopportunities highlight the potential of quantum cryptography, it's important to note that widespread adoption may still be some time away.
Challenges such as scalability, cost, and practical implementation need to be addressed to make quantum cryptography accessible and commercially viable.

2. Contribution to Burundi development Vision

The Government of Burundi has led several activities in relation to the use of Information and Communication Techology"ICT" in the service of the socio-economic development and Good Governance under the responsibility of the National Committee. These activities include: development of the National Policy in Science, Technology and Innovation "STI", launch of an optical fibre project, plans to provide computers in the Higher Education system, a policy for free changes when importing ICT equipment and the development of partners in ICT Networking[114].

The National ICT Policy was revised and adopted in 2011 to make it more compliant with the regional framework and more in line with technology convergence. It has ten pillars including:

1. Capacity building
2. Enhancement of the Legal and Regulatory Environment
3. Promotion of ICT infrastructure
4. E-government, e-Governance and Online Administration.
5. ICT and Economic development
6. ICT and Social Development
7. Rural Connectivity and Universal Access
8. ICT Research and Innovation
9. Electronic Transactions and Cybersecurity
10. Local and Regional Content Development

Unfortunately, Burundi did not embrace the cryptomoney revolution and did not perceive it as an opportunity to create wealth, make money on crypto markets, and attract major companies in its jurisdiction. It requires a complete legal arsenal to be put in place in order to establish a crypto-friendly jurisdiction. With the new technology "Quantum Cryptography", Burundi could even become a leader in the region for international trade based on the blockchain.

Cryptocurrencies are much helpful for developing economies since they can increase their economic and social status. Entrepreneurs get more control, and thus, access to capital becomes much easier due to the advent of blockchain technologies. Everything contributes to the rise in economic activities.

Finally and most importantly, this research could contribute through quantum cryptography policy that can build on Government of Burundi initiatives and aim to assist in achieving its vision **"Burundi, an Emerging Country in 2040 and a Developed Country in 2060"** by serving as a key catalyst in achieving quantum cryptographic protection in social, economic, political and cultural transformation within the country based on cryptographic mechanism as asurance during the process.

Considering all the components in which cryptography has a significant impact, the advantages of cryptography being used by the government, and the continuous development of technology, we can say that the importance of cryptography in government of Burundi could undoubtedly be increased.

Chapter Five

Conclusion and Perspectives

Contents

5.1 General context 89

5.2 Achieved Results Briefings 90

5.3 Challenges and Perspectives 92

5.1 General context

In today's digital landscape, where privacy and data security are of utmost concern, post-quantum cryptography has emerged as a groundbreaking solution that holds immense potential for securing our day-to-day lives. By leveraging the principles of post-quantum mechanics, post-quantum cryptography offers unbreakable security measures that can protect sensitive information from sophisticated cyber threats.

The application of post-quantum cryptography extends to various domains, ranging from secure communication networks and financial transactions to government and defense operations, healthcare, and IoT security. Implementing quantum key distribution protocols and quantum-resistant encryption algorithms can safeguard personal data, confidential communications, and critical infrastructure from unauthorized access, interception, and tampering.

While there are challenges to overcome, such as the development of practical quantum key distribution systems and the establishment of a quantum-ready infrastructure, researchers and organizations are actively working towards advancing post-quantum cryptography. As these efforts progress, we can anticipate greater integration of quantum-resistant security measures in our daily lives, ensuring the confidentiality and integrity of our digital interactions.

As post-quantum cryptography continues to evolve and mature, it has the potential to revolutionize the way we approach cybersecurity. By embracing this innovative technology, we

Protais Ndagijimana © Doctoral school - University of Burundi

can forge a more secure and resilient digital future, empowering individuals, businesses, and governments to navigate the digital field with confidence and trust.

5.2 Achieved Results Briefings

Realization of practical quantum information technologies can not be accomplished without involvement of the network research community. The advances in computer processing power and the threat of limitation for today's cryptography systems will remain a driving force in the continued research and development of quantum cryptography[**?**]. The technology has the potential to make a valuable contribution to the network security among government, businesses, and academic environment.

At present, much of the quantum cryptography is theoretical as the equipment required is still under development or exists as a prototype yet to be named a true quantum computer. However, the introduction of true quantum computers will bring about a major change in the technological world by not only enabling other theoretical components of quantum cryptography but also begin a domino- effect potentially taking the digital world into the next big leap.

Therefore, future security proof incorporating imperfections should also incorporate the finite key size. On the experimental side there is still work to do: implement and scrutinize a detector scheme where the detector parameters are verified to be within the model in the security proof. In the short term, this could involve designing and implementing a calibrated light source in destination or receiver, to avoid detector control attacks. For both the experimental and theoretical future, the biggest challenge remains: will it be possible to implement Quantum Kek exchange in a way that is provable secure?

Apart the overview of a quantum computer,through chapter three, we described the evolution of cryptography and the theory related to computationnal performance, efficiency, prototype and predictive modeling of a quantum computer. The properties of the superposition state of a quantum system to perform data operation has been described. The quantum computer, apart it is in its experimental phase, it is not intended to replace our classical ones because its applications will be different.

However, the development of quantum computer could pose different challenges for research

and society today: on the one side, the technical feasibility of development; on the other side, the possible global impact on digital security. Quantum computing capabilities and technologies will serve as the foundation of a second information age. The current researches allow to better understand this quantum universe and more necessarily they open the life to a new technological revolution.

Random numbers are the lifeline of any cryptographic operation in modern computing. It is important for developers to understand what interface to use, and how to handle random numbers correctly in their code. In chapter four, we explained with details a distinctive difference between Pseudo-random Number Generator(PRNG) and True Random Number Generator "TRNG" that is the provability of the latter. Indeed, the only provable feature of a PRNG is that it is not random because all numbers produced thereof can be calculated from a single initial number: the seed. On the other hand TRNGs is able to produce a sequence of numbers for which there is no known deterministic link paradoxically to the pseudo-random number generator.

A mechanism for true random number generation which can resist to an attacker with quantum computers has been proposed . This mechanism uses the fundamentals of thermal noise theory which is a random phenomenon. For tests and experiments, we used an ATMega microcontroller as a solid space that generates volume elements. We sample the temperature of these volume elements to determine the power of thermal noise for each volume. Thus, we have obtained for seven volume elements, a series of random numbers of 187 digits which conversion into binary represents the cryptographic key. Our analysis show that it is not possible for an attacker to determine the generated sequence numbers for an infinity of volume elements. In appendices of this document, prerequisite purposes of "quantum key distribution "QKD" mechanism, has been mentioned to try to describe a method of exchanging the generated key and associating it the BB84 cryptographic protocol.That method would involve encoding the encryption key onto a quantum particle "or Qubit" that is sent to the other person, who measures the qubit to obtain the value of the key. The approach is particularly interesting in security because it relies on the laws of quantum physics, which state that Qubits collapse as soon as they are measured.

In general perspectives, organizations, both governmental and private, need to invest time and money to get ready for the challenges of a post-quantum world! It's already possible to outline the steps to be taken. Weighting all the change management that will be required it

is certain that any plan will be an ambitious one, with a lot of bottlenecks. If this plan is addressed with success, cryptosystem designers will be the silent heroes of the future, with the knowledge we have today new systems will be more crypto-agile[1] to make them more robust and future proof.

Like in many other branches of cybersecurity, cryptography is part of a cat-and-mouse race between those who try to keep data secure and those who try to break the systems with illegitimate interests. Science has proven to be a savior of mankind throughout history and once again mathematics will have to show its value in ensuring that keys are only available to those who have permission.

A lot is certainly left to be said, including the variants of each algorithm, the different approaches to each implementation, and how each can be made more secure for different attacks. A deeper knowledge and more widespread availability of quantum computers in the future will bring more challenges, and more attacks but looking at all the published articles regarding the subject, it's an alive community that is up for current and future challenges.

Apart the previous approaches, we may also face to other Security Challenges in the future, this is about 5G Network[2]. Due to the global service demands the number of connected machines as mobiles, IoT, and IIoT devices, has been immensely increased.

This improvement has a great impact on the regular network efficiency and capacity for that matter a 5G network technology is proposed to provide an efficient network that can cope with the recent technology revolution.

5.3 Challenges and Perspectives

While post-quantum cryptography holds great promise for enhancing the security of communications, there are several challenges that need to be addressed before it can become more widely adopted. Here are some of the key challenges and the perspectives or future outlook for post-quantum cryptography:

[1] Crypto-agility is defined as the ability of a security system to be able to rapidly switch between algorithms, cryptographic primitives, and other encryption mechanisms without the rest of the system's infrastructure being significantly affected by these changes.

[2] 5G is the fifth generation of wireless cellular technology, offering higher upload and download speeds, more consistent connections, and improved capacity than previous networks.

1. Technical Complexity: Post-quantum cryptography involves complex technologies and requires specialized infrastructure, including quantum key distribution (QKD) systems. These systems are currently expensive and not easily scalable, which limits their widespread deployment. Overcoming these technical challenges and developing more cost-effective and scalable solutions will be crucial for the future of post-quantum cryptography.

2. Post-quantum Computing Development: Quantum computers have the potential to break certain cryptographic algorithms that are widely used today. Therefore, the development of quantum-resistant encryption algorithms is crucial to ensure the security of communications in the future. Researchers are actively working on post-quantum cryptography, which focuses on developing encryption methods that can withstand attacks from quantum computers. The future outlook depends on advancements in both quantum computers and quantum-resistant algorithms.

2. Infrastructure and Standards: Establishing a robust infrastructure and standardized protocols for post-quantum cryptography is essential for its widespread adoption. Currently, there is a need for standardized protocols that ensure interoperability and compatibility between different post-quantum cryptographic systems. Developing these standards will require collaboration among researchers, industry stakeholders, and regulatory bodies.

3. Integration with Existing Systems: Integrating post-quantum cryptography with existing communication systems can be challenging. It requires modifications to existing infrastructure and protocols to accommodate the unique features of post-quantum cryptography. Ensuring a smooth transition and compatibility with legacy systems will be crucial for the practical implementation of post-quantum cryptography.

4. Education and Awareness: Post-quantum cryptography is a highly specialized field, and there is a need for education and awareness among professionals, decision-makers, and end users. Promoting understanding of post-quantum cryptography, its benefits, and its limitations will be essential for its successful adoption in various industries and everyday life.

Despite these challenges, the future outlook for post-quantum cryptography is promising. Ongoing research and development efforts, coupled with advancements in quantum computing and infrastructure, will likely lead to more practical and accessible solutions. As the technology matures, we can expect to see increased deployment of post-quantum cryptography in critical sectors such as finance, government, healthcare, and telecommunications.

Appendix A

Appendix

1. Quantum Key Distribution general understanding

The purpose of this section is to study Quantum Key Distribution "QKD", a cryptographic primitive that allows two remote users to generate an arbitrary amount of secret key even in the presence of an eavesdropper, provided they share an initial secret. QKD works in a similar way to traditional cryptography: data is encoded into an unreadable message using a cryptographic key that the recipient needs to decrypt the information. The method involves encoding the encryption key onto a quantum particle "or Qubit" that is sent to the other person, who measures the qubit to obtain the value of the key. This approach is particularly interesting in security because it relies on the laws of quantum physics, which state that qubits collapse as soon as they are measured. This means that if a third party eavesdrops on the exchange and measures the Qubits to obtain the cryptographic key, they will inevitably leave a sign of their intrusion[1].

We already knew, in introduction, that the key, the plain-text and the cipher-text are classical because they are constructed by classical "conventional" bits. Even the encryption algorithm OTP[2] (One-time Pad)is classical[115][116]. Let's take this example: Alice sends the encryption algorithm and the cypher-text to Bob through the classical "public" channel. Eve is an attacker needs to intercept the cipher-text and the encryption algorithm sent by Alice to Bob. Eve obtains the knowledge of the length of the key and the length of the plain-text,n , which is equivalent to the length of the cipher-text intercepted. Then Eve establishes the quantum state of the key, $|k\rangle$, superposition of $N\,(N = N^n)$ states of $|k_i\rangle$ (of n bits):

[1]Since eavesdroppers cannot clone or divide a photon, any action will introduce errors.

[2]Automatically generated numeric or alphanumeric string of characters that authenticates a user for a single transaction or login session.

Protais Ndagijimana © Doctoral school - University of Burundi

$$
\begin{aligned}
|k\rangle &= \tfrac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) \otimes \tfrac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) \otimes ... \otimes \tfrac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) \\
&= \frac{1}{\sqrt{2}}\Big(|00...0\rangle + |00...1\rangle + ... + |11...1\rangle\Big) \\
&= \tfrac{1}{\sqrt{N}} = \textstyle\sum_{i=0}^{N-1} |k_i\rangle
\end{aligned}
\tag{A.1}
$$

where n is the number of the bits of the key of any one of BB84, E91 and B92. Eve also establishes the quantum state of the plain-text (2). After that, Eve establishes her search equation.

$$\mathrm{OTP}(k_i, p_j) = C \quad (0 \leqslant i \leqslant N-1, 0 \leqslant j \leqslant N-1)$$

where OTP is the OTP encryption algorithm [21], k_i is the bit string of $|k_i\rangle, p_j$ is the bit string of $|p_j\rangle$, C is the Cipher-text. Eve's searching is to solve the search equation to find the plain-text p_t.

with:

k_i: the bit string of the i component of the quantum state of the key;

p_j: the bit string of the j component of the quantum state of the plain-text;

k_s: the bit string of the key, whose value is set by Alice;

p_t: the bit string of the plain-text, whose value is set by Alice;

C : the bit string of the cypher-text produced by Alice's encryption.

2. Some developments in QKD

A key distributed using quantum cryptography would be almost impossible to steal because QKD systems continually and randomly generate new private keys that both parties share automatically. QKD was proposed roughly 20 years ago, but its premise rests on the formulation of Heisenberg's uncertainty principle in 1927. The very act of observing or measuring a particle such as a photon in a data stream changes its behavior. Any moving photon can have one of four orientations: vertical, horizontal, or diagonal in either direction. A standard laser can be modified to emit single photons, each with a particular orientation[117]. Would be hackers (eavesdroppers) can record the orientations with photon detectors, but doing so changes the orientation of some photons and, thus, alerts the sender and receiver of a compromised transmission.

Since the publication of BB84, many other QKD protocols were proposed. They typically follow the same outline[118]:

1) Prepare and measure. Quantum states are generated by Alice and transmitted to Bob for measurement through a quantum channel.

2) Parameter estimation. Communicating on the authenticated channel, Alice and Bob estimate the relevant quantities to derive a bound on the information accessible to Eve.

3) Information reconciliation. Typically using error correcting codes, Alice and Bob extract from the measurement a common data string that is still unsafe.

4) Privacy amplification techniques are used to generate a private key from the shared data, using the result of step 2.

Let note that only the first two steps of the protocols involve quantum mechanics. That is why most experimental proof-of-principle works do not implement the last two steps. They usually exchange the quantum states and estimate the achievable length of the secret key using security proofs. Some protocols follow a slightly different approach, based on entangled states. In these protocols, Alice prepares two entangled states, sends one of them to Bob and measures the other one. Steps 2, 3 and 4 remain conceptually unchanged. Let us illustrate a pair of conventional techniques conceived for achieving information security, as shown in Fig.6.1.

QKD exploits the laws of quantum physics to distribute unconditionally secure symmetric secret keys between Alice and Bob. Generally, the basic elements of a QKD system are a transmitter and a receiver as well as a QKD link connecting the transmitter and receiver. The combination of the transmitter and receiver is commonly referred to as the QKD transceiver. The QKD transmitter/receiver encapsulates a set of hardware and software components used for QKD within a defined secure boundary. The QKD link relies on both a quantum channel and a classical channel. The quantum channel is used for transmitting quantum signals in which information is conveyed by quantum states, such as the polarization[3] of a single photon. The classical channel is used to exchange classical information for synchronization and key

[3]An individual photon can be described as having right or left circular polarization, or a superposition of the two. Equivalently, a photon can be described as having horizontal or vertical linear polarization, or a superposition of the two.

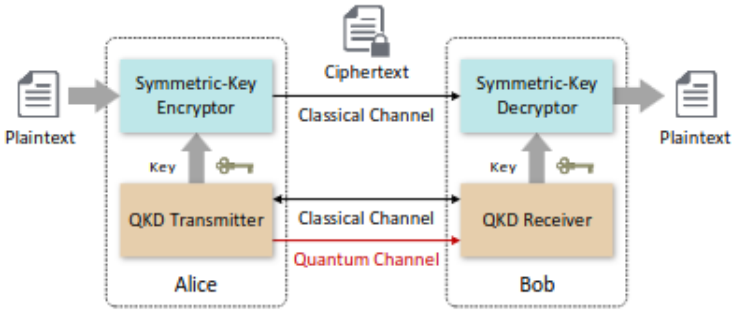


Figure A.1: Illustration of a QKD-based cryptographic scheme.

[119]

distillation between Alice and Bob [120][121]

If an eavesdropper "called Eve" captures some of the quantum states during the passage of single photons through the quantum channel, those quantum states will not be used to distill secret keys, since they are not received by Bob. Eve can then potentially measure those quantum states, but the laws of quantum physics guarantee that following measurement or observation by Eve the quantum state collapses back into the classical domain. Hence, any potential eavesdropping on QKD can be detected.

3. Use cases of Quantum Key Distribution

Quantum Key Distribution will potentially play a major role in enhancing the security and privacy of data in future communication networks. The secret keys generated from the QKD protocol can be used for OTP-based physical layer security. Moreover, the keys can also be used for higher layer symmetric key encryption algorithms such as advanced encryption standards "AESs" and digital encryption standards "DESs"[122]. The following are the detailed description of some Quanyum Key Distribution use cases: *Data centres and cloud computing, Quantum cryptography for beyond 5G networks, Internet of Things "IoT", Government and banking, Healthcare.*

3.1. Data centres and cloud computing

Data centres[4] store and process a large amount of data. They also transmit the data from one server to another during which various malicious attacks may compromise the security of the sensitive data in transmission.

These secret keys can then be used to secure the data centres by providing quantumsafe encryption for the data transmission between two or more data centres. The data transmitted to high performance computers for processing can also be secured by using the secret keys generated from QKD.Moreover, QKD can also be used as a cloud service where quantum-safe secret keys are distributed upon request to the end users by the servers.

Cloud computing[5] has recently emerged as a new paradigm for hosting and delivering services over the Internet. Cloud computing is attractive to business owners as it eliminates the requirement for users to plan ahead for provisioning, and allows enterprises to start from the small and increase resources only when there is a rise in service demand. With the rapid development of processing and storage technologies and the success of the Internet, computing resources have become cheaper, more powerful and more ubiquitously available than ever before.

3.2. Quantum cryptography for beyond 5G networks

With the proliferation of 5G mobile devices, QKD can be used to secure the 5G[6] network and beyond by securing the base station to the core 5G network link as well as the base station to the user link in order to provide quantum-safe end-to-end voice, text and data communication services. Currently, the secret key generator cannot ensure absolute security if the physical channel is eavesdropped on. Additionally, QKD can also be used to improve the

[4]A data center or data centre is a building, a dedicated space within a building, or a group of buildings used to house computer systems and associated components, such as telecommunications and storage systems

[5]Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. Large clouds often have functions distributed over multiple locations, each of which is a data center.

[6]In telecommunications, 5G is the fifth-generation technology standard for cellular networks, which cellular phone companies began deploying worldwide in 2019, and is the successor to 4G technology that provides connectivity to most current mobile phones.

5G network virtualisation services by enhancing the security of virtual network infrastructure management.

Furthermore, QKD can be used to support various privacy preserving services, such as secure multi-party computation, federated learning and homomorphic encryption in beyond 5G networks.

3.3. Internet of Things (IoT)

The threat of malicious attacks will increase with the huge number of devices and sensor nodes being deployed in the IoT[7] networks. The IoT devices will be utilised for collecting sensitive personal data such as location and video surveillance[123]. The security and privacy of the data collected by IoT sensors can be enhanced by using the secret keys generated from QKD. Since IoT devices have limited power and computing capabilities, IoT controllers need to distribute the secret keys to the edge devices. The devices can then use the secret keys to encrypt the data before sending it to a central data processor.

3.4. Government and banking

Data security and sovereignty is of utmost importance for government agencies and the military in order to safeguard critical national data, such as defence secrets, intellectual property and citizen data from hackers. QKD will play a major role in providing quantum-safe security for critical national data. In this regard, QKD can be used for securing the private communication links between different government agencies for sharing confidential data between them. Moreover, secret keys generated using QKD can be used by the banking sector for secure (ATM) Automated Teller Machines[8] transactions, online credit card transactions and securing the customer data stored in the bank data centres. The government agencies and banks can deploy a trusted repeater-based local quantum network in order to provide QKD enabled end-to-end encryption.

[7] IoT refers to the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves.

[8] Are banking outlets where you can withdraw cash without going into a branch of their bank. Some ATMs only dispense cash, while others allow transactions such as check deposits or balance transfers.

3.5. Healthcare

Telemedicine and e-healthcare[9] services have become a major part of the healthcare sector due to the pandemic. Hence, it may become extremely necessary to exploit the secret keys generated by QKD for securing the storage, transmission and processing of sensitive patient data. Moreover, various bio- sensors are now embedded in smartwatches and other wearable devices that collect and transmit personal health data and the day-to-day activity of the user.The unconditional security and confidentiality of these intimate health data in the era of quantum computing can be ensured by using QKD-based encryption schemes.
Eventually, QKD constitutes the near commercialisation quantum technologies with multiple potential benefits for our future communication technologies. As we have described comprehensively in this treatise, while immeasurable amount of investment has been poured down for the research and development of QKD, a massive standardisation effort are required to guarantee the sustainability and reliability of near future deployment and to accommodate multiple potentialuse cases and several plausible QKD protocols.

2. Attacks on ideal Protocols

Before we start to analyze the security of QKD in more detail, let us have a look at how Eve could actually perform her eavesdropping activity. From the theory of quantum mechanical measurements we know that any eavesdropping can be thought of as an interaction between a probe[10] and the signals. Eve can then measure the probe to obtain information about the signals. We distinguish three main types of eavesdropping attacks:[124]
Individual Attack: In the individual attack Eve lets each signal interact with a separate probe. Eve performs then a measurement on each probe separately after the interaction. This type of attack is easy to analyze since it does not introduce correlations between the signals.

[9] e-Health describes healthcare services which are supported by digital processes, communication or technology such as electronic prescribing, Telehealth, or Electronic Health Records "EHRs". The use of electronic processes in healthcare dated back to at least the 1990s. Usage of the term varies as it covers not just "Internet medicine" as it was conceived during that time, but also "virtually everything related to computers and medicine".

[10] A feature that routes user-specified signals to output pins without affecting the existing fit of a design, allowing you to investigate internal device signals without completing a full compilation.

Collective Attack: The collective attack starts as the individual attack, as each signal interacts with its own independent probe. At the measurement stage, however, Eve can perform measurements that act on all probes coherently. We know from quantum estimation theory that such measurement can in some cases give more information about the signals than the individual measurement. For the analysis it is convenient that also this attack does not introduce correlations between the signals.
Coherent Attack: This is the most general attack which an eavesdropper can launch on the quantum signals exchanged between Alice and Bob. Actually, one can assume the worst case scenario that Eve has access to all signals at the same time. Then the sequence of signals is described by one high-dimensional quantum state, on which Eve can perform a measurement via a single probe. This type of interaction can introduce any type of correlations, also between subsequent signals, as seen by Alice and Bob.

Further variations of these attacks can be obtained by distinguishing whether Eve has to measure her probes before Alice and Bob continue their protocol, e.g. by exchanging basis information in the BB84 protocol, or whether she can delay her measurement until the very end of the protocol executed by Alice and Bob[125][126]. Note that Eve does not necessarily have to measure the probe to extract information about the key. The secret key will be used to encrypt a secret, or be used in a different cryptographic application, which might also use quantum tools. Eve might use her probes from the QKD protocol to attack the subsequent cryptographic application.

3. Quantum Key Distribution protocol: BB84

Charles Bennett and Gilles Brassard proposed in 1984 "BB84" the first key distribution protocol with security based on quantum mechanical theory. The founding idea is based on the non-cloning property of a quantum state. In short, Alice sends to Bob polarized photons on a quantum channel. The eavesdropper cannot perfectly clone or divide the photons. She has to measure them, and generate new ones to send to Bob with the measured polarization. In doing so, she introduces errors in the protocol, that betray her presence. The protocol assumes that Alice and Bob also have access to an authenticated classical channel, to monitor the protocol and identify if the channel is being eavesdropped. The "BB84" protocol [127][128] was the

first to show how conjugate coding could be used for an information-theoretically secure key agreement protocol. In a nutshell, the protocol consists in Alice sending a sequence of single qubits, chosen randomly from the states $\{|\updownarrow\rangle,|\leftrightarrow\rangle\}$ Bob chooses to measure them according to his own random choice of measurement bases. They communicate their basis choice for each encoded qubit; eavesdropper detection is performed by comparing the measurement results on a fraction of the bases on which their choices coincide if successful, this procedure gives a bound on the secrecy and similarity of the remaining shared string, which can be used to distill an almost perfect shared secret between Alice and Bob. In order to prevent man-in-the-middle attacks, this procedure requires authenticated classical channels. Usually, authentication is achieved by an initial shared classical secret between Alice and Bob. Thus, QKD is more accurately described as a key-expansion primitive.

As already mentioned, one of the possible physical quantities to implement the BB84 protocol is the polarization of photons. Alice transmits random bits to Bob by encoding them on an orthonormal basis. For example a horizontal polarization, noted $|\leftrightarrow\rangle$, encodes a 0, and a vertical polarization, noted $|\updownarrow\rangle$, a 1.

Alice has at her disposal a second basis inclined by a 45° angle: a polarization of 45° to the left, noted $|\nwarrow\rangle$, encodes a 0, and a polarization of 45° to the right, noted $|\nearrow\rangle$, encodes a 1. The BB84 scheme1 uses single photons transmitted from Alice to Bob, which are prepared at random in four partly orthogonal polarization states: $0°, 45°, 90°, 135°$.

Polarisation	**Symbol**	**Bit Value 0**	**Bit Vlue 1**
Rectilinelar Basis	+	0°,↔	90°, ↕
Diagonal Basis	X	45°,↗	135°, ↖

Table A.1: Polarization Basis and Encoding rule in the 4-state BB84 protocol.

If Eve tries to extract information about the polarization of the photons she will inevitably introduce errors, which Alice and Bob can detect by comparing a random subset of the generated keys. In general the two non-orthogonal bases are:

-Base + having horizontal polarization (0°) and vertical polarization (90°), and we represent the base states with intuitive notation: $|0\rangle$ and $|1\rangle$. So, we have $+ = \{|0\rangle,|1\rangle\}$.

-Base x having diagonal polarizations (45°) and (135°). The two different base states are $|+\rangle$ and $|-\rangle$ with $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. So, we have $X = \{|+\rangle,|-\rangle\}$[129].

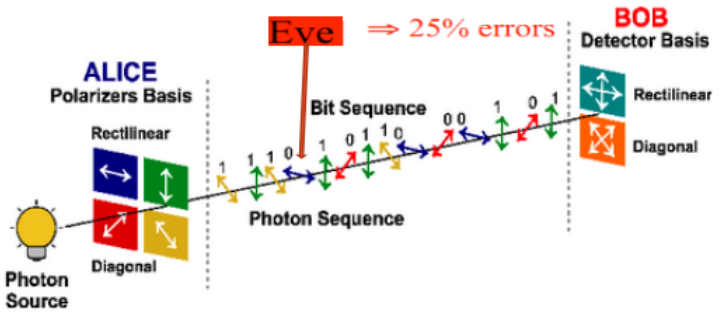


Figure A.2: The key exchange in the BB84 protocol implemented with the polarization of photons.

[130]

For each bit to be transmitted, Alice randomly chooses the encoding basis and the bit with uniform probability. Bob is not informed of her choice. For his measurement, he chooses arbitrarily one of the two basis. If his choice does not coincide with Alice's, the polarization he measures is random, and the information is unusable. Using the authenticated channel, Alice and Bob communicate to each other their basis choices and dismiss the bits measured with incompatible bases. This step of the protocol is called sifting. What if Eve tries to eavesdrop the channel? Since she cannot clone or divide a photon, any action will introduce errors. For instance, she can measure the polarization, and then generate a new photon to send to Bob corresponding to her measurement. This basic attack is called intercept-and-resend. Like Bob, she has to decide on the basis to use, with probability 1/2 of making a mistake. This induces a 1/4 error probability in the bit read by Bob. Thus, if Alice and Bob reveal a fraction of their bits on the authenticated channel to estimate the bit error rate, they are able to estimate the quantity of information leaked to Eve. In fact, Eve is capable of subtle attacks consisting in imperfect cloning of the photons. The BB84 protocol must used for the polarization of the photons in the quantum channel for producing the order of the qubits that transmitted in the channels. For example, after a measurement run, Alice and Bob extract the coincidences measured with parallel analyzers, $(0°, 0°)$ and $(45°, 45°)$, which occur in half of the cases, and generate the raw keys. Alice and Bob collected ~ 80000 bits of key at a rate of 850 bits/second, and observed a quantum bit error rate of 2.5 %, which ensures the security of the quantum channel.

In the QKD protocol, information can be encoded into the physical states of particles,

Quantum Transmission																			
Alice	random bits	0	1	...	1	1	0	...	0	1	1	...	1	...	1	0	...	1
	sending bases		×				+				+			...		×		
	sending photons	⤢	⤡	...	⤡	↕	↔	...	↔	↕	↕	...	↕	...	⤡	⤢	...	⤡
Eve	receiving and sending bases		×				+				×			...		+		
	receiving and sending photons	⤢	⤡	...	⤡	↕	↔	...	↔	⤢	⤢	...	⤡	...	↔	↔	...	↕
Bob	receiving bases		×				×				+			...		×		
	receiving photons	⤢	⤡	...	⤡	⤡	⤡	...	⤢	↔	↕	...	↔	...	⤢	⤡	...	⤡
	receiving bits	0	1	...	1	1	1	...	0	0	1	...	0	...	0	1	...	1
Public Discussion																			
Bob reports receiving bases per group			×				×				+			...		×		
Alice replies identical bases per group			○								○			...		○		
Bob shares decoding results (K bits)		0	1	...	1					0	1	...	0	...	0	1	...	1

Table A.2: Sample of grouped BB84 protocol with presence of Eve. [131]

where the state is referred to as a quantum bit "qubit". The QKD protocol exchanges a sequence of qubits between two entities "from Alice to Bob" in a secure manner against the presence of an eavesdropper (Eve). The secure exchange of qubits in the QKD protocol is guaranteed by the nocloning principle in quantum mechanics [132]. The information encoded in the qubits can be used as a secret key to encrypt/decrypt the plaintext between Alice and Bob. In this study, we use the terms eavesdropper and Eve interchangeably.

The security issues facing quantum key distribution "QKD" are explained in the previous section, herein focusing on those issues that are cryptographic and information theoretic in nature and not those based on physics. The problem of security criteria is addressed. It is demonstrated that an attacker's success probabilities are the fundamental criteria of security that any theoretic security criterion must relate to in order to have operational significance. The errors committed in the prevalent interpretation of the trace distance criterion are analyzed.

The security proofs of QKD protocols are discussed and assessed in regard to three main features: their validity, completeness, and adequacy of the achieved numerical security level. Problems are identified in all these features. It appears that the QKD security situation is quite different from the common perception that a QKD-generated key is nearly perfectly secure.

Then, using privacy amplification techniques, they generate from their shared data a smaller key, which is unknown to the eavesdropper with high probability.Built into our discussion is a simple but complete quantitative description of the information theoretic security of classical key distribution that is also applicable to the quantum situation.
There are many other serious issues facing QKD security proofs, many of which relating to physics and implementation. These issues will not be discussed in this section, which concentrates on a careful exposition of the above four points. Much of the technical content in this section is conceptual analysis, especially on the use of probability in real-world applications. They are not essentially mathematical or physical in nature, which is partly why they are easy to miss and result in various confusions.

Thus, Alice and Bob can calculate a bound on the amount of Eve's information, regardless of the attack. They can use this knowledge to extract a secret from their correlated data. To do so, they have first to correct the errors by using error-correcting codes to obtain a common error-less key, in a step called information reconciliation. In the BB84 protocol,

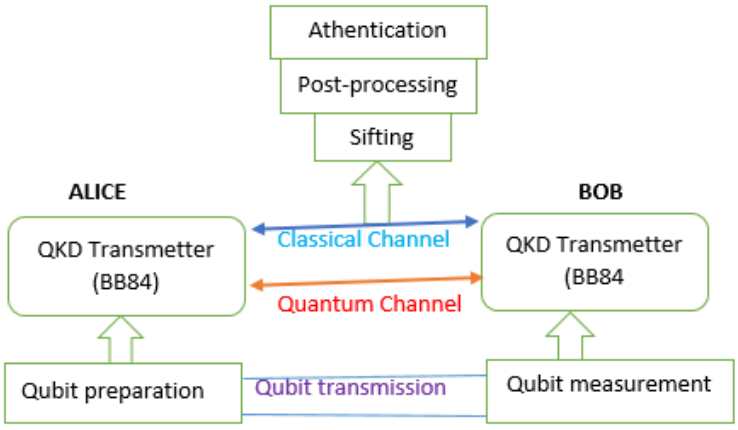


Figure A.3: Illustration of five stages in the BB84 protocol.

five stages are performed, as illustrated in Fig.6.3 and explained as follows:
Qubit preparation, transmission, and measurement: Alice generates a sequence of classical bits "called raw keys" and encodes them into a stream of single photons to generate qubits.
Sifting: Alice and Bob, respectively, share their encoding and measurement bases through a classical channel, whic may however be accommodated within a single fiber using wavelength-division multiplexing "WDM". The specific qubits associated with mismatched polarization

states and measurement bases are discarded, while the remaining qubits corresponding to the matching bases are decoded into a stream of bits "called sifted keys".

Parameter estimation: At this stage, the quantum bit error rate "QBER" is estimated by sacrificing a portion of the sifted keys to verify that it is below a predetermined threshold value.

Post-processing: Alice and Bob perform error correction, verification, and privacy amplification through a classical channel to distill the final string of secure bits "called secret keys".

Authentication: The first QKD session is authenticated using the full pre-shared secret key between Alice and Bob. Subsequent QKD sessions can be authenticated using a small part of the agreed secret keys to avoid the man-in-the-middle attack [133].

A perfect single-photon source is required by the BB84 protocol, but this is still unavailable in practice. Instead, a highly attenuated laser source that can generate weak coherent pulses is commonly adopted by the BB84-protocol-based QKD systems. Such a laser source may emit multiple photons in a pulse, making the QKD system vulnerable to a photon number splitting attack [134][135].

The intuition behind the security of quantum key distribution is based on one of the tenets of quantum mechanics: measurement disturbs a quantum system. A second property of quantum mechanics, the No-Cloning theorem [136][46], completes the security intuition for quantum key distribution by showing that its impossible for an eavesdropper to clone or copy the photons sent to Alice and Bob; thus, preventing her from interacting with copies so as not to disturb Alice and Bob's original photons. This means that any eavesdropper attempting to gain information about the photons as they are sent to Alice and Bob will necessarily disturb their state. This disturbance will have measurable consequences for Alice and Bob and will show up in the error rate induced in their measurements on their photons. There are then two important error rates[137] by which I will claim my QKD system is secure in the following chapters:

1. Error Rate $< 14.6\%$: QKD system secure against symmetric individual attacks[11].
2. Error Rate $> 11\%$: QKD system secure against coherent attacks[12].

[11]Symmetric individual attacks are attacks where Eve is restricted to interacting with each qubit being sent from Alice to Bob one at a time, ie. she interacts with them individually.

[12]Coherent attacks are the most general attacks allowed by quantum mechanics where Eve can

with both of these being in the long key limit.

Security proofs and the vulnerabilities of QKD systems is a PhD thesis in its own right. Most of the attacks in the literature exploit deficiencies in a particular implementation of a QKD system rather than problems with the QKD protocol itself. As such, each paper is usually quite specific to a particular implementation or a particular piece of hardware being used. By far, the biggest overall vulnerability is side-channel attacks where the implementation deviates from the ideal protocol and leaks information into various side channels that the security proofs do not take into account. While it is virtually impossible to rule out all side-channel attacks for a system, particularly the prepare-and-measure systems; one possible solution is device-independent security proofs[138] which might finally provide a complete proof of security for a real QKD system. Currently though detection efficiencies are nowhere near as good as they need to be in order to apply device-independent security proofs and consequently almost all QKD systems, commercial or educational, display vulnerabilities which a potential eavesdropper might exploit. A part the current security system, a technique for the analysis of device-independent cryptographic protocols will be introdused. It will be provided a flexible protocol and give a security proof that provides quantitative bounds that are asymptotically tight, even in the presence of general quantum adversaries. At a high level the approach amounts to establishing a reduction to the scenario in which the untrusted device operates in an identical and independent way in each round of the protocol.This will be achieved by leveraging the sequential nature of the protocol and makes use of a newly developed tool, the "entropy accumulation theorem" of Dupuis, Fawzi, and Renner[139] [Entropy Accumulation, preprint, 2016]. As concrete applications we give simple and modular security proofs for device-independent quantum key distribution and randomness expansion protocols based on the CHSH inequality. For both tasks, we establish essentially optimal asymptotic key rates and noise tolerance.

collectively interact her own quantum systems with every qubit sent from Alice to Bob, delay any measurements she might make on her quantum systems until Alice and Bob announce their measurement bases, and make a collective measurement on all her systems at once. This attack allows Eve to maximize the information she might gain about their key and minimize the disturbance she causes in their error rate.

Bibliography

[1] Paar, C., and Pelzi, J. (2010). Understanding cryptography: A textbook for students and practitioners. New York, NY: Springer.

[2] D. Selent. Advanced Encryption Standard. Rivier Academic Journal, 6(2), 2010. Retrieved from https://www.rivier.edu/journal/ROAJ-Fall-2010/J455-Selent-AES.pdf.

[3] P. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pp. 124 - 34, 1994.

[4] L. Grover. A fast quantum mechanical algorithm for database search. Proceedings of the 28th ACM Symposium on Theory of Computing, pp. 212 - 219, 1996.

[5] S. Singh. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptog- raphy, February 2006. Retrieved from https://www.math.uci.edu/ brusso/freshman6.pdf. UCI Freshman Seminar.

[6] Cohen, Fred 1990-1995. "A Short History of Cryptography." Retrieved on March 27th, 2017 from URL: http://web.itu.edu.tr/ orssi/dersler/cryptography/Chap2-1.pdf

[7] D. P. Mowry. German Cipher Machines of World War II. National Security Agency, 2014.

[8] Keith Wagstaff, July 14, 2015, 3:28 PM UTCh. Retrieved from ttps://www.nbcnews.com/tech/tech-news/rare-enigma-machine-sells-auction-232-000-n391776

[9] Singh, S. (2000). The code book: The science of secrecy from Ancient Egypt to quantum cryptography. New York, NY: Anchor Books.

Protais Ndagijimana © Doctoral school - University of Burundi

[10] Sadkhan, Sattar B., and Zainab Hamza. "Cryptosystems used in IoT-current status and challenges." 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT). IEEE, 2017.

[11] Lobna Yehia, Ayman Khedr, Ashraf Darwish, "Hybrid Security Techniques for Internet of Things Healthcare Applications",2015

[12] Renner, Renato, and Ramona Wolf. "Quantum advantage in cryptography." AIAA Journal 61.5 (2023): 1895-1910.

[13] Aung, D. M. M., Kay Thwe Kywe Aye, and Tun Myat Aung. "On the Study of Quantum Computing." Proceedings of the Conference on Science and Technology Development (CSTD-2019), Pyin Oo Lwin, Myanmar. Vol. 31.

[14] Kitaev, Alexei Yu, Alexander Shen, and Mikhail N. Vyalyi. Classical and quantum computation. No. 47. American Mathematical Soc., 2002.

[15] Rodenburg, Brandon, and Stephen P. Pappas. "Blockchain and quantum computing." Retrieved from (2017).

[16] LaPierre, Ray, and Ray LaPierre. "Shor algorithm." Introduction to Quantum Computing (2021): 177-192.

[17] Armanuzzaman, Md, Kazi Md Rokibul Alam, Md Mehadi Hassan, and Yasuhiko Morimoto. "A secure and efficient data transmission technique using quantum key distribution." In 2017 4th International Conference on Networking, Systems and Security (NSysS), pp. 1-5. IEEE, 2017.

[18] Abidin, Aysajan, and Jan-Ake Larsson. "Security of authentication with a fixed key in quantum key distribution." arXiv preprint arXiv:1109.5168 (2011).

[19] Benioff, Paul. "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines." Journal of statistical physics 22 (1980): 563-591.

[20] Feynman, Richard P. "Simulating physics with computers." Int. j. Theor. phys 21.6/7 (2018).

[21] Deutsch, David. "Quantum theory, the Church-Turing principle and the universal quantum computer." Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences 400.1818 (1985): 97-117.

[22] Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM review 41.2 (1999): 303-332.

[23] Grover, Lov K. "A fast quantum mechanical algorithm for database search." Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. 1996.

[24] A.Steane, Quantum computation, Repprts on progress in physics, 61,pp. 117-173, 1988. LANL e-preprinting quant-ph/9708022.

[25] With CB Insights Center: Quantum Computing Vs. Classical Computing In One Graphic(February,2021)

[26] Retrieved from https://timesmicrowave.com/the-difference-between-classical-and-quantum-computing/ (April 2021)

[27] Hagar, Amit, and Michael Cuffaro. "Quantum computing." (2006).

[28] Van Meter, Rodney, and Dominic Horsman. "A blueprint for building a quantum computer." Communications of the ACM 56.10 (2013): 84-93.

[29] Bennett, Charles H., Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. "Strengths and weaknesses of quantum computing." SIAM journal on Computing 26, no. 5 (1997): 1510-1523.

[30] Hagar, Amit. "Quantum algorithms: Philosophical lessons." Minds and Machines 17 (2007): 233-247.

[31] M. S. Hwang and C. Y. Liu, Authenticated encryption schemes: current status and key issues," International Journal of Network Security, vol. 1, no. 2, pp. 61-73, 2005.

[32] M. H. Ibrahim, A method for obtaining deniable publickey encryption," International Journal of Network Security, vol. 8, no. 1, pp. 1-9, 2009

[33] M. H. Ibrahim, Receiver-deniable public-key encryption," International Journal of Network Security, vol. 8, no. 2, pp. 159-165, 2009

[34] Hameed, Thamer Hassan, and Haval Tariq Sadeeq. "Modified Vigenére cipher algorithm based on new key generation method." Indones. J. Electr. Eng. Comput. Sci. 28.2 (2022): 954-961.

[35] F. Mushtaq and S. Ali, "Enhancing security of Vigenere Cipher by Stream Cipher," International Journal of Computer Applications, vol. 100, no. 1, pp. 0975-8887, 2014.

[36] A. L. Hananto, A. Solehudin, A. S. Y. Irawan, and B. Priyatna, "Analyzing the Kasiski method against Vigenere Cipher," vol. 6, no. 6, pp. 1-8, Dec. 2019, [Online]. Available: http://arxiv.org/abs/1912.04519.

[37] Saeed, Fauzan, and Mustafa Rashid. "Integrating Classical Encryption with Modern Technique." IJCSNS International Journal of Computer 280 (2010): 280-285.

[38] International Journal of Advanced Research in Computer Science and Software Engineering. Volume 2, Issue 10, October 2012 ISSN: 2277 128X "Enhancing Security of Caesar Cipher by Double Columnar Transposition Method" Mr. Vinod Saroha ,Suman Mor, Anurag Daga

[39] Oladipupo, Esau Taiwo, and Oluwakemi Christiana Abikoye. "Modified Playfair cryptosystem for improved data security." Computer Science and Information Technologies 3.1 (2022): 51-64.

[40] S. Hamad, A. Khalifa, A. Elhadad, and S. Rida, "A modified Playfair cipher for encrypting digital images," Journal of Communications and Computer Engineering, vol. 3, no. 2, p. 1, 2014, doi: 10.20454/jcce.2013.731

[41] Sharbaf, Mehrdad S. "Quantum cryptography: a new generation of information technology security system." 2009 Sixth International Conference on Information Technology: New Generations. IEEE, 2009.

[42] Wiesner, S., "Conjugate coding" SIGACT News , 1983, 15, p. 78-88.

[43] Bruss, D., Erdelyi, G., Meyer, T., Riege, T., and Rothe, J., "Quantum cryptography: A survey". ACM Computing Surveys, 39(2), 2007, p. 1-27.

[44] Hrg, D., Budin, L., and Golub, M.,"Quantum cryptography and security of information systems", IEEE Proceedings of the 15 th Conference on Information and Intelligent System, 2004, p. 63-70.

[45] Papanikolaou, N., "An introduction to quantum cryptography", ACM Crossroads Magazine, Vol.11 No.3, 2005, pp. 1-16.

[46] Wootters, W. K., and Zurek, W. H., "A single quantum cannot be cloned". Nature, 299, 1982, p. 802

[47] Kan, Kazutoshi, and Masashi Une. "Recent trends on research and development of quantum computers and standardization of post-quantum cryptography." (2021).

[48] D. J. Bernstein. Introduction to post-quantum cryptography. In Post-quantum cryptography, pp. 1 - 14. Springer, 2009.

[49] Kumar, Manoj, and Pratap Pattnaik. "Post quantum cryptography (PQC)-An overview." 2020 IEEE High Performance Extreme Computing Conference (HPEC). IEEE, 2020.

[50] Kumar, Adarsh, Carlo Ottaviani, Sukhpal Singh Gill, and Rajkumar Buyya. "Securing the future internet of things with post-quantum cryptography." Security and Privacy 5, no. 2 (2022): e200.

[51] Niederhagen, Ruben, and Michael Waidner. "Practical post-quantum cryptography." Fraunhofer SIT (2017).

[52] Konyukhov, Vitaliy. "Mathematics of Post-Quantum Cryptography." (2022).

[53] Hulsing, Andreas, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe. "From 5-pass MQ-based identification to MQ-based signatures." IACR Cryptol. ePrint Arch. 2016 (2016): 708.

[54] Panek, Luciano, Marcelo Firer, and Marcelo Muniz Silva Alves. "Classification of niederreiter "rosenbloom" tsfasman block codes." IEEE Transactions on information theory 56.10 (2010): 5207-5216.

[55] R. Overbeck and N. Sendrier. "Code-based cryptography". In: Post-Quantum Cryptography [8]. Ed. by D. J. Bernstein, J. Buchmann, and E. Dahmen. Springer, 2009, pp. 95-145 (cit. on p. 10).

[56] M. Ajtai. "Generating Hard Instances of Lattice Problems (Extended Abstract)". In: ACM Symposium on Theory of Computing ; STOC-96. ACM, 1996, pp. 99-108 (cit. on p. 9).

[57] A. Childs, D. Jao, and V. Soukharev. "Constructing elliptic curve isogenies in quantum subexponential time". In: Journal of Mathematical Cryptology 8.1 (2014). arXiv:1012.4019, pp. 1-29 (cit. on p. 18).

[58] Pappu, Ravikanth, Ben Recht, Jason Taylor, and Neil Gershenfeld. "Physical one-way functions." Science 297, no. 5589 (2002): 2026-2030.

[59] Sobti, Rajeev, and Ganesan Geetha. "Cryptographic hash functions: a review." International Journal of Computer Science Issues (IJCSI) 9.2 (2012): 461.

[60] Zhang, Xiaojun, et al. "FS-PEKS: Lattice-based forward secure public-key encryption with keyword search for cloud-assisted industrial Internet of Things." IEEE Transactions on dependable and secure computing 18.3 (2019): 1019-1032.

[61] Chao, Hui-Mei, Chin-Ming Hsu, and Shaou-Gang Miaou. "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records." IEEE transactions on information technology in biomedicine 6.1 (2002): 46-53.

[62] Ahmed, Maryam, Baharan Sanjabi, Difo Aldiaz, Amirhossein Rezaei, and Habeeb Omotunde. "Diffie-Hellman and its application in security protocols." International Journal of Engineering Science and Innovative Technology (IJESIT) 1, no. 2 (2012): 69-73.

[63] Retrieved from: https://www.hypr.com/security-encyclopedia/diffie-hellman-algorithim (c.1969)

[64] Shand, Mark, and Jean Vuillemin. "Fast implementations of RSA cryptography." In Proceedings of IEEE 11th Symposium on Computer Arithmetic, pp. 252-259. IEEE, 1993.

[65] Kalpana, Parsi, and Sudha Singaraju. "Data security in cloud computing using RSA algorithm." International Journal of research in computer and communication technology, IJRCCT, ISSN (2012): 2278-5841.

[66] J. Fauquet et C. Vastine : L'Esprit Sorcier :Le principe de l'ordinateur quantique(2020); https://youtu.be/2aCS5mEeiwg

[67] Kumar, Manish. "Post-quantum cryptography Algorithm's standardization and performance analysis." Array 15 (2022): 100242.

[68] Bindel, Nina, et al. "Drive (Quantum) Safe! ac" Towards Post-Quantum Security for V2V Communications." IACR Cryptol. ePrint Arch. 2022 (2022): 483.

[69] Kumar, Manoj, and Pratap Pattnaik. "Post quantum cryptography (PQC)-An overview." 2020 IEEE High Performance Extreme Computing Conference (HPEC). IEEE, 2020.

[70] Rieffel, Eleanor, and Wolfgang Polak. "An introduction to quantum computing for non-physicists." ACM Computing Surveys (CSUR) 32.3 (2000): 300-335.

[71] Marella, Surya Teja, and Hemanth Sai Kumar Parisa. "Introduction to quantum computing." In Quantum Computing and Communications. IntechOpen, 2020.

[72] Gill, Sukhpal Singh, Adarsh Kumar, Harvinder Singh, Manmeet Singh, Kamalpreet Kaur, Muhammad Usman, and Rajkumar Buyya. "Quantum computing: A taxonomy, systematic review and future directions." Software: Practice and Experience 52, no. 1 (2022): 66-114.

[73] G. Birkhoff and J. von Neumann. The logic of quantum mechanics. Annals of Mathematics, 37:823 - 843, 1936.

[74] P. Benioff. The computer as a physical system. Journal of Statistical Physics, 22:563 - 591,1980.

[75] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. Proceedings of the Royal Society, A 400:97 - 117, 1985.

[76] N. Bohr. The philosophical writings of Niels Bohr. Ox Bow Press, 1987.

[77] N. Gershenfeld and I. L. Chuang. Bulk spin resonance quantum computing. Science, pp. 212 - 219, 1997.

[78] Vandersypen, L. MK, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood and I. L. Chuang. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. Nature, 414(6866):883 - 887, 2001.

[79] N. Xu, J. Zhu, D. Lu, X. Zhou, X. Peng and J. Du. Quantum factorization of 143 on a dipolar-coupling nuclear magnetic resonance system. Physical Review Letters, 108(13):130,501,2012.

[80] N. S. Dattani and N. Bryans. Quantum factorization of 56153 with only 4 qubits. arXiv preprint arXiv:1411.6758, 2014.

[81] R. Tanburn, E. Okada and N. Dattani. Reducing multi-qubit interactions in adiabatic quantum computation without adding auxiliary qubits. Part 1: The "deduc-reduc" method and its application to quantum factorization of numbers. arXiv preprint arXiv:1508.04816, 2015.

[82] Linnhoff-Popien, C. (2019). Quantum Computing "a new hype". Digitale Welt, 3(2), 9-10.

[83] B. Heim et al., "Quantum programming languages," Nat. Rev. Phys., vol. 2, no. 12, pp. 709-722, 2020, doi: 10.1038/s42254-020-00245-7.

[84] Lov K. Grover, "Fast Quantum Mechanical Algorithm for Database Search", STOC-96: Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing July 1996, pp 212-219.

[85] Landry Bretheau. "Les ordinateurs quantiques : comment ça marche ?" July, 2021

[86] Vergnaud, Damien. "Primitives et constructions en cryptographie asymétrique." PhD diss., Ecole normale supèrieure, 2014.

[87] Plesa, Mihail-Iulian, and Togan Mihai. "A new quantum encryption scheme." Advanced Journal of Graduate Research 4, no. 1 (2018): 59-67.

[88] Bhaskar, M. K., Hadfield, S., Papageorgiou, A., and Petras, I. (2015). Quantum algorithms and circuits for scientific computing. arXiv preprint arXiv: 1511.08253.

[89] P. Shor, " Algorithm for Quantum Computation: Discrete Logarithms and Factoring " , Proc. 35 th Annual Symposium on Foundations of Computer Science. IEEE Press, pp 124-134, November 1994, quant-ph/9508027.

[90] I G,E I "A Fast Quantum Mechanical Algorithm for Database Search". In : Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. STOC-96. Philadelphia, Pennsylvania.

[91] Upama, Paramita Basak, Md Jobair Hossain Faruk, Mohammad Nazim, Mohammad Masum, Hossain Shahriar, Gias Uddin, Shabir Barzanjeh, Sheikh Iqbal Ahamed, and Akond Rahman. "Evolution of quantum computing: A systematic survey on the use of quantum computing tools." In 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 520-529. IEEE, 2022.

[92] L'Ecuyer, Pierre. "Uniform random number generation." Annals of Operations Research 53 (1994): 77-120.

[93] L'Ecuyer, P. (1998, December). Uniform random number generators. In 1998 Winter Simulation Conference. Proceedings (Cat. No. 98CH36274) (Vol. 1, pp. 97-104). IEEE.

[94] Shih Liu "On Fourrier's law of heat conduction" Continuum Mechanics and Thermodynamics, pp 301-305, December 1990.

[95] Stip 'evi', Mario, and cetin Kaya Koc "True random number generators." Open Problems in Mathematics and Computational Science. Cham: Springer International Publishing, 2014. 275-315.

[96] Bernhard Fechner, Andre Osterloh " A meta-level true random number generator " International Journal of Critical Computer-Based Systems, January 2010.

[97] Mario STIPCEVIC, Cetin Kaya KOC, "True Random Number Generators ", Open Problem in Mathematics and Computational Science, pp 275-315.

[98] Lishuang Gong, Jianguo Zhang, Haifang Liu, Luxiao Sang, Yuncai Wang, "True Random Numbers Generators Using Eletricals Noise", DOI 10.1109/ACCESS. 2019.2939027, IEEE.

[99] Scott A. Wilber, "True Random Number Generator and Entropy Calculation Device and Method" US 6,862,605 B2. March. 1, 2005.

[100] Shonda Walker, Simon Y. Foo, "Evaluating metastability in electronic circuits for random number generation " , Proceedings IEEE Computer Society Workshop on VLSI, 2001.

[101] Vittorio Bagini, Marco Bucci, "A design of reliable true random number generator for cryptographic applications" Cryptographic Hardware and Embedded Systems, First International Workshop, August 12-13, 1999, Proceedings (pp.204-218), CHES-99 Worcester, MA USA.

[102] Dustin Moody, Stephen P. Jordan, Lily Chen, Yi-Kay Li, "NIST Report on Post-Quantum Cryptography", National Institute of Standards and Technology Internal Report 8105, 15 pages (April 2016).

[103] Masanori Ohya, Natsuki Masuda, "Np Problems in Quantum Algorithm", Open Systems and Information Dynamics, Vol.7, pp33-39 (2000).

[104] Martin Furer, "Solving NP-Complete Problems with Quantum Search", Theoretical Informatics, 8 th Latin American Symposium, Buzios, Brazil, April 7-11, 2008; Proceedings, pp784-792.

[105] Jurgen Schurr, Harald Moser, Klaus Pierz, Gunther Ramm, "Johnson-Nyquist Noise of the Quantized Hall Resistance" IEEE Transactions on Instrumentation and Measurement 60(7):2280-2285 August 2011.

[106] H. Nyquist , "Thermal agitation of electric charge in conductors" , Physical Review, 32:110-113, 1928.

[107] C.E. Shannon, " A mathematical theory of communication " , Bell System Technical Journal, vol. 27, Oct. 1948, pp.379-423, and 623-656.

[108] G. Parisi, F. Rapuano, " Effects of the random number generator on computer simulations " , Physic Letters B, 157:301-302, 1985.

[109] Berk Sunar, William J. Martins, Douglas R. Stinson, " A provable secure true random number generator with build in tolerance to active attacks " , IEEE Transaction on Computer January 2007, Vol. 56, No.1. pp 109-119.

[110] de la Fraga, Luis Gerardo, Esteban Torres-Pérez, Esteban Tlelo-Cuautle, and Cuauhtemoc Mancillas-LÓpez. "Hardware implementation of pseudo-random number generators based on chaotic maps." Nonlinear Dynamics 90 (2017): 1661-1670.

[111] Wang, Luyao, and Hai Cheng. "Pseudo-random number generator based on logistic chaotic system." Entropy 21, no. 10 (2019): 960.

[112] C.E. Shannon, "Communication theory of secrecy systems ", Bell System Technical Journal, vol. 28, Oct. 1948, pp.565-15, October 1979.

[113] Hirosuke Yamamoto, "Coding Theorems for Shannon's Cipher System with Correlated Source Outputs and Common Information" IEEE Transaction on Information Theory vol.40. Issue 1, pp85-95, Jan1994.

[114] The IST-Africa Guide to ICT-related Bilateral Cooperation provides an overview of the current ICT related bilateral cooperation with Botswana, Burundi, Cameroon, Egypt, Kenya, Lesotho, Mauritius, Mozambique, Namibia, Senegal, South Africa, Tanzania and Uganda as at January 2012. ISBN No: 978-1-905824-33-5

[115] Dash, Avinash, Sumit Rout, Bikash K. Behera, and Prasanta K. Panigrahi. "Quantum locker using a novel verification algorithm and its experimental realization in IBM quantum computer." arXiv preprint arXiv:1710.05196 (2017).

[116] Szikora, Péter, and Kornélia Lazányi. "The end of encryption" "The era of quantum computers." In Security-Related Advanced Technologies in Critical Infrastructure Protection: Theoretical and Practical Approach, pp. 61-72. Dordrecht: Springer Netherlands, 2022.

[117] Ouellette, J. (2004). Quantum key distribution. Industrial Physicist, 10(6), 22-25.

[118] Roumestan, François. Advanced signal processing techniques for continuous variable quantum key distribution over optical fiber. Diss. Sorbonne Université, 2022.

[119] Cao, Y., Zhao, Y., Wang, Q., Zhang, J., Ng, S. X., and Hanzo, L. (2022). The evolution of quantum key distribution networks: On the road to the qinternet. IEEE Communications Surveys and Tutorials, 24(2), 839-894.

[120] "Overview on networks supporting quantum key distribution," Recommendation ITU-T Y.3800, Oct. 2019.

[121] "Quantum key distribution (QKD); Device and communication channel parameters for QKD deployment," ETSI GS QKD 012 V1.1.1, Feb. 2019

[122] Liu, R., Rozenman, G. G., Kundu, N. K., Chandra, D., and De, D. (2022). Towards the industrialisation of quantum key distribution in communication networks: A short survey. IET Quantum Communication, 3(3), 151-163.

[123] Farooq, M.U., Waseem, M., Mazhar, S., Khairi, A. and Kamal, T., 2015. A review on internet of things (IoT). International journal of computer applications, 113(1), pp.1-7.

[124] Hendrych, Martin. "Miloslav Du-ek Department of Optics, Palacky University 17. listopadu 50, 77200 Olomouc, Czech Republic Norbert Lutkenhaus Institut fur Optik, Information und Photonik." arXiv preprint quant-ph/0601207.

[125] Lee, Chankyun, Ilkwon Sohn, and Wonhyuk Lee. "Eavesdropping detection in BB84 quantum key distribution protocols." IEEE Transactions on Network and Service Management 19.3 (2022): 2689-2701.

[126] Boyer, Michel, Rotem Liss, and Tal Mor. "Security against collective attacks of a modified BB84 QKD protocol with information only in one basis." arXiv preprint arXiv:1704.01388 (2017).

[127] Ruiz Alba Gaya, Antonio, David Calvo DIaz-Aldagalan, Victor Garcia Munoz, Alfonso Martinez Garcia, Waldimar Alexander Amaya Ocampo, JUAN GUILLERMO ROZO CHICUE, José Mora Almerich, and José Capmany Francoy. "Practical quantum key distribution based on the BB84 protocol." In Waves, vol. 1, no. 3, pp. 4-14. Instituto de Telecomunicaciones y Aplicaciones Multimedia (iTEAM), 2011.

[128] Renner, R. (2008). Security of quantum key distribution. International Journal of Quantum Information, 6(01), 1-127.

[129] Sahoo, J. R., and S. Satapathy. "Simulation and analysis of BB84 protocol by model checking." International Journal of Engineering Science and Technology (IJEST) 3.7 (2011).

[130] Konyukhov, Vitaliy. "Mathematics of Post-Quantum Cryptography." (2022).

[131] Lee, Chankyun, Ilkwon Sohn, and Wonhyuk Lee. "Eavesdropping detection in BB84 quantum key distribution protocols." IEEE Transactions on Network and Service Management 19.3 (2022): 2689-2701.

[132] W. Wootters and W. Zurek, "A single quantum cannot be cloned," Nature, vol. 299, pp. 802-803, Oct. 1982

[133] C. Pacher, A. Abidin, T. Lorunser, M. Peev, R. Ursin, A. Zeilinger, and J.-A. Larsson, "Attacks on quantum key distribution protocols that employ non-ITS authentication," Quantum Inf. Process., vol. 15, no. 1, pp. 327-362, Jan. 2016.

[134] . Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," Phys. Rev. Lett., vol. 85, no. 6, pp. 1330-1333, Aug. 2000.

[135] N. Lutkenhaus, "Security against individual attacks for realistic quantum key distribution," Phys. Rev. A, vol. 61, no. 5, May 2000, Art. no. 052304

[136] Erven, Chris. "On experimental quantum communication and cryptography." (2012).

[137] J. Hasegawa, M. Hayashi, T. Hiroshima, and A. Tomita. Security analysis of decoy state quantum key distribution incorporating finite statistics. eprint, quant-ph/0707.3541, 2007.

[138] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device- independent security of quantum cryptography against collective attacks. Phys. Rev. Lett., 98:230501, 2007.

[139] Advances in device-independent quantum key distribution:npj Quantum Information, Vol. 9, No. 1 | 18 February 2023

[140] O.L. Guerreau, F.J. Malassenet, S.W. McLaughlin, J.M. Merolla, "Quantum key distribution without a single-photon source using a strong reference," IEEE Photonics Technology Letters, vol.17, no.8, pp.1755-1757, Aug. 2005.