THE CONSTRUCTION OF QUANTUM BLOCK CIPHER FOR GROVER ALGORITHM

ALMAZROOIE MISHAL EID

UNIVERSITI SAINS MALAYSIA

2018

THE CONSTRUCTION OF QUANTUM BLOCK CIPHER FOR GROVER ALGORITHM

by

ALMAZROOIE MISHAL EID

**Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosphy**

January 2018

ACKNOWLEDGEMENT

Always All Thanks to Almighty Allah

- My father, my mother, my second mother, my Sultan, my Sultanah, my Gassan, my brothers, my sisters, my nephews, all of my family, **Thank you**.

- My supervisor Prof. Azman Samsudin, my co-supervisor Prof. Rosni Abdullah, my co-supervisor Dr. Kussay N. Mutter, **Thank you**.

- My dear friends, **Thank you**.

- A word of appreciation goes to https://stackexchange.com/, and https://arxiv.org/.

- To accomplish this work and write this draft, I have been using several free softwares that vary from Operating System, Compilers, SDK, Applications, Libraries, to small scripts such as Linux kernel, GCC, Python, Gnuplot, LaTeX, libquantum, and many others. Hence, to all those researchers and developers who have contributed in these free softwares, **Thank you**.

Thank you

TABLE OF CONTENTS

CHAPTER 4 – IMPLEMENTATION, EXPERIMENTS AND RESULTS

LIST OF TABLES

LIST OF FIGURES

Page

KONSTRUKSI SIFER BLOK KUANTUM UNTUK ALGORITMA GROVER

ABSTRAK

Kriptografi asimetrik dan simetrik dipercayai selamat daripada sebarang serangan dengan menggunakan komputer klasik. Walau bagaimanapun, pandangan ini tidak lagi sah dengan wujudnya pengkomputeran kuantum. Dengan adanya serangan kuantum adalah dianggap bahawa tiada jaminan keselamatan untuk algoritma kriptografi asimetrik yang berdasarkan pemfaktoran integer atau masalah logaritma diskret. Walaubagaimana pun ancaman yang ditunjukkan oleh pengkomputeran kuantum terhadap kriptografi simetrik tidak jelas berbanding dengan kriptografi asimetrik. Serupa dengan pengkomputeran klasik, untuk melakukan serangan kuantum pada sifer blok klasik, sifer blok tersebut perlu direka bentuk dan dilaksanakan sebagai litar terbalik kuantum di dalam platform kuantum. Namun begitu, tiada reka bentuk litar terbalik kuantum untuk sebarang algoritma kriptografik klasik simetri yang membolehkan seseorang itu mengkaji dan membuat analisa mengenai kebarangkalian ancaman yang mungkin dipamerkan oleh saingan kuantum terhadap keselamatan algoritma kriptografi simetrik. Dalam kajian ini, reka bentuk kuantum untuk struktur Feistel dan sifer blok SPN dibentangkan. Pertamanya, komponen utama yang digunakan untuk menghasilkan kesan dan kekeliruan dalam tulisan rahsia sifer blok direka sebagai litar terbalik. S-Boxes yang direka khas seperti yang terdapat pada sifer DES dan S-Boxes yang dihasilkan berdasarkan kepada matematik seperti yang terdapat pada AES dibina sebagai litar kuantum. Medan terhingga (finite fields) $\mathbb{F}_2[x]/(x^4+x+1)$ dan $\mathbb{F}_2[x]/(x^8+x^4+x^3+x+1)$ yang digunakan oleh SAES dan AES telah dipakai guna dalam kajian ini. Seterusnya, semua litar digabung untuk membentuk versi kuantum sifer blok. Dengan menggunakan Simulator Quantum, serangan kuantum telah dilakukan dengan menggunakan algoritma Grover untuk mencari kunci rahsia. Sifer kuantum yang dicadangkan telah digunakan sebagai kotak hitam untuk pencarian kuantum. Pencarian kunci dengan menggunakan jangkaan sifer blok kuantum yang dicadangkan perlu sepadan dengan keputusan pencarian dengan menggunakan sifer blok klasik yang lain. Di samping itu, untuk kunci bersaiz n-bit dan ruang kunci bersais N seperti $N = 2^n$, kunci rahsia tersebut boleh dicari dalam langkah pengiraan O$(\frac{\pi}{4}\sqrt{N})$ seperti yang ditafsirkan oleh algoritma Grover. Keputusan menunjukkan bahawa sifer yang berdasarkan pada struktur Feistel dan sifer yang berdasarkan pada blok SPN boleh direka sebagai litar terbalik kuantum dengan kos polinomial. Oleh itu, untuk melancarkan serangan kuantum kepada sifer blok klasik adalah satu kemungkinan yang boleh berlaku.

THE CONSTRUCTION OF QUANTUM BLOCK CIPHER FOR GROVER ALGORITHM

ABSTRACT

Asymmetric and symmetric cryptography are believed to be secure against any attack using classical computers. However, this view is no longer valid in the presence of quantum computing. Asymmetric cryptographic algorithms which are based on integer factorization or discrete logarithms problems are rendered unsecured against quantum attacks. In contrast, threats posed by quantum computing to symmetric cryptography is not clear compared with asymmetric cryptography. Similarly to classical computing, to conduct a quantum attack on a classical block cipher, the block cipher must be designed and implemented as a quantum reversible circuit in a quantum platform. There is no existing quantum design for any classical symmetric cryptographic algorithm such that one could study and analyze in practice the possible threats that might be posed by a quantum adversary to the security of the symmetric cryptographic algorithms. In this study, quantum designs for Feistel structure and SPN block ciphers are presented. First, the main building components that are used to provide diffusion and confusion in block ciphers are designed as reversible circuits. The hand crafted S-Boxes such as in DES cipher and the mathematically generated S-Boxes such as in AES are constructed as quantum circuits. The finite fields $\mathbb{F}_2[x]/(x^4+x+1)$ and $\mathbb{F}_2[x]/(x^8+x^4+x^3+x+1)$ in SAES and AES respectively, are considered in this study. Then, all the circuits are put together to form the quantum version of the block cipher. By using a Quantum Simulator, quantum attacks are conducted by using Grover's algorithm to recover the secret key. The proposed quantum cipher is used as a Black-box for the quantum search. The expected results of the proposed quantum block ciphers have to match those ones of the classical block ciphers. In addition, for a key of n-bit size and key space of N such that $N = 2^n$, the key can be recovered in $O(\frac{\pi}{4}\sqrt{N})$ computational steps as expected by Grover's algorithm. The results show that Feistel structured and SPN block ciphers can be designed as quantum reversible circuits in polynomial costs. Therefore, it is possible to mount quantum attacks on classical block ciphers.

CHAPTER 1

INTRODUCTION

1.1 Motivation

Information security heavily relies on modern cryptography. Most of the cryptographic algorithms are designed to be resistant against attacks. Asymmetric cryptography or public-key cryptography is one of the cryptographic primitives that is based on computationally hard problems. Although asymmetric cryptosystems that are based on hard problems have been proven secure, they are not efficient for the use in real-time encryption of large messages. Thus, one of the main uses of asymmetric cryptosystems (for example RSA) is to distribute the secret key shared by two parties that are communicating in a secure channel; in this task, the second primitive of cryptography (symmetric cryptography or private-key cryptography) performs the real-time encryption.

In symmetric cryptography, when the symmetric cryptosystem exhibits good randomness level and the exhaustive search for the secret key is the only attack that can break the cryptosystem, the hardness or strength of the cryptosystem is determined by the size of the encryption key. A key with n bits size has 2^n possibilities of keys and therefore $O(2^n)$ steps are needed to try all of these possibilities. For example, 2^{128} operations are required to try all the possibilities of a 128-bit key, which cannot be achieved by using conventional or classical computing techniques.

Asymmetric and symmetric cryptography along with some other cryptographic primitives play the crucial role in information security. Thus, ensuring of the strength and security of the cryptographic algorithms against any possible threats is at most concern to everyone. A new arising threat comes from a relatively new technology of computation which is completely different from the classical computing. Thus, the primarily motivation of this work is to study the impact of quantum computing on the security of the classical symmetric block ciphers.

1.2 Problem Statement

There is no existing quantum design for any classical symmetric cryptographic algorithm such that one could study and analyze in practice the possible threats that might be posed by a quantum adversary to the security of the symmetric cryptographic algorithms. Hence, the research problem states that studying the practical impact of the quantum computing on symmetric cryptography cannot be accomplished unless the symmetric cryptographic algorithm is designed as a quantum reversible circuit and implemented on a quantum platform. Moreover, there are only very few published works (Akihiro et al., 2000; Kaplan, 2014; Roetteler et al., 2015; Grassl et al., 2016) that have discussed the impact of quantum computing on the current symmetric cryptographic algorithms and those papers are completely based on assumptions that the symmetric algorithms had already been designed and implemented in a quantum platform as quantum circuits.

Asymmetric and symmetric cryptography are believed to be secured against any attack using classical computers. In fact, this view is no longer valid for a different technology where the calculations are performed based on the behavior of particles at subatomic levels (laws of quantum mechanics). Thus, quantum computing poses threats to asymmetric and symmetric cryptography. For asymmetric cryptography, in the presence of scalable quantum computers, the cryptographic algorithm based on the factoring problem would be completely jeopardized (Shor, 1997). Various studies have been published on quantum number factorization (Lanyon et al., 2007; Markov et al., 2013; Martin et al., 2012). Consequently, other hard problems besides the factoring problem are being investigated, such as code-based cryptography and lattice-based cryptography (Bernstein et al., 2008). Moreover, some solutions to the key distribution problem have come from quantum mechanics and subsequently opened the field of quantum cryptography (Mihara, 2008; Nascimento et al., 2010; Zhang et al., 2013; Kabgyun et al., 2015).

Regarding cryptanalysing symmetric cryptography, the situation remains doubtful compared to the quantum computing on asymmetric cryptography. The only known quantum threat to symmetric algorithms is that the exhaustive key search can be performed more efficiently on the quantum platform with quadratic speedup by using Grover's algorithm (Grover, 1996). However, the quantum exhaustive search attack cannot be applied unless the symmetric algorithm is implemented on the quantum platform as a quantum circuit.

For quantum asymmetric cryptanalysis such as RSA, to factor a large integer N into its two prime numbers p and q, designing a quantum circuit for the RSA algorithm on a quantum platform is unnecessary. In contrast, studying the quantum impact on symmetric cryptography against any possible quantum attack will remain ambiguous and unclear unless the symmetric algorithms are implemented as quantum circuits.

1.3 Research Questions

Studying the impact of the quantum computing on symmetric cryptography cannot be accomplished unless the symmetric cryptographic algorithm is implemented on quantum platform. Hence, the questions of the current research are as follows:

1. How to design quantum circuits for the main core components that provide the diffusion and confusion properties of a block cipher?

2. What are the costs of the quantum design of a block cipher?

3. If a block cipher is implemented as a quantum circuit in a polynomial cost, what will be the impact of the quantum exhaustive key search attack on the block cipher?

1.4 Research Objectives

The main goal of this research is first to come up with concepts for new quantum designs for classical symmetric cryptographic algorithms. Then, implementing those designs experimentally as quantum circuits to be tested on a quantum mechanics simulation. Thus, to accomplish the main goal, we have to design a quantum circuit for every building component of a symmetric algorithm. Hence, the objectives of this study are:

1. To design reversible quantum circuits for the core components of the classical symmetric cryptographic algorithms.

2. To analyze the complexity of the quantum block cipher.

3. To prove the validity of the quantum designs.

4. To calculate the quantum costs of the quantum exhaustive key search attack.

1.5 Research Scope

This study involves two different technologies: classical and quantum computing. Since the main goal of this work is to come up with new quantum designs for classical symmetric cryptography specifically the block ciphers, both classical and quantum computing will be explored in detail.

In respect to classical computing, since cryptography is a multidisciplinary field, the main primitives of classical cryptography will be explored. Then, the focus will be narrowed down on symmetric cryptography. The classical block ciphers will be covered in detail in term of functionality, and the building components. Although classical asymmetric cryptography is beyond the scope of this research, but the public key algorithm RSA will be discussed since it is involved in the launch of the revolution of quantum computing.

Regarding quantum computing, the technology of quantum mechanics will be explored first in detail. Then, this thesis will highlight the differences and similarities between classical and quantum computing. The quantum elementary gates and the main quantum algorithms will be deeply explored. After that, the methods of designing reversible circuits will be studied in order to design quantum circuits for the classical block cipher to investigate the impact of quantum technology on those block ciphers.

1.6 Research Methodology

Cryptology is a branch in Mathematics that encompasses cryptography and cryptanalysis (Schneier, 2015). Cryptography is the science of keeping messages secure whereas cryptanalysis is the science of breaking hidden messages. In Figure 1.1, the field of cryptography is to propose cryptosystems while the cryptanalysis field is to analyze the security of those cryptosystems against all possible threats. This current study is being conducted from the cryptanalysis perspective. More specifically, this study is to contribute in the **practice** of the quantum cryptanalysis as it will be discussed in the following context.

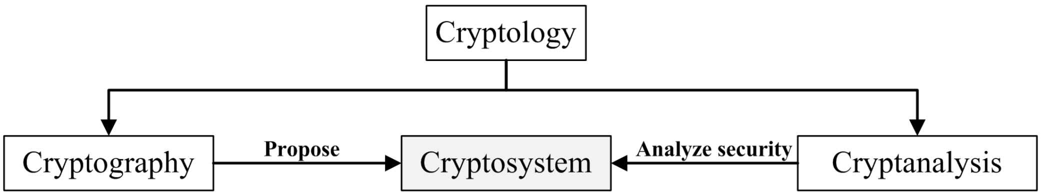

Figure 1.1: Cryptology overview

Since the scope of this work is on classical block ciphers, let consider the five AES (Advanced Encryption Standards) finalists cryptosystems: Rijndael (also known as AES), Serpent, Twofish, RC6, and MARS (NIST, 2017). The best public cryptanalysis of each of these ciphers are shown in Table 1.1.

Table 1.1: Best cryptanalysis of the five AES finalists block ciphers. Note that, brute force refers to *Classical Exhaustive Key Search Attack.*

Block cipher	Key size	Brute Force	Best cryptanalysis	Reference
AES	128-bit	$\mathcal{O}(2^{128})$	$\mathcal{O}(2^{126.1})$	(Bogdanov et al., 2011)
	192-bit	$\mathcal{O}(2^{192})$	$\mathcal{O}(2^{175})$	(Biryukov et al., 2009)
	256-bit	$\mathcal{O}(2^{256})$	$\mathcal{O}(2^{99.5})$	(Biryukov et al., 2009)
Serpent	128-bit	$\mathcal{O}(2^{128})$	$\mathcal{O}(2^{107})$	(Nguyen et al., 2011)
	192-bit	$\mathcal{O}(2^{192})$	$\mathcal{O}(2^{107})$	(Nguyen et al., 2011)
	256-bit	$\mathcal{O}(2^{256})$	$\mathcal{O}(2^{107})$	(Nguyen et al., 2011)
Twofish	128-bit	$\mathcal{O}(2^{128})$	$\mathcal{O}(2^{51})$	(Moriai et al., 2000)
	192-bit	$\mathcal{O}(2^{192})$	$\mathcal{O}(2^{51})$	(Moriai et al., 2000)
	256-bit	$\mathcal{O}(2^{256})$	$\mathcal{O}(2^{51})$	(Moriai et al., 2000)
RC6	128-bit	$\mathcal{O}(2^{128})$	$\mathcal{O}(2^{119})$	(Ebrahim et al., 2014)
	192-bit	$\mathcal{O}(2^{192})$	$\mathcal{O}(2^{119})$	(Ebrahim et al., 2014)
	256-bit	$\mathcal{O}(2^{256})$	$\mathcal{O}(2^{119})$	(Ebrahim et al., 2014)
MARS	128-bit	$\mathcal{O}(2^{128})$	$\mathcal{O}(2^{128})$	–
	192-bit	$\mathcal{O}(2^{192})$	$\mathcal{O}(2^{192})$	–
	256-bit	$\mathcal{O}(2^{256})$	$\mathcal{O}(2^{256})$	–

For instance, all the attacks that are shown in Table 1.1 are based on classical computing or classical Turing Machine (TM). In practice, all of those attacks can be implemented either in software or hardware. For example, consider the brute-force attack (classical exhaustive key search attack) on a block cipher B which has n-bit key size. Assume a message p (plaintext) and its corresponding encrypted message c (ciphertext) such that $\mathsf{B}_k(p) \to c$ where k is the secret key such that $k \in \{0,1\}^n$. The steps of the classical exhaustive key search attack on the block cipher B are shown in Algorithm 1.

Algorithm 1 Classical exhaustive key search attack on a block cipher $\mathbf{B}$

```
Assumption: An algorithm (function $\mathbf{B}(k, p) \rightarrow c$) for the block cipher $\mathbf{B}$ of $n$-bit key size
Input: A chosen pair of a plaintext $p$ and its corresponding ciphertext $c$
Output: The secret key $k$
1 for $k < 2^n$ do
2     if $\boldsymbol{B}(k, p) = c$ then
3         return $k$ //"return" terminates the program and return a value.
```

The steps of the attacks in Algorithm 1 can be easily implemented in software. At line 2 in Algorithm 1, the algorithm of the block cipher $\mathbf{B}$ (cryptographic algorithm or cryptosystem) takes place. Intuitively, the implementation of $\mathbf{B}$ is not an obstacle that may hinder this classical exhaustive key search attack.

In the presence of a scalable quantum computer, the security levels of all existing block ciphers are dramatically altered. The well known quantum threat will be the quantum exhaustive key search attack by using Grover's algorithm. Consequentially, the cryptanalysis of the five AES finalists cryptosystems will be quadratically reduced. For example, the upper bound of the classical exhaustive key search attack on a 128-bit block cipher is $\mathscr{O}(2^{128})$ whereas the quantized version of this attack (*quantum exhaustive key search attack*) has an upper bound of $\mathscr{O}(2^{64})$. Now, consider the same block cipher $\mathbf{B}$ shown in Algorithm 1 and also consider the similar p, c, and $k \in \{0,1\}^n$. The task is to find the secret key k in $\mathscr{O}(2^{n/2})$ queries by using a quantum computer. The steps of this quantum exhaustive key search attack by using Grover's algorithm are illustrated in Figure 1.2.

At ψ_0 in Figure 1.2, the initialization step of Grover's algorithm takes place. The Oracle (Black-Box) of Grover's algorithm takes place at ψ_1. The third component of Grover's algorithm is the Control Phase Flip (CPF) for amplitude amplification of Grover's algorithm which takes place at ψ_2 in Figure 1.2. Note that, all the steps of Grover's algorithm will be discussed

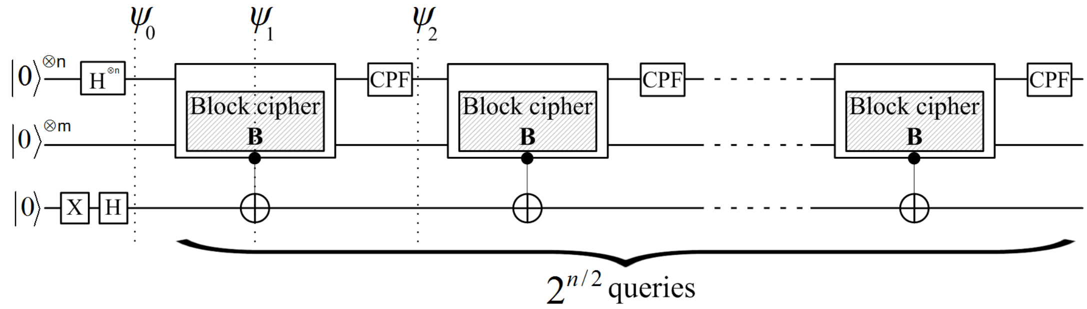

Figure 1.2: Quantum exhaustive key search attack on a block cipher **B**. The shaded boxes refer to quantum circuit of **B**. n is the key size and m is the number of the qubits needed for the workspace.

thoroughly in Chapter 2 in Section 2.2.2. For instance, to apply this attack **in practice**, all the steps at ψ_0, ψ_1, and ψ_2 are needed to be implemented as quantum circuits. Both ψ_0 and ψ_2 can be easily implemented whereas the implementation of ψ_1 completely depends on the algorithm of the block cipher **B** which is analogue to the function at line 2 in Algorithm 1. In this current study, we propose quantum design for the block cipher **B**.

Classical block ciphers are composed of some building components which provide the needed diffusion and confusion properties. These building components involve key mixing, bits swapping, expansion, compression, bits shifting, bits substitution, logic and Arithmetic operations. In this work, we propose quantum circuits for most of the building components used in the standard block ciphers. Moreover, we propose quantum versions for three case studies (three classical block ciphers) adopted in this work.

In parallel with this work, a recent work by Grassl et al. (Grassl et al., 2016) that studied the estimated quantum resources needed to design a quantum circuit for the block cipher AES (AES, 2015). Grassl et al. proposed quantum circuits for the three variants of AES-k where $k = \{128, 192, 256\}$. In this work, we present a complete quantum circuit for AES-128 with the exact quantum resources required to implement it. This current study improves the previous result of Grassl et al. (Grassl et al., 2016) by proposing a more space-efficient method for implementing AES-128 quantumly which reduces the difficulty of this task in practice.

A systematic plan for the research methodology is set to achieve the research objectives. The approach of this research is illustrated in Figure 1.3. The research methodology consists of three main stages: literature review, design stage, and implementation and testing. In the first stages, the research problem and gap are identified. Quantum computing is completely different from the classical computing and classical Turing Machine (TM). Hence, the laws of quantum mechanics are studied in this stage since quantum computing is based on quantum mechanics. Also, the quantum design methods are investigated.

In the second stage, quantum designs for the core components of block ciphers are presented. These core components are permutations and substitution that provide respectively the diffusion and confusion properties stated in Shannon's theory. Then, a complete quantum design for classical block ciphers are presented. Three block ciphers of different structures and approaches of providing diffusion and confusion are adopted in this work as case studies. In this methodological stage, the first research question is addressed.

A quantum key search attack is constructed in the third stage. The quantum block cipher is integrated into a Black-box as a Boolean function in Grover's algorithm to conduct a quantum key search attack. The complexity analysis of the quantum design and the costs calculation of the quantum attack are conducted in this stage. Thus, the second and third research questions are addressed.

The last stage in the research approach is to validate the designs by comparing the results of the quantum block ciphers with the classical results. Moreover, Grover's algorithm is used as a benchmark to verify the quantum design. Grover's algorithm outperforms quadratically faster than any other classical exhaustive search algorithm. Hence, the validity benchmark of

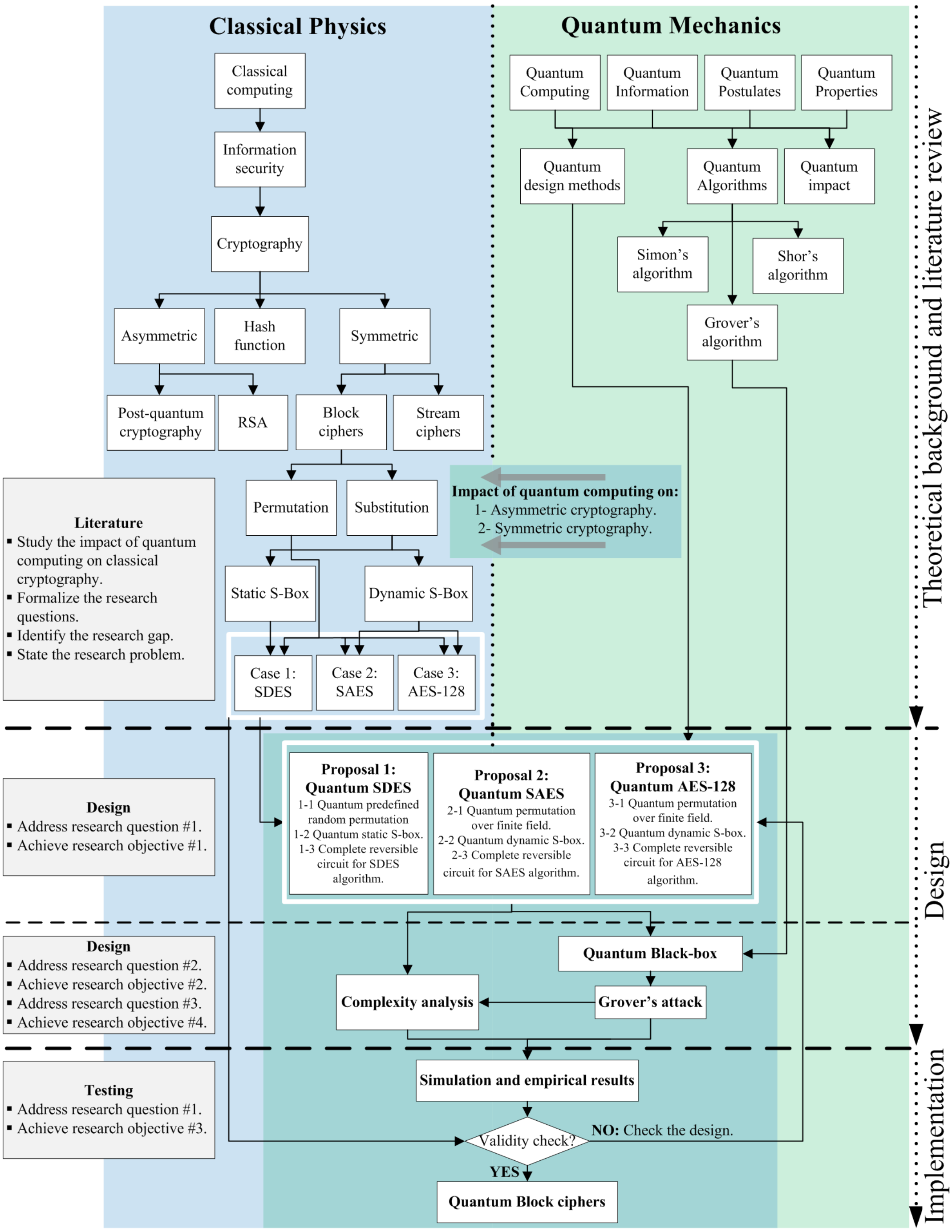
Classical Physics
Quantum Mechanics
Classical computing
Information security
Cryptography
Asymmetric
Hash function
Symmetric
Post-quantum cryptography
RSA
Block ciphers
Stream ciphers
Permutation
Substitution
Static S-Box
Dynamic S-Box
Case 1: SDES
Case 2: SAES
Case 3: AES-128
Quantum Computing
Quantum Information
Quantum Postulates
Quantum Properties
Quantum design methods
Quantum Algorithms
Quantum impact
Simon's algorithm
Shor's algorithm
Grover's algorithm
Impact of quantum computing on:
1- Asymmetric cryptography.
2- Symmetric cryptography.
Literature
Study the impact of quantum computing on classical cryptography.
Formalize the research questions.
Identify the research gap.
State the research problem.
Design
Address research question #1.
Achieve research objective #1.
Design
Address research question #2.
Achieve research objective #2.
Address research question #3.
Achieve research objective #4.
Testing
Address research question #1.
Achieve research objective #3.
Proposal 1: Quantum SDES
1-1 Quantum predefined random permutation
1-2 Quantum static S-box.
1-3 Complete reversible circuit for SDES algorithm.
Proposal 2: Quantum SAES
2-1 Quantum permutation over finite field.
2-2 Quantum dynamic S-box.
2-3 Complete reversible circuit for SAES algorithm.
Proposal 3: Quantum AES-128
3-1 Quantum permutation over finite field.
3-2 Quantum dynamic S-box.
3-3 Complete reversible circuit for AES-128 algorithm.
Quantum Black-box
Complexity analysis
Grover's attack
Simulation and empirical results
Validity check?
NO: Check the design.
YES
Quantum Block ciphers
Theoretical background and literature review
Design
Implementation

Figure 1.3: Research methodology

the proposed quantum design is the quadratic speedup to recover the secret key.

1.7 Significant of Research

In this work, we will try to put one step forward to clarify the ambiguity in the quantum threats to classical block ciphers. Mainly, this study is conducted to fill the research gap between quantum computing and symmetric cryptography by presenting for the first time quantum circuits for the symmetric building components.

1.8 Thesis Structure

This thesis is organized as follows: Chapter 2 provides a literature on both technologies classical and quantum computing. The literature review in Chapter 2 deals with both the theoretical background and the related works. The theoretical background introduces the main differences between classical Physics and Quantum mechanics, the development of quantum computing, quantum Turin Machine, Quantum complexity class, and the principles of quantum computing and reversible circuits. While some of the related works include studies that examined the impact of quantum computing on classical asymmetric cryptography, other related works investigated the classical symmetric cryptography. The proposed quantum designs are presented in Chapter 3. This chapter presents the proposed method and it is composed of subsections, each of which presents the quantum design of a single case study. Chapter 4 presents the results of simulating the proposed designs. Chapter 4 is also divided into some subsections, each of which presents the results of one case study. The research questions are discussed in Chapter 5. The final chapter presents the conclusions of the study and presents some directions for future studies.

CHAPTER 2

BACKGROUND AND LITERATURE REVIEW

> *"What I am going to tell you about is what we teach our physics students in the third or fourth year of graduate school... It is my task to convince you not to turn away because you don't understand it. You see my physics students don't understand it. ... That is because I don't understand it. Nobody does."*
>
> – Feynman, Richard P., *Nobel Lecture, The Strange Theory of Light and Matter*

This chapter consists of two main sections: theoretical background and literature review. In the theoretical background section, the cryptography and its crucial role in the information security will be introduced. Then, the primitives of cryptography will be discussed with narrowing down the focus on the symmetric cryptography. In addition. the principles of quantum mechanics, quantum elementary gates, and basic quantum algorithms are explained. In the second section, literature study on relevant concepts is performed. Even though, the related works to the scope of this study are very few, the impact of the quantum computing on both cryptographic main branches: asymmetric and symmetric is discussed.

2.1 Background

2.1.1 Classical Cryptography

Confidentiality, Integrity, and Availability are the three core concepts of information security. The three concepts form what is called CIA triad (Perrin, 2015). After establishing CIA triad and even though it was well established to define security objectives, some more concepts have been included in order to present a complete picture of security. Authenticity, accountability, auditability, privacy, and non-repudiation are the concepts that included to CIA triad (Stallings, 2010).

Cryptography plays the essential role to provide the fundamental security requirements for information and computing services. In the famous book Codebreakers by Khan David (Kahn, 1974), the author has stated cryptography as the science of the secret writing. Cryptography have become a multidisciplinary science where disciplines of computer science, mathematics, electrical engineering and physics intersect. Mostly, cryptographic algorithms depend on hard problems or mathematical hard problems to provide the fundamental concepts of information security. The cryptographic algorithms are designed such that within the available computational resources of the existing classical computing technology, it is very hard for the adversary to break the algorithm. Cryptography consists of three basic primitives: asymmetric, symmetric and hash functions. The following subsections will present these three primitives with more detail in symmetric primitives hence they are within the scope of this study.

2.1.1(a) Asymmetric Cryptography

Asymmetric cryptography or public-key cryptography is the set of the cryptographic algorithms that employ a pair of two distinct keys; one is called public key and the other is private key. The public key is used for encryption and announced publically whereas the private key is kept secret and used for decryption. Public-key cryptography was established by Diffie and Hellman in 1976 (Diffie and Hellman, 1976). Generally, asymmetric algorithms are based on mathematical hard problems such as integer factorization as in RSA (Rivest et al., 1978), discrete logarithms as in ElGamal cryptosystem (ElGamal, 1985), and Elliptic Curve as in elliptic curve Diffie-Heilman (ECDH) (Lopez et al., 2000) also in Elliptic Curve Digital Signature (ECDSA) (Daniel, 2005). All of those algorithms are designed such that the generation of public and private keys is computationally easy but it is infeasible for any adversary to determine the private key from its corresponding public key.

Unlike most of symmetric algorithms, most of the known asymmetric cryptographic algorithms so far are computationally costly. Due the computational complexity of asymmetric algorithms, they are normally used in either symmetric key distribution or digital signature. Regarding symmetric key distribution, since the public-key cryptosystems do not require a secure channel to establish the connection between the parties involved in the communications, they are used to encrypt the symmetric key and distribute it to the communication parties. This is a scenario where asymmetric cryptography provide the confidentiality in information security. Figure 2.1 illustrates the scenario when an asymmetric cryptosystem is used for encryption of short messages. As shown in Figure 2.1, Allice sends a message M to Bob, she uses Bob's public key to encrypt the message M. Only Bob's private key can decrypt the produced ciphertext.

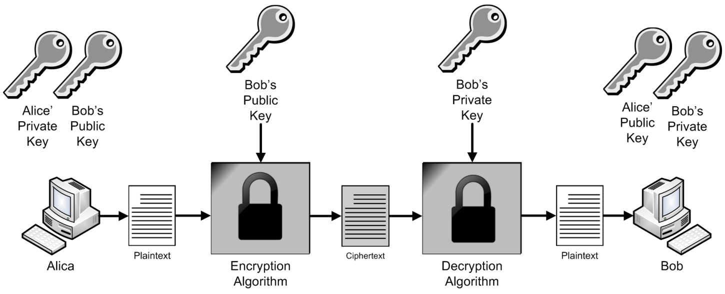

Figure 2.1: Simplified model of asymmetric cryptographic system

The other main usage of asymmetric cryptography is to provide message authentication which is one of the concepts of information security. For message authentication, first the message will be hashed to produces what called digest. Then, the digest is encrypted using user private key which producing digital signature. Thus, the message can be easily verified by anyone using the corresponding public key of the sender. Some of asymmetric algorithms used in digital signature are DSA, ECDSA, ElGamal, and Rabin signature algorithm.

2.1.1(b) Symmetric Cryptography

Symmetric-key cryptographic are the set of algorithms that make use of an identical secret key shared by both parties of the communication. In symmetric cryptography, the same key is used to encrypt a plaintext and to decrypt the ciphertext. Privacy and authenticity are the main two goals provided by symmetric cryptography for information security. There are two types of symmetric-key encryption: stream ciphers and block ciphers. In stream ciphers, the message or the plain text is typically encrypted byte by byte. Some of the well known stream ciphers are such as Slasa20 (Bernstein, 2008), Rabbit (Boesgaard et al., 2003). Whereas, a block of bytes of the message is encrypted at once in block ciphers. Examples of some of the common block ciphers are DES, AES, Blowfish, Serpent, Twofish and some more others.

Figure 2.2 shows that both of Alice and Bob share same secret key (K). The key (K) is used by Alice to encrypt (E) the message (M) and generate the ciphertext (C) as ($C = E_K(M)$). Bob who shares the same key with Alice, is the only one who capable to decrypt (D) the message (M). The ciphertext is decrypted by Bob using (K) to get the message (M) as $M = D_K(C)$.

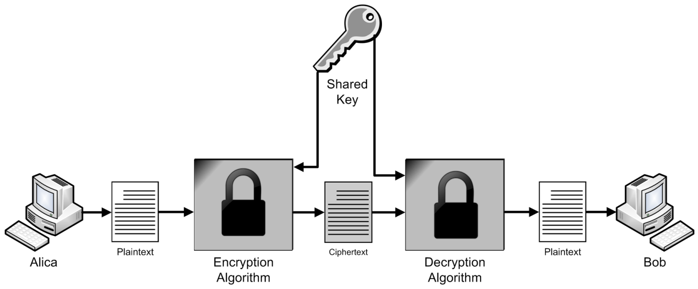

Figure 2.2: Simplified model of symmetric cryptographic system

Although symmetric cryptography are fast and efficient compared with asymmetric cryptography, but it requires a secure channel to initiate the communication. Thus, an asymmetric cryptosystem such as RSA is used to distribute the symmetric secret key to the communication parties. The strength of a symmetric cryptosystem is determined by the secret key size. That statement is true if the symmetric cryptosystem exhibits a good randomness level and it is very hard to detect any linearity in the produced ciphertext. Hence, the only effective attack is the exhaustive search for the key.

The theory of provable security of symmetric cryptography was established in 1949 by Shannon (Shannon, 1949). Shannon theory or Shannon perfect secrecy implies that for any message m and its corresponding ciphertext c there is at least one unique key k that connects them. A cryptosystem (K,P,C,E,D), where K is the set of keys, P is the set of plaintexts, C is the set of ciphertexts, E is the encryption rule such that $for\ k \in K : E_k(x)$,and D is the decryption rule such that $for\ k \in K : D_k(x)$, has perfect secrecy if and only if:
$Pr(x|y) = Pr(x),\ \forall x \in P,\ y \in C$, where:

- $Pr(k) = \frac{1}{|K|},\ \forall k \in K,$
- $\forall x \in P,\ y \in C,\ \exists$ unique k such that $E_k(x) = y$.

According to Shannon theory, a secure cipher should incorporate the two properties of *confusion* and *diffusion*. Confusion means that the ciphertext must not show any relation with its corresponding plaintext. The diffusion property emphasizes that there is no any statistical structure between the ciphertext and the key. The diffusion can be achieved by using *permutation* on the bytes or bits of the plaintext. Whereas, the confusion property can be achieved by using some complex *substitution* subroutines.

2.1.1(c) Hash Function

The third cryptographic primitive is called hash function. Hash functions or unkeyed cryptographic primitives convert a variable length message into a specific length hash value. They concern about the authentication and integrity of messages. Normally, a fixed length output called digest is produced from a message of arbitrary length that is fed into a hash function as an input. Figure 2.3 represents the cryptographic hash function.

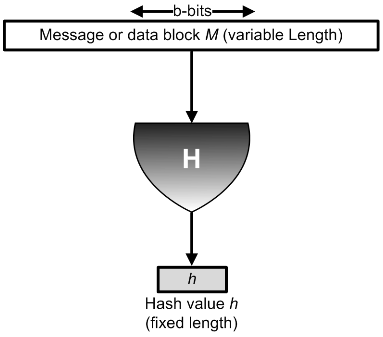

Figure 2.3: Cryptographic hash function

2.1.2 Classical Physics and Quantum Physics

For the sake of understanding the big picture of the Quantum Mechanics theories, a fast glance on the classical Physics is presented first. It should be noted that, the following overview on the Physics is an attempt of a none physicist who attempts to know the types of problems that Physics tries to solve and the solutions proposed by physicists. Knowing how physicists solve the problems is not discussed in this overview.

2.1.2(a) Classical Physics

This work is a computer science thesis. Therefore, for the benefit of the computer science reader, an introductory section on Quantum Physics is included. The study of matter properties, evolutions, and behavior is the heart of the science of Physics. In addition, Physics attempts to explain any phenomena in the nature, regardless of the objects involved in this phenomena, which could be so huge such as the whole universe or could be extremely small particles. For the sake of simplicity, it is plausible to classify the modern Physics into classical Physics (or Newtonian Physics) and Quantum Mechanics. The classical Physics is the study of the physical reality of objects that are larger than the subatomic sizes such as atoms, molecules, “me”, our solar system, our galaxy, and the universe. On the other hand, Quantum Mechanics is the study of the physical “reality” of the objects (called particles) at the subatomic sizes such as electrons, protons, positrons, and photons. It should be noted that, the term reality is placed between quotation marks in the definition of quantum mechanics because this is the keyword to differentiate between the classical Physics and quantum Physics.

For instance, before introducing Quantum Mechanics, a glance on the classical Physics would be helpful in order to facilitate the comparison between both of them. A series of scientific discoveries arose in the last two centuries. These scientific discoveries are some of the main reasons for all revolutions we can see nowadays in all aspects of our life. Some of these discoveries which play crucial roles in both classical and quantum Physics will be introduced later. Other important basic premises and concepts such as determinism, realism, causality, and locality are discussed in details in the following sections. However, it is worthy to mention that these premises are intuitively considered to be facts, rather than being premises (axioms or postulates). Although from the **logical** view of classical Physics, such premises and concepts are considered to be facts, it is important to provide a meaning for *logical*. While some authors such as in (Patrick Hurley, 2011) have defined logic as “the study of the correct reasoning”, some other authors such as (Shapiro Stewart, 2013; What is Logic?, 2015) have defined it as “a tool to develop reasonable conclusions based on a given set of data”. Here are some examples of logical models in classical Physics. Example 1: if $x > 7$, then $x > 2$, Example 2: if someone is in Malaysia, then he is not in Saudi Arabia, and Example 3: in this model, let the sizes and the dimensions of this model are shrunk to the sub-atomic scales, if a very tiny particle of some nanometres dimensions is in the location x_1, then the particle is not in the location x_2. All the three examples given above hold true according to the logic of the classical Physics. However, in the beginning of the 20th century, scientists discovered some strange phenomena which do not obey the classical logic. For example, a very tiny particle could be in the location x_1 and at the same time it could be in the location x_2 where $x_1 \neq x_2$. Hence, since there are some arising doubts about the logic itself, it is plausible to consider the basic premises (determinism, realism, causality, and locality) as postulates in classical Physics. Some justification will be presented in some of the following sections. Before going through these postulates, it is worth to introduce the spacetime cones (light cones or Einstein-Minkowski spacetime) in order to use it while discussing the classical postulates.

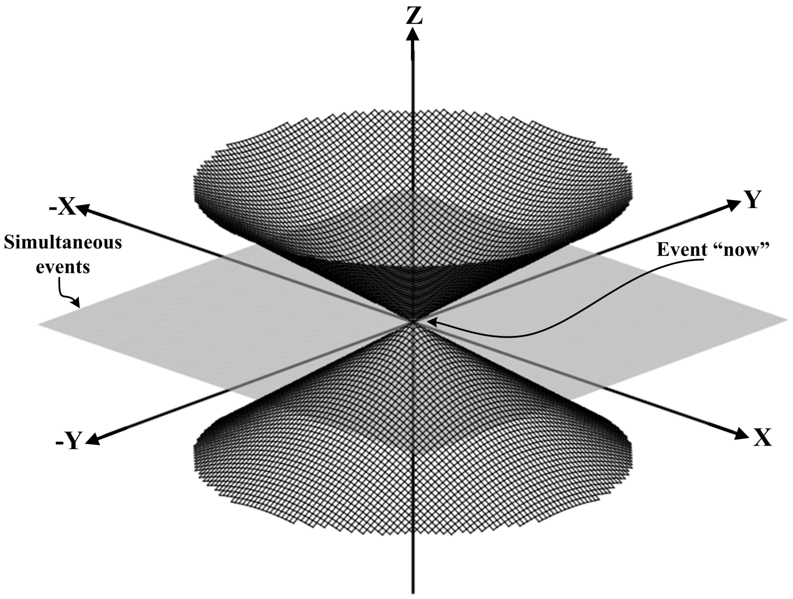

Figure 2.4: Einstein-Minkowski spacetime

Figure 2.4 shows the spacetime cones (Einstein-Minkowski spacetime) (Einstein, 1905; Einstein and Minkowski, 1920). In this figure, the X- and Y-axes represent the space (the physical dimensions of objects). Usually, the physical dimensions of an object are represented by three axes X for length, Y for width, and Z for height. In the spacetime cones, if the space is represented by three dimensions and one extra dimension for the time, the figure would be very complex. Moreover, this model was a result of the special relativity theory not the general relativity theory (Einstein, 1916). All the past and the future events related to the event "now" lie on the surface of the past and the future cones. The events outside the cones cannot communicate; they rather affect the event “now” unless their speed is greater than the speed of light. According to the relativity theory, it should be noted that there is no object can go faster than the speed of light. In the following discussion, the classical postulates are discussed with respect to the light cones.

Determinism: With the complete knowledge about the past events that caused an event now, the future event(s) can be determined with certainty (Hoefer, 2016). Some physicists such as Einstein[1] believe that the universe is just a super deterministic machine which was initiated with an initial state at the *BigBang* and everything in the nature is deterministic even though for the first time it may look like randomness (Stewart, 1989).

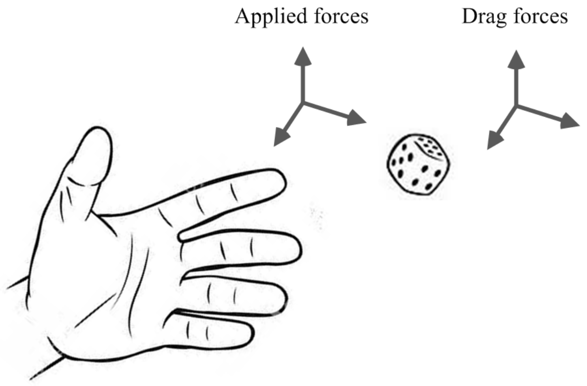

Figure 2.5: Forces affect the process of throwing a dice. This figure is developed based on the figure from (Gettyimages, 2017).

Tossing coins and throwing dices are the well-known examples of random-like behavior. However, according to the classical Physics, a process (such as tossing coins or throwing dices) is completely deterministic and not probabilistic. This is because the random-like behavior is due to the lack of information about the forces applied to such objects, as shown in Figure 2.5. Mainly, there are two types of forces: applied forces and drag forces. The applied forces are the

[1] Albert Einstein was one of the major players in the development of the Quantum Mechanics because he was against Quantum theories.

ones that cause the dice movement. While the drag forces are the ones that oppose the motion of the dice such as air resistance. If all the forces affecting on the process of throwing a dice are known, the results can be predicted with certainty.

Another example is the random functions that are used in Computer Sciences to generate random numbers. From the classical Physics perspectives, such random functions are deterministic where the random-like behavior is because of the lack of information. Logically[2], the previous statement holds true and hence two examples are given. The first example is the pseudo random number generator (PRNG) function $rand()$ in the $math$ library. If the initial seed of the function and the number of the function calls are both known, one can predict the new output of that function with certainty. One could argue that such $rand()$ function is pseudo random not a true random function. Hence, the second example is a true random number generator (TRNG) approach that was proposed by Jesen et al. (Teh et al., 2015). In that TRNG approach the authors have made use of random-like behavior of the chaotic map (logistic chaotic map) and the phenomena of the race condition in the multi-cores processors. If the initial state of the chaotic map along with the number of the map iterations are known, the new value of the chaotic function can be determined. The race condition happens when the concurrent threads race to update a particular memory location in a parallel platform (Heterogenous or Homogenous). Initially, the concurrent threads are spawned simultaneously to invoke a similar task. Surprisingly, some threads execute the job faster than others. If the processor's scheduling, threads mapping, and the accurate physical wiring dimensions are known, the thread that will win the racing could be defined.

As shown in Figure 2.4, to demonstrate the Determinism postulate on the space-time model, one could say that the future event of any event "now" can be determined if there is complete

[2] The adverb *logically* is spontaneously used in the sentence. However, one may asks: is it the classical logic or another new logic? At this particular point, the logic refers to the classical one which we are used to recognize.

knowledge about the past events that caused the event “now”.

Realism: It is the second postulate in the classical Physics. It states that an object exists prior observing it. Obviously, at the first while, one will consider this postulate as a fact since the physical objects exist either we observe them or not (Paul Marmet, 1993). However, this postulate has not yet been proven true, and at the same time it is not falsified. Realism can be demonstrated on the spacetime model in Figure 2.4, so that at any particular moment of time, a physical object (an event) exists somewhere whether the object is being observered or not.

Causality: In causality, for any effect (an event) occurs by a preceding cause (past event). Causality is sort of a chain of cause-effect (Hoefer, 2016). As shown in Figure 2.4, any effect “now” occurs due to some preceding causes (past events).

Locality: It states that any event in the spacetime is influenced by its surrounding events (Haag Rudolf, 1992). In addition, an even at a particular point in the spacetime model as shown in Figure 2.4, cannot cause a simultaneous event at a different point.

All the mentioned four postulates (determinism, realism, causality and locality) hold true in the real life for objects whose sizes are larger than the sub-atomic sizes. Although from a philosophical point of view, the determinism contradicts with the free-will theorem, the postulates hold true in classical Physics. On the other hand, at the sub-atomic level, the objects (particles) behave completely different. As the world down there at the sub-atomic levels seems to be non-deterministic, Quantum Mechanics tries to explain the Physics at that levels.

2.1.2(b) Development of Quantum Mechanics

Here are some of the scientific discoveries that were revealed in the last century which play crucial roles in the development of the classical Physics as well as Quantum Mechanics. When

Max Planck studied the Black Body Radiation Experiment in 1900 (Max Planck, 1900), he formulated the relation between the energy and the frequency such that: $E = hf$ where E is energy, f is frequency and h is the Planck's constant (one of the most important numbers $h = 6.626070040 \times 10^{-34} J.s$). He also hypothesized that the omitted electromagnetic energy (radiation) is “quantized”; i.e. in discrete amounts.

Einstein was one of the few researchers who took the Planck's hypothesis seriously. In 1905, he published his seminal paper about the photoelectric effect (Einstein, 1905). He proposed that the light photons are discrete quantum energy. This work of Einstein and the previous work by Planck were the fundamental core for the launch of the Quantum Mechanics. In the same year, Einstein published his other three profound papers that revolutionized sciences (Brownian motion, Special relativity, and Mass-Energy Equivalence). The year of 1905 was called “Annus Mirabilis” or extraordinary year due to the publication of Einstein's papers in Annalen der Physik journal. This is the direct great contribution of Einstein in the start of Quantum Mechanics. Another indirect contribution of Einstein was in the field of quantum theory when he was unfortunately fighting for years to prove the incompleteness of the Quantum Mechanics as a description of the physical reality. This will be dealt with later in the following sections.

The double slits experiment (a well-known experiment to illustrate the wave superposition in Quantum Mechanics), was demonstrated again by Taylor in 1909 (Taylor, 1909). He showed that the $interference$ or $diffraction$[3] pattern can be generated with only one photon of light energy. His work marked the beginning of what known as wave-particle duality which means that the tiny particle can be described as a particle (physical object) or a wave. This term plays a significant role in all theories of Quantum Mechanics, as it will be shown later.

[3] Interference of the waves is the most explicit demonstrations of the superposition of the waves or the particles.

In 1913, Niels Bohr developed the atomic model based on quantum aspects (Niels Bohr, 1913). In his model of an atom, some orbital shells are stable around the nucleus. He succeeded to quantize those electron orbits in some units (based on Planck's constant).

A historical moment in the development of the Quantum Mechanics was in 1926 when Erwin Schrödinger published his paper entailed "Quantisierung als Eigenwertproblem" (in English Quantization as an Eigenvalue Problem) (Schrödinger, 1926)[4]. He finally developed a wavefunction that can predict the particle evolution. The Schrödinger wavefunction has become as a symbol of Quantum Mechanics such that it resembles the second Newton law in classical Physics which predicts the future amplitude of a wave. Schrödinger came up with a wave function that can calculate correctly the energy levels of the Hydrogen atom as follows:

$$\left[\frac{-\hbar^2}{2m}\nabla^2 + V(r,t)\right]\psi(r,t) = i\hbar\frac{\partial}{\partial t}\psi(r,t) \tag{2.1}$$

where $\hbar$ is the Planck's constant divided by 2π, m is the mass of the particle, V is the potential energy of the charged particle at each position, r the position vector (in a spherical space), t is the time, ψ is the wave function (it is discussed below), i is the imaginary number, $\frac{\partial}{\partial t}$ is the partial derivative with respect to t, and $\nabla^2 = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}$. The generalized form of Schrödinger equation using Dirac Notation (Dirac notation is discussed later) is:

$$\hat{H}\left|\psi\right\rangle = i\hbar\frac{\partial}{\partial t}\left|\psi\right\rangle. \tag{2.2}$$

Equation 2.2 has become a symbol for Quantum Mechanics too. In the following, we are going

[4] Schrödinger's equation is one of the greatest achievements of the mankind. The world down at the sub-atomic levels is very weird and the particles (physical objects) behave strangely. A particle could be in two different locations at the same time, or simultaneously could move in two different directions, or could travel in two different speeds simultaneously. The scientists know all that weirdness but yet they could not describe how. The particles evolution over time, is represented in a form of what called a wavefunction which it is complicated by itself. Then, Schrödinger has come up with an equation to solve the wavefunction which enables us to study quantum weirdness. "Where did we get that equation from? Nowhere. It is not possible to derive it from anything you know before. It came out from the mind of Schrödinger" –R. Feynman