CHAPTER 1

INTRODUCTION

1.1 Background of the Research

The Malaysian government has seen the importance of cybersecurity in safeguarding the well-being of the people. As such, the National Cyber Security Policy (NCSP) was developed in 2006 to safeguard Malaysia's Critical National Information Infrastructure (CNII) against cyber threats. Looking at the alarming cyber incidents that have happened over the years, the government adopted the National Cryptography Policy (NCP) in 2013 after seeing the growing importance of the use of cryptography to protect confidentiality, integrity, authenticity, and non-repudiation in communications. Due to the increasing use of cryptography in security products, the National Trusted Cryptographic Algorithm List (MySEAL) was developed between 2016 and 2020 to provide national trusted cryptographic algorithms for implementation within the Malaysian context (Buja, 2018). With the initiative from the government that supports cryptography research in Malaysia, cryptography plays a critical role in our communication today.

Cryptography secures communications and transactions, as well as protects personally identifiable information (PII) and other confidential data, making it an essential component in information security technology. Four major objectives of information security that can be achieved with cryptography are to ensure information can only be accessed by an authorized party (confidentiality), to detect whether the data has been compromised (integrity), to prove one's identity (authenticity), and to prevent an individual from denying having sent or received the data (non-repudiation). Looking at the importance

of cryptography in protecting data, its applications have increased rapidly in parallel to the development of security products in the market.

Security products are designed to protect services, machines, or networks against cyber-attacks (Bajan et al., 2018). The security products can be in the form of software or hardware with different purposes and advantages. Software encryption product typically relies on a password that is passed through an encryption algorithm that modifies the data. Software encryption is cheap to implement, thus making it popular among security product developers. On the other hand, hardware encryption product is considered safer than software due to the encryption process is separated from the rest of the machine, which makes it harder for an attacker.

Encryption is the main component of security products to prevent unauthorized access to data. In order to ensure data security, block cipher is preferred in most security products as it is faster than asymmetric encryption which is known for its longer key lengths and complex encryption algorithm (Nayancy et al., 2020). On top of that, to keep up with the demand for high-speed data processing products, lightweight block cipher gains very much attention as it is more compact due to its design simplicity and requires small computing power to execute encryption on electronic devices such as mobile phones.

Lightweight block cipher offers low-cost implementation for security products that focuses on fast encryption, low memory requirements, and energy efficiency (Xiang et al., 2020). However, since lightweight block ciphers are used in environments where hardware and software resources are very limited, their security is at a disadvantage compared to conventional block ciphers (Chen et al., 2021). In order to provide high security in data

protection, this research intends to develop a new encryption algorithm using a 3D rotation method that would strengthen the security of the lightweight block cipher.

1.2 Problem Statement

Cyber security awareness has given a positive impact on the increasing development of security products in the market across various fields. Most people around the world have at least a smartphone to communicate, browse the Internet, read e-mails, perform their job, and also attend classes. According to the prediction, the number of mobile users worldwide is likely to rise to 7.26 billion users out of the 7.9 billion world population by end of 2022 (O'Dea, 2021). Looking at the potential for cyber-attacks, almost everyone in the world needs security protection (Daud et al., 2018). Information security is crucial due to interception and modification of data can lead to loss of availability, integrity, confidentiality, and possibly other losses such as loss of life, money, and assets (Dhanda et al., 2020). Therefore, encryption is an important tool in security products that must be associated with the smartphone to ensure the safety of user data.

Security product such as software encryption application that includes email, message, file, voice, and disk encryption can be embedded into the smartphone. However, mobile encryption application shares the device's processing resources, which can cause the entire system in the smartphone to slow down while data is being encrypted (Kulah et al., 2019). Consequently, accessing and closing encrypted files take a longer time than usual due to the heavy process, especially at higher levels of encryption.

Taking into account the advantages and disadvantages of the mobile encryption application, the main issue identified is that most software encryption application available in the market relies on the conventional standard encryption algorithms such as the AES block cipher. Although AES is one of the most widely accepted encryption algorithms, the conventional block cipher requires huge memory and high power consumption which is not practical to be implemented in software encryption applications (Salunke et al., 2019).

As an alternative, lightweight block cipher has caught the attention of researchers over the past years. Numerous new variants of lightweight block cipher have been proposed for security products implementation. However, lightweight algorithms used for security products may not provide an adequate security-efficiency balance (Toprak et al., 2020). Many lightweight block ciphers aim for better efficiency but do not prioritize the security aspect of the algorithms, which should be the main objective of the cipher development.

RECTANGLE is one of the lightweight block ciphers designed to satisfy efficiency requirements that achieves very competitive software performance and requires very low implementation costs (Senol, 2017). Although the RECTANGLE algorithm achieves such high merit in terms of efficiency, its security aspect requires more attention. Based on the previous studies, two security weaknesses found in RECTANGLE block cipher need to be addressed.

Firstly, RECTANGLE does not provide enough confusion and diffusion properties in the algorithm (Omrani et al., 2019). As a result, RECTANGLE lightweight block cipher is vulnerable to cryptanalysis attacks (Selvam et al., 2014; Selvam et al., 2015; Kosuge et al., 2016). Therefore, RECTANGLE needs to be enhanced to be secure against any type of cryptographic attack.

Secondly, non-robust round key generation appears to be its weakest point in RECTANGLE (Naser & Naif, 2022). The key schedule algorithm of RECTANGLE affects the security performance of the lightweight block cipher as the key schedule generates weak round keys to be fed into the encryption algorithm (Yan et al., 2019). In addition, RECTANGLE key schedule algorithm uses a matrix to store the round keys which lead to non-resistance against related-key attacks (Pehlivanoğlu et al., 2017).

In conclusion, this research aims to develop a lightweight block cipher for mobile applications to solve the issues in security products by addressing the security weaknesses found in RECTANGLE algorithm. For a start, cryptographic components that can solve the security weaknesses in RECTANGLE block cipher are analysed. Then, the secure cryptographic components are designed which are implemented in the newly developed lightweight block cipher. Lastly, cryptanalysis and performance tests are conducted in order to measure the effectiveness of the new algorithm in solving security issues in lightweight block ciphers. Overall, this research contributes to the field of cybersecurity to support the Malaysian government's initiatives in safeguarding the well-being of the people by producing a secure cryptographic algorithm for security product implementation.

1.3 Research Questions

Based on the identified research problems, eight research questions are identified as follows:

i) How does lightweight block cipher become the security solution for resource-constrained devices?

ii) How does the strength of lightweight block cipher being determined in accordance with cryptographic standards?

iii) How do cryptographic components give impact to the security of a lightweight block cipher?

iv) How does the 3D rotation method improve the strength of cryptographic algorithm design?

v) How does the encryption algorithm solve issues highlighted in security product?

vi) How do encryption algorithms being distinguished in terms of security strength and software performance?

vii) How does cryptographic design influence the security of an encryption algorithm?

viii) How does cryptographic design influence the software performance of an encryption algorithm?

1.4 Research Objectives

The main objective of this research is to develop a secure lightweight block cipher for data protection on a mobile application. In achieving the main objective, the following are the specified objectives of the research:

i) To analyse cryptographic components that can enhance the security strength of a lightweight block cipher.

ii) To design secure cryptographic components for the use of a lightweight block cipher.

iii) To develop a lightweight block cipher proposed for mobile applications using the secure cryptographic components.

iv) To evaluate the security and efficiency of the lightweight block cipher through cryptanalysis and performance test.

1.5 Research Contributions

In completion of this research, three contributions are expected as follows:

i) Secure cryptographic components that can be used to design a secure lightweight block cipher.

ii) New lightweight block cipher developed using the secure cryptographic components proposed for mobile applications.

iii) Cryptanalysis and software performance tests on the designed lightweight block cipher that measures the security and efficiency of the new algorithm.

1.6 Scope of Study

The main focus of this research is the development of a secure lightweight block cipher. Figure 1.1 displays the overall scope of this research. The basic construction of the new algorithm is the block cipher. Lightweight cryptography is selected due to its suitability for small computing device implementation. Substitution-permutation network is implemented to fit the structure of the algorithm. 3D cipher design is adopted to enhance the security of the lightweight block cipher. The coverage of this study is limited to the cryptanalysis and software performance tests of the block cipher. For the cryptanalysis, Avalanche effect tests (correlation, bit error rate, and key sensitivity tests), randomness tests using NIST Statistical Test Suite, and cryptanalysis attacks (differential and linear cryptanalysis) are applied to evaluate the security strength of the new algorithm. Meanwhile, in the software performance tests, execution speed and throughput evaluations are carried out to evaluate the efficiency of the lightweight block cipher.

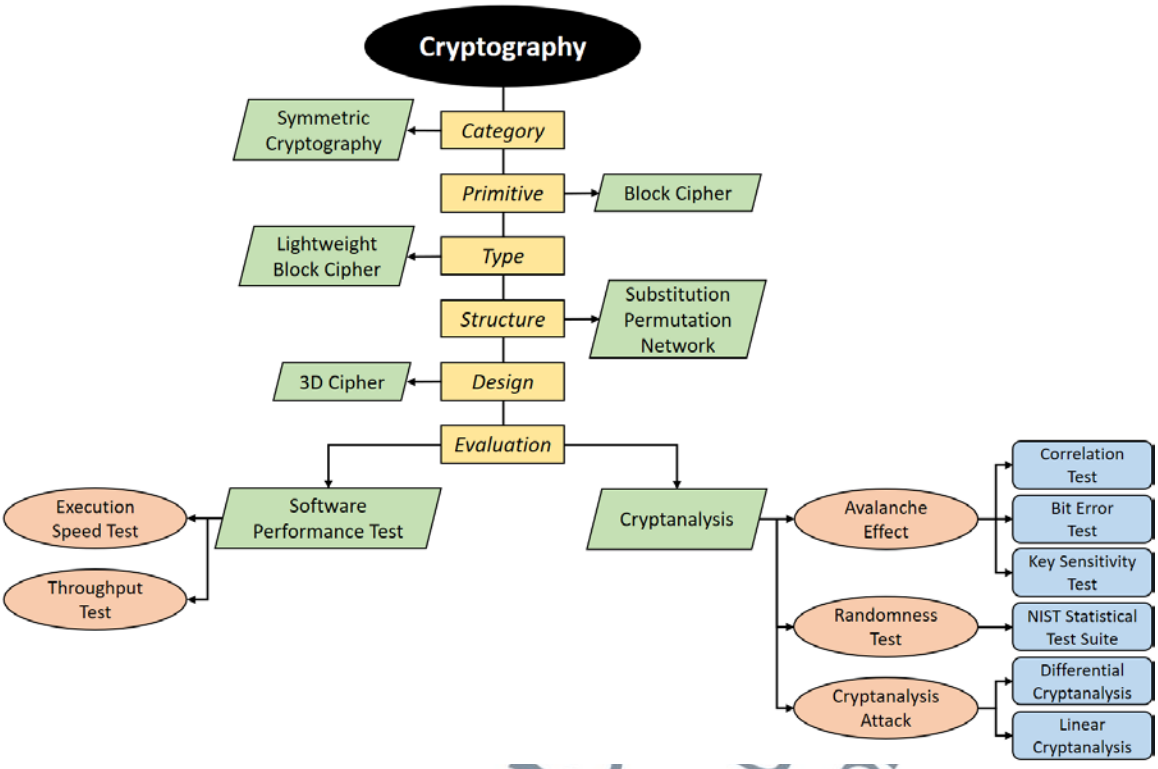

Figure 1.1: Research Scope

This research work has limitations whereby the new lightweight block cipher is not be applied on any of the electronic integrated circuits such as IC, chip, or microchip to observe its performance on hardware implementation. Limited resources and time constraints are the two factors that lead to the research limitations. However, the new algorithm is implemented in a mobile application to observe its encryption functionality.

1.7 Thesis Organization

The thesis is split into ten chapters, including the current chapter which consists of an introduction to the study. Chapter 2 details the literature review conducted in the research. Chapter 3 explains the research methodology used in this work. Chapter 4 identifies the secure cryptographic components of lightweight block cipher. Chapter 5 discusses the detailed structure of RECTANGLE block cipher. Chapter 6 describes the main objective of the research which is the development of a new algorithm called LAO-3D lightweight block cipher. Chapter 7 presents the cryptanalysis tests conducted on the proposed algorithm. Chapter 8 compares the experimental results of the proposed algorithm against existing block ciphers. Chapter 9 shows the implementations of the proposed lightweight block cipher. Finally, Chapter 10 summarizes the conclusion of the research and recommends future works.