CHAPTER 10

CONCLUSION AND FUTURE WORKS

10.1 Introduction

This chapter presents the revision of the research objectives, recommendations for future works, and conclusion of the conducted research. Outputs from the research indicate the effectiveness of the studies conducted in answering all of the research questions that arose from the beginning of the research. The research outputs are presented corresponding to each research objective to review the significance of works that have been conducted throughout the research process.

10.2 Objectives Revisited

The aim of the research is to develop a secure lightweight block cipher named Light Algorithm Operation (LAO-3D) based on a 3D rotation method for data protection on a mobile application. Based on the conducted research, it can be concluded that the four research objectives have been accomplished.

10.2.1 Research Objective 1

The *Research Objective 1* is to analyse cryptographic components that can enhance the security strength of a lightweight block cipher. In order to achieve the research objective, three processes were carried out. First, the basic requirements in developing a lightweight block cipher were defined. Second, the security evaluation criteria for the lightweight block cipher were identified. Third, cryptographic components that can enhance the security strength of a lightweight block cipher were analysed.

10.2.1.1 Research Output 1

Cryptographic components of lightweight block cipher were analysed from the existing cryptographic algorithms in Chapter 4. In this research, 99 existing lightweight block ciphers were studied to explore each of the algorithm designs. Component details of the lightweight block ciphers were presented including the block size, key size, structure, number of rounds, and cryptographic functions.

To be specific, the aim of the analysis is to search for cryptographic components that can improve the confusion and diffusion properties of block ciphers. From the conducted analysis, multiple techniques of substitution (S-box) and permutation (permutation and rotation) components that can be used to develop a secure lightweight block cipher were identified as the secure cryptographic components. The output of the research process is considered as *Research Contribution 1* which was used as the input for *Research Objective 2*.

10.2.2 Research Objective 2

The *Research Objective 2* is to design secure cryptographic components for the use of a lightweight block cipher. In order to achieve the research objective, a 3D rotation function was formulated, which is an improvement from the existing method in the literature.

10.2.2.1 Research Output 2

One of the secure cryptographic components identified in *Research Contribution 1* known as the 3D rotation function was further enhanced to improve its security strength. A new secure cryptographic component for the use of a lightweight block cipher named *Double3DRotation* function was designed in Chapter 6. The *Double3DRotation* function combines three sub-functions including the *3DBitRotation_X-axis*, *AddRoundKey*, and *3DBitRotation_Z-axis*.

The selection of the 3D rotation approach is due to its capability to enhance the security strength of the block cipher by providing significant diffusion property to the new lightweight block cipher. The output of the research process is considered as a part of *Research Contribution 2* which was used as the input for *Research Objective 3*.

10.2.3 Research Objective 3

The *Research Objective 3* is to develop a lightweight block cipher proposed for mobile applications using the secure cryptographic components. In order to achieve the research objective, two processes were carried out. Firstly, a key schedule algorithm for lightweight block cipher was designed. Secondly, an encryption algorithm was developed.

10.2.3.1 Research Output 3

A new lightweight block cipher called LAO-3D that is designed for security products is developed in Chapter 6. LAO-3D algorithm consists of 64-bit block and 128-bit key sizes with 20 encryption rounds. Three operations have been applied in the encryption algorithm that includes *AddRoundKey*, *SubColumn*, and *Double3DRotation* functions. The main component of LAO-3D design is based on the 3D rotation method which is one of the enhanced secure cryptographic algorithm components.

The basic construction of LAO-3D is referencing the RECTANGLE block cipher as the benchmark algorithm. With the addition of enhanced 3D rotation method and a few modifications to the original algorithm, the newly developed LAO-3D block cipher offers better confusion and diffusion properties. On top of that, two software implementations were successfully carried out on LAO-3D that include desktop and mobile applications which indicated the functionality of the algorithm in real applications. Therefore LAO-3D lightweight block cipher can provide security through its encryption technique and is efficient for implementation due to its design simplicity. The output of the research process is considered as a part of *Research Contribution 2* which was used as the input for *Research Objective 4*.

10.2.4 Research Objective 4

The *Research Objective 4* is to evaluate the security and efficiency of the lightweight block cipher through cryptanalysis and performance tests. In order to achieve the research objective, three processes were carried out. First, the experimental setups for the security and efficiency evaluations were prepared. Second, cryptanalysis on the lightweight block cipher was conducted. Third, software performance tests on the lightweight algorithm were executed.

10.2.4.1 Research Output 4

Three types of cryptanalysis were conducted to evaluate the security strength of LAO-3D lightweight block cipher that include three avalanche effects experiments (correlation coefficient, bit error, and key sensitivity tests), randomness analysis, and two cryptanalytic attacks (differential cryptanalysis and linear cryptanalysis) in Chapter 7. These security analyses can distinguish the security strength of block ciphers that have been adopted in cryptography research.

Avalanche effect consists of three experiments such as correlation coefficient, bit error rate, and key sensitivity tests. Firstly, LAO-3D recorded 98.20% correlation coefficients result shows a weak linear relationship between the plaintext and ciphertext. Secondly, 50% result obtained from the bit error rate test indicates that the ciphertext is completely changed whenever one plaintext bit is modified. Thirdly, 50% result achieved in the key sensitivity test suggests that each bit of the ciphertext depends on the entire key bits.

Randomness tests were performed by adopting 15 statistical tests from the NIST Statistical Test Suite. On top of that, nine data categories were applied to produce the input data in plaintexts and keys format that generated a different set of 1,000 ciphertext samples for each data category. The experimental results produced a 100% passing rate in the randomness tests. As a result of the combinations of substitution and permutation components of the lightweight block cipher, LAO-3D has optimized the confusion and diffusion properties that contribute to the randomness characteristics of the ciphertext.

Two types of cryptanalysis that include differential and linear attacks were used to analyse LAO-3D lightweight block cipher. Out of 20 rounds of LAO-3D, the maximum number of rounds that can be attacked using differential and linear cryptanalysis on the new algorithm are five and six rounds. As a comparison with RECTANGE, LAO-3D is better than the original algorithm which is attackable at the 14^{th} and 8^{th} rounds using similar cryptanalysis attacks.

The software performance tests results of LAO-3D show that the new algorithm is competitive among the existing lightweight block ciphers. LAO-3D algorithm recorded 10.85% faster execution speed and produced 12.18% more throughput than the closest competitor which is the RECTANGLE block cipher. Overall, the output of the research process is considered as *Research Contribution 3*, thus completing all of the research objectives.

10.3 Recommendation for Future Works

From the conducted research, a few recommendations can be considered as a guide for future research and it would be interesting to investigate these directions. Looking at the broad areas that can be investigated from the research, the potential findings can be transformed into many publications in the future.

i) As mentioned in Chapter 1, the coverage of this research is limited to the software implementation of the lightweight block cipher. Due to limited resources, LAO-3D lightweight block cipher has not been implemented in hardware devices. Therefore, it is recommended to embed LAO-3D into a chip to observe its performance on hardware and to maximize the application of the new algorithm.

ii) Studies conducted in Chapter 4 show that there are many secure cryptographic components of a lightweight block cipher that can be used to develop a secure cryptographic algorithm. Therefore, other than the 3D rotation method implemented in this research, there are vast opportunities for researchers to explore other secure cryptographic components in developing lightweight block ciphers such as the formulation permutation and two-way directions rotation that potentially have their undiscovered cryptographic strengths.

iii) Other than those cryptanalysis presented in Chapter 7, there exist a variety of other cryptanalysis attacks that can be used to evaluate the security of block ciphers. As a result, it is recommended to analyse the security of LAO-3D algorithm against other types of cryptanalysis techniques such as side-channel attack and algebraic attack to show its security strength against multiple attacks.

10.4 Conclusion

In conclusion, this research aimed to solve the issues in security products, specifically for mobile applications, by addressing the security weaknesses found in lightweight algorithms. All of the research questions were answered which provided guidance in achieving the main contribution of this research which is the development of a secure algorithm called LAO-3D lightweight block cipher. This research has contributed to fundamental knowledge of analyzing, testing, enhancing, designing, and developing lightweight block cipher. Firstly, the identified secure cryptographic components can be used as a guideline for the future development of lightweight block cipher by cryptographic developers. Secondly, the new lightweight block cipher can be implemented in mobile applications to solve security products issues. Thirdly, the presented cryptanalysis and software performance tests can be used to distinguish the strength of lightweight block ciphers. The findings from the research will benefit academic researchers, cryptography developers, cryptography evaluators, and security product users. This research has an impact on the field of cybersecurity in supporting the Malaysian government's initiatives to safeguard the well-being of the citizen in line with the National Cyber Security Policy.

PUBLICATIONS

Zakaria, A. A., Azni, A. H., Ridzuan, F., Zakaria, N. H., & Daud, M. (2020). Modifications of key schedule algorithm on RECTANGLE block cipher. In *International Conference on Advances in Cyber Security* (pp. 194–206). Springer, Singapore.

Zakaria, A. A., Azni, A. H., Ridzuan, F., Zakaria, N. H., & Daud, M. (2020). Randomness analysis on RECTANGLE block cipher. In *Cryptology and Information Security Conference* 2020 (pp. 133–142).

Zakaria, A. A., Azni, A. H., Ridzuan, F., Zakaria, N. H., & Daud, M. (2020). Extended RECTANGLE algorithm using 3D bit rotation to propose a new lightweight block cipher for IoT. *IEEE Access*, *8*, 198646–198658.

Zakaria, A. A., Azni, A. H., Ridzuan, F., Zakaria, N. H., & Daud, M. (2020). Randomness tests on nine data categories of RECTANGLE using NIST statistical test suite. *International Journal of Cryptology Research*, *10*(2), 1–22.

Zakaria, A. A., Azni, A. H., Ridzuan, F., Zakaria, N. H., & Daud, M. (2022). Analysis of permutation functions for lightweight block cipher design. In *Cryptology and Information Security Conference* 2022 (pp. 69–84).