UNIVERSITI TEKNOLOGI MARA

DYNAMIC S-BOXES AND SPIRAL PERMUTATION FUNCTION ON FIBONACCI SEQUENCE FOR SECURE BLOCK CIPHER

KAMSIAH BINTI MOHAMED

Thesis submitted in fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Computer Science)

Faculty of Computer and Mathematical Sciences

January 2022

ABSTRACT

Cryptography requires a secure technique to ensure that the enemy is prevented while securing legitimate users gaining access to information. Thus, the design of symmetric key cryptography is often enhanced to ensure that information is secure. In the symmetric key, a block cipher is an important primitive to provide confidentiality for data transmitted in insecure communication environments. Secure cipher relies on substitution and permutation function to protect the cipher against any attacks. However, poor substitution and permutation functions will render the block cipher unsecure. Therefore, improving the substitution and permutation function in a block cipher is an effective way to provide information security. In this thesis, a new design of symmetric encryption block cipher inspired by the Fibonacci sequence is studied. The concept of the Fibonacci sequence was applied in the block cipher as it comprises recursive property in the substitution function. It is a linear recurrence in which the n^{th} element of the sequence is related to its predecessors through a recurrence of recursive algorithms. Meanwhile, the nine dynamic S-box was designed based on the key generated to improve the substitution function. Hence, the complexity of the S-box is assumed to increase based on the dynamic S-box generated. This is because the dynamic S-box would make it difficult for an attacker to recognise its elements. In this thesis, the Spiral Fibonacci is proposed for a permutation function to diffuse bit permutation in improving cryptography algorithm efficiency. Therefore, this research was carried out using an experimental design framework to analyse the proposed block cipher. The experimental results showed that the proposed block cipher satisfied confusion and diffusion properties to increase security and was seen as suitable for secure communication. Most significantly, the recursive property of Fibonacci will considerably increase the information capacity effectively and efficiently. Based on the results, it was shown that the proposed block cipher algorithm has successfully passed 15 NIST Statistical Tests. For the avalanche effect, the result shows that the proposed block cipher satisfied the avalanche effect with a 50 per cent output bit change in ciphertext. Therefore, it can be concluded that the proposed block cipher's output is random with a significant value. Besides, for the linear cryptanalysis, the results showed that the proposed block cipher S-box has a low probability bias (0.062). Meanwhile, differential cryptanalysis demonstrated that the proposed block cipher S-box revealed a probability bias of two, which is the maximum DDT value. For truncated differential, the transformation operations for the proposed block cipher S-box was implemented on bytes rather than individual bits so that it can resist cryptanalysis attack. As a result, the proposed block cipher is resistant to linear and differential cryptanalysis as well as truncated differential. In conclusion, this proposed block cipher can also be used as a secure algorithm by nations, organisations or stakeholders to improve data protection besides contributing to computer security research as an alternative to other cryptographic algorithms. In addition, it can be combined with other cryptographic techniques to provide layered security in the event of a data leak or a regular hack attack.

ACKNOWLEDGEMENT

In the name of Allah, the most gracious and the most merciful. May all praises and salutations of the Lord be upon the Messenger of Allah and upon his Family and Companions, and those who are guided by the light of his ‘sunnah’ till the Day of Judgment. Alhamdulillah. Thank you Allah, for all His blessings in this challenging PhD journey.

The journey is made possible through the endless support and encouragement of many people. To them goes my greatest thanks. From the bottom of my heart, I would like to express my deepest thanks to my main supervisor, Dr. Fakariah Hani Hj. Mohd Ali and co-supervisor, Assoc. Prof. Dr. Suriyani Ariffin, for their tremendous support and guidance in every possible way throughout this journey. This thesis would not have been completed without their guidance. I wish to express my gratitude to Prof. Dr. Ramlan Mahmood, Dr. Muhammad Reza Bin Z'aba and Dr. Nur Hafiza Zakaria for the guidance and advice in undertaking the research activities. To all my friends, thank you for the support and help.

Most importantly, my sincere appreciation goes to my beloved husband, Mohd Nazran bin Mohammed Pauzi for his love, patience and endless support throughout this journey. Finally, I would like to express my deepest gratitude to my parents and my siblings for their constant encouragement, prayers and support in my entire life. To my beloved sons, Muhammad Hasanul Hadif, Muhammad Hasanul Hazeeq, Muhammad Hasanul Harith and my lovely daughter, Nur Qaisah Husna; you are my inspiration to achieve greatness. Thank you for being an inspiration in my life.

TABLE OF CONTENTS