CHAPTER 6

CONCLUSION AND FUTURE ENHANCEMENT

6.1 Overview

In this dissertation, we have presented a new block cipher, the rationale behind its design and the results of tests performed on this block cipher. Design of a strong block cipher requires a lot of knowledge. Various mathematical theories such as number theory, abstract algebra, complexity theory, information theory, probability theory and finite fields are used throughout the design of the block cipher. Besides that, important cryptographic properties of block cipher and various cryptanalysis techniques have been studied in order to develop a good block cipher.

The proposed block cipher is a Substitution-Permutation network cryptosystem with a block length of 128 bits and key length of 256 bits. A modular design approach was applied. The cipher has three major building blocks and their interaction has been carefully chosen to achieve better security and performance. S-Box is an essential part in the construction of a block cipher that provides confusion and nonlinearity in the cipher. Hence, the properties of S-Box were studied to find a good S-Box. One of the design goals of the block cipher is to use the same function for encryption and decryption. Therefore, it is required that every components in the block cipher to be self-inverse. Initially, S-Box that maps $x \rightarrow x^{-1}$ was used. But this S-Box does not satisfy the design criteria due to its simplicity of algebraic structure. Other S-Box that is not self-inverse has been used. Although it is not self-inverse, some modification was applied to the round transformation to make the cipher selfreverse. This is done by finding the inverse of the S-Box. The pair of S-Boxes is used in alternate rounds. This arrangement makes the cipher self-inverse.

The diffusion layer uses four-input-port-four-output-port mixers that mix data from every part of the plaintext block to guarantee the overall diffusion in block cipher. The linear mixers are byte-oriented. This makes the proposed cipher suitable for both hardware and software implementations. Key scheduling is an integral part of the cipher design. It is carefully designed to avoid weak keys, complement keys, equivalent keys, etc. Linear key scheduling is not used to prevent exhaustive key search. The modular design approach allows the analysis of the cipher to be done separately on each component. This greatly increases the efficiency of analysis to identify the strength and weaknesses of the cipher.

We have subjected the proposed block cipher to a range of statistical tests. Tests have been performed to examine important properties of the block cipher. A differential distribution table was generated for each S-Box to test its differential characteristics. All operations in block cipher are linear except the S-Boxes. For the testing of nonlinearity, a linear approximation table was derived. In addition, we also performed tests to examine other important cryptographic properties of the block cipher, including avalanche effect, completeness, involution and cyclic property. In all cases, results indicate that the proposed cipher satisfies all the cryptographic properties.

6.2 Achievements

In this research we introduce a new block cipher with a block length of 128 bits and key length of 256 bits. It is a new class of Substitution-Permutation

Networks with the advantage that the same network can be used to perform both the encryption and the decryption operations. The block cipher has various cryptographic properties that make it secure, good in performance and suitable for hardware and software implementations. The strengths of the proposed system are as follow:

Simplicity of Design

Simplicity the main guiding principles behind the design process of the algorithm. The algorithm bases its security on well-understood interactions between arithmetic operations. The design reused the same primitives in multiple parts of the cipher, which simplifies the analysis of the algorithm.

Strength Against Timing and Power Analysis Attack

The algorithm uses table lookup, Boolean operation and fixed shift operation. It does not employ addition, multiplication and variable rotation operations, which are difficult to defend against timing and power analysis attack.

Good Avalanche Effect

The proposed cipher uses a highly diffusive diffusion layer, which is a combination of linear mixers, to ensure that fewer rounds are required to achieve avalanche effect. In addition, we use SP network as the structure of the block cipher. Unlike Feistel cipher where only half of the bits are transformed in each round transformation, SP network has a uniform round structure that allows all bits to be transformed in every round. This contributes to the overall avalanche effect of the proposed cipher.

Identical functions for Encryption and Decryption

The algorithm utilizes identical functions for encryption and decryption, except for the reversal of the key schedule. Only one function needs to be included in the implementation. In the case where encryption and decryption are distinct functions, extra space needs to be allocated for decryption. This is done despite Feistel structure is not used. The round transformation has been designed such that the algorithm uses the same function for both encryption and decryption.

Implementations on Hardware and Software platform

The proposed cipher works well on hardware as well as software platform. The algorithm avoids the use of bit-oriented operations and uses linear mixer instead of bit permutation to achieve diffusion.

Extensions

The proposed cipher has a fixed number of rounds, but this can be modified in the case of security problems.

Key Size

The proposed cipher supports a key size of up to 256 bits. This is significantly higher than DES, which uses a 56-bit key. The security of a block cipher is a function of two things: the strength of the algorithm and the length of the key. The long key size makes attacks on the algorithm more difficult.

Strength Against Linear and Differential Cryptanalysis

The cipher is designed to be highly nonlinear and has low differential characteristic. This increases the cipher's strength against linear and differential cryptanalysis.

Performance

The block cipher is designed to be fast. It uses table lookup and simple Boolean operations in its algorithm. This contributes to the speed of the algorithm compared to other algorithm that uses key-dependent S-Boxes, variable rotation, etc.

6.4 Future Enhancement

The work of this dissertation is a preliminary into the practical and theoretical aspects in designing a block cipher. Because of time constraint, many avenues have not been pursued. Some modification and enhancement can be made to the algorithm to make the algorithm stronger.

Supports variable block and key size

The algorithm should support variable block size and key length to make it suitable for a variety of implementations.

Modification to the algorithm

The current proposed block cipher reuses S-Box used in SHARK, SQUARE and Rijndael because of its strong cryptographic properties. If other S-Boxes with better properties can be found, the S-Box can be replaced. Other modifications can also be made, e.g. key scheduling to make it more secured.

More Testing

Due to time constraint, testing was performed on the important cryptographic properties of the block cipher. However, more testing should be performed on various components of the cipher so that any weaknesses found can be fixed.

More Cryptanalysis

Cryptanalysis is essential in the design and analysis of block cipher. There are various types of cryptanalysis techniques, such as differential cryptanalysis, linear cryptanalysis, related-key cryptanalysis, interpolation attack, truncated and higher order differentials cryptanalysis, etc. To ensure that a block cipher is resistant to different cryptanalysis techniques, it has to be cryptanalysed extensively.

6.5 Conclusion

The project has achieved its objectives to develop an encryption algorithm. In the dissertation, a block cipher that uses algorithmic S-Boxes in a SP network was designed. The rationale behind its design, the testing methodology and results are presented in the dissertation.

In the design process, invaluable knowledge about cipher design was gained. Knowledge gained throughout the life cycle of the development, from the planning, studies of the subject, analysis and design to testing of the block cipher was a richly rewarding experience.

There is still much room for improvement in the block cipher. The successful design of the block cipher is the first step towards the future development of similar systems. It is hoped that this dissertation can provide a foundation to a more enhanced system in the future.