DYNAMIC KEY SCHEDULING ALGORITHM FOR BLOCK CIPHERS USING QUASIGROUP STRING TRANSFORMATION

ABDULKADIR HASSAN DISINA

A thesis submitted in partial
fulfillment of the requirement for the award of the
Degree of Doctor of Philosophy

Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia

JANUARY, 2018

I dedicated this research work to my mother, father, wife, children and siblings.

ACKNOWLEDGEMENT

In the name of Allah the most beneficent and the most merciful, all praise and gratitude be to Him the cherisher and the sustainer of the whole world. Oh Allah, send prayers and blessings upon Muhammad and upon the family of Muhammad, as You sent prayers and blessings upon Ibraheem and upon the family of Ibraheem; You are indeed Worthy of Praise, Full of Glory.

I would like to use this opportunity to express my deepest gratitude to my soft-hearted, kind and loving supervisor Associate Prof. Dr. Sapiee Jamel who treated us in the best way possible and prepared us for the real world challenges. I would like to thank him for all the financial support I have received from him, the fishing lesson and all the leisure trips around Malaysia, you are the best sir, and I am indeed grateful.

I would never forget the love, the prayers and the financial support given to me by my family and friends, may the Almighty Allah reward you all.

I would also like to extend my sincere gratitude to the leadership of FSKTM and the FSKTM postgraduate student's society for the conducive environment and company given to me throughout my PhD journey, for being there for me during difficult times and lastly for given me the room to explore my leadership and administrative skills during my stay.

Finally, my sincere gratitude goes to Office for Research, Innovation, Commercialization and Consultation (ORICC) for financing my research work under the GIPS Grant with Vote number U195.

ABSTRACT

Cryptographic ciphers depend on how quickly the key affects the output of the ciphers (ciphertext). Keys are traditionally generated from small size input (seed) to a bigger size random key(s). Key scheduling algorithm (KSA) is the mechanism that generates and schedules all sub-keys for each round of encryption. Researches have suggested that sub-keys should be generated separately to avoid related-key attack. Similarly, the key space should be disproportionately large to resist any attack on the secret key. To archive that, some algorithms adopt the use of matrixes such as quasigroup, Hybrid cubes and substitution box (S-box) to generate the encryption keys. Quasigroup has other algebraic property called "Isotophism", which literally means Different quasigroups that has the same order of elements but different arrangements can be generated from the existing one. This research proposed a Dynamic Key Scheduling Algorithm (KSA) using isotope of a quasigroup as the dynamic substitution table. A method of generating isotope from a non-associative quasigroup using one permutation with full inheritance is achieved. The generic quasigroup string transformation has been analyzed and it is found to be vulnerable to ciphertext only attack which eventually led to the proposal of a new quasigroup string transformation in this research to assess its strength as it has never been analyzed nor properly implemented before. Based on the dynamic shapeless quasigroup and the proposed new string transformation, a Dynamic Key Scheduling Algorithm (DKSA) is developed. To validate the findings, non-associativity of the generated isotopes has been tested and the generated isotopes appeared to be non-associative. Furthermore, the proposed KSA algorithm has been validated using the randomness test proposed and recommended by NIST, avalanche test and has achieved remarkable result of *94%*, brute force and correlation assessment test with -***0.000449*** correlations. It was fully implemented in a modified Rijndael block cipher to validate it performance and it has produced a remarkable result of *3.35332* entropy.

ABSTRAK

Cipher kriptografi bergantung kepada kepantasan kunci yang mempengaruhi pengeluaran cipher (ciphertext). Kekunci dihasilkan secara tradisional daripada input yang bersaiz kecil kepada bersaiz besar secara rawaknya. Algoritma penjadualan utama Key Scheduling Algorithm (KSA) adalah mekanisme yang menjana dan menjadualkan semua sub-kunci untuk setiap pusingan penyulitan. Penyelidik telah disarankan bahawa sub-kunci perlu dijana secara berasingan untuk mengelakkan serangan dari kunci yang berkaitan. Begitu juga dengan ruang kekunci seharusnya besar untuk menentang sebarang serangan terhadap kunci rahsia. Untuk mencapainya, beberapa algoritma perlu mengamalkan matriks seperti Quasigroup, kiub Hibrid dan kotak penggantian substitution box (S-box) untuk menghasilkan kunci penyulitan. Quasigroup mempunyai beberapa algebra lain yang dipanggil "Isotophism", yang secara literal bermaksud Quasigroup yang berbeza dan mempunyai susunan elemen yang sama tetapi pengaturan yang berbeza dapat dihasilkan dari yang ada. Kajian ini mencadangkan Algoritma Penjadualan Kunci Dinamik (Dynamic Key Scheduling Algorithm (KSA)) menggunakan Isotop dari Quasigroup sebagai jadual penggantian dinamik. Satu kaedah untuk menghasilkan Isotop dari Quasigroup bukan sekutu adalah dengan mengunakan satu permutasi dengan warisan yang penuh pecapaian. Transformasi dari Quasigroup generik telah dianalisi dan didapati terdedah terhadap serangan ciphertext yang akhirnya membawa kepada cadangan transformasi rentetan Quasigroup baru dalam kajian ini untuk menilai kekuatannya kerana ia tidak pernah dianalisis atau dilaksanakan dengan baik sebelum ini. Berdasarkan Quasigroup yang tidak berbentuk dinamik dan transformasi rentetan baru yang dicadangkan, Algoritma Penjadualan Kunci Dinamik telah dibangunkan. Untuk mengesahkan penemuan, bukan bersekutu Isotop yang dihasilkan telah diuji dan Isotop yang dihasilkan kelihatan tidak bersekutu. Selain itu, algoritma KSA yang dicadangkan disahkan menggunakan ujian Randomness yang dicadangkan dan disyorkan oleh ujian NIST, ujian Avalanche dan telah mencapai

hasil sebanyak *94%*, ujian Brute Force dan ujian penilaian korelasi dengan *-0.000449* korelasi. Ia telah dilaksanakan sepenuhnya dalam cipher block Rijndael yang telah diubah suai untuk mengesahkan prestasi dan menghasilkan hasil yang luar biasa iaitu entropi *3.35332*.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

$\otimes$	-	Exclusive OR operation
$\rightarrow$	-	Direct mapping
$*$	-	Binary operation
σ	-	Permutation
π	-	Permutation
$\alpha, \beta, \gamma \in \mathrm{K}$	-	Elements in set K
Hisea	-	Hybrid Cube Encryption Algorithm
AES	-	Advance Encryption Standard (Rijndael)
$f(x)$	-	Function of (x)

LIST OF APPENDICES

LIST OF PUBLICATIONS

Journal

i) Abdulkadir Hassan Disina, Sapiee Jamel, Zahraddeen Abubakar Pindar & Mustafa Mat Deris. “Statistical Analysis, Ciphertext Only Attack, Improvement of Generic Quasigroup String Transformation and Dynamic String Transformation” ASL (In press) 2017.

ii) Abdulkadir Hassan Disina, Sapiee Jamel, Muhammad Aamir, Zahraddeen A. Pindar. Mustafa Mat Deris. “Dynamic Key Scheduling Algorithm Based on Dynamic Quasigroup String Transformation All-Or-Nothing Key Derivation Function” *Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 9*(3-5), 1-6. 2017.

Conferences

i. Abdulkadir Hassan Disina, Sapiee Jamel, Zahraddeen Abubakar Pindar, Mustafa Mat Deris. "All-or-Nothing Key Derivation Function Based on Quasigroup String Transformation." *Information Science and Security (ICISS), 2016 International Conference on*. IEEE, 2016.

ii. Abdulkadir Hassan Disina, Sapiee Jamel, Zahraddeen Abubakar Pindar & Mustafa Mat Deris. “Statistical Analysis, Ciphertext-only-Attack and Improvement of Generic Quasigroup String Transformation” ICSEMSS 2016.

CHAPTER 1

INTRODUCTION

1.1 Background

Networking has become a very important aspect of every one's life if the rate of Internet usage is considered. Information is usually being sent through the Internet and sometimes shares classified data (Campbell, 2016). Some of those classified information contains account numbers, meeting venue, addresses, and other crucial information that need confidentiality. Likewise the information may contain some banks and academic related documents that require some privacy. In most cases, senders of those messages are not really concern about the security of the communication channels (Abu-salma et al., 2017). Malicious individuals could tap into the unsecured channel of the communication illegitimately, to make illegal use of the resources (compromises confidentiality) or to temper (compromises availability and integrity) with the data (Conti et al., 2017).

To secure the reliability of the communication channel, restriction methods can be applied on the channels so that only the original sender and intended receiver can unlock and decode the message. However, user might like to make sure that the message at the destination is the same as the original from the source, which means to ensure the integrity of the message (Agrawal, Chang, & Sanadhya, 2015). In this case, some sort of pad lock has to be applied to lock the data. This could not only be done on a physical surface, can also be applied on logical or digital data as well, but only with the help of some mathematical and algebraic algorithms called cryptography. However, the idea of locking of messages such that any individual with the key can access the message is called cryptography.

The word cryptography came from Greek word “kryptos” and “graphein” which means hidden and writing respectively (Sharma et al., 2012), this means converting a written message (plain text) into unreadable form (cipher text) to prevent its confidentiality (Jamel, Herawan & Deris, 2010). It is also the art and science of using mathematics and logics to prepare a coded or protected communication that can only be understood by the sender and intended recipient (Sharma et al., 2012). The sender encrypts the message using a key such that the receiver needs to possess the key in order to decrypt the message into its original readable form. Cryptographic algorithms are categorized into two categories, stream ciphers and block ciphers. Graphical representation of the categories can be visualized in Figure 1.1.

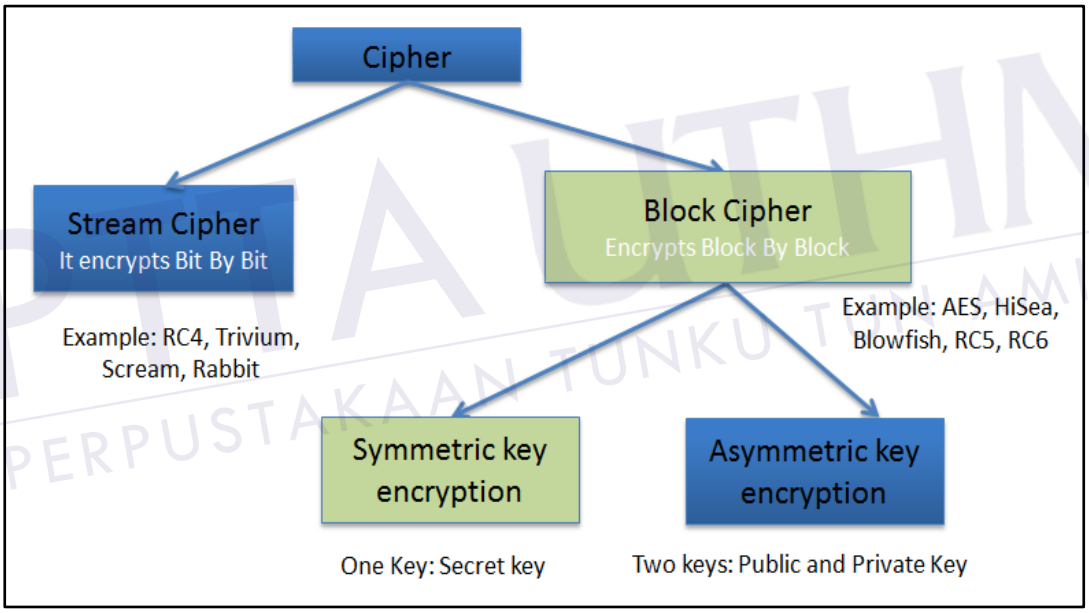

Figure 1.1: Encryption System

There are two criteria to logically use the cryptographic key, symmetric (secret key) and Asymmetric (two keys, public and private) key cryptography (Gaurav, Pal & Dilbahar, 2013) as shown in Figure 1.1, while Figure 1.2 visually described the symmetric key encryption technique.

Encryption started with simple pen-and-paper methods based on letter substitutions. Then it further evolved into special machines built to encrypt messages. Today we have moved away from the more physical methods, and the focus is on digital encryption that can only be done using computers (Gaurav et al.,

2013). With the help of secured cryptographic algorithms, two people can communicate with each other securely (Jamel & Deris, 2011). Eavesdropper could find it difficult to intercept or eavesdrops the message. It further moves to ensure message integrity, authentication and digital signature.

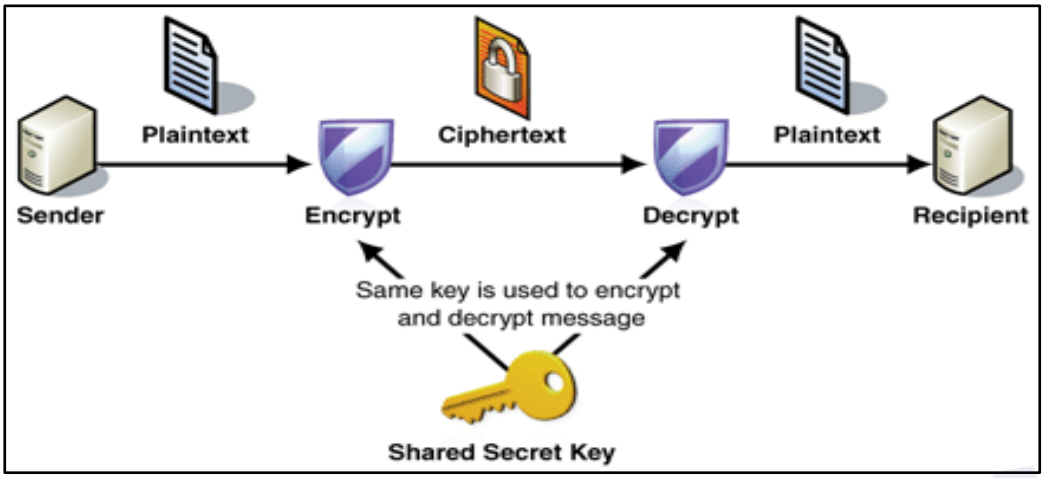

Figure 1.2: Symmetric Key Encryption

Nowadays recipient of a message can check if the message sent was not modified by the interceptor or eavesdropper and the message he received was the actual message from the original source (Rogaway & Shrimpton, 2004).

Encryption techniques can be divided into two classes: traditional encryption techniques and modern encryption techniques. Traditional encryption techniques are pen-and-paper based techniques developed when computers did not exist, although some of these ideas can be, and have been, transformed into computer-based algorithms (Gaurav et al., 2013). With the beginning of the Computer Era, which can be marked with the appearance of the first computer encryption techniques underwent a major change. Encryption techniques were being specifically designed for computer usage and used 'bits' instead of alphabets. These encryption techniques are called modern encryption techniques (Jamel & Deris, 2011; Mushtaq, Jamel, Mohamad, Kamal & Deris, 2017).

The modern day cryptography is not only to provide confidentiality, but simultaneously authenticates and verifies the integrity of the message and the sender respectively (Agrawal et al., 2015). That ability can also be attributed to cryptographic keys as strength of most ciphers rely on the keys (Jamel & Deris,

2011). Key Scheduling Algorithm (KSA) is a cryptographic algorithm that generates and manages session keys for all the rounds of encryption and decryption. Researches were conducted to provide a powerful key to withstand related key attack and increase the difficulty to cryptanalyze and to recover secret key (Gaurav et al., 2013; Biryukov et al., 2010). It leads to the use of matrices and groups to proportionately enlarge the key space (possible key) so as to make a brute force attack computationally difficult. Hybrid cube, cubicle hybrid cube and encryption based on rotation of Magic cube are some of the recent encryption algorithms that are based on matrices (Jamel & Deris, 2011). The key space depends solely on the size of the matrix or cube. Some of those matrices are empirically sufficient in terms of key space but generating them requires high powered machines and that could be costly. However, static matrices can be vulnerable to attack, an adversary may recover the encryption key by determining the exact matrix used. Cubicle Hybrid Cube proposed cube rotations to convert the static nature of Hybrid Cube to dynamic, thus increases the complexity of the algorithm (Rajavel & Shantharajah, 2012; Mushtaq, Jamel & Deris, 2017b).

This research proposed a dynamic Key Scheduling Algorithm from a highly non-associative non-commutative Quasigroup to convert the static nature of matrix based KSAs. A quasigroup is an $n \times n$ matrix (n number of rows and n number of columns) where each row and column is a permutation of n elements and each element appears only once in each row and column (Belyavskaya, 2014). The terms non-commutative and non-associative simply means that the entries of the quasigroup are highly nonlinear and are being chosen at random (Krape, 2017). On the other hand, isotope is a quasigroup generated from another, such that both the quasigroup and the isotope have the same size and elements in entirely different arrangement (Belyavskaya, 2014). Quasigroup string transformation has been used in cryptography as one of the efficient substitution technique used in transforming input into an unpredictable output (Pindar et al., 2015a). The nature and shape of the quasigroup (non-linearity) described as associativity and commutativity also plays a vital role in making sure that the output of the transformation is pseudorandom (Olsson, 2017).

The proposed algorithm is primitively based on All-Or-Nothing Key Derivation Function (AKDF). The AKDF is a function built based on quasigroup string transformation that accepts a small size input from user and produces a

disproportionately large pseudorandom output with potentials of being used as encryption key(s). The proposed algorithm uses the user-given key alongside predefined quasigroup to generate isotope as a dynamic substitution table. A new method of generating isotope from highly non-associative non-commutative quasigroup is achieved using one permutation. The proposed DKSA has been implemented as a standalone program to generate sample keys to validate its strength and resistance to cryptanalysis. There is also a need to practically observe the behavior and impact of the proposed algorithm in existing block cipher. Therefore Rijndael block cipher has been employed with reduced rounds of encryption and without the mix-column function, the proposed DKSA is integrated into it to clearly visualize the impact of the encryption keys on the ciphertext.

The validation process begins with testing the strength and resistance of individual components to statistical analysis and attacks scenarios. The non-associativity and non-commutativity of the generated isotope is analyzed first and appeared to have inherited all the properties of the parent quasigroup. The output of the proposed DKSA has also been analyzed based on correlation assessment, avalanche effect, NIST (National Institute of Standards and Technology) test suit, brute force and entropy. Similarly, the output of the encryption algorithm is also analyzed based on test mentioned above, and it has achieved a remarkable result.

1.2 Problem Statement

The mechanism behind any cryptographic algorithm is the number of possible combinations in a set of characters (Key space). Ciphers use substitutions and transposition to produce the encryption and decryption keys (Jamel et al, 2010; Mushtaq et al., 2017). Algorithms should have both substitution and transposition integrated together to enhance the complexity and strength of algorithm (Wang, Chang & Lin, 2003). Whatever technique is used, the requirement is always confusion (effect of key on ciphertext) and diffusion (effect of algorithm on ciphertext) in the cipher. Key scheduling algorithm (KSA) is the mechanism that generates encryption key and all other round keys for each round of encryption. Traditionally, Key Scheduling Algorithms (KSAs) concatenate private strings with predefined public string in the process of generating the key(s) (Chuah, Dawson &

Simpson, 2013), thus reveals the secrecy of the secret key, it has been the case in the current block cipher standard (Advance Encryption Standard (AES)), (Kumar & Tewari, 2017) when a round key is recovered, all other round keys could easily be recovered. Logical operations such as Exclusive-Or (XOR) and Arithmetic operations are the common techniques used in mixing the private with the public string (Nag et al., 2011) in KSAs and KDFs rather than substitution techniques, SIMON Block Cipher is a good example of algorithms that relies on such operations (Kölbl, Leander & Tiessen, 2015) and those operations are easily reversible with little effort. With those kind of operations in an algorithm, an adversary may study the behavior and relationship between all round keys to find a loophole (Fluhrer, Mantin & Shamir, 2001; Kölbl et al., 2015) and launch his attack. This issue has to be addressed in order to produces a resilient cryptographic algorithm that resists the attack using substitution operation. Substitution is one of the confusion elements that provides unpredictability in algorithms and one of the most widely used in cryptography (Matsui, 1996).

Researches were conducted to produce a powerful non-linear encryption key to withstand related key attack and increase the difficulty to cryptanalyze and recover secret keys. The use of matrices and groups to proportionately enlarge the key space so as to make a brute force attack harder was employed. Hybrid cube, cubicle hybrid cube and encryption based on rotation of magic cube are some of the recent encryption algorithms that are based on matrices (Rajavel & Shantharajah, 2012; Krawczyk, 2010; Mushtaq, Jamel & Deris, 2017a). The key space depends solely on the size of the matrix or cube. But generating those matrices empirically requires a high speed processing capacity (Jamel et al., 2010) which can be costly to resource-constrain environments. However, static matrices can be vulnerable to attack too, an Adversary may recover the encryption key(s) by determining the exact matrix used. Cubicle Hybrid Cube proposed cube rotations to convert the static nature of Hybrid Cube to dynamic, thus increases the complexity of the algorithm (Rajavel & Shantharajah, 2012; Mushtaq et al., 2017). Similar loopholes have been discovered in the Advance Encryption Standard algorithm (AES) (Gaurav et al., 2013; Kumar & Tewari, 2017) and many other algorithms, if an adversary manages to recover any of the round keys, all other keys could easily be recovered due to the static nature of the algorithm (Ferguson; Niels, 2010), thus makes algorithms susceptible to related key attack and other attack scenarios. This weakness has to be addressed using a light

weight dynamic substitution table to produce highly unrelated, unpredictable and random encryption keys that is resistant to all the above mentioned attacks.

This research will investigate the potentials of non-associative and non-commutative quasigroup as a dynamic substitution table to nurture the problems highlighted in AES, Hybrid Cube, TCE etcetera, in producing pseudorandom numbers as a primitive to key derivation function and key scheduling algorithms. It will also study the generic quasigroup string transformations to evaluate its strength and to eventually propose a robust quasigroup string transformation if the existing scheme is found vulnerable. This is based on the efficiency of quasigroup in developing cryptographic algorithms advocated by researchers.

1.3 Objectives of the Study

The objectives of this research are as follows:

i) To study the Key Scheduling Algorithm, quasigroup string transformation and asymmetric block cipher.

ii) To model a dynamic key schedule algorithm based on the key derivation function and dynamic substitution table, and implement it into an existing block cipher.

iii) To evaluate the proposed key schedule algorithm and the block cipher best on the test tailored for KSAs and block ciphers.

1.4 Scope of the Study

This research concentrates on the development of dynamic key scheduling algorithm using non-associative non-commutative quasigroup which is used in the development of new block cipher.

1.5 Contributions

Encryption algorithms play an important role in ensuring the confidentiality of information from adversary while on transit. Such algorithms requires unpredictable encryption key to be shared between the sender and receiver to ensure the

confidentiality. Notable researchers in this field have reaffirmed that the strength of encryption algorithm solely depends on the strength of its key. Therefore this research has produced a key scheduling algorithm and implemented it in a modified Rijndael block cipher and the ultimate goal is to contribute to the body of knowledge and society.

The contribution given by this research to the body of knowledge is the fact that it has introduced the use of highly shapeless quasigroup as a dynamic substitution table for generating encryption key(s). A highly shapeless quasigroup is generated from existing quasigroup using a single permutation. In the proposed scheme, all generated quasigroups from predefined quasigroup appear to have inherited all the properties of the parent quasigroup. The quasigroup string transformation was analyzed to explore vulnerabilities and it is found prone to attack as such, a new string transformation technique is proposed to suit the proposed Key Derivation Function (KDF). The research further proposed a dynamic key scheduling algorithm from the above mentioned components. The proposed KSA adopted the AKDF as the mechanism for stretching the key. All generated keys and sub keys have been tested using a modified Rijndael algorithm and proved to have a reasonable randomness.

On the other hand, construction of a secured encryption algorithm for protecting confidentiality of information is a huge contribution to the society. The proposed algorithm has displayed a significant improvement over the world must popular encryption algorithm (AES) which is the current standard of block cipher at the moment. This will serve not only as robust alternative to the existing algorithms, but will also nurture the restriction problem that prevented other algorithms to be used elsewhere.

The future work of this research is to developing a secured lightweight authenticated encryption algorithm from the proposed modified Rijndael algorithm. Mathematical proof will also be considered in the future work to obtain the mathematical view of its performance.

1.6 Thesis Organization

This thesis section described how the thesis is being organized and what is contained in each chapter. The following is the outlines of the thesis.

Chapter 1 is the introduction part that defined what a key scheduling algorithm is all about, how it is being used in asymmetric block cipher. It also highlighted the problems of existing algorithms and proposed solutions to the existing problems. Importance and benefits of the proposed solutions are also part of this chapter. Similarly, the scope and objectives of the research has also been highlighted in the chapter.

Chapter 2 describes related literature reviews which are relevant in the design, development and suitable security analysis for the proposed key scheduling algorithm and the block cipher. Previous researches and related works have been discussed in this chapter with examples and figures to ease understanding. Various techniques for evaluating the security and resistance to attacks for key scheduling algorithm and block cipher are also presented in this chapter.

Chapter 3 presents theoretical concepts related to the design of the dynamic key scheduling algorithm, the block cipher and the overall framework of this research. This chapter is divided into two sections. The first section outlines the concepts, design and process of generating the isotope, the key derivation function and the key scheduling algorithm. The second section discusses the design of and integration of key scheduling algorithm into a block cipher, with pilot test of the encryption and decryption algorithm.

Chapter 4 provides the implementation of the new modified block cipher. This chapter is also divided into two sections. The first section describes the implementation of the Key Scheduling algorithm, Encryption and Decryption algorithm while the second phase gives the account of the full implementation of the proposed block cipher.

Chapter 5 contains the security analysis of the proposed algorithm to examine its strength and reliability. Several standardized test and attack scenarios were used for the test. The results from the analysis are presented and discussed to verify the strength of the proposed algorithm.

Chapter 6 provides conclusion and direction for further research on symmetric key cryptography.

REFERENCES

Abed, F., List, E., Lucks, S., & Wenzel, J. (2014). Differential Cryptanalysis of Round-Reduced Simon and Speck. In *International Workshop on Fast Software Encryption* (pp. 525–545). Springer, Berlin, Heidelberg.

Abu-salma, R., Sasse, M. A., Bonneau, J., Danilova, A., Naiakshina, A., & Smith, M. (2017). Obstacles to the Adoption of Secure Communication Tools. *IEEE Security & Privacy*, 137–153. http://doi.org/10.1109/SP.2017.65

Agrawal, M., Chang, D., & Sanadhya, S. K. (2015). A New Authenticated Encryption Technique for Handling Long Ciphertexts in Memory Constrained Devices. *IACR Cryptology ePrint Archive*, *2015*, 331. Retrieved from http://dblp.uni-trier.de/db/journals/iacr/iacr2015.html#AgrawalCS15

Ahmad, H., Hassan, A., Saeb, M., & Hamed, H. D. (2005). The " PYRAMIDS " Block Cipher. *IJ Network Security*, *2*, 50–60.

Aiden A. Bruen and Mario A. Forcinito. (2005). *Cryptography, Information Theory, and Error-Correction*. John Wiley & Sons, Inc.

Bakeva, V. (2011). Parastrophic quasigroup string processing, (Ciit), 19–21.

Battey, M., & Parakh, A. (2014). Cryptanalysis of the Quasigroup Block Cipher. In *Proceedings of the 2014 ACM Southeast Regional Conference* (pp. 3–6). http://doi.org/10.1145/2638404.2737600

Battey, M., Parakh, A., & Mahoney, W. (2015). Cryptanalysis and Improvements of the Quasigroup Block Cipher. *Journal of Information Assuarance and Security*, *10*, 31–39.

Belyavskaya, G. B. (2014). Parastrophically equivalent identities characterizing quasigroups isotopic to abelian groups. *Quasigroups and Related Systems*, *22*, 19–32.

Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D., & Shamir, A. (2010). Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds. *Lecture Notes in Computer Science (Including Subseries Lecture Notes*

in Artificial Intelligence and Lecture Notes in Bioinformatics), 6110 LNCS(October 2000), 299–319. http://doi.org/10.1007/978-3-642-13190-5_15

Campbell, J. (2016). Cryptography, Network Exploitation, Crime & Policy Impact. Saint Leo University.

Chen, J., & Jia, K. (2010). Improved related-key boomerang attacks on round-reduced Threefish-512. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6047 LNCS*(2007), 1–18. http://doi.org/10.1007/978-3-642-12827-1_1

Chuah, C. W., Dawson, E., & Simpson, L. (2013). Key Derivation Function : The SCKDF Scheme. *Springer Berlin Heidelberg.*, 125–138.

Clark, W. E. (2001). *Elementary Abstract Algebra. The American Mathematical Monthly* (Vol. 74). http://doi.org/10.2307/2316071

Clark, W. E. (2003). *Elementary Number Theory. The American Mathematical Monthly* (Vol. 78). http://doi.org/10.2307/2318039

Consortium, N. (2004). *Nessie Report*. *Springer-Verlag*.

Conti, M., Di Natale, G., Heuser, A., Pöppelmann, T., & Mentens, N. (2017). Do We Need a Holistic Approach for the Design of Secure IoT Systems? *Proceedings of the Computing Frontiers Conference*, 425–430. http://doi.org/10.1145/3075564.3079070

Damm, M. (2003). On the existence of totally anti-symmetric quasigroups of order 4k + 2. *Computing (Vienna/New York)*, *70*(4), 349–357. http://doi.org/10.1007/s00607-003-0017-3

Dimitrova, V., & Markovski, J. (2004). On Quasigroup Pseudo Random Sequence Generators. *Proc. of the 1-St Balkan Conference in Informatics, Y. Manolopoulos and P. Spirakis Eds*, 21–23.

Disina, A. H. (2014). *Robust Caesar Cipher against frequency cryptanalysis using bi-directional shifting*. Universiti Tun Hussein Onn Malaysia. Retrieved from eprints.uthm.edu.my

Disina, A. H., Jamel, S., Pindar, Z. A., & Deris, M. M. (2016). All-or-nothing Key Derivation Function Based on Quasigroup String. *International Conference on Information Science and Security (ICISS)*, 6–10. http://doi.org/10.1109/ICISSEC.2016.7885839

Dodis, Y. (2013). The Cost of Cryptography. *New York University*. Retrieved from http://nautil.us/issue/7/waste/the-cost-of-cryptography

Ferguson; Niels, S. L. B. S. D. W. M. B. T. K. J. C. J. W. (2010). The Skein Hash Function. *Hash, First Candidate, Function Leuven, Conference*, (February).

Fluhrer, S., Mantin, I., & Shamir, A. (2001). Weaknesses in the Key Scheduling Algorithm of RC4. *Lecture Notes in Computer Science*, *Springer*, *2259*, 1–24. http://doi.org/10.1007/3-540-45537-X_1

Gaurav, K., Pal, K., & Dilbahar, S. (2013). Change in the Key Expansion Function of AES. *IJITEE*, *Volume 2*(4), 267–269.

Gerlock, L., & Parakh, A. (2016). Linear Cryptanalysis of Quasigroup Block Cipher. In *Annual Cyber and Information Security Research Conference* (p. 19:1-19:4). http://doi.org/10.1145/2897795.2897818

Glenn, R., & Kelly, S. (2003). *The AES-CBC Cipher Algorithm and Its Use with IPsec Status*.

Grošek, O. (2010). Isotopy of Latin Squares in Cryptography. *Tatra Mt. Math. Publ*, *45*, 27–36. http://doi.org/10.2478/v10127-010-0003-z

Hall, C., & Ferguson, N. (2001). *Chapter 7 The Advanced Encryption Standard (AES).*

ISO (the International Organization for Standardization). (2013). *INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Privacy framework* (Vol. 2010).

Jamel, S., Herawan, T., & Deris, M. M. (2010). A cryptographic algorithm based on hybrid cubes. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6019 LNCS*(PART 4), 175–187. http://doi.org/10.1007/978-3-642-12189-0-16

Jindal, P., & Singh, B. (2015). Analyzing the security-performance tradeoff in block ciphers. *International Conference on Computing, Communication and Automation, ICCCA 2015*, 326–331. http://doi.org/10.1109/CCAA.2015.7148425

Jones, G. A. (2014). Primitive permutation groups containing a cycle. *Bulletin of the Australian Mathematical Society*, *89(1).*(2), 159–165. http://doi.org/10.1112/jlms/s2-10.2.225

Jorstad, N., & Landgrave, T. (1997). Cryptographic algorithm metrics. In *20th National Information Systems Security*. Retrieved from http://csrc.nist.gov/nissc/1997/proceedings/128.pdf

Kailkhura, B., Nadendla, V. S. S., & Varshney, P. K. (2015). Distributed inference in

the presence of eavesdroppers: A survey. *IEEE Communications Magazine*, *53*(6), 40–46. http://doi.org/10.1109/MCOM.2015.7120015

Kak, A. (2015). Lecture 8 : The Advanced Encryption Standard Lecture Notes on " Computer and Network Security ."

Katiyar, S., & Jeyanthi. (2016). Pure Dynamic S-box Construction. *International Journal of Computers S. Katiyar, N. Jeyanthi*, *1*(1), 42–46.

Kim, S.-J., Umeno, K., & Hasegawa, A. (2004). Corrections of the NIST Statistical Test Suite for Randomness. *Quantum*, *18*(6), 1367–1379. http://doi.org/10.1364/OE.18.005512

Kishan, C. G., & Ray, I. G. (2014). On Constructions of Circulant MDS Matrices for Lightweight Cryptography. In *International Conference on Information Security Practice and Experience* (pp. 564–576). Springer-Verlag New York, Inc..

Knudsen, L. (1999). Some thoughts on the AES process. *Comment Submitted to NIST*, 1–5. Retrieved from http://reference.kfupm.edu.sa/content/s/o/some_thoughts_on_the_aes_process_117648.pdf

Kölbl, S., Leander, G., & Tiessen, T. (2015). Observations on the SIMON block cipher family. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9215*, 161–185. http://doi.org/10.1007/978-3-662-47989-6_8

Krape, A. (2017). Weak associativity and quasigroup units. *Mathematics Subject Classi Cation*, 1–8.

Krawczyk, H. (2010). Cryptographic extraction and key derivation: The HKDF scheme. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6223 LNCS*, 631–648. http://doi.org/10.1007/978-3-642-14623-7_34

Kumar, A., & Tewari, R. R. (2017). Expansion of Round Key Generations in Advanced Encryption Standard for Secure Communication, *13*(7), 1679–1698.

Lee, Y., Kim, Y.-S., & No, J.-S. (2017). Ciphertext-Only Attack on Linear Feedback Shift Register-Based Esmaeili-Gulliver Cryptosystem. *IEEE Communications Letters*, *21*(5), 971–974. http://doi.org/10.1109/LCOMM.2017.2654238

Li, Y., Zhou, J., & Li, Y. (2015). Ciphertext-Only Attack on an Image Homomorphic Encryption Scheme with Small Ciphertext Expansion. *Proceedings of the 23rd ACM International Conference on Multimedia*, 1063–1066.

http://doi.org/10.1145/2733373.2806406

Marnas, S. I., Angelis, L., & Bleris, G. L. (2003). All-Or-Nothing Transforms Using Quasigroups. *Proc. 1st Balkan Conference in Informatics*, 183–191.

Matsui, M. (1996). Block Encryption Algorithm MISTY. *Technical Report of IEICE ISEC 96*, *167*, 35–48. http://doi.org/10.1007/BFb0052334

Meyer, K. A. (2006). A new message authentication code based on the non-associativity of quasigroups. *Retrospective Theses and Dissertations*.

Michael Damm, H. (2007). Totally anti-symmetric quasigroups for all orders. *Discrete Mathematics*, *307*(6), 715–729. http://doi.org/10.1016/j.disc.2006.05.033

Mileva, A., & Markovski, S. (2010). Quasigroup String Transformations and Hash Function Design. *ICT Innovations 2009*, 367–376.

Mileva, A., & Markovski, S. (2012). Shapeless Quasigroups Derived by Feistel Orthomorphisms. *Glasnik Matematicki*, *47*(67), 333–349. http://doi.org/10.3336/gm.47.2.09

Mushtaq, M. F., Jamel, S., & Deris, M. M. (2017a). Triangular Coordinate Extraction (TCE) for Hybrid Cubes. *Journal of Engineering and Applied Sciences*, *8*(12), 2164–2169.

Mushtaq, M. F., Jamel, S., & Deris, M. M. (2017b). Triangular Coordinate Extraction (TCE) for hybrid cubes. *Journal of Engineering and Applied Sciences*. http://doi.org/10.3923/jeasci.2017.2164.2169

Mushtaq, M. F., Jamel, S., Mohamad, K. M., Kamal, S. K. A., & Deris, M. M. (2017). Key Generation Technique based on Triangular Coordinate Extraction for Hybrid Cubes. *Journal of Telecommunication, Electronic and Computer Engineering*, *9*(3–4), 195–200.

Nag, A., Singh, J. P., Khan, S., Ghosh, S., Biswas, S., Sarkar, D., & Sarkar, P. P. (2011). Image encryption using affine transform and XOR operation. *2011 - International Conference on Signal Processing, Communication, Computing and Networking Technologies, ICSCCN-2011*, (Icsccn), 309–312. http://doi.org/10.1109/ICSCCN.2011.6024565

Olsson, C. (2017). *Secret Communication Using Latin Squares and Quasigroups*. UMEA UNIVERSITY.

Pindar, Z., Jamel, S. H., Disina, A., & Deris, M. M. (2015a). Compression Function Based on Permutations Quasigroups. *ARPN Journal*, (X), 1–8.

Pindar, Z., Jamel, S. H., Disina, A., & Deris, M. M. (2015b). Compression Function Based on Permutations Quasigroups. *ARPN Journal*, *(In press)*(X), 1–8.

Rajavel, D., & Shantharajah, S. P. (2012). Cubical Key Generation and Encryption Algorithm Based on Hybrid Cube ' s Rotation. In *Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering*.

Ramanujam, S., & Karuppiah, M. (2011). Designing an algorithm with high Avalanche Effect. *International Journal of Computer Science and Network Security*, *11*(1), 106–111.

Refaey, A., Loukhaoukha, K., & Dahmane, A. (2017). Cryptanalysis of Stream Cipher Using Density Evolution. In *IEEE Conference on Communications and Network Security (CNS)* (pp. 382–383).

Rihan, S. D., Osman, S. E. F., & Khalid, A. (2015). A Performance Comparison of Encryption Algorithms AES and DES. *Intetnational Journal of Engineering Research & Technology*, *4*(12), 151–154.

Rivest, R., Robshaw, M. J. B., Sidney, R., & Yin, Y. L. (1998). The RC6 Block Cipher. *In First Advanced Encryption …*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.35.7355

Rogaway, P., & Shrimpton, T. (2004). Fast Software Encryption. *FSE 2004: Fast Software Encryption*, *3017*(Fse 2004), 371–388. http://doi.org/10.1007/b98177

Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., … Vo, S. (2001). *A STATISTICAL TEST SUITE FOR RANDOM AND PSEUDORANDOM NUMBER GENERATORS FOR CRYPTOGRAPHIC APPLICATIONS* (Vol. 22).

Sapiee Jamel, Mustafa Mat Deris, I. T. Y. and T. H. (2011). The Hybrid Cubes Encryption Algorithm (HiSea) Sapiee. *Communications in Computer and Information Science*, *154 CCIS*, 191–200. http://doi.org/10.1007/978-3-642-21153-9_18

Schmidt, N. O. (2016). *Latin squares and their applications*. *Academic Press BOISE STATE UNIVERSITY GRADUATE COLLEGE*. http://doi.org/10.1016/B978-0-444-63555-6.50008-8

Schneier, B. (1996). *Applied Cryptography* (Second Edi). John Wiley & Sons, Inc.

Schneier, B. (2010). *Crypto Engineering Design Principles and Practical Applications*. Wiley Publishing Inc.

Sharma, A., Bhatnagar, A., Tak, N., Sharma, A., & Avasthi, J. (2012). an Approach

of Substitution Method Based on Ascii Codes in Encryption Technique. *IJASCSE*, *1*(3).

Shcherbacov, V. A. (2015). Prolongations of quasigroups. *arXiv Preprint arXiv:1507.05608*. Retrieved from http://arxiv.org/abs/1507.05608

Smile Markovski. (2015). Design of Crypto Premitives Based on Quasigroup. *Quasigroup and Related Systems*, *23*, 41–90.

Smile Markovski and Verica Bakeva. (2007). QUASIGROUP STRING PROCESSING: PART 4, *2*(1), 41–53.

Stallings, W. (2006). Cryptography and Network Security (p. chapter 14 Entity Authentication).

SUŠIL, P. (2015). *Algebraic Cryptanalysis of Deterministic Symmetric Encryption*. ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE. Retrieved from http://infoscience.epfl.ch/record/210605/files/EPFL_TH6651.pdf

Wang, J.-F. W. J.-F., Chang, S.-W. C. S.-W., & Lin, P.-C. L. P.-C. (2003). A novel round function architecture for AES encryption/decryption utilizing look-up table. *IEEE 37th Annual 2003 International Carnahan Conference onSecurity Technology 2003 Proceedings*, 132–136. http://doi.org/10.1109/CCST.2003.1297549

Xu, Z. D. Q. (2015). The Design of A Key Expansion Algorithm Based On Dynamic Dislocation Counts. http://doi.org/10.1109/CIS.2015.90

Yuen, H. P. (2014). Can Quantum Key Distribution Be Secure. *arXiv:1405.0457v2 [Quant-Ph] 22 Sep 2014 HAS*, 1–14. Retrieved from http://arxiv.org/abs/1405.0457

Zorkta, H., & Kabani, T. (2011). New Cipher Algorithm Based on Multiple Quasigroups. *International Journal of Machine Learning and Computing*, *1*(5), 454–459. http://doi.org/10.7763/IJMLC.2011.V1.68