UNIVERSITI PUTRA MALAYSIA

MATHEMATICAL ASPECTS OF SELECTED BLOCK CIPHERS

YAZEED SAEED ALQARNI

IPM 2015 1

MATHEMATICAL ASPECTS OF SELECTED BLOCK CIPHERS

By

YAZEED SAEED ALQARNI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

June 2015

To

They brought me up when I was small,

I lower to them the wing of humility out of mercy,

my parents.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science

MATHEMATICAL ASPECTS OF SELECTED BLOCK CIPHERS

By

YAZEED SAEED ALQARNI

June 2015

Chairman: Assoc. Prof. Mohamad Rushdan Md Said, PhD

Faculty: Institute for Mathematical Research

Block ciphers play a key role in many cryptographic protocols that provide communications security in modern society. The security of such cryptographic protocols is depending basically on the underlying block ciphers that are being used. In order to achieve a secure block cipher, it is important to have a good understanding in how to design and analyse such block cipher. However, the current level of understanding has still not reach the peak, and the progress is active to improve our understanding of how to design and analyse them. Evaluating some common and important mathematical primitives will provide more optimization of block cipher design and analysis.

The main objective of this thesis is to analyse the mathematical primitives used in the design of many block ciphers and point out which primitives are essential and important in the fulfilment of confusion and diffusion properties.

The findings of the thesis can be divided into the following main contributions: an overview of the different types of block ciphers primitives are given, the block ciphers are explored in terms of their underlying algebraic structure operations, and the algebraic primitives used in block ciphers design are evaluated from their security and efficiency aspects and then compared with random substitution boxes (S-boxes). The main focus is to measure how algebraic primitives are exhibited to meet diffusion and confusion properties. After that, the requirements of Boolean functions and S-boxes are discussed. In addition, an analysis of several Boolean functions and S-boxes is presented in terms of the desired cryptographic properties, and the comparison is drawn in order to show the different strengths and weaknesses.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia

sebagai memenuhi keperluan untuk ijazah Master Sains

ASPEK MATEMATIK BLOK SIFER TERPILH

Oleh

YAZEED SAEED ALQARNI

June 2015

Pengerusi: Prof. Madya. Mohamad Rushdan Md Said, PhD

Fakulti: Institut Penyelidikan Matematik

Blok sifer memainkan peranan penting dalam banyak protokol kriptografi yang menyediakan keselamatan komunikasi dalam masyarakat moden. Keselamatan protokol kriptografi itu bergantung pada dasarnya di blok sifer asas yang digunakan. Dalam usaha untuk mencapai blok sifer selamat, ia adalah penting untuk mempunyai pemahaman yang baik dalam bagaimana untuk merekabentuk dan menganalisis blok sifer tersebut. Walau bagaimanapun, tahap semasa persefahaman masih belum mencapai puncak, dan kemajuan yang aktif untuk meningkatkan pemahaman kita tentang bagaimana untuk mereka bentuk dan menganalisanya.

Objektif utama projek ini adalah untuk menganalisis primitif matematik yang digunakan dalam reka bentuk tulisan blok sifer banyak dan menunjukkan yang primitif adalah penting dan penting sebagai memenuhi kekeliruan dan resapan hartanah.

Hasil tesis boleh dibahagikan kepada sumbangan utama berikut: gambaran keseluruhan pelbagai jenis sifer blok primitif diberi kita meneroka blok sifer dari segi operasi struktur algebra asas dan menilai primitif. Fokus utama adalah untuk mengukur bagaimana primitif algebra dipamerkan untuk memenuhi sifat penyebaran dan kekeliruan. Selepas itu, kami menganalisis moden primitif blok sifer berdasarkan keperluan fungsi Boolean dan S-kotak dan membandingkan mereka dari segi sifat-sifat kriptografi dikehendaki.

ACKNOWLEDGEMENTS

I have to admit that for being able to complete this thesis I owe everybody. However thanking everybody is like thanking nobody. That's why next I shall try to single out the names of a few notable individuals, without whose help I would have never been able to accomplish the task of successfully beginning and completing my thesis.

First and all the time, all praise to the Almighty Allah who taught by the pen, taught me that which I knew not.

I am greatly grateful to my supervising committee especially Dr Rushdan for his kindness, humility, and directions. I believe this research would not be completed without him. Many thanks also to Dr. Zuriati Ahmad for her support and advice. I thank also Dr. Rezal for his comments and corrections.

I would like also to express my gratitude to emeritus Prof. G J Kühn who inspired me to study cryptography. I have learned a lot lessons from him even at the age of 80. He was encouraging me to continue my postgraduate study in cryptography. Prof. Kühn is my best Influential teacher, my thanks to him.

I most gratefully thank my UPM teachers: Dr. Adem Kilicman, Dr. Azizol Abdullah and Dr. Ramlan Mahmod for their efforts in class teaching.

Next I would like to thank who have given pleasure to me, my wife and my son. I believe the environment makes a good researcher more than talent and brains.

I gracefully thank the Ministry of Higher Education Saudi Arabia for financing my research. Their support is highly appreciated.

Yazeed Al-Qarni

Putrajaya, December 2014

I certify that a Thesis Examination Committee has met on 10 June 2015 to conduct the final examination of Yazeed Al-Qarni on his thesis entitled "Mathematical Aspects of Selected Block Ciphers" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Master of Science.

Members of the Thesis Examination Committee were as follows:

Mahendran Shitan, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Chairman)

Siti Hasana Sapar, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Internal Examiner)

Eddie Shahril Ismail, PhD
Associate Professor
Faculty of Science and Technology
Universiti Kebangsaan Malaysia
Malaysia
(External Examiner)

ZULKARNAIN ZAINAL, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 17 June 2015

This thesis submitted to the Senate of Universiti Putra Malaysia has been accepted as fulfilment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

Mohamad Rushdan Md Said, PhD
Associate Professor
Institute for Mathematical Research
Universiti Putra Malaysia
(Chairman)

Zuriati Ahmad Zukarnain, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ZULKARNAIN ZAINAL, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 17 June 2015

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: _____ Date: _____

Name and Matric No.: _____

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: _____
Name of
Chairman of
Supervisory
Committee: _____

Signature: _____
Name of
Member of
Supervisory
Committee: _____

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
CRYPTREC	Cryptography Research and Evaluation Committees
DES	Data Encryption Standard
GF	Galois Field
IDEA	International Data Encryption Algorithm
MDS	Maximum Distance Separable
NESSIE	New European Schemes for Signature, Integrity, and Encryption
PES	Proposed Encryption Standard
PGM	Permutation Group Mapping
PHT	Pseudo Hadamard Transform
RFID	Radio Frequency Identification
SAC	Strict Avalanche Criterion
SAFER	Secure and Fast Encryption Routine
SPN	Substitution Permutation Network

LIST OF NOTATIONS

$\mathbb{Z}_2$	set of residues modulo 2, i.e., {0,1}
$\mathbb{Z}_2^n$	set of all binary vectors with components in $\mathbb{Z}_2$
$GF(2^n)$	Galois field of 2^n elements
x	a vector
x_i	component i of the vector x
$\oplus$	exclusive-OR
$\boxplus$	addition modulo 2^n
$\odot$	multiplication modulo $2^n + 1$
M	a matrix
M^{-1}	a matrix inverse
Δ	difference between two elements
DP	differential probability
$n \times n$	size of S-box
LP	linear approximation probability
$L_{a,b}$	maximum linear approximation
bs	linearity bias
$Tr(x)$	trace function of x
$\hat{f}$	polarity function f

CHAPTER 1

INTRODUCTION

In the modern era, communication has become an important pillar in our social life. With rapid development in communication, information security has become a general concern. The transmission of information from one place to another could be exploited by eavesdropping, modification or changing path. For instance, when a bank user gives an online order to transfer a specified amount of money, the user expect no entity other than bank has known the order, the amount has not changed, and the order delivered to the correct recipient bank. These three concerns are equivalent to confidentiality, integrity, and authenticity respectively. Eventually, the need of modern secret writing techniques, or cryptology, has been arisen.

Cryptology is the science that concern with security solutions such as confidentiality between users, data integrity, and data origin authentication. Conventionally, cryptology can be divided into cryptography and cryptanalysis. While cryptography deals with design new algorithms and application, cryptanalysis concerns with possible attacks on cryptographic algorithms.

To achieve confidentiality of messages, the used cryptographic algorithm has to be secure. The security of cryptographic algorithms is based on practical method. It is measured by estimating the computing power that is necessary to break the algorithm. This measure can be done by exhaustive search or by known attack on such algorithm. Even the security of cryptographic algorithm is the main criterion; it is not enough to evaluate cryptographic algorithms based on security criterion only. The performance of algorithm is also one of the most important concerns. Typically, slow cryptographic algorithms are useless in term of encryption even they are very secure.

It is customary to categorize cryptographic algorithms into three types based on the number of used keys: symmetric key (or secret) cryptography, asymmetric (or public key) cryptography, and hash functions. In symmetric key cryptography, one key is being used for encryption and decryption, while in asymmetric cryptography one key used for encryption and the other for decryption. Furthermore, symmetric key cryptography can be categorized into block ciphers and steam ciphers. The main difference between block and steam ciphers is the steam ciphers are time-varying and based on small units like bits, while block ciphers encryption are fixed through time and typically based on large units like bytes. Hash function techniques are typically keyless and concerned with data integrity; it guarantees no modification has done on hashed data.

In this thesis, we narrow our interest to block ciphers cryptographic algorithms. Typically, symmetric modern block cipher is a process of encrypting a block of plaintext into a block of ciphertext using secret key, the decrypting is identically the

inverse process using the same key. Moreover, block ciphers can be seen as a permutation determined by secret key from input to output bits.

Problem Statement and Objectives

Block ciphers today are used in many commercial and military applications: credit cards, wireless network connections, secure voice devices etc. The security of applications is depending basically on the underlying block ciphers that being used. The most widely accepted principles in block cipher design are confusion and diffusion due the terms of Shannon [1]. For that matter, many block ciphers have been designed since 1970s. Several ciphers used some aspects of mathematics to satisfying Shannon principles and overcoming new types of attacks. Motivations for all design choices are based on resistance against known types of attacks.

However, the current level of understanding has still not reach the peak, and many gaps in block cipher design have to be bridged. In particular, the balance between security and performance is still an active research. In addition, many block ciphers are suffering from arbitrary components that are lacking mathematical analysis and justification. Furthermore, block cipher primitives based on mathematical description need to be formalized to achieve high standard of security.

In this context, we give much attention to analyse existing mathematical primitives. By this way it is worthy to benefit from existing successes and failures. This thesis presents a study of block cipher from mathematical point of view. It follows these mathematical aspects and investigates the strength and weakness of them from security and performance perspectives. We define our hypothesis: that indeed constructing a good cipher based on well-defined mathematics primitives will tend to a better understanding, easy to analyse and provable security.

The main objectives of this thesis are:

- To analyse the mathematical primitives used in design of many block ciphers and point out which primitives are essential and important in fulfilment confusion and diffusion properties.
- To explore block ciphers in terms of their underlying algebraic structure operations and evaluate the primitives from their security and efficiency aspects, and to examine how primitives exhibit to meet diffusion and confusion properties.
- To analyse modern block cipher primitives based on the requirements of Boolean functions and S-boxes and to compare them in terms of desired cryptographic properties.

Therefore, it helps to get a better understanding, and participates in developing fast and secure block ciphers. Additionally, we aim to open more insights toward constructing rigorous mathematical models in the future.

Outline and Main Contributions

The block cipher design philosophy is briefly presented in Chapter 2. First, the block cipher configuration is defined. Then, the components of block cipher design are addressed on the whole. Whereas the upper and low level structure is described, the

small primitive operations are also instanced. We contribute by studying five block ciphers in term of elementary operations they are used, the comparison are summarized in Table 2.1. Finally, a historical journey of block ciphers development is reviewed.

In Chapter 3, we study several varying block cipher primitives based on operations of three common algebraic structures: groups, rings, and fields. We examine how block cipher primitives exhibit to meet diffusion and confusion properties using algebraic structures operations. Finally, we give analysis on primitive based on finite field $GF(2^n)$. Our original work for this chapter consists of exploring several ciphers, to construct the underlying algebraic structure operations and then evaluate them from security or performance prospective at the end of each studied primitive. Moreover, we write our program to generate 100 samples of random substitution boxes (S-boxes) and compare the result with S-box realised by inversion in Galois field. The results are summarized in Table 3.2, Table 3.3, Table 3.4, and Table 3.5.

The aim of Chapter 4 is to analyse modern block cipher primitives based on the requirements of Boolean functions and S-boxes. In the first part of this chapter we study Boolean functions from cryptography point of view. Then, we show the relation between Boolean function properties and S-box quality with fair analysis of modern S-boxes. Our original work for this chapter consists of analysing several Boolean functions and S-boxes that are being used in recent block. Then, we compare them in term of desired cryptographic properties. The results of Boolean functions analysis are summarized in Table 4.2, Table 4.3, and Table 4.4 where the results of our analysis of cryptographic properties of several block ciphers S-boxes are summarized in Figure 4.1, Figure 4.2, Figure 4.3, Figure 4.4, Table 4.5, and Table 4.6.

Finally, we end this thesis with conclusions and present some open research area in the future.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal,* p. 656–715, 1949.

[2] L. R. Knudsen, and M. J. B. Robshaw, The block cipher companion, Springer, 2011.

[3] A. F.Webster and S. E. Tavares, "On the design of S-boxes," *Advances in Cryptology - CRYPTO '85,* vol. 218, p. 523–534, Springer,1986.

[4] National Institute of Standards and Technology, "Data encryption standard," Federal Information Processing Standard (FIPS), Publication 46, Washington D.C., 1977.

[5] X. Lai, J. L. Massey, and S. Murphy, "Markov ciphers and differential cryptanalysis," *Advances in Cryptology - EUROCRYPT '91,* vol. 547, p. 17–38, Springer,1992.

[6] National Institute of Standards and Technology, "Advanced encryption standard," Federal Information Processing Standard (FIPS), Publication 197, Washington D.C., 2001.

[7] R. L. Rivest, "The RC5 encryption algorithm," *Fast Software Encryption, FSE 1994,* vol. 1008, p. 86–96, Springer,1995.

[8] H. Feistel, W. A. Notz, and J. L. Smith, "Some cryptographic techniques for machine to machine data communications," in *Proceedings of IEEE,* 1975.

[9] R. L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin, "The RC6 block cipher," Submitted as candidate for AES, [Online]. Available: www.nist.gov/aes.

[10] B. Schneier, J. Kelsey, D. Whiting, D.Wagner, C. Hall, and N. Ferguson, "Twofish: A 128-bit block cipher," Submitted as candidate for AES, [Online]. Available: www.nist.gov/aes.

[11] D. Coppersmith, "The Data Encryption Standard and its strength against attacks," IBM Technical Report, RC18613 (81421), 1992.

[12] S. Miyaguchi, "The FEAL-8 cryptosystem and a call for attack," *Advances in Cryptology - CRYPTO '89,* vol. 435, p. 624–627, Springer,1990.

[13] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptology*, p. 3–72, 1991.

[14] X. Lai and J. L. Massey, "A proposal for a new block encryption standard," *Advances in Cryptology - EUROCRYPT '90,* vol. 473, p. 389–404, Springer,1991.

[15] R. C. Merkle, "Fast software encryption functions," *Advances in Cryptology - CRYPTO '90,* vol. 537, p. 476–501, Springer,1991.

[16] M. Matsui, "Linear cryptanalysis method for DES cipher," *Advances in Cryptology - EUROCRYPT '93,* vol. 765, p. 386–397, Springer,1994.

[17] M. Matsui, "The first experimental cryptanalysis of the Data Encryption Standard," *Advances in Cryptology - CRYPTO '94,* vol. 839, p. 1–11, Springer,1994.

[18] J. L. Massey, "SAFER K-64: A byte-oriented block-ciphering algorithm," *Fast Software Encryption, FSE 1993*, vol. 809, p. pages 1–17, Springer,1994.

[19] S. Vaudenay, "On the need for multipermutations: Cryptanalysis of MD4 and SAFER," *Fast Software Encryption, FSE 1994*, vol. 1008, p. 286–297,

Springer,1995.

[20] L. R. Knudsen, "A key-schedule weakness in SAFER K-64," *Advances in Cryptology - CRYPTO '95,* vol. 963, p. pages 274–286, Springer,1995.

[21] R. G. a. J. V. J. Daemen, "A new approach to block cipher design," *Fast Software Encryption, FSE 1993,* vol. 809, p. pages 18–32, Springer,1994.

[22] V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, and E. De Win, "The cipher SHARK," *Fast Software Encryption, FSE 1996,* vol. 1039, p. 99–111, Springer,1996.

[23] J. Daemen, L. R. Knudsen, and V. Rijmen, "The block cipher Square," *Fast Software Encryption, FSE 1997,* vol. 1267, p. 149–165, Springer,1997.

[24] C. M. Adams, "Constructing symmetric ciphers using the CAST design procedure. Designs,," *Designs, Codes, and Cryptography,* p. 283–316, 1997.

[25] J. Daemen and V. Rijmen, "AES proposal: Rijndael. Version 2.0," [Online]. Available: www.nist.gov/aes.

[26] NESSIE, "New European schemes for signatures, integrity and encryption," [Online]. Available: www.cryptonessie.org.

[27] CRYPTREC, "Cryptography research and evaluation committee.," [Online]. Available: www.ipa.go.jp/security.

[28] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-bit blockcipher CLEFIA," *Fast Software Encryption, FSE 2007,* vol. 4593, p. 181–195, Springer,2007.

[29] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw,Y. Seurin, and C. Vikkelsoe, "PRESENT: An ultra-lightweight block cipher," *Cryptographic Hardware and Embedded Systems - CHES 2007,* vol. 4727, p. 450–466, Springer,2007.

[30] Bogdanov, Andrey, Dmitry Khovratovich, and Christian Rechberger, "Biclique cryptanalysis of the full AES," *Advances in Cryptology–ASIACRYPT 2011,* pp. 344-371, Springer,2011.

[31] J. L. Massey, "Applied digital information theory II. Lecture notes 19," 1984. [Online]. Available: www.isiweb.ee.ethz.ch/archive/massey_scr/adit2.pdf.

[32] Magliveras, Spyros S., and Nasir D. Memon, "Algebraic properties of cryptosystem PGM," *Journal of Cryptology,* vol. 5, no. 3, pp. 167-183, 1992.

[33] S. S. Magliveras, "A Cryptosystem from Logarithmic Signatures of Finite Groups," *Proceedings of the 29th Midwest Symposium on Circuits and Systems,* 1986.

[34] T. Horvath, "Cryptosystem TST - Ph.D. thesis," 1998. [Online]. Available: http://www.exp-math.uni-essen.de/~trung/tst/DissTST.zip.

[35] V. Canda, "Scalable Symmetric Block Ciphers Based on Group Bases - Ph.D. thesis," University of Essen, Germany, 2001. [Online]. Available: http://duepublico.uni-duisburg-essen.de/servlets/DerivateServlet/Derivate-10406/Diss.ps.

[36] J. L. Massey, "SAFER-K: a byte-oriented block-ciphering algorithm," *Fast Software Encryption,* vol. 809, p. 1–17, Springer-Verlag, 1994.

[37] L. R. Knudsen, "A key-schedule weakness in SAFER K-64," pp. 274-286, 1995.

[38] Daemen J, Rijmen V, The design of Rijndael-AES: the advanced encryption

standard, Springer, Berlin, 2002.

[39] Barreto, P. S. L. M., and Vincent Rijmen, "The Khazad legacy-level block cipher," *Primitive submitted to NESSIE 97,* 2000.

[40] Aoki, Kazumaro, et al., "Specification of Camellia-A 128-bit block cipher," 2000. [Online]. Available: https://info.isl.ntt.co.jp/crypt/eng/camellia/dl/cryptrec/00espec.pdf.

[41] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, 1977.

[42] K. Nyberg, "Differentially uniform mappings for cryptography," *Advances in Cryptology — EUROCRYPT '93,* vol. 765, pp. 55-64 , 1994.

[43] Joan Daemen, Vincent Rijmen, "Two-round AES Differentials," *IACR ePrint, eprint.iacr.org/2006/039.pdf,* 2006.

[44] O. Rothaus, "On bent functions," *Journal of Combinatorial Theory,* pp. 300-305, 1976.

[45] H. Feistel, "Cryptography and computer privacy.," *Scientific American* , p. 228, 1973.

[46] Zhang, X.M., Zheng, Y., "GAC-the criterion for global avalanche characteristics of cryptographic functions," *J. Univers.*, p. 316–333, 1995.

[47] Webster, A.F., Tavares, S.E., "On the design of S-boxes.," *Advances in Cryptology CRYPTO 85,* p. 523–534, 1986.

[48] M. T. Inc., "KeeLoq Authentication Products," *http://www.microchip.com/keeloq/.*

[49] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An ultra-lightweight block cipher," *Cryptographic Hardware and Embedded Systems - CHES,* pp. 450-466, 2007.

[50] Kim J, Phan RC-W, "Advanced differential-style cryptanalysis of the NSA's skipjack block cipher," *Cryptologia,* p. 246–270, 2009.

[51] P Barreto, V Rijmen, "The Anubis block cipher, Submission to the NESSIE Project," 2000. [Online]. Available: https://www.cosic.esat.kuleuven.ac.be/nessie/workshop/submissions/anubis.zip.

[52] Anderson, Ross, Eli Biham, and Lars Knudsen, "Serpent: A proposal for the advanced encryption standard," NIST AES Proposal 174, 1998. [Online]. Available: ftp://dijkstra.urgu.org/crypto/Serpent/v1/res/serpent.pdf.

[53] G. J. Kuhn, "A family of binary group operations for block cipher applications," in *South African Symposium on. IEEE,* 1991.

[54] Dénes, J., Keedwell, A.D., Latin Squares and Their Applications, New York, NY: Academic Press, 1974.

[55] Čanda, V., van Trung, T., Magliveras, S., & Horváth, T., "Symmetric block ciphers based on group bases," *Selected Areas in Cryptography,* pp. 89-105, 2001.