COPYRIGHT© INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

EHANCEMENT OF LIGHTWEIGHT BLOCK CIPHER ALGORITHMS

BY

SUFYAN SALIM MAHMOOD AL-DABBAGH

A thesis submitted in fulfilment of the requirement for the degree of Doctor of Philosophy
(Information Technology)

Kulliyyah of Information and Communication Technology
International Islamic University of Malaysia

APRIL 2015

ABSTRACT

Although the Advanced Encryption Standard (AES) is an excellent and preferred choice for almost all block cipher applications, it is not suitable for extremely constrained environments such as Radio-Frequency IDentification (RFID) tags and sensor networks. Therefore, the demand for lightweight algorithms is very strong and vital. Lightweight block ciphers are new and important branch of cryptography and they are the best way to secure the information in constrained devices. This research dealt with three problems; First, it is difficult to optimized three factors at same time. Second, there are many researches still trying to find an algorithm that has the highest level of security. Third, there is lack knowledge on key dependent S-box within lightweight algorithms. All these problems solved in three directions. The first direction proposed lightweight block cipher algorithm called **OLBCA** (**O**ptimized **L**ightweight **B**lock **C**ipher **A**lgorithm) that it outperformed PRESENT, which is one of the famous lightweight algorithm through three factors security, performance and cost. The results showed that **OLBCA** is more secure than PRESENT in terms of (differential cryptanalysis, integral cryptanalysis and boomerang attack). Also, the cost of **OLBCA** is less than PRESENT and the **OLBCA** is faster than PRESENT. The second direction proposed another lightweight block cipher algorithm called **HISEC** (**Hi**ghest **Sec**urity lightweight block cipher algorithm). The results showed that **HISEC** has the higher security than many existing lightweight algorithms especially in the resistance of (differential cryptanalysis, integral cryptanalysis and boomerang attack) while the cost of **HISEC** still reasonable. The third direction proposed five novel methods for generating key dependent S-box in lightweight block cipher algorithms and we did intensive analysis regarding to the security and cost. To the best of our knowledge, this is the first study that analyse the methods for generating key dependent S-box with lightweight block cipher algorithms.

خلاصة البحث

على الرغم من أن معيار التشفير المتقدم (AES) هو خيار ممتاز ومفضل لمعظم تطبيقات Block cipher ، فإنه ليس مناسبا لبيئات مقيدة او محددة في كل من العوامل التالية: الاداء، الكلفة و الامن وكمثال لهذه البيئات RFID و sensor networks. وبالتالي، فإن الطلب على خوارزميات Lightweight Block Cipher قوي جدا وحيوي. خوارزمية Lightweight Block Cipherهو فرع جديد ومهم من التشفير وأنه هو أفضل طريقة لتأمين المعلومات في الأجهزة المقيدة. في هذا البحث، تعاملنا مع ثلاث مشاكل. المشكلة الاولى، من الصعب تحسين ثلاثة عوامل في نفس الوقت. ثانيا، هناك العديد من البحوث لا تزال تحاول العثور على الخوارزمية التي لديها أعلى مستوى من الأمن. ثالثا، هناك نقص في المعرفة dependent S-box Key مع خوارزمية lightweight . كل هذه المشاكل حلت في ثلاثة اتجاهات. الاتجاه الأول تم اقترح خوارزمية جديدة اطلق عليها OLBCA . تفوقت الخوارزمية المقترحة OLBCA على خوارزمية PRESENT والتي تعد واحدة من الخوارزميات الشهيرة من خلال ثلاثة عوامل الأمن والأداء والكلفة. أظهرت النتائج أن OLBCA هو أكثر أمانا من PRESENT من حيث تطبيق الهجوميات الثلاثة (Differential cryptanalysis, Integral cryptanalysis and Boomerang cryptanalysis). أيضا، فإن تكلفة OLBCA أقل من PRESENT و OLBCA كذلك هو أسرع من PRESENT. في الاتجاه الثاني تم اقترح خوارزمية جديدة ايضا اطلق عليها HISEC. أظهرت النتائج أن HISEC لديه أمان أعلى من العديد من الخوارزميات الموجودة حاليا من حيث مقاومة الهجوميات الثلاثة (Differential cryptanalysis, Integral cryptanalysis and Boomerang cryptanalysis). في حين أن تكلفة HISEC تزال معقولة. في الاتجاه الثالث تم اقترح خمس طرق جديدة لتوليد Key Dependent S-box وتم عمل تحليل مكثف فيما يتعلق بلامن والتكلفة. على حد علمنا، هذه هي الدراسة الأولى التي حللت طرق لتوليد Key Dependent S-box مع خوارزميات Lightweight Block Cipher.

APPROVAL PAGE

The thesis of Sufyan Salim Mahmood Al-Dabbagh has been approved by the following:

_____

Imad Fakhri Alshaikhli
Supervisor

_____

Muhammad Reza Zaba
Co-Supervisor

_____

Akram M. Zeki
Internal Examiner

_____

Alaa Al-Hamami
External Examiner

_____

Aziza Binti Abdul Manaf
External Examiner

_____

Radwan Jamal Yousef Elatrash
Chairman

DECLARATION

I hereby declare that this dissertation is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Sufyan Salim Mahmod Al-Dabbagh

Signature..... Date.....

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

Copyright © 2015 by Sufyan Salim Mahmood Al-Dabbagh. All rights reserved

ENHANCEMENT OF LIGHTWEIGHT BLOCK CIPHER ALGORITHMS

No parts of this unpublished research may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission of the copyright holder except provided below.

1. Any material contained in or derived from unpublished research may only be used by others in their writing with due acknowledgement

2. IIUM or its library will have the right to make and transmit copies (print or electronic) for institutional and academic purposes

3. The IIUM library will have the right to make, store in a retrieval system and supply copies of this unpublished research if requested by other universities and research libraries.

Affirmed by Sufyan Salim Mahmood Al-Dabbagh

....

Signature Date

Dedicated to all Muslims…

ACKNOWLEDGEMENTS

This thesis would have been impossible to complete without the help and encouragement of several people. First of all, I wish to express my deepest gratitude and sincere appreciation to my supervisors Dr. Imad Fakhri Alshaikhli and Dr. Muhammad Reza Za'ba for their continues support all the time. Secondly, I am grateful to my lovely parent, my father Prof. Salim, my wife Alyaa, my brother Ph.D candidate Marwan, my sisters (Sura and Dr. Marwa) for their unshakable believe in me since my childhood to achieve my life goals. Last, but not the least, I thank my colleagues (Mustafa Abuzaraida, Rabiul Awal and Fardous Eljadi) for their continues administration help toward my PhD achievement.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

RFID	Radio Frequency IDentification
AES	Advanced Encryption Standard
OLBCA	Optimise three factors of Lightweight Block Cipher Algorithm
HISEC	HIghest SECurity
S-Box	Substitution Box
DDT	Differential Distribution Table
GE	Gate Equivalent
DES	Data Encryption Standard
MACs	Message Authentication Codes
SPN	Substitution and Permutation Network
IP	Initial Permutation
NIST	National Institute of Standards and Technology
GF	Galois Field
ROM	Read Only Memory
LED	Light Encryption Devise
mCrypton	Miniature of Crypton
GFS	Generalized Feistel Structure
IC	Integrated Circuit
LC	Linear Cryptanalysis
DC	Differential Cryptanalysis
ISO/IEC	International Organization for Standardization and the International Electro technical Commission
MNAS	Minimum Number of Active S-box
FPGA	Field Programmable Gate Array

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND

In every part of our life, the utilisation of diminutive computing devices like radio frequency identification (RFID) tags and sensor networks are gaining popularity and they are becoming an integral part of a ubiquitous pervasive communications infrastructure.

The applications for sensor networks and RFID tags are wide and varied; such as ocean and wildlife monitoring, manufacturing machinery performance monitoring, building safety and earthquake monitoring, military applications, monitoring of highway traffic, pollution, wildfires, building security, water quality and even people's heart rates (Weinstein, 2005).

Many of these applications are vital to human safety and health. There are many examples of applications of RFID tags and sensor networks for safety and tracking purposes including personal identification. Accordingly, there is a very high demand for security algorithms to protect the information on these devices (Atzori et al., 2010).

The applications for RFID tags include supply chain management and the tracking of consequential objects and personnel. In supply chain management, RFID tags are used to track products throughout the supply chain from the point of delivery from the supplier to warehouse stock and to the point of sale. There are major and broad applications of RFID for security and personal identification applications. In that regard, an E-passport or electronic passport is one of the most important government applications to enhance boarder security and to make travel easier for

passengers. However, the RFID tags used in E-passports are unusual and they require different technology in comparison to other applications (Weinstein, 2005).

Importantly, to verify the identity of a passport holder without touch or contact with the person, RFID tags can broadcast biometric data of that passport tag. Data can then be transmitted efficiently to a reader and compared with original templates of that user that was previously saved. A passport with a RFID tag is more difficult to forge or clone (Sheetal, 2006).

As mentioned earlier, an identification card is one of the prevalent uses for RFID. A RFID tag in an identification card can be utilised, for instance, to give access to a building; to a floor within a building, and so on. Also, there are RFID tags in credit cards to use for automatic fare payment in mass-transit systems (Osaka et al., 2009).

Moreover, RFID tags can be incorporated with keys for new cars. This added more level of security to ensure the RFID tag can be read by a reader and the reader accepts only the codes that have been saved previously. In that event, if a reader in the car does not match the code in the key then the car will not work. Therefore, the RFID is added a protection to the car from a theft (Francillon et al., 2011).

There are many applications for RFID in the medical field and in the hospitals. One of the important applications is using RFID tags with newborns for ensuring that they are individually identified and preventing anyone unauthorised from steeling the baby from the hospital by alerting the hospital staff. Similarly, RFID is used with the surgical patients for identification and for storing all the relevant information including the patient's history. Also, in the United States of America the Food and Drug Administration (FDA) can ensure the authenticity of prescription drugs by using RFID (Ashar & Ferriter, 2007; Bendavid & Boeck, 2011).

In the education system a RFID could be used to monitor attendance and to locate lost children. For instance, in some schools children are required to wear tag-embedded bracelets or wrist bands while on school grounds.

As many of these applications are for devices that are vital to human safety and health it is crucial to employ well-designed cryptography algorithms for security purposes for these devices. For almost all block cipher applications, the Advanced Encryption Standard (AES) is an excellent and preferred choice. However, it is not suitable for tiny computing devices for many reasons: (Wu & Zhang, 2011).

- Cryptographic functions may introduce an unacceptable delay in RFID systems that require very fast read or write transactions.
- Cryptographic functions require additional power to complete.
- Constrained devises that support onboard encryption currently are most costly than those that do not. One reason for the increased cost is that onboard encryption requires additional logic gates to perform the necessary computations.

Therefore, a new field of cryptography has been developed which termed lightweight cryptography. This research will propose two lightweight block cipher algorithms to secure the information in constrained devices. Also, this research will propose and analyse many novel methods for a key dependent S-box (Ahson & Ilyas, 2010).

1.2 PROBLEM STATEMENT

This research will focus on three problems.

1. It is believed that every designer of lightweight cryptography ought to take into consideration three important factors: cost; security; and performance.

For block ciphers, the key length provides the security –cost trade-off, while the amount of rounds provides the security – performance trade – off and the hardware architecture provides the cost – performance trade – off as shown in Figure (1.1). It is easy to optimise any two of the three factors security and cost, security and performance or cost and performance. However, at the same time it is difficult to enhance all three factors at once (Poschmann, 2009; Thomas, 2007).

To the best of the researcher's knowledge, no other proposal has addressed the problem to enable all three factors to be enhanced at once. Also, as researchers are continuing to try to design an algorithm to enhance all these factors this research will propose a lightweight algorithm that can optimise all these factors.

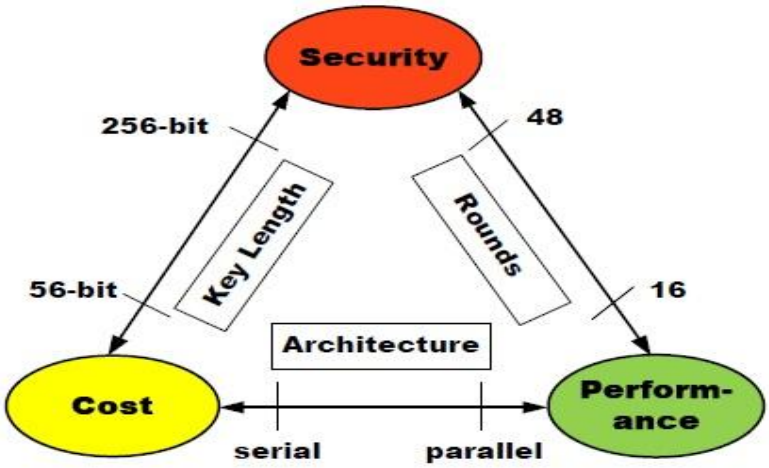

Figure 1.1 The balance between security, cost and performance (Poschmann, 2009; Thomas, 2007)

2. Many existing applications like E-passport are focus on security rather than others factors (Mostowski et al., 2009). Therefore, there are many researches still trying to find an algorithm that has the highest level of

security. This research will propose a lightweight algorithm which has a higher level of security than some other existing algorithms. At the same time, there is no major effect on the cost.

3. The S-box is an important part in block cipher and it is the only non-linear part. All lightweight block ciphers are using fixed 4-bit S-box and the values of those S-boxes are chosen carefully to resist linear and differential cryptanalysis (Borghoff et al., 2012; Suzaki et al., 2013; Yap et al., 2011). Moreover, there are many researchers are claimed that the fixed S-box is less secure than key dependent S-box or secret S-box (Kazlauskas & Kazlauskas, 2009); (Runtong & Like, 2008); (Krishnamurthy & Ramaswamy, 2008); (Abd-ElGhafar et al., 2009); (Juremi et al., 2012); (Hosseinkhani & Javadi, 2012).

   Accordingly, the security of lightweight block cipher algorithms will be improved by designing a method called a key dependent S-box. To best of the researcher's knowledge, there is only one paper that analyzed the using of key dependent S-box or secret S-boxes within PRESENT lightweight block cipher algorithm which means there is lack knowledge on key dependent S-box within lightweight algorithms. Therefore, this research will propose and analyze novel methods for key dependent S-box within lightweight algorithms.

1.3 RESEARCH QUESTIONS

Further to the discussion as highlighted above, the following four questions will be addressed by this research:-

1. Can the three factors (security, cost and speed) be optimised in one lightweight block cipher algorithm?
2. Can we protect the information on lightweight algorithms using a new design with highest security lightweight algorithm?
3. What are the possible methods for generating key dependent S-box?
4. What are the pros and cons for key dependent S-box?

1.4 RESEARCH OBJECTIVES

Further to the four questions posed above, the objectives of this research have been identified as follows:

1. To optimise the three factors (security, cost and speed) together of a lightweight algorithm.
2. To propose a new algorithm with the highest possible level of security.
3. To propose methods for generating key dependent S-box.
4. To study the pros and cons of the key dependent S-box.

1.5 SCOPE OF THE STUDY

Many constrained devices need to secure their data and information. Lightweight algorithms provide the best method of security and they are compatible with these devices. This thesis will design a new lightweight block cipher algorithm based on the function to optimise the three factors of Lightweight Block Cipher Algorithm (OLBCA) with a 64-bit plain text and key size 80-bit. Regarding to the security side, three attacks are applied: differential, integral and boomerang attacks while the speed of the algorithm is measured by using code in C++. Moreover, the cost of algorithm is calculated by using number of GE like other researchers. It will optimise the three