

ANALYSIS AND MODIFICATION OF GRAIN - 128 STREAM
CIPHER ALGORITHM

Norul Hidayah Binti Lot @ Ahmad Zawawi

(Matric No. 3110120)

Thesis submitted in fulfilment for the degree of
MASTER OF SCIENCE
INFORMATION SECURITY AND ASSURANCE

Faculty of Science and Technology

UNIVERSITI SAINS ISLAM MALAYSIA


Kaif

July 2015

AUTHOR DECLARATION

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged

Date :

Signature : 
Name : Norul Hidayah Bt. Lot @ Ahmad Zawawi
Matric No : 3110120
Address : No 3 Jalan Polo Air, 13/57 Seksyen 13
40100 Shah Alam Selangor

UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

BIODATA OF AUTHOR

Norul Hidayah Binti Lot @ Ahmad Zawawi (3110120) was born on the 18th December 1983. She is currently working at CyberSecurity Malaysia, who involved in research and development in cyber technologies related field (specialized in cryptography). She previously was a student of UiTM and obtained Bachelor of Science (Hons) Management Mathematics from Faculty of Information Technology & Quantitative Sciences (currently known as Computer & Mathematical Sciences). She is at present a part-time Master student of USIM majoring in Cryptography.

UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية الماليزية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

ACKNOWLEDGEMENTS

In the name of Allah, the Beneficent, the Merciful. Praise be to Allah, Lord of the Worlds. I want to take this chance to acknowledge the contribution, assistance and support of several people who help to complete my research project.

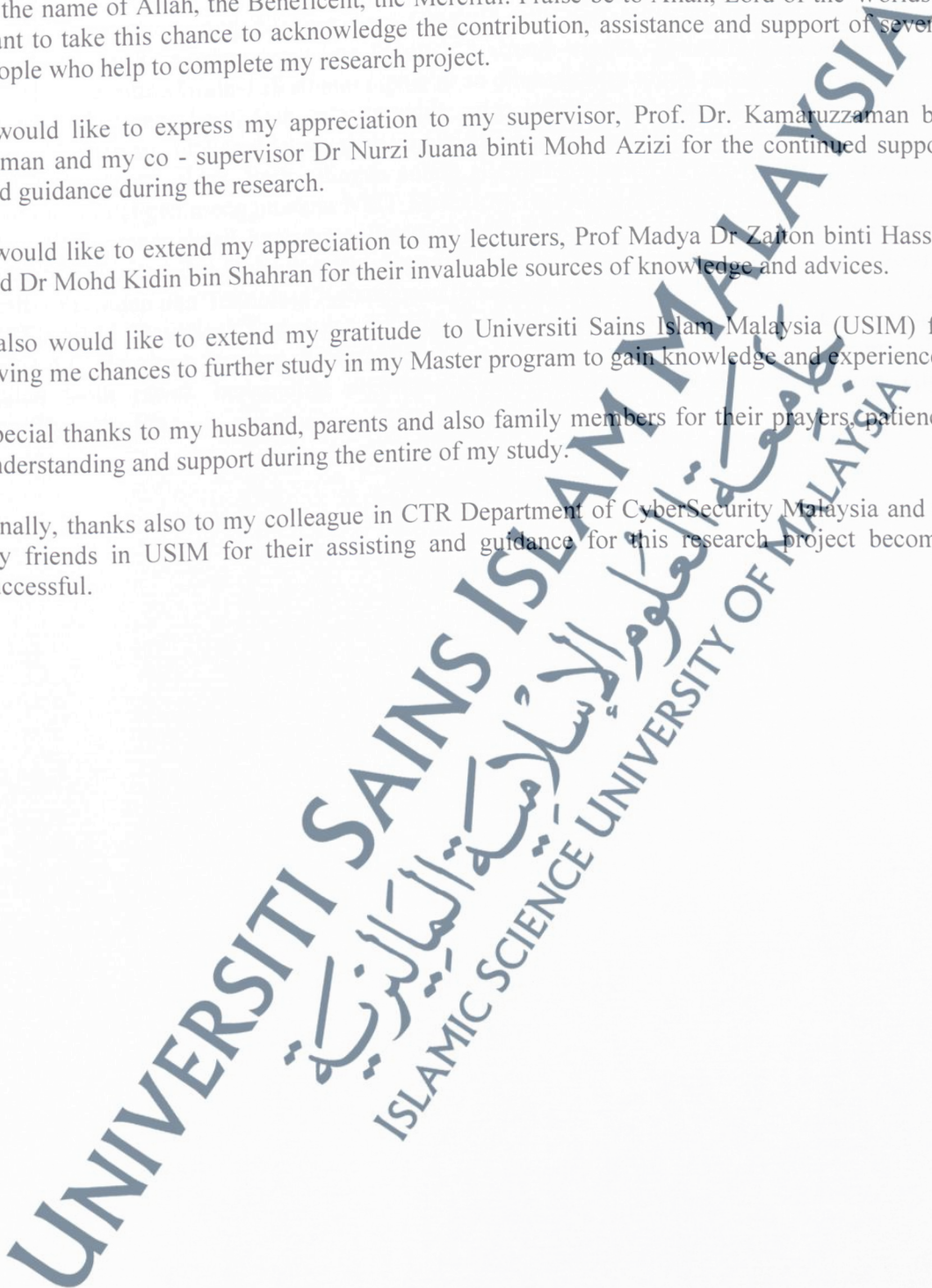
I would like to express my appreciation to my supervisor, Prof. Dr. Kamaruzzaman bin Seman and my co - supervisor Dr Nurzi Juana binti Mohd Azizi for the continued support and guidance during the research.

I would like to extend my appreciation to my lecturers, Prof Madya Dr Zaiton binti Hassan and Dr Mohd Kidin bin Shahrhan for their invaluable sources of knowledge and advices.

I also would like to extend my gratitude to Universiti Sains Islam Malaysia (USIM) for giving me chances to further study in my Master program to gain knowledge and experience.

Special thanks to my husband, parents and also family members for their prayers, patience, understanding and support during the entire of my study.

Finally, thanks also to my colleague in CTR Department of CyberSecurity Malaysia and all my friends in USIM for their assisting and guidance for this research project becomes successful.



ABSTRAK

Tesis ini membentangkan tentang algoritma stream cipher yang baru. Algoritma stream cipher yang baru ini merupakan satu usul yang berdasarkan kepada algoritma yang sedia ada iaitu algoritma Grain-128 stream cipher. Dalam mencapai tujuan pembentangan ini, terdapat tiga objektif utama yang dibentangkan. Objektif yang pertama bagi kajian ini ialah untuk mengenalpasti kerawakan algoritma Grain-128 stream cipher. Seterusnya, pengubahsuaian terhadap algoritma Grain-128 stream cipher akan dilaksanakan untuk menghasilkan algoritma stream cipher yang baru. Dan yang terakhir, ujian kerawakan terhadap algoritma Modified Grain-128 stream cipher dilaksanakan untuk menentukan samada algoritma yang baru ini adalah rawak atau tidak. Perbandingan antara algoritma Grain-128 dan Modified Grain-128 akan dinilai dengan menggunakan NIST Statistical Test Suite. NIST Statistical Test Suite ini telah dibangunkan hasil kerjasama diantara Bahagian Keselamatan Komputer (Computer Security Division) dan Bahagian Kejuruteraan Statistik (Statistical Engineering Division) di Institut Piawaian dan Teknologi Kebangsaan (Nasional Institute of Standard and Technology, NIST). NIST Statistical Test Suite ini dilaksanakan bagi menentukan kerawakan terhadap kedua-dua algoritma tersebut. Kesimpulannya, algoritma Modified Grain-128 stream cipher adalah lebih rawak berbanding algoritma Grain-128 stream cipher berdasarkan tahap signifikan 1%-5%.

UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

ABSTRACT

This thesis presents a new stream cipher algorithm. The new stream cipher algorithm have been proposed based on the existing Grain - 128 stream cipher algorithm. There are three main objectives in order to achieve this purpose. The first objective of this research is to identify the randomness of Grain – 128 stream cipher algorithm. Next, the modification of the algorithm will be conducted against Grain - 128 stream cipher algorithm. Finally, the randomness testing of Modified Grain – 128 of stream cipher algorithm is conducted to determine whether this algorithm is random or not random. The comparison of Grain - 128 and Modified Grain - 128 will be evaluated by using NIST Statistical Test Suite. The NIST Statistical Test Suite was developed by collaboration between the Computer Security Division and the Statistical Engineering Division at National Institute of Standard and Technology (NIST). The NIST Statistical Test Suite is conducted to determine the randomness of both algorithms. Conclusively, the Modified Grain - 128 is random based on 1% - 5% of significance level compared to the Grain - 128 which is not random at the same significance level.

UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

ملخص

تقدم هذه الرسالة الخوارزمية تيار الشفرات الجديدة. لقد تم اقتراح خوارزمية تيار الشفرات جديدة تقوم على الحبوب الموجودة - خوارزمية التشفير 128 تيار. هناك ثلاثة أهداف رئيسية لتحقيق هذا الغرض. الهدف الأول من هذا البحث هو التعرف على العشوائية من الحبوب 128-تيار خوارزمية تشفير. وبعد ذلك، سيتم إجراء تعديل خوارزمية ضد الحبوب 128-تيار خوارزمية تشفير. وأخيراً، فإن الاختبارات العشوائية من الحبوب المعدلة - وأجرى 128 من خوارزمية تيار والشفرات لتحديد ما إذا كان هذا الخوارزمية عشوائية أو غير عشوائي. وسيتم تقييم 128 باستخدام NIST الإحصائية اختبار جناح -المقارنة من الحبوب 128 - والتعديل الحبوب. وقد تم تطوير NIST الإحصائية اختبار جناح من التعاون بين شعبة الهندسة الإحصائية في المعهد الوطني للستاندرد والتكنولوجيا (NIST) شعبة أمن الحاسوب و. وأجرى NIST الإحصائية اختبار جناح لتحديد العشوائية في كل من الخوارزميات قاطع، والحبوب المعدلة 128 -هو عشوائي على أساس 5% - 1% من مستوى الأهمية بالمقارنة مع الحبوب 128 - وهي ليست عشوائية عند مستوى الدلالة نفسه.

UNIVERSITI SAINS ISLAM MALAYSIA
 جامعة العلوم الإسلامية الماليزية
 ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

CONTENTS

AUTHOR DECLARATION	i
BIODATA OF AUTHOR	ii
ACKNOWLEDGEMENTS	iii
ABSTRAK.....	iv
ABSTRACT	v
MULAKHKHAS	vi
CONTENTS.....	vii
LIST OF TABLES.....	ix
LIST OF FIGURES.....	xi
LIST OF ABBREVIATIONS.....	xii
CHAPTER I	
INTRODUCTION	1
BACKGROUND OF PROBLEM	3
PROBLEM STATEMENT	4
CONCEPTUAL FRAMEWORK.....	5
OBJECTIVE OF RESEARCH.....	5
SIGNIFICANCE OF STUDY.....	6
SCOPE OF STUDY.....	6
OUTLINE OF THESIS.....	7
CHAPTER II	
LITERATURE REVIEW.....	9
CRYPTOGRAPHY	9
STREAM CIPHER DESIGN	10
GRAIN – 128 STREAM CIPHER ALGORITHM	13
RANDOMNESS TESTING	17
NIST STATISTICAL TEST SUITE	21
CHAPTER III	
RESEARCH METHODOLOGY	50
RESEARCH DESIGN.....	50
POPULATION AND SAMPLE	53
RESEARCH TOOLS.....	54
EXPERIMENTAL SETUP.....	55
SUMMARY	66
CHAPTER IV	
RESULT AND DISCUSSION ON GRAIN – 128.....	67
EXPERIMENTAL SETUP FOR GRAIN – 128.....	67
RESULT AND ANALYSIS FOR GRAIN – 128	71

CONCLUSION	91
CHAPTER V	
RESULT AND DISCUSSION ON MODIFIED GRAIN – 128.....	95
MODIFICATION OF GRAIN – 128.....	95
EXPERIMENTAL SETUP FOR MG – 128.....	104
RESULT AND ANALYSIS FOR MG – 128.....	107
COMPARISON BETWEEN GRAIN – 128 AND MG – 128.....	112
CONCLUSION	121
CHAPTER VI	
CONCLUSION AND RECOMMENDATION	122
OVERVIEW	122
CONCLUSION	122
FUTURE WORK/RECOMMENDATION	123
BIBLIOGRAPHY	124
PUBLICATIONS	127

UNIVERSITI SAINS ISLAM MALAYSIA
 جامعة العلوم الإسلامية الماليزية
 ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

LIST OF TABLES

No.	Table	Page
1	Table 1 : Mathematical function used in NIST Statistical Test Suite	22
2	Table 2 : List of M values, minimum bit sequence and frequencies v_i	26
3	Table 3 : Values of M , K , N and π_i	26
4	Table 4 : Values of L , <i>expectedValue</i> and α	33
5	Table 5 : Compute partial sums	39
6	Table 6 : The Theoretical Probabilities	41
7	Table 7 : Number of p -values obtained per sample	60
8	Table 8 : Number of minimum bits of sequence required	63
9	Table 9 : Parameter value(s) required for Parameterized test selection	64
10	Table 10 : Parameter value(s) for Parameterized Tests Selection used for Grain - 128	68
11	Table 11 : Number of maximum rejection for keystream	69
12	Table 12 : Number of maximum rejection for output of LFSR (fx)	69
13	Table 13 : Number of maximum rejection for output of NLFSR (gx)	69
14	Table 14 : Number of maximum rejection for output of Boolean Function (hx)	70
15	Table 15 : Results for keystream at 1% significance level	71
16	Table 16 : Results for keystream at 2% significance level	72
17	Table 17 : Results for keystream at 3% significance level	73
18	Table 18 : Results for keystream at 4% significance level	74
19	Table 19 : Results for keystream at 5% significance level	75
20	Table 20 : Results for LFSR (fx) at 1% significance level	76
21	Table 21 : Results for LFSR (fx) at 2% significance level	77
22	Table 22 : Results for LFSR (fx) at 3% significance level	78
23	Table 23 : Results for LFSR (fx) at 4% significance level	79
24	Table 24 : Results for LFSR (fx) at 5% significance level	80
25	Table 25 : Results for NLFSR (gx) at 1% significance level	81
26	Table 26 : Results for NLFSR (gx) at 2% significance level	82
27	Table 27 : Results for NLFSR (gx) at 3% significance level	83
28	Table 28 : Results for NLFSR (gx) at 4% significance level	84
29	Table 29 : Results for NLFSR (gx) at 5% significance level	85
30	Table 30 : Results for Output of Boolean Function (hx) at 1% significance level	86
31	Table 31 : Results for Output of Boolean Function (hx) at 2% significance level	87
32	Table 32 : Results for Output of Boolean Function (hx) at 3% significance level	88
33	Table 33 : Results for Output of Boolean Function (hx) at 4% significance level	89
34	Table 34 : Results for Output of Boolean Function (hx) at 5% significance level	90
35	Table 35 : Number of rejected result for keystream	91
36	Table 36 : Number of rejected result for output of LFSR (fx)	92

37	Table 37 : Number of rejected result for output of NLFSR (gx)	93
38	Table 38 : Number of rejected result for output of Boolean Function (hx)	94
39	Table 39 : Parameter value(s) for Parameterized Tests Selection used for Modified Grain - 128	105
40	Table 40 : Number of maximum rejection for keystream	106
41	Table 41 : Results for keystream of MG-128 at 1% significance level	107
42	Table 42 : Results for keystream of MG-128 at 2% significance level	108
43	Table 43 : Results for keystream of MG-128 at 3% significance level	109
44	Table 44 : Results for keystream of MG-128 at 4% significance level	110
45	Table 45 : Results for keystream of MG-128 at 5% significance level	111
46	Table 46 : Comparison of NIST Statistical Results between Grain - 128 and Modified Grain - 128 for 1% of significance level.	116
47	Table 47 : Comparison of NIST Statistical Results between Grain - 128 and Modified Grain - 128 for 2% of significance level.	117
48	Table 48 : Comparison of NIST Statistical Results between Grain - 128 and Modified Grain - 128 for 3% of significance level.	118
49	Table 49 : Comparison of NIST Statistical Results between Grain - 128 and Modified Grain - 128 for 4% of significance level.	119
50	Table 50 : Comparison of NIST Statistical Results between Grain - 128 and Modified Grain - 128 for 5% of significance level.	120

37	Table 37 : Number of rejected result for output of NLFSR (gx)	93
38	Table 38 : Number of rejected result for output of Boolean Function (hx)	94
39	Table 39 : Parameter value(s) for Parameterized Tests Selection used for Modified Grain - 128	105
40	Table 40 : Number of maximum rejection for keystream	106
41	Table 41 : Results for keystream of MG-128 at 1% significance level	107
42	Table 42 : Results for keystream of MG-128 at 2% significance level	108
43	Table 43 : Results for keystream of MG-128 at 3% significance level	109
44	Table 44 : Results for keystream of MG-128 at 4% significance level	110
45	Table 45 : Results for keystream of MG-128 at 5% significance level	111
46	Table 46 : Comparison of NIST Statistical Results between Grain - 128 and Modified Grain - 128 for 1% of significance level.	116
47	Table 47 : Comparison of NIST Statistical Results between Grain - 128 and Modified Grain - 128 for 2% of significance level.	117
48	Table 48 : Comparison of NIST Statistical Results between Grain - 128 and Modified Grain - 128 for 3% of significance level.	118
49	Table 49 : Comparison of NIST Statistical Results between Grain - 128 and Modified Grain - 128 for 4% of significance level.	119
50	Table 50 : Comparison of NIST Statistical Results between Grain - 128 and Modified Grain - 128 for 5% of significance level.	120

LIST OF FIGURES

No.	Figure	Page
1	Figure 1 : The conceptual framework	5
2	Figure 2 : Stream cipher process	11
3	Figure 3 : The key initialization process	13
4	Figure 4 : The keystream generation process	14
5	Figure 5 : Representation 1 of NIST Statistical Test Suite	44
6	Figure 6 : Representation 2 of NIST Statistical Test Suite	45
7	Figure 7 : Representation 3 of NIST Statistical Test Suite	46
8	Figure 8 : Representation 4 of NIST Statistical Test Suite	47
9	Figure 9 : Representation 5 of NIST Statistical Test Suite	48
5	Figure 10 : Workflow of research design	52
6	Figure 11 : Generating the data for Grain - 128	57
7	Figure 12 : Generating the data for Modified Grain - 128	58
8	Figure 13 : The process of conducting the statistical test	61
9	Figure 14 : Key initialization process of MG-128	98
10	Figure 15 : Keystream generation process of MG-128	99
11	Figure 16 : The process of constructing LFSRs	100
12	Figure 17 : The process of constructing NLFSR	101

LIST OF ABBREVIATIONS

NIST	-	National Institute of Standards and Technology
IV	-	Initial Value
LFSR	-	Linear Feedback Shift Register
NLFSR	-	Non-Linear Feedback Shift Register
MG-128	-	Modified Grain-128
DSA	-	Digital Signature Algorithm
AES	-	Advanced Encryption Standard
DES	-	Data Encryption Standard
IDEA	-	International Data Encryption Algorithm
RC4	-	Rivest Cipher 4
FISH	-	Fibonacci Shrinkage
XOR	-	Exclusive-or
SPRNG	-	Scalable Parallel Pseudorandom Number Generator
GUI	-	Graphical User Interface
DFT	-	Discrete Fourier Transform