
UNIVERSITI PUTRA MALAYSIA

# NONLINEARITY ANALYSES AND ADAPTATION OF NONLINEARITY TRAITS OF KEY GENERATION PROTOCOL OF EL-GAMAL AA_ CRYPTOSYSTEM

MIZA MUMTAZ AHMAD

IPM 2011 16

# NONLINEARITY ANALYSES AND ADAPTATION OF NONLINEARITY TRAITS OF KEY GENERATION PROTOCOL OF EL-GAMAL $AA_\beta$ CRYPTOSYSTEM

By

MIZA MUMTAZ AHMAD



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

May 2011

# DEDICATION

To

My Beloved Parents

En. Ahmad Yahaya and Azizah Dahari

for their unconditional love

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

# NONLINEARITY ANALYSES AND ADAPTATION OF NONLINEARITY TRAITS OF KEY GENERATION PROTOCOL OF EL-GAMAL $AA_\beta$ CRYPTOSYSTEM

By

**MIZA MUMTAZ AHMAD**

**May 2011**

**Chair: Assoc. Prof. Mohamad Rushdan Md. Said, PhD**

**Faculty: Institute for Mathematical Research**

This thesis documents nonlinearity analyses performed on the key generation protocol of El-Gamal $AA_\beta$ Cryptosystem. The main aim of this research is to improve the security of the cryptosystem with regards to its key generation protocol against linear cryptanalysis, and this is achieved through series of tests and evaluations of the strength of the protocol in terms of nonlinearity measurement and bijectivity evaluation. Basically, the work is done in two phases.

In the first phase, the bijectivity of $AA_\beta$ function in the cryptosystem is evaluated. The process consisted of investigating the function in the protocol and inspecting bit distribution in the public key to determine whether it is balanced or not. In the second phase, a statistical approach based on the original work of Matsui (1993) is extended to perceive any possible linear relation between public key and ephemeral private key. There have been three major evolutional phases of the key generation protocol and the tests are done onto each of it.

Though theoretically the key generation protocol is nonbijective, it still satisfies the bijectivity criterion. Also, the nonlinearity measurement of the key generation protocol is very high making it almost impossible to extend linear cryptanalysis onto it, especially for higher bit input size. Thus for 128-bit

ephemeral key, it is conjectured that the success probability to guess the correct ephemeral private key using linear cryptanalysis is close to nil. However, it is easier to attack the key generation protocol using less complicated attack such as dictionary attack because only a single round of function is involved in it.

Based on the findings, we propose two methods to improve the security of ElGamal $AA_{\beta}$ cryptosystem against linear cryptanalysis. Since the nonlinearity level of the key generation protocol is phenomenal, the function in the protocol should be iterated at least twice to amplify its security. This is done not only to reduce the chance of guessing the correct ephemeral private key via linear cryptanalysis, but also to increase cryptanalysis work of dictionary attack. The second method is to multiply the generator point with a large number to increase the linear cryptanalysis work as well as obtain a better bit distribution in the public key.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

# ANALISIS-ANALISIS HUBUNGAN TAK LINEAR DAN ADAPTASI DARI SIFAT-SIFAT TAK LINEAR DALAM PROTOKOL PENGHASILAN KUNCI BAGI SISTEM KRIPTOGRAFI $AA_\beta$ EL-GAMAL


Oleh

**MIZA MUMTAZ AHMAD**


**Mei 2011**


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

**Fakulti: Institut Penyelidikan Matematik**



Tesis ini mendokumentasikan analisis-analisis hubungan tak linear ke atas protokol penghasilan kunci bagi sistem kriptografi $AA_\beta$ El-Gamal. Matlamat utama penyelidikan ini adalah demi meningkatkan keselamatan sistem kriptografi ini dari segi protokol penghasilan kuncinya terhadap kriptanalisis linear, dan semua ini dicapai melalui siri-siri ujian dan penilaian ke atas kekuatan protokol ini dari aspek ukuran tak linear dan penilaian bijektif. Pada dasarnya, kaedah kajian dijalankan dalam dua fasa.

Dalam fasa pertama, status bijektif fungsi $AA_\beta$ dalam sistem kriptografi dinilai. Proses ini merangkumi siasatan ke atas fungsi tersebut dan pemeriksaan taburan bit dalam kunci awam bagi menentukan sama ada ianya seimbang atau tidak. Dalam fasa kedua, pendekatan statistik berdasarkan hasil kerja asli Matsui (1993) dilanjutkan bagi memeriksa sebarang kemungkinan adanya perkaitan linear di antara kunci awam dan kunci rahsia singkat. Protokol penghasilan kunci ini melalui tiga fasa evolusi dan ujian-ujian ini dilakukan ke atas setiap daripada fasa-fasa tersebut.

Walaupun secara teorinya, protokol penghasilan kunci kita adalah tidak bijektif, ia masih memenuhi ciri-ciri kebijektifan. Malahan, tahap tak linear protokol ini sangat tinggi menjadikannya hampir mustahil untuk ditembusi oleh kriptanalisis linear, terutamanya bagi saiz bit kemasukan yang tinggi. Justeru, bagi kunci peribadi singkat bersaiz 128-bit, disimpulkan bahawa kebarangkalian untuk menduga kunci peribadi singkat yang betul adalah hampir sifar. Namun,

adalah lebih mudah untuk menyerang protokol penghasilan kunci ini menggunakan kaedah yang kurang rumit seperti serangan kamus memandangkan hanya satu pusingan fungsi terlibat di dalamnya.

Berdasarkan penemuan-penemuan ini, kami mencadangkan dua kaedah bagi meningkatkan keselamatan sistem kriptografi $AA_\beta$ El-Gamal terhadap kriptanalisis linear. Memandangkan tahap tak linear protokol penghasilan kunci adalah sangat mengagumkan, fungsi yang digunakan dalam protokol haruslah diulang sekurang-kurangnya dua kali bagi menguatkan keselamatannya. Ini dilakukan bukan sahaja demi mengurangkan kebarangkalian meneka kunci rahsia singkat melalui kriptanalisis linear, tetapi juga bagi menambah kerja kriptanalisis serangan kamus. Kaedah kedua adalah dengan mendarab generator dengan nilai yang besar bertujuan untuk meningkatkan kerja kriptanalisis linear disamping mencapai taburan bit yang lebih baik dalam kunci awam.

## ACKNOWLEDGEMENTS

*Assalamu'alaykum wa rahmatullahi wa barakatuh*,

Verily, all praises and thanks are due to ALLAH SWT. He is the Bestower and the Provider for all of His creations in the heavens and the earth. In attaining my Master degree in Universiti Putra Malaysia, there are people whom I owe my thanks too.

First and foremost, I would like to thank my parents for being extremely supportive and patient with me. They have been helping and sissting me in whichever way they can to make sure that my work go smooth and uninterrupted. Also, thanks to Mr. Thanveer Hamza who have been assisting me without fail in proofreading some of my writings.

I am greatly grateful to my supervising committees especially my Chief Supervisor, Assoc. Prof. Dr. Mohamad Rushdan Md. Said for his kindness, invaluable advices, guidance and assistance. Many thanks also to Dr. Muhammad Rezal Kamel Ariffin for giving me the opportunity to work under his project in which this whole thesis is based on. Special thanks to Assoc. Prof. Ramlan Mahmoud for helping me kick start my Master studies at Universiti Putra Malaysia and also for constantly guiding me from the very first step of the research till the last. Last and definitely not least, my thanks goes to Prof. Mohamed Othman who kept on pushing me to do my best in research and help me think out of the box.

Also, I would like to show my gratitude to my sponsors, employer, teachers, family and friends who have helped me pursue my Master degree in UPM. Jazakumullahu khayran kathiran!

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of **Master of Science**.

Members of the Supervisory Committee were as follows:

**Mohamad Rushdan Md. Said, PhD**
Associate Professor
Faculty of Science
University Putra Malaysia
(Chairman)

**Mohamed Othman, PhD**
Professor
Faculty of Computer Science and Information Technology
University Putra Malaysia
(Member)

**Ramlan Mahmod, PhD**
Associate Professor
Faculty of Computer Science and Information Technology
University Putra Malaysia
(Member)

**Muhammad Rezal Kamel Ariffin, PhD**
Senior Lecturer
Faculty of Science
University Putra Malaysia
(Member)

**HASANAH MOHD GHAZALI, PhD**
Professor and Dean
School of Graduate Studies
University Putra Malaysia
Date:

## DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at University Putra Malaysia or at any other institution.

**MIZA MUMTAZ AHMAD**
Date: 3 May 2011

TABLE OF CONTENTS