PRACTICAL APPROACH IN EVALUATING THE RESISTANCE OF STREAM CIPHERS AGAINST ALGEBRAIC ATTACKS

MOHD FAIDZAL JANTAN

UNIVERSITI TEKNOLOGI MALAYSIA

PRACTICAL APPROACH IN EVALUATING THE RESISTANCE OF STREAM CIPHERS AGAINST ALGEBRAIC ATTACKS

MOHD FAIDZAL JANTAN

A project report submitted in partial fulfillment of the requirements
for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information System
UNIVERSITI TEKNOLOGI MALAYSIA

APRIL 2010

ACKNOWLEDGEMENT

Firstly, I would like to express my highly appreciation to Dr. Rabiah Ahmad as my supervisor and for giving me this opportunity to complete this project. While going through out this thesis, I received great encouragements, guidance and advices from her and not forgotten also my friends like Tan, Hafiz, Hamidi, Wan Said, Zaim and others for their 'never fear' spirit. I also would like to give specials thanks to my family for being great supporter and their passions and all blessing really enriched me with great energy to pursuing throughout the years of study.

To my wife

Anisah Ekhlas

and my kids

Akmal Fanshuri

Adlan Fatihin

Alysa Fadhlin

ABSTRACT

Stream ciphers are the oldest technique in cryptography subject and still applicable in the modern era as it provides better speed and accuracy during encryption decryption process. It is also easy to be abuse and breakable if the algorithm is not designed properly because its key generator was constructed based on Boolean function which normally using Line Feedback Shift Register technique. Together with secret key, it will generate key stream bit that will be used to encrypt the plaintext into cipher text. Far from that, Algebraic Attacks and Fast Algebraic Attack has become popular among cryptographers as the nature of the attack was to recover the secret key by solving or decomposing the Boolean function that constructed the cryptosystems. This study mainly is to provide a practical way or approach on how to evaluate the resistance of stream ciphers against these two types of attack. As all of us know that cryptography always involve complex discrete arithmetic by nature. As a result, we as non-mathematician computer scientist or information systems practitioner practically leave any cryptographic problems to the mathematician to evaluate and observe the cryptosystems they want to implement. Hence, this case study has also presented some practical method on how to construct an evaluation capability from mathematical formulas designed by mathematician cryptographers. The prototype solution was built using Microsoft Visual Studio VB.Net 2008 and the simulation testing was successfully done and shows similar result when we compare with cryptanalysis report produced by cryptographers.

ABSTRAK

'Stream ciphers' adalah salah satu teknik purba kriptografi yang prinsipnya masih digunapakai dalam teknologi masakini kerana ia menunjukkan prestasi yang lebih baik dalam aspek kelajuan pemprosesan serta mempunyai kadar ketepatan tinggi dalam proses enkripsi dan dekripsi data. Ia juga mudah disalahguna dan digodam jika tidak dirangka dengan baik kerana penjana kunci yang dimajukan selalunya menggunakan teknik 'Line Feedback Shift Register' dengan asas fungsi Boolean. Bersama dengan kunci rahsia ia menghasilkan suatu siri kunci secara rawak yang akan digunakan untuk membentuk kriptogram dari data asal. Dalam pada itu, dengan kepantasan pembangunan teknologi, teknik 'Serangan Algebra (Pantas)' menjadi popular kerana lazimnya serangan sedemikian, ia menggunakan kaedah penyelesaian masalah persamaan fungsi Boolean di mana secara tidak langsung ia mendedahkan kunci rahsia sesuatu kriptosistem. Dengan itu, kertas kajian ini bertujuan mencadangkan suatu kaedah praktikal dalam menilai tahap dayatahan 'Serangan Algebra (Pantas)' kriptosistem tersebut. Tambahan pula, kebanyakan saintis komputer atau pengamal Sistem Maklumat bukanlah terdiri dari ahli matematik. Lantaran itu, kajian ini menunjukkan cara mudah untuk membina fungsi penilaian berdasarkan formula matematik yang dibentuk oleh pakar matematik kriptografi. Fungsi-fungsi tersebut telah dimajukan dengan Microsoft Visual Studio VB.Net 2008 dan simulasi yang dilaksanakan mendapati bahwa model-model fungsi tersebut boleh diketengahkan setelah kami membandingkan hasil tersebut dengan laporan analisa kriptografi oleh para ahli matematik kriptografi.

TABLE OF CONTENT

LIST OF TABLE

LIST OF FIGURE

LIST OF APPENDIX

LIST OF ABBREVIATIONS

AI	-	Algebraic Immunity
AA	-	Algebraic Attack
FAA	-	Fast Algebraic Attack
IS	-	Information Systems
LSFR	-	Line Feedback Shift Register
OTP	-	One Time Pad
VB	-	Visual Basic

CHAPTER I

INTRODUCTION

1.1 Background

Algebraic attacks on stream cipher are one of the popular cryptanalysis techniques in evaluating the resistances of stream ciphers. It was proposed by T. Courtois in 2002 and improved with the new algorithm proposed in 2003, enhancement from Algebraic Attacks, which named as Fast Algebraic Attacks. This research will focus on the practical way of assessing the resistance by creating application environment instead of evaluating it through mathematical approach. From this perspective, hopefully the approach would give more understanding of the attacks and how to portray it within the application environment and could benefits non-mathematician computer scientist.

In this Chapter I, basically is describing the project objectives that strategically answering the problem statement. This chapter also, the boundary of research and development is defined so that the project scope will give objectively significant value and guidance throughout the project.

Chapter II narrates some literature review regarding on subject matter that we are focusing on. It covering topic that explaining the principles, characteristic value and the nature underlies stream ciphers subject and the algebraic attack.

Chapter III presents the methodology of the projects. This is vital as we need to lay some guidelines when executing this project. Without it, our focus might be lost and produce unexpected result that far from the project aims and objectives.

Chapter IV describing mainly on the design of component that made the evaluation tools. For the thesis, some mathematical theorems and theoretical framework is selected in drawing the logical structure of the tool. This chapter also has selected a benchmark result to be used as a guide in reaching the target results.

Chapter V narrates the development of the tool. In this we can see how to extract related mathematical formulations was translated in computer language. We also describing in general about Microsoft Visual Studio VB.Net 2008, the selected programming language for the development.

Chapter VI presents the simulation test of the completed tool that we had developed. We also discuss on the results yielded from the test execution and illustrate level of accuracy and reliability of the tool.

Chapter VII concludes the findings and list down suggestions for future enhancement to the tool.

1.2 Problem Statement

Most of the research in cryptanalysis usually use mathematical approach when evaluating the resistance of the stream ciphers against the algebraic attacks but rarely done in application software as alternative tool.

1.3 Project Objectives

- To explore an appropriate practical approach in observing the algebraic attacks against stream ciphers.
- To develop a tool that would provide a practical way in evaluating the resistance of stream ciphers against the algebraic attack and gain more understanding how the algebraic attack works on stream ciphers.
- To test the tool on at least two stream ciphers in measuring the resistance of stream ciphers against the algebraic attacks in order to ensure it is viable for non-mathematician information system practitioner usage.

1.4 Project Aim

The project aim is to provide a tool for non-mathematician Information Systems practitioner to understand the cryptosystems and the nature of the algebraic attacks in a practical way.

1.5 Project Scope

The research coverage is bounded on Algebraic Attacks against selected stream ciphers algorithm. Application programs will be built based on theoretical research paper describing all necessary algorithm and sample code given which opened to the public by the original author of the algorithm.

In order to achieve the objectives of the research, development tools chosen is Microsoft Visual Studio VB.Net 2008 that runs on Windows platform.

1.6 Significant of the Project

It expected that this project would provide a tool that will facilitate the information systems practitioner to obtain more understanding on the cryptosystems and the algebraic attack in practical approach. From the tool also, the practitioner would aware on how to build a secured application by implementing a suitable cryptosystems in their application software.