UNIVERSITI PUTRA MALAYSIA

ANNIHILATORS THROUGH FAULT INJECTION ANALYSIS ON SELECTED STREAM CIPHERS

Wan Zariman Omar @ Othman

IPM 2019 24

ANNIHILATORS THROUGH FAULT INJECTION ANALYSIS ON SELECTED STREAM CIPHERS

By

WAN ZARIMAN OMAR @ OTHMAN

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

March 2019

COPYRIGHT

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

ANNIHILATORS THROUGH FAULT INJECTION ANALYSIS ON SELECTED STREAM CIPHERS

By

WAN ZARIMAN OMAR @ OTHMAN

March 2019

Supervisor : Muhammad Rezal bin Dato' Kamel Ariffin, PhD
Faculty : Institute for Mathematical Research

Algebraic attacks on stream cipher are important in cryptanalysis to both designers and attackers. Generally, complexity of an algebraic attack will increase as the degree of an equation increases. In conducting this attack, we aim to decrease the degree of the targeted boolean equation by constructing low degree annihilator equation(s). We adopt the Fault Injection Analysis (FIA) methodology to achieve our objectives. In this study, we found annihilator(s) through FIA (inject with value of one (1)) on boolean function of selected stream ciphers. With these injected boolean functions, we proceed to utilize Hao's method to find new annihilator(s). Then we obtained new annihilator(s) on boolean function of Pomaranch, Grain v0 and also LILI-128 stream ciphers. As a result, these newly identified annihilators successfully reduce the complexity of the published boolean function to guess the initial secret key. It also provides much needed information on the security of these selected stream ciphers with respect to FIA.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

PEMUSNAH MELALUI ANALISIS SUNTIKAN KESILAPAN PADA SIFER ALIR TERPILIH

Oleh

WAN ZARIMAN OMAR @ OTHMAN

Mac 2019

Pengerusi : Muhammad Rezal bin Dato' Kamel Ariffin, PhD
Fakulti : Institut Penyelidikan Matematik

Serangan algebra pada sifer alir sangat penting dalam analisis kriptografi kepada pembangun algorithma dan juga pemecah kod kriptografi. Secara umumnya, kerumitan serangan algebra akan meningkat dengan tahap persamaan yang berdarjah tinggi. Bagi melakukan serangan ini, kita berhasrat untuk mengurangkan darjah persamaan yang dipilih dengan membina persamaan pemusnah berdarjah rendah. Analisa suntikan kerosakan (FIA) adalah serangan yang boleh dilaksanakan bagi mencapai objektif ini. Dalam kajian ini, kami mencari panghapus melalui FIA (dengan suntikan nilai satu (1)) ke atas fungsi boolean bagi sifer alir yang dipilih. Dengan fungsi boolean yang disuntik ini, kami akan menggunakan kaedah Hao untuk mencari persamaan pemusnah yang baharu. Kami memperolehi beberapa persamaan pemusnah yang baharu pada fungsi boolean bagi sifer alir Pomaranch, Grain v0 dan LILI-128 dan kesemua persamaan pemusnah yang diperolehi berjaya mengurangkan kerumitan fungsi boolean yang asal untuk meneka kunci rahsia awal. Output ini juga memberikan maklumat mengenai keselamatan sifer alir yang dipilih berdasarkan analisa FIA.

ACKNOWLEDGEMENTS

Bismilahir-Rahmanir-Rahim

To ALLAH s.w.t. the creator of all creations, all praise be to Him who is eternal and exists without place, the Most Beneficent and the Most Merciful, the Lord of the worlds.

High gratitude and respect to my supervisor **Associate Professor Dr Muhammad Rezal bin Dato' Kamel Ariffin** for his never ending guidance and patience pushes me forward throughout this journey. Sincere appreciation goes to my co-supervisor Associate Professor Dr Mohamad Rushdan Md Said for giving me spiritual motivation in completing this thesis.

As to my lovely wife, **Wan Maisarah Md Isa**, my pretty daughters **Wan Hannah Zahra**, **Wan Hawwa Zareen**, my handsome son **Wan Haadi Zafir** and my new born princess, **Wan Hajar Zafreen** thank you for your never ending love and understanding of my lifelong passion - Information Security especially in cryptography.

Nothing can replicate the care and support from my mother **Shahriah Ismail** and mother in law **Sharifah Norain Syed Hashim** as they are my inspiration to make this life better everyday.

Kind regards to my friends who row in the same ship of cryptography; my superior and also my co-supervisor Ts. Dr Solahuddin Shamsuddin, Ts. Dr Maslina Daud, Miss Hazlin Abdul Rani, Suhairi Mohd Jawi, all staff of Cryptography Development Department of CyberSecurity Malaysia , Zahari Mahad, Amir Hamzah, Dr Muhammad Asyraf, all Al-Kindi Lab's members of Universiti Putra Malaysia and many other whose names shall never be forgotten because without their contributions and teachings, this thesis will never be completed.

See you all again in the next adventure!

I certify that a Thesis Examination Committee has met on 21 March 2019 to conduct the final examination of Wan Zariman Omar @ Othman on his thesis entitled "Annihilators Through Fault Injection Analysis on Selected Stream 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:

Azmi bin Jaafar, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairperson)

Zuriati binti Ahmad Zulkarnain, PhD
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Shekh Faisal bin Abdul Latip, PhD
Senior Lecturer
Falcuty of Information Technology and Communication
Universiti Teknikal Malaysia
(External Examiner)

ROBIAH YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 4 September 2019

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. The members of the Supervisory Committee were as follows:

Muhammad Rezal bin Dato' Kamel Ariffin, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Chairman)

Mohamad Rushdan bin Md. Said, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Member)

Solahuddin bin Shamsuddin, PhD
Chief Technology Officer
CyberSecurity Malaysia
Malaysia
(Member)

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

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: Wan Zariman Omar @ Othman, GS31689

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
Assoc. Prof. Dr. Muhammad Rezal bin Dato' Kamel Ariffin

Signature: _____
Name of Member of Supervisory Committee
Assoc. Prof. Dr. Mohamad bin Rushdan Md. Said

Signature: _____
Name of Member of Supervisory Committee
Dr. Solahuddin bin Shamsuddin

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AI	Algebraic Immunity
AES	Advance Encryption Standard
ANF	Algebraic Normal Form
CNF	Conjunctive Normal Form
DNF	Disjunctive Normal Form
GD	Guess and Determine
GF	Galois Field
JC	Jump Control
LFSR	Linear Feedback Shift Register
LC	Linear Complexity
LCM	Linear compacting modules
NIST	National Institute of Standards and Technology (USA)
NLFSR	Non-Linear Feedback Shift Register
NSA	National Security Agency (NSA)
PKI	Public Key Infrastructure
S-Box	Substitution Box
TMTO	Time-Memory Trade-off
v0	Version 0

CHAPTER 1

INTRODUCTION

1.1 Cryptography

Cryptology is a science that incorporate both cryptography and cryptanalysis (Katz et al., 1996). Cryptography originated from the Greek words *kripto* and *graphia* which means ”hidden” and ”writing”. This science of securing messages began since early civilization when human started to communicate and the need to hide their communication. The fundamental and classical task of this science is to provide confidentiality by encryption methods (Delfs and Knebl, 2015), where both the encryption and decryption process used a secret key that was initially agreed by both parties. The importance of encryption became critical after telegraph, especially radio telegraph, was invented. Long distance communication allows information being intercepted much easier than ever. To protect the confidentiality of information, encryption is widely used in military, intelligence and diplomatic services. The consequence is that cryptanalysis techniques improved significantly. During World War II, both the German Enigma cipher and the Japanese Purple cipher were successfully broken by the Allies. The two weak ciphers contributed significantly to the failure of Germany and Japan in World War II.

Cryptography is a long-established way to keep information secret. Julius Caesar used a type of cipher known as Caesar cipher in the Gallic wars and this is an example of a mono alphabetic cipher. As time evolved, more sophisticated ciphers were designed such as poly alphabetic ciphers. Examples are the Vigenere and Porta Ciphers. Both the mono alphabetic and poly alphabetic ciphers are based on alphabets. Such systems are no longer in use and were proven to be weak. These ciphers can be broken based on the analysis of the statistics of the cryptogram. Now that majority of information systems transport data from place to place (as well as processing and storing it), the place of cryptography in the data security is assured. It is the beginning of cryptography to be accepted as the basic tool for achieving data security.

Very few people in the modern society live a day without using some electronic communication network such as the banking system (automatic teller machines, electronic funds transfer), the telephone system, electronic mail, the World Wide web, or cable television. The distinction between all these systems is becoming blurred with time, and it is not unusual to be able to access a service from any one of these sources. The widespread use of smart cards and digital cash needs privacy and integrity of information to be maintained for the success of these global systems. The broad subject dealing with these security issues is called cryptology. The subject of cryptology is the study of security and can be further subdivided into two main

branches. Cryptography is the design and provision of security systems that is designing an encryption and decryption algorithm and cryptanalysis is the analysis and breaking of such systems.

With the introduction of the computer and electronic communication system, modern cipher systems are needed to be more efficient to keep certain messages that have to be kept secret. To achieve this, the communicants must take steps to conceal and protect the content of the messages and the amount of protection required will vary. Occasionally, it is sufficient to prevent a listener from understanding the message. However, there are certain times when it is crucial that even the most determined interceptor must not deduce it. Upon realizing this, there are so many types of encryption algorithms existed today and being used by most of the government, military, financial institutions and large companies.

In recent years, blackmail, fraud and the stealing of commercial secrets are examples of crimes using information as the medium. There was a time, not many years ago, when it was necessary to alter the accounts books in order to cover up a fraud; now the same effect can be produced at a computer terminal in the communication network. The widespread introduction of information technology into business inevitably leads to its misuse for crime, which data security aims to prevent.

Essentially, security means controlling access to data, depriving the blackmailer of his information, protecting commercial secrets and preventing the falsifying of records. The need to control access in the computer network first became serious when time-sharing began to operate. In 1983, the film War Games, and the publicity it created, introduced people to a new and surprising cult, the computer hackers, who spend their time obsessively trying to break into computer systems or network. Their devotion to a basically tedious pastime is extraordinary, and it shows up one advantage of an amateur attacker over the professional defenders. The attackers time is apparently unlimited and uncosted; the defenders time is expensive. The systems that hackers have broken into were protected only by weak password schemes, but the hackers success and excitement it generated prepares the way for more advanced attacks when simple hacking fails to satisfy them. A special feature of illegal attacks on the computer network is that there is no tradition of associated guilt-feelings. The law in most country has not begun to define the new kinds of crime. With no likelihood of punishment, the probing of defenses of computer network is considered to be a game. It could become the tool of organized crime. Singh (1999) Callahan (2013).

To this end, the security goals in modern cryptography can be divided into four categories:

1. **Authentication**: The process of verifying the identity of the sender/user. A

computer login authenticates a user by requesting a password. The user proves his identity by showing that he knows a secret. In a challenge-response scheme the verifier sends a challenge, e.g., a random number A, to the prover. The prover calculates a new number B = f(A, K) where K is some shared secret, and then return B to the verifier. Since the verifier knows K, he can also find B and if the returned number is correct, the prover has proved his identity. In a zero-knowledge proof, the goal is to allow the prover to prove that he knows a secret by not revealing the secret to the verifier. Authentication is closely related to authorization. Authorizing a user means to verify that an authenticated user has access to information. Thus, authentication must be performed before authorization.

2. **Confidentiality**: Ensuring that only the intended recipient (an authorized user) is able to read the message. This is achieved by encrypting the data using a cipher. Examples of classical ciphers are Caesar cipher and the Scytale.

3. **Integrity**: Assuring the receiver of a message that it has not been altered. Data sent on a computer network, passing through several hosts, can be maliciously altered on one host before sent to the next. Ensuring message integrity can be done using a Message Authentication Code (MAC), which computes a key dependent check sum of the message.

4. **Non-repudiation**: The goal here is to prove that the sender really sent the data. As an example, after signing a contract, the signer should not be able to deny that he signed it. Non-repudiation can be provided using digital signatures.

Cryptography is divided into two types, which is, asymmetric-key cryptography and symmetric-key cryptography. In symmetric-key cryptography, only one key will be used to encrypt and decrypt the data. Meanwhile for asymmetric-key cryptography, there will be two different keys to encrypt and decrypt.

1.2 Asymmetric Cryptography

Asymmetric cryptography is also known as public key cryptography, it uses a pair of key known as public and private keys to encrypt and decrypt data. The keys are a numbers that have been paired together but are not identical.

1. Public key: One key in the pair that can be shared with everyone.

2. Private key: The other key in the pair that is kept secret.

1.3 Symmetric Cryptography

Today more and more people are connected to the internet with huge amount of confidential information (emails, online transactions) being transmitted every day.

Cryptography starts to play an important role in daily life. Modern cryptography is developed to protect information confidentiality, integrity and provide authentication. In modern cryptography, symmetric key cipher is essential in protecting information confidentiality. With a public key infrastructure (PKI) that can support key establishment protocol, two parties can share a secret key and carry out symmetric key encryption in a convenient way.

Symmetric key encryption is important for secret information transmission and storage. Two parties, the sender and receiver, share the same symmetric key cipher and the same secret key. The sender encrypts the message (plaintext) with the cipher and key to obtain the ciphertext. The ciphertext is transmitted (or stored) over an insecure channel. The receiver decrypts the ciphertext to retrieve the original message. An attacker may intercept the ciphertext. Strong cipher and strong key should be used for encryption o ensure that no information is leaked to the attacker. Basically, this symmetric cryptosystem can be divided into two; block and stream cipher. Rueppel describe the differences as (Simmons, 1992) the follows:

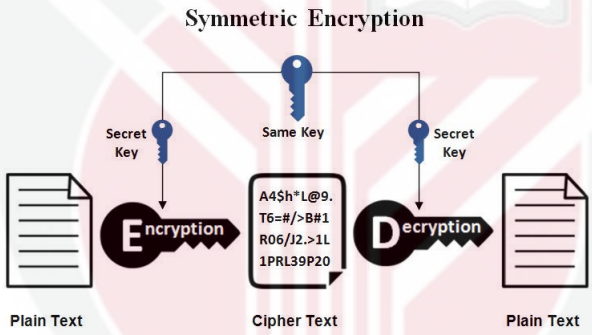

Figure 1.1: Example of Symmetric-key Cryptography

1. Block cipher: Operate with a fixed transformation on large block of plaintext data.
2. Stream cipher: Operate with a time-varying transformation on individual plaintext digits.

However, this explanation is not overall because any block cipher can be used as a stream cipher by using certain modes of operation. As we know there are three following modes of operation for block cipher (international standard ISO/IEC) such as:

1. Cipher feedback mode The cipher feedback mode (CFB) turns a block cipher into a self-synchronizing stream cipher. The combining function is XOR, and the next block of keystream is determined by encrypting the last block of

ciphertext.

$C_i = P_i \oplus E_k(C_{i-1})$
$C_{-1} = IV$

2. Output feedback mode The *output feedback mode* (OFB) is structurally similar to the CFB mode, but as the resulting stream cipher is synchronous instead of self-synchronizing, the resulting cipher is vastly different. Instead of encrypting the last block of ciphertext, the last block of keystream is encrypted.

$C_i = P_i \oplus Z_i$
$Z_i = E_k(Z_{i-1})$
$Z{-}1 = IV$

3. Counter mode The *Counter Mode* (CTR) is newer than the other modes. The keystream is obtained by encrypting a block consisting of the IV concatenated with a counter. The counter can be any function $f(i)$ that does not repeat for a long time. The simplest and most popular choice is an actual counter $f(i) = i$. CTR mode allows a random access property for decryption.

$C_i = P_i \oplus E_k(B_i)$
$B_i = IV||f(i)$

1.3.1 Block Cipher

As already mentioned in the previous section 1.1, block ciphers belong to the class of symmetric encryption algorithms that aim to provide data confidentiality by sharing a secret between communication parties and transforming plaintexts to ciphertexts using this secret in a way that the adversary (possessing no knowledge of the secret) is not able to obtain the plaintext.

Cryptologists alert and recognized that secrecy is very important during communication. Already in 1949, Shannon [238] defined perfect secrecy based on the stochastic notion of mutual information. A cipher provides perfect secrecy if the ciphertext does not give the attacker any additional information about the plaintext. Shannon proved that the entropy of the key in a cipher possessing perfect secrecy has to be at least as high as the entropy of the plaintext. This result implies that such ciphers require a key which has to have at least the length of the plaintext and cannot be reused for different plaintexts. This will makes ciphers with perfect secrecy impractical in most settings, where large amounts of data need to be encrypted. Thus, one needs other designs of encryption algorithms and other (probably not that strict) approaches to the definition of security notions. Block ciphers represent one of such

more efficient ways to construct encryption algorithms.

1.3.1.1 Definition

A block cipher can be thought of as a keyed permutation. The key chooses a certain permutation from a class of permutations. For a fixed key, the mapping becomes bijective. More formally, one can give the following definition:

Definition 1.1. *(Block cipher). A mapping $E = \mathbb{F}_2^b \times \mathbb{F}_2^k \to \mathbb{F}_2^b$ is called a block cipher with block size b bits and key size k bits, if the mapping $E(K,)$ is a bijection for each $K \in \mathbb{F}_2^k$, that is, if the inverse mapping $E^{-1}(K,\cdot)$ exists with $E^{-1}(K,E(K,x)) = x$ for each $K \in \mathbb{F}_k^2$ and $x \in \mathbb{F}_2^b$.*

The input and output of $E(K,\cdot)$ are called plaintext and ciphertext, respectively. K is referred to as the encryption key.

1.3.1.2 Design Principles

Confusion and Diffusion is the two important elements in block cipher, introduced by Shannon in 1949 **Communication Theory of Secrecy Systems**. The purpose of confusion is to eliminate known plaintext statistics in the encrypted ciphertext. The goal of introducing diffusion to a block cipher, is to complicate, for the attacker, the relation between plaintext bits and key bits in the ciphertext. It is clear that confusion and diffusion are highly desirable properties for a block cipher, and it is the task for the designer to determine how to obtain them, while still keeping the requirements for the block cipher in mind.

1.3.2 Stream Cipher

Stream ciphers are symmetric systems, so both sender and receiver share a common secret key and both encryption and decryption depend on this key. In general, stream ciphers are much faster than public key systems that have two keys. Stream ciphers can be viewed as approximating the action of a proven unbreakable cipher, the one-time pad (OTP), sometimes known as the Vernam cipher. A one-time pad uses a keystream of completely random digits. The keystream is combined with the plain text digits one at a time to form the cipher text. This system was proved to be secure by Claude E. Shannon in 1949. However, the keystream must be generated completely at random with at least the same length as the plain text and cannot be used more than once. This makes the system cumbersome to implement in many practical applications, and as a result the one-time pad has not been widely used, except for the most critical applications. Key generation, distribution and management are critical for those applications.

A stream cipher makes use of a much smaller and more convenient key such as 128 bits. Based on this key, it generates a pseudorandom keystream which can be combined with the plain text digits in a similar fashion to the one-time pad. However, this comes at a cost. The keystream is now pseudorandom and so is not truly random. The proof of security associated with the one-time pad no longer holds. It is quite possible for a stream cipher to be completely insecure.

Most of the stream cipher algorithm are based on two main classical models as shown in Figure 1.2:

1. **Combination**
2. **Filter generators**

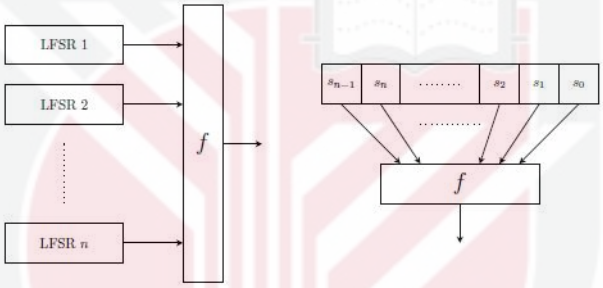

Figure 1.2: Combination and Filter Generators of Stream Cipher

This two models which in turn depend on Linear Feedback Shift Register (LFSRs). The outputs of LFSRs are provided as input to a boolean function which produces the key stream. Therefore, the security of such cipher relies on the appropriate choice of boolean functions. The boolean functions should satisfy a number of cryptographic properties in order to be a cryptographically strong boolean function.(Rizomiliotis, 2010).

Other than that, basic properties in stream cipher are balancedness, high nonlinearity and algebraic degree.High nonlinearity is to helps to resist linear approximation attack meanwhile for balancedness is to help avoid the existences of bitwise bias in the truth table of a boolean function. Another property needed in the combination generator model is correlation immunity. This properties is important because this will prevent the combining generator function from leaking information regarding the individual LFSR sequences into the output sequence which can be exploited by correlation attack (Wei and Hu, 2007).

Last but not least, one more property that is an important cryptographic property for boolean functions is the algebraic immunity due to the appearance of algebraic attacks against stream ciphers.

1.3.3 Boolean Functions in Stream Cipher

This subsection provides introduction on boolean functions (Carlet, 2010).

Definition 1.2. ***(Boolean function)****. A boolean function on n may be viewed as a mapping from* $\{0,1\}^n$ *into* $\{0,1\}$*. A boolean function* $f(x_1,...,x_n)$ *is also can be write as the output of its truth table f.*

Definition 1.3. ***Algebraic normal form of boolean function - ANF)****. Every boolean function* f *can be expressed as a multivariate polynomial over* $\mathbb{F}_2$*. This polynomial is known as algebraic normal form of the boolean function* f*. The general form of algebraic normal form of* f *is given by,*

$$f(x_1,\ldots,x_n) = a_0 \oplus \bigoplus_{1\le i\le n} a_1 x_i \oplus \bigoplus_{1\le i<j\le n} \oplus \cdots \oplus a_{12.....n} x_1 x_2 \ldots x_n. \tag{1.1}$$

Definition 1.4. ***Degree of boolean function)*** *Degree of a boolean function f is defined as* $deg(f)$ *= number of variables in the highest order product term in the algebraic normal form of* f*. Functions of degree at most one are called affine function. An affine function with constant term equal to zero is called linear function.*

Definition 1.5. *Annihilator of a boolean function A non-zero boolean function g of n variables is said to be a annihilator of a boolean function* $f \Longleftrightarrow g(X)\cdot f(X) = 0, \forall X \in \{0,1\}^n$.

As mentioned in previous subsection and we can summarize that there are six main cryptography properties required for boolean function.

1. **Balancedness** :A boolean function is balanced if its truth table contains an equal number of 1s and 0s, that is, if its Hamming weight equals 2^{n-1}. Also if $W_f(0) = 0$.
2. **High Nonlinearity** : The nonlinearity of -variable function is its minimum distance from the set of all $n$variable affine functions, i.e.

$$nl(f) = \min_{g\in A_n}(d(f,g)) \tag{1.2}$$

$$nl(f) = 2^{n-1} - \frac{1}{2}\max_{w\in F_2^n}|W_f(w)| \tag{1.3}$$

3. **Correlation immunity (Resilience)** :An n-variable boolean function f is m^{th}-order correlation immune, denoted by $CI(m)$, if, for every such that

$1 \leq wt(w) \leq m, F(w) = 0$. An -variable boolean function which is both balanced and m^{th}-order correlation immune is known as an m-resilient boolean function.

4. **Algebraic degree** : The algebraic degree, $deg(f)$, is the number of variables in the highest order term with none zero coefficient in ANF.

5. **Algebraic immunity** :Algebraic immunity of f, denoted by $AI(f)$, is defined as the minimum (or low)degree annihilators of f or $f+1$.

6. **Low autocorrelation** : The autocorrelation AC_f of boolean function $f(x)$ is given by:

$$AC_f = max_s |\sum_x f(x)\dot{f}(x \oplus s)| \tag{1.4}$$

where $s \neq 0$

1.3.4 Attacks in Cryptography

In building a cryptosystem, a cryptologist will build their best cryptographic algorithm meanwhile a cryptanalyst will take opportunity to tackle the method of breaking the cryptosystem. Every analysis and attack to the cryptosystem is important because it will used to be a benchmark of strengthen of that particular cryptosystem.

By Martin (2012), attackers in cryptography can be divided into two types:

1. **Passive attacker** are the attacks where the attacker indulges in unauthorized eavesdropping, just monitoring the transmission or gathering information. The eavesdropper does not make any changes to the data or the system. Unlike active attack, the passive attack is hard to detect because it doesnt involve any alteration in the data or system resources. Thus, the attacked entity doesnt get any clue about the attack. Although, it can be prevented using encryption methods in which the data is firstly encoded in the unintelligible language at the senders end and then at the receivers end it is again converted into human understandable language.

2. **Active attacker** are the attacks in which the attacker tries to modify the information or creates a false message. The prevention of these attacks is quite difficult because of a broad range of potential physical, network and software vulnerabilities. Instead of prevention, it emphasizes on the detection of the attack and recovery from any disruption or delay caused by it. An active attack usually requires more effort and often more dangerous implication. When the hacker attempts to attack, the victim gets aware of it.

There is six categories of attackes that can be launched on encryption scheme:

1. **Ciphertext-only attack** is an attack model for cryptanalysis where the attacker is assumed to have access only to a set of ciphertexts. While the attacker has no channel providing access to the plaintext prior to encryption, in all practical ciphertext-only attacks, the attacker still has some knowledge of the plaintext. For instance, the attacker might know the language in which the plaintext is written or the expected statistical distribution of characters in the plaintext. Standard protocol data and messages are commonly part of the plaintext in many deployed systems and can usually be guessed or known efficiently as part of a ciphertext-only attack on these systems.

2. **Known-plaintext attack** is where attacker know some of the plaintexts with their respective ciphertexts and tries to deduce the secret part of the cryptosystem.

3. **Chosen-plaintext attack** is where the attacker has access to the encryption oracle and can choose plaintext to be encrypted. The ciphertexts produced and the plaintext are used to deduce any previous unknown plaintexts encrypted using the same oracle.

4. **Chosen-ciphertext attack** is where The attacker has capability to make the victim (who obviously knows the secret key) decrypt any ciphertext and send him back the result. By analysing the chosen ciphertext and the corresponding received plaintext, the intruder tries to guess the secret key which has been used by the victim. Chosen-ciphertext attacks are usually used for breaking systems with public key encryption. For example, early versions of the RSA cipher were vulnerable to such attacks. They are used less often for attacking systems protected by symmetric ciphers. Some self-synchronizing stream ciphers have been also attacked successfully in that way.

5. **Adaptive chosen-plaintext attack** is similar with chosen plaintext attack but the choices of plaintext may rely on ciphertext encrypted from the previous requests to the encryption oracle.

6. **Adaptive chosen-ciphertext attack** is similar with chosen ciphertext attack but the choices of ciphertext may rely on plaintext encrypted from the previous requests to the encryption oracle.

1.4 Research Motivation

Stream cipher is among widely used cryptographic methodology in secure modern communication. Among all attacks upon stream cipher, the Fault Injection Analysis (FIA) is a practical method that can be used by attackers in real-world scenarios. Hoch and Shamir (2004) states that fault analysis is a very powerful cryptanalytic method upon many cryptosystems which at a glance is not vulnerable to direct attacks.

This thesis is motivated by FIA techniques together with Hao's method to gauge the security of Pomaranch, Grain v0 and LILI-28 by identifying new annihilators.

After the analysis, if one does not obtain annihilator(s) in the selected stream cipher, it would give higher sense of security to that algorithm(s). However, if annihilator(s) are obtained from the specific algorithm, it can be used for an algebraic attack that algorithm(s). As such, we are also motivated to compile all new annihilators upon our selected stream ciphers that went through our FIA technique.

1.5 Research Question

It is the task of cryptanalysts to innovate existing cryptanalyst methods to conduct attacks upon published cryptosystems. In this research, we will inject fault within boolean functions of selected stream cipher algorithms such as Pomaranch, Grain v0 and also LILI-128. We identified four (4) research gaps as follows:

1. Can we find annihilators by via FIA upon boolean Function of Pomaranch, Grain v0 and LILI-128 stream ciphers?
2. How many annihilator(s) can we obtain using FIA?
3. Can we obtain low-degree equation with found annihilator(s)?
4. Can we reduce complexity of solving the boolean function?

We choose Pomaranch stream cipher is because this algorithm is one of the e-STREAM project candidate and for Grain v0, it is original algorithm of Grain family that also one of candidate of e-STREAM project. Both algorithm have boolean function of five (5) coefficients ($n = 5$) and third degree ($d = 3$). For LILI-128 algorithm, it is from NESSIE project and its boolean function was given as ten (10) coefficients ($n = 10$) and sixth degree ($d = 6$). NESSIE and e-STREAM are the top cryptographic projects in Europe.

1.6 Research Objective

The aim of this research is to obtain and build low degree equation of selected boolean function as to reduce the complexity to find the initial key. To achieve the aim, four main objectives were set as followings:

1. To generate and find new annihilators, g, via FIA upon boolean Functions of Pomaranch, Grain v0 and LILI-128 stream cipher.
2. To populate annihilator(s), g, using FIA upon boolean Functions of Pomaranch, Grain v0 and LILI-128 stream cipher.
3. To find low-degree equation.
4. To reduce complexity of selected boolean function.

1.7 Research Methodology

In the research, we will find annihilator(s) in selected stream ciphers Pomaranch, Grain v0 and LILI-128 via FIA upon its boolean function. Our first strategy is to inject value of one (1) into each of the active coefficient in each boolean function using PERL script as in Appendix A. Then proper analysis can be conducted on the new generated injected boolean function using Hao et al. (2007) method. Then output of this result will be used for analysis of complexity for find the initial secret key.

1.8 Contribution of Research

- Compilation of new annihilator(s) using FIA on selected stream cipher's boolean function.
- New annihilator(s) will be utilized to reduce complexity of published boolean function.
- New annihilator(s) will be utilized to launch algebraic attack upon selected stream cipher.

1.9 Scope and Limitation of the Study

The scope to do this analysis by FIA on selected stream cipher's boolean function focuses only to find get and compile annihilator(s). We will present the attack model and the method used in the analysis. Then we will go further into the analysis to find either annihilator(s) exits or not.

The limitation in this study of the analysis is the usage of the obtained annihilator(s) in algebraic attack. That is, in this study we do not proceed with the algebraic attack with the annihilator(s) we found.

1.10 Overview of the Thesis

This thesis divide into eight chapter including the current chapter which contains an introduction of cryptography, research motivation, research problem statement, research objective, research methodology, contribution of this research and also research scope and limitation.

In **Chapter 2** present literature review that was done at the earlier stage of the research. It consists of boolean function, attacks in stream cipher, attack and cryptanalysis of Pomaranch, Grain v0 and LILI-128 stream cipher. It also including literature review of FIA and Hao's algorithm (Hao et al., 2007).

Chapter 3 explained the research methodology used in this study beginning from how to inject the fault value into the boolean function and to generate injected boolean function. Then, we explain how to implement Hao's method.

In **Chapter 4**, we will present an introduction of Pomaranch stream cipher algorithm, result of fault injection analysis on this algorithm and also discussion on the security impact and its summary.

In **Chapter 5** we will present an introduction of Grain v0 stream cipher algorithm, result of fault injection analysis on this algorithm and also discussion on the security impact and its summary.

In **Chapter 6** we will present an introduction of LILI-128 stream cipher algorithm, result of fault injection analysis on this algorithm and also discussion on the security impact and its summary.

Finally in **Chapter 7** consists of the overview, the conclusion of works conducted in this study including future work that can be extended from this research.

REFERENCES

Ahmadi, H. and Eghlidos, T. (2009). Heuristic guess-and-determine attacks on stream ciphers. *IET Information Security*, 3(2):66–73.

Alhamdan, A., Bartlett, H., Dawson, E., Simpson, L., and Wong, K. K. H. (2012). Slide attacks on the sfinks stream cipher. In *Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on*, pages 1–10. IEEE.

Armknecht, F. (2004). Improving fast algebraic attacks. In *International Workshop on Fast Software Encryption*, pages 65–82. Springer.

Armknecht, F. (2005). Algebraic attacks and annihilators. In *WEWoRC*, pages 13–21.

Babbage, S. (1995). Improved exhaustive search attacks on stream ciphers.

Babbage, S. (2001). Cryptanalysis of lili-128. In *Proceedings of the 2nd NESSIE Workshop*.

Banegas, G. (2014). Attacks in stream ciphers: A survey. *IACR Cryptology ePrint Archive*, 2014:677.

Banik, S., Maitra, S., and Sarkar, S. (2012). A differential fault attack on the grain family of stream ciphers. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 122–139. Springer.

Barenghi, A., Breveglieri, L., Koren, I., and Naccache, D. (2012). Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures. *Proceedings of the IEEE*, 100(11):3056–3076.

Biryukov, A., Priemuth-Schmid, D., and Zhang, B. (2010). Differential resynchronization attacks on reduced round snow 3gŁ. In *International Conference on E-Business and Telecommunications*, pages 147–157. Springer.

Biryukov, A. and Shamir, A. (2000). Cryptanalytic time/memory/data tradeoffs for stream ciphers. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 1–13. Springer.

Biryukov, A. and Wagner, D. (1999). Slide attacks. In *International Workshop on Fast Software Encryption*, pages 245–259. Springer.

Boege, W., Gebauer, R., and Kredel, H. (1986). Some examples for solving systems of algebraic equations by calculating groebner bases. *Journal of Symbolic Computation*, 2(1):83–98.

Buchberger, B. (1985). Grobner bases: An algorithmic method in polynomial ideal theory. *Multidimensional systems theory*.

Callahan, K. (2013). The impact of the allied cryptographers on world war ii: Cryptanalysis of the japanese and german cipher machines. Technical report, Technical report, Georgia College Mathematics Department.

Carlet, C. (2010). Boolean functions for cryptography and error correcting codes. *Boolean models and methods in mathematics, computer science, and engineering*, 2:257–397.

Cid, C., Gilbert, H., and Johansson, T. (2006). Cryptanalysis of pomaranch. *IEE Proceedings-Information Security*, 153(2):51–53.

Coppersmith, D., Halevi, S., and Jutla, C. (2002). Cryptanalysis of stream ciphers with linear masking. In *Annual International Cryptology Conference*, pages 515–532. Springer.

Courtois, N., Klimov, A., Patarin, J., and Shamir, A. (2000). Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 392–407. Springer.

Courtois, N. T. (2003). Fast algebraic attacks on stream ciphers with linear feedback. In *Annual International Cryptology Conference*, pages 176–194. Springer.

Dawson, E., Clark, A., Golic, J., Millan, W., Penna, L., and Simpson, L. (2000). The lili128 keystream generator. In *Proceedings of first NESSIE Workshop*.

Delfs, H. and Knebl, H. (2015). Symmetric-key cryptography. In *Introduction to Cryptography*, pages 11–48. Springer.

Ding, L. and Guan, J. (2013). Related key chosen iv attack on grain-128a stream cipher. *IEEE Transactions on Information Forensics and Security*, 8(5):803–809.

Dinur, I. and Shamir, A. (2009). Cube attacks on tweakable black box polynomials. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 278–299. Springer.

Dinur, I. and Shamir, A. (2012). Applying cube attacks to stream ciphers in realistic scenarios. *Cryptography and Communications*, 4(3-4):217–232.

Englund, H., Hell, M., and Johansson, T. (2007). A note on distinguishing attacks. In *Information Theory for Wireless Networks, 2007 IEEE Information Theory Workshop on*, pages 1–4. IEEE.

Hao, C., Shimin, W., and Zepeng, Z. (2007). Several algorithms to find annihilators of boolean function. In *isdpe*, pages 341–343. IEEE.

Hell, M., Johansson, T., Maximov, A., and Meier, W. (2006). A stream cipher proposal: Grain-128. In *Information Theory, 2006 IEEE International Symposium on*, pages 1614–1618. IEEE.

Hell, M., Johansson, T., Maximov, A., and Meier, W. (2008). The grain family of stream ciphers. In *New Stream Cipher Designs*, pages 179–190. Springer.

Hell, M., Johansson, T., and Meier, W. (2007). Grain: a stream cipher for constrained environments. *International Journal of Wireless and Mobile Computing*, 2(1):86–93.

Hellman, M. (1980). A cryptanalytic time-memory trade-off. *IEEE transactions on Information Theory*, 26(4):401–406.

Hoch, J. J. and Shamir, A. (2004). Fault analysis of stream ciphers. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 240–253. Springer.

Jansen, C. J. (2004). Streamcipher design: Make your lfsrs jump. In *The State of the Art of Stream Ciphers, Workshop Record, ECRYPT Network of Excellence in Cryptology*, pages 94–108.

Jansen, C. J., Helleseth, T., Kholosha, E., and Bv, D. (2006). Cascade jump controlled sequence generator and pomaranch stream cipher (version 2). estream, ecrypt stream cipher. In *eSTREAM, ECRYPT Stream Cipher Project, Report 2006/006*. Citeseer.

Jeong, K., Lee, Y., Sung, J., and Hong, S. (2011). Fault injection attack on a5/3. In *Parallel and Distributed Processing with Applications (ISPA), 2011 IEEE 9th International Symposium on*, pages 300–303. IEEE.

Joux, A. and Muller, F. (2003). A chosen iv attack against turing. In *International Workshop on Selected Areas in Cryptography*, pages 194–207. Springer.

Katz, J., Menezes, A. J., Van Oorschot, P. C., and Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.

Martin, K. M. (2012). Everyday cryptography. *The Australian Mathematical Society*, 231(6).

Massey, J. (1969). Shift-register synthesis and bch decoding. *IEEE transactions on Information Theory*, 15(1):122–127.

Meier, W., Pasalic, E., and Carlet, C. (2004). Algebraic attacks and decomposition of boolean functions. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 474–491. Springer.

Meier, W. and Staffelbach, O. (1989). Fast correlation attacks on certain stream ciphers. *Journal of Cryptology*, 1(3):159–176.

Mihaljević, M. J. and Golić, J. D. (1992). Convergence of a bayesian iterative error-correction procedure on a noisy shift register sequence. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 124–137. Springer.

Raddum, H. and Semaev, I. A. (2006). New technique for solving sparse equation systems. *IACR Cryptology ePrint Archive*, 2006:475.

Rizomiliotis, P. (2010). On the resistance of boolean functions against algebraic attacks using univariate polynomial representation. *IEEE Transactions on Information Theory*, 56(8):4014–4024.

Roy, D., Datta, P., and Mukhopadhyay, S. (2015). Algebraic cryptanalysis of stream ciphers using decomposition of boolean function. *Journal of Applied Mathematics and Computing*, 49(1-2):397–417.

Roy, D. and Mukhopadhyay, S. (2015). Fault analysis on the stream ciphers lili-128 and achterbahn. *IACR Cryptology ePrint Archive*, 2015:1077.

Siegenthaler, T. (1985). Decrypting a class of stream ciphers using ciphertext only. *IEEE Transactions on computers*, (1):81–85.

Simmons, G. J. (1992). *An Introduction to Shared Secret and/or Shared Control Schemes and Their ApplicationThis work was performed at Sandia National Laboratories and supported by the U.S. Department of Energy under contract number DEAC0476DPOO789.* IEEE.

Singh, S. (1999). *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography*. Doubleday, New York, NY, USA, 1st edition.

Verdult, R., Garcia, F., and Balasch, J. (2012). Gone in 360 seconds: Hijacking with hitag2. pages 237–252.

Wei, Y. and Hu, Y. (2007). Maximum autocorrelation analysis of nonlinear combining functions in stream ciphers. In *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, pages 176–180. IEEE.

BIODATA OF STUDENT

Wan Zariman Omar (born 03 April 1983) is a Senior Analyst in CyberSecurity Malaysia. He is graduated in BSc. Applied Mathematic (Mathematical Modelling) from University Science Malaysia. He was born at Hospital Sultanah Aminah, Johor Bahru, Johore on 3rd April 1983. He got married on 27th June 2008 and was give with 3 daughters and 1 son. He started his cryptology research in September 2007 with CyberSecurity Malaysia. His is doing his research until now in latest technology regarding cryptography.

He can be contacted by e-mail at *wanzariman@cybersecurity.my* and *wan_zariman@yahoo.com*.

LIST OF PUBLICATIONS

Publications that arise from the study are:

Wan Zariman Omar, Muhammad Rezal Kamel Ariffin, Solahuddin Shamsuddin, Zahari Mahad and Suhairi Mohd Jawi. (2019). Findings Annihilator(s) via Fault Injection Attack (FIA) on Boolean Function of Grain v0 *ITM Web of Conferences*, Accepted.

Wan Zariman Omar, Muhammad Rezal Kamel Ariffin, Solahuddin Shamsuddin, Zahari Mahad and Suhairi Mohd Jawi. (2019). New vulnerabilities upon Pomaranch Boolean Function through Fault Injection Analysis (FIA) *International Journal Of Cryptology Research*, Submitted.