Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 72 (2015) 292 – 299

Procedia Computer Science

The Third Information Systems International Conference

Fixed point attack in PGV-5 scheme using SIMON algorithm

Sofu Risqi Y.S[1], Steven Yohanes[2], Susila Windarta [3]

National Crypto Institute, Ciseeng, Bogor 16330, Indonesia

Abstract

Block cipher-based hash function is a hash function that is constructed by applying a block cipher algorithm on a scheme to form a hash algorithm. So that the strength of the block cipher-based hash function depends on the strength of a block cipher algorithm which is used. In this research, fixed point attack is done to determine the application of SIMON lightweight block cipher scheme PGV-5 hash function in accordance with the characteristics of the fixed point attack. SIMON is a lightweight block cipher algorithm which uses Feistel network as its structure and is recommended as an alternative algorithm beside AES. Fixed-point attack is applied to generate all possible 2^{32} plaintext with some random and extreme IV. The result of this research is plaintext that meets the characteristics of fixed point that does not affect the plaintext hash value because the resulting output is the used IV value itself. Plaintext is used to construct collision. Apparently the result of the application of the PGV-5 scheme is not resistant to collision attack because there is a collision with probability of fixed point 0.00000000093 in the thirty-two IV samples which are used.

Keywords : SIMON, collision resistance, PGV-5 scheme, fixed point attack;

1. Introduction

Information is one of the needs in companies, organizations, agencies and any kind of environments outside the system. In building a good information system, the data’s security must be guaranteed in this terms are data confidentiality and integrity. There are several information classifications, one of them is confidential information which its confidentiality needs to be secured from threats such as eavesdropping, message forgery until message thievery. Therefore a system to protect this kind of information is necessary with the existence of cryptographic system.

Cryptography is a mathematical science technique that related to information security aspect. Cryptography is expected to meet the needs of confidentiality, data integrity, entity authentication and data origin authentication [1]. While in general cryptanalysis is mathematical science technique intended

doi:10.1016/j.procs.2015.12.143

to break cryptographic technique and information security services [1]. Cryptography and cryptanalysis are developed in line. These two science areas are affecting each other in the development. According to taxonomy, cryptography is divided into three categories which are un-keyed primitives, symmetric-key primitives and asymmetric primitives. While in principles there are three cryptography applications. Those applications are symmetric, asymmetric and hash function. Hash function is used in more general context to protect data integrity by replacing a huge size data into shorter string with fixed length (m bit) as the hash output. For more efficient implementation process in a system whether it's in hardware or software, a block cipher-based hash function is constructed [1].

There are 64 block cipher-based hash function schemes called Preneel-Govaerts-Vandewalle (PGV) which are introduced by Bart Preneel, Rene Govaerts and Joos Vandewalle in 1993, one of the scheme is PGV-5 [2]. PGV-5 scheme can be applied to a block cipher algorithm with different key length and block process where fixed point attack can be done [5]. Fixed point attack is easier to apply than other kind of attack towards hash functions with Merkle-Damgard construction. If the value of message m_i is known and processed produces $f(IV_{i-1}, m_i) = IV_i$ then, if it is placed on the i^{th} round, it will produce the same hash value from the $i^{th} - 1$ round.

In this paper a lightweight block cipher algorithm, SIMON, is applied as the encryption function in PGV-5 scheme. The used of SIMON algorithm is because it's recommended by NSA, which is more efficient than other lightweight block cipher for instance PRESENT, CLEVIA, KATAN, etc. [3]. SIMON is part of lightweight block cipher family with Feistel Network as its structure. SIMON is designed to fulfill the needs of security, flexibility, analysis and also to optimize the performance of devices that has limitation in memory. SIMON is also designed to give its best performance in hardware. Lightweight block cipher is also can be implemented well as block cipher-based hash function because it's efficient to be applied in hardware [11]. A good block cipher will be a construction block in hash function [1]. In this research SIMON is tested whether it has a good strength as a hash function constructor not only efficient in hardware. A performance test by using fixed point attack is done to test the collision resistance of produced block cipher-based hash function [4]. The purpose of this research is to know the security level of SIMON light weight block cipher algorithm in PGV-5 scheme with fixed point attack. So the research can contribute as reference in selecting a lightweight block cipher algorithm with collision resistance properties to be implemented in PGV-5 scheme.

We organized this paper as follows. In section 1 we introduce about hash function and the attacks on the scheme. Section 2 comprises theoretical basis of the paper. In Section 3 we describe the stage of the attack. The results of the attack are depicted on Section 4. Conclusions follow on Section 5.

2. Theoretical Basis

2.1. Hash Function

Hash function is a function that maps message with arbitrary length into a hash value with fixed length from a message. In general the purpose of hash function is to guarantee data integrity, but recently hash function also can be used for commitment scheme, key derivation, and pseudorandom number generation [12].

Hash function can also be defined as h function that transforms message M with arbitrary length into hash value with fixed m length, where $m = h(M)$. h function algorithm which is used must be efficient in its computation. Hash function that is used to support data security is cryptographic hash function. The purpose of Cryptographic hash function is to guarantee data integrity by forming hash value or message digest from a data. If the data is stored in unsecured place, the integrity can be checked by reconstructing the data's hash value [6].

Hash function can be classified into three categories. Those categories are block cipher-based hash function, customized hash function and hash function based on modular arithmetic [1]. Block cipher-based hash function is a hash function that is formed by applying block cipher algorithm in certain scheme. If in a hash function, collision is not easily found in a hash function (efficiently solved) then it is said to have collision resistance properties.

2.2. PGV-5 Hash function scheme

In 1993 Bart Preneel, Rene Govaerts and Joos Vaandewalle made a general model of round function that is used in block cipher-based hash function, mainly in single length (n-bit) scheme. The number of single length scheme that can be used as construction for block cipher-based hash function are $4^3 = 64$ different constructions based on the combinations of input and output, the use of constants and also feed forward functions that are used. All of these 64 schemes are called as Preneel-Govaerts-Vandewalle (PGV). From 64 possibilities, PGV-5 scheme can be applied for block cipher algorithm with different key length and block process also fixed point attack is possible to be done [5].

PGV-5 scheme is developed by S. Matyas, C. Meyer and J. Oseas. PGV-5 scheme is likely known as Davies Mayer Scheme [1]. In this scheme, produced hash value from previous iteration is used as key for block cipher to encrypt message block as plaintext. The encryption result is then to be XOR-ed again with the previous hash value to produce new hash value [7].

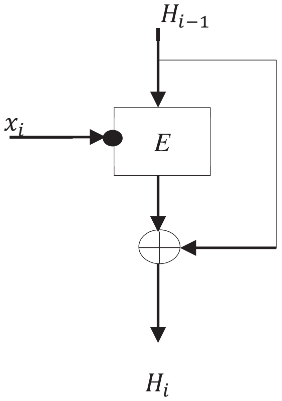

Fig. 1. PGV-5 Scheme

Hash function's steps using PGV-5 scheme:

1. Input message X with arbitrary length, if the message input length is not multiple of k then padding has to be done (k is the size of key input in key schedule algorithm of the block cipher).
2. Message with a length multiple of k is divided into j blocks per k bit, denoted as $x_1, x_2, \dots, x_j$
3. In this scheme every H_{i-1} block is treated as message that will be encrypted in block cipher E with key input is the length of x_i block input. The value of IV and H_0 with the size of b bit is firstly determined.

Here is the general equation for PGV-5 scheme:

$$H_0 = IV;$$
$$H_i = E_{x_i}(H_{j-1}) \oplus H_{i-1}, 1 \leq i \leq j$$

2.3. SIMON Lightweight block cipher

Cipher algorithm is a systematic procedure to run mathematical operation to convert message into encrypted message, an example of cipher algorithm is SIMON. SIMON is a lightweight block cipher algorithm with Feistel Network as its structure. This algorithm is recommended as alternative algorithm beside AES for program with small resources [10]. SIMON has the size for input/output and master key in variety, and has 32 rounds in its algorithm. In Table 1, we give variations of block size and key in SIMON algorithm.

Table 1. Key Size and Block Size of SIMON

No.	Block size	Key size
1	32	64
2	48	72, 96
3	64	96, 128
4	96	96, 144
5	128	128, 192, 256

Figure 2 and 3 depicted key expansion and round function of SIMON algorithm.

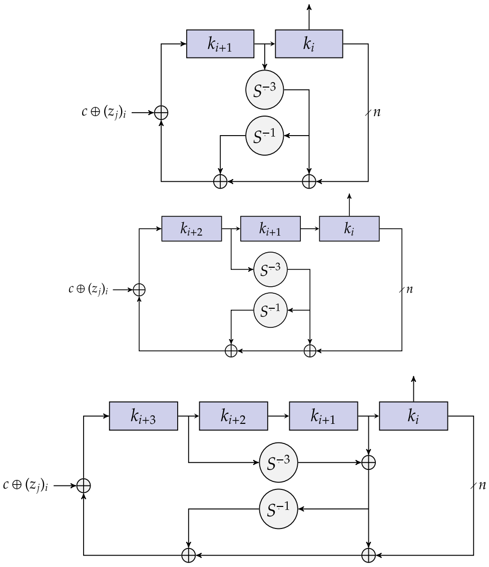

Fig. 2. SIMON key expansion

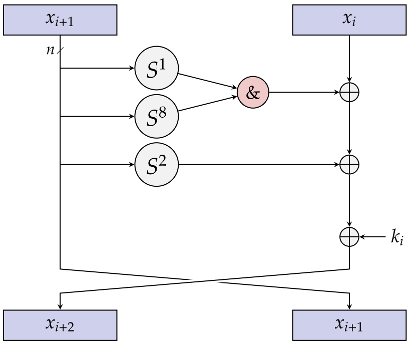

Fig. 3. SIMON Round function

Function in SIMON algorithm uses XOR operation, AND operation and rotation in each round. While key expansion algorithm uses AND operation and XOR operation only. Key expansion algorithm in SIMON requires the value of c, z and k. Where z are bits consist of z_0, z_1, z_2, z_3, z_4 with $z_0 = u$ and $z_1 = v$, $z_2 = t \oplus u, z_3 = t \oplus v\, z_3 = t \oplus w$. It is defined that the value of u, v, w and t as follows:

$$u = 111110100010010101100001110011 \ldots$$
$$\mathrm{v} = 100011101111100100110000101101 \ldots$$
$$\mathrm{w} = 100001001011001111100011011101 \ldots$$
$$\mathrm{t} = 101010101010101010101010101010 \ldots$$

Then the value of c is defined by $\mathrm{c} = 2^n - 4$, such that the value of k is obtained as follows:

$$k_{i+m} = \begin{cases} c \oplus (z_j)_i \oplus k_i \oplus (I \oplus S^{-1})S^{-3}k_{i+1} & if\ m = 2 \\ c \oplus (z_j)_i \oplus k_i \oplus (I \oplus S^{-1})S^{-3}k_{i+2} & if\ m = 3 \\ c \oplus (z_j)_i \oplus k_i \oplus (I \oplus S^{-1})(S^{-3}k_{i+3} \oplus k_{i+1}) & if\ m = 4 \end{cases}$$

2.4. Fixed point attack

For the last two decades, many types of hash functions have been defined but, the most widely used in many of the cryptographic applications currently are hash functions based on block ciphers and the dedicated hash functions. Almost all the dedicated hash functions are generated using the Merkle-Damgard construction which is developed independently by Merkle and Damgård in 1989 [13].

In 2007 Murali Krishna Reddy Danda introduce type of attack on hash function with Merkle-Damgard construction that are fixed point attack, message expansion attack, joux's multi-collision attack and herding attack. A fixed point attack for compression function $f(IV_{i-1}, m_i) = IV_i$ is the pair of (IV_{i-1}, m_i) , such that $f(IV_{i-1}, m_i) = IV_{i-1}$. The illustration of fixed point as follows [4]:

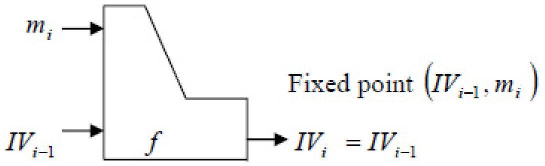

Fig. 4. Fixed point attack

So m_i doesn't affect the hash value. Therefore, this characteristic can be used to find collision. If hash value is known, then collision can be found with two different messages which are m_i and $m_i||m_j$. It can be written as follows: $f(m_i, IV_i) = y$ and $f(m_i||m_{\,j}, IV_i) = y$

3. Stage of attack

3.1. Sample and sampling technique

Fixed point attack needs minor modified inputs from a message as much as $2^{n/2}$ where n is output bits from hash function. The used input samples consist of values in hexadecimal from 0 until f. Minor modification of the message is done by changing the last 32 bits (8 hexadecimal values) from the right as much as 2^{32} or 4.294.967.296 bits. Minor modification that is done only uses pairs of input $00000000 - ffffffff$ (hexadecimal) with same value that produced the same hash value with the used IVs.

3.2. Processing technique and data analysis

The data is processed using C++ compiler which the program itself is Dev C++ 5.6.3 version and a laptop with its specifications are: Intel Core i3-3110 CPU 2.40 GHz with the size of Random Access Memory (RAM) is 2 Gigabyte to run the fixed point attack simulation. Data analysis technique is done by performing analysis with attack resistance which is to test its resistance against collision attack.

4. Application of fixed point attack on implementation of SIMON algorithm in PGV-5 scheme

4.1. PGV-5 scheme using SIMON algorithm

SIMON is a lightweight block cipher algorithm with Feistel Network as its structure. SIMON is recommended by national security agency in 2013, since it is more efficient than the other lightweight block cipher for instance PRESENT, CLEVIA, KATAN, etc. [3]. Therefore the application of SIMON algorithm in PGV-5 block cipher-based hash function scheme is expected to create a secure scheme, in this case it's resistance against collision.

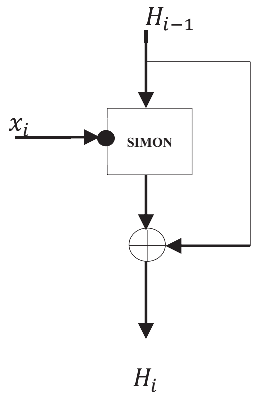

Fig. 5. PGV-5 Scheme with SIMON Algorithm

Explanation:

1. In PGV-5 scheme with SIMON algorithm, hash input is used as key in SIMON Block Cipher
2. IV is used as message input in SIMON block Cipher
3. The length of used hash input value is 64 bit (SIMON's key length is 64 bit which operates 16 bit at a time)
4. The key of the block cipher will be assign as samples for PGV-5 scheme using SIMON algorithm resistance research, which are 2^{32} or 4.294.967.296 samples.

4.2. Fixed point attack in PGV-5 scheme using SIMON algorithm

The research is done by trying to find collision in 2^{32} or 4.294.967.296 inputs, where all input values are in range of "$0000\ 0000\ 0000\ 0000 - 0000\ 0000\ ffff\ ffff$" (hexa) by using 32 kinds of IVs which are consist of 16 extreme IVs and 16 random IVs, these values is expected to be able to represent all other IV values. Total attempts that have been done is 32 x 4.294.967.296 attempts. Table 2 and Table 3 shows the collision input value and the IVs that are used.

Table 2. Fixed point attack result with IV extreme

No.	IV (8 *hex*)	Collision (16 *hex*)	Sum of collision
1	0000 0000	0000 0000 2006 0571	1
2	1111 1111	–	0
3	2222 2222	0000 0000 d1f2 3364	1
4	3333 3333	0000 0000 7888 de5a	1
5	4444 4444	0000 0000 cecd 217d	1
6	5555 5555	0000 0000 bd48 64f7	1
7	6666 6666	–	0
8	7777 7777	–	0
9	8888 8888	0000 0000 0076 bc23 0000 0000 e792 96ed	2
10	9999 9999	0000 0000 1763 8b86 0000 0000 8840 b0f0	2
11	aaaa aaaa	0000 0000 1fa9 1d7e 0000 0000 3659 010b	2
12	bbbb bbbb	–	0
13	cccc cccc	–	0
14	dddd dddd	0000 0000 f064 5c7b	1
15	eeee eeee	–	0
16	ffff ffff	0000 0000 5180 b129	1

Table 3. Fixed point attack result with IV random

No.	IV (8 *hex*)	Collision (16 *hex*)	Sum of collision
1	4bc2 a004	0000 0000 0da8 e62b 0000 0000 8203 58af	2
2	46ec b7ae	0000 0000 7509 2579	1
3	76fe b324	0000 0000 f6be 5a9d	1
4	234b a45c	0000 0000 b42f d38f	1
5	662b bc3c	0000 0000 a2f0 9c9f	1
6	773b ceba	0000 0000 5eb1 ebbd	1
7	930c a3b4	0000 0000 18af eb9a	1
8	1735 8263	0000 0000 5fb3 7871	1
9	a80f e34c	0000 0000 b9bf 4e0f	1
10	be73 f20a	0000 0000 c7de 9126	1
11	c45f e78a	–	0
12	ce23 5fea	0000 0000 e54b f689	1
13	ceb2 3c50	–	0
14	de3b cc52	0000 0000 256f e2b6	1
15	de34 7ab6	0000 0000 4835 052f 0000 0000 aa2c a23c 0000 0000 e5dc 13f8 0000 0000 ee16 a37c	4
16	f12c 76cb	–	0

From the data above, it is shown that there are 30 collisions from 32 used IVs. For extreme IVs, it is obtained 2 collision at most while for random IV it is obtained 4 collision at most from 4.294.967.296 input variations in the last block. Therefore it can be said that block cipher-based hash function with

PGV-5 scheme using SIMON-32 is not resistant against fixed point attack where the probabilities to obtain fixed point is 0.00000000093.

5. Conclusion

Based on the result, experiment and data analysis, the conclusion that can be taken from the research is there are 30 collisions from 32 used IVs. For extreme IVs, it is obtained 2 collision at most while for random IV 4 collision at most from 4.294.967.296 input variations in the last block. Therefore it can be said that block cipher-based hash function with PGV-5 scheme using SIMON-32 is not resistant against fixed point attack where the probabilities to obtain fixed point is 0.00000000093.

Acknowledgement

We would like to thank to National Crypto Institute for financial and non-financial supports.

6. Reference

[1] Menezes, Alfred J., Paul C. van Oorschot, Scott A. Vanstone. 1997. *Handbook of Applied Cryptography*. Boca Raton : CRC Press LLC .

[2] Preneel, Bart. 2003. *Analysis and Design of Cryptographic Hash Functions.* PhD thesis, Katholieke Universiteit Leuven.

[3] Beaulieu, Ray et. al. 2013. *The SIMON and Speck Families of Lightweight Block Ciphers*. National Security Agency.

[4] Danda, M.K. Reddy. 2007. *Design and Analysis of Hash Functions.* Thesis in Network security and Cryptography, Victoria University.

[5] Bartkewitz, Timo. 2009. *Building Hash Functions from Block Ciphers, Their Security and Implementation Properties.* Ruhr-University Bochum.

[6] Stinson, Douglas R. 2002. *Cryptography Theory and Practice, third edition.* Chapman & Hall/CRC.

[7] Preneel, Bart, Rene Govaerts, Joos Vandewalle. 1993. Hash Functions Based on Block Cipher: a Synthetic Approach. *Advanced in Cryptology- CRYPTO 1993*, LNCS 773, pp. 368-378.

[8] Winarno, Agus.2014. *Analisis Pengaruh Penerapan Fungsi Simplified MA MESH-64 Pada Simplified IDEA Dengan Skema Davies Meyer Menggunakan Uji SAC, Yuval's Birthday Attack, Message Expansion Attack Dan Fixed Point Attack.* Sekolah Tinggi Sandi Negara. Bogor

[9] Stamp, Mark. Richard M. Low. 2007. *Applied Cryptanalysis Breaking Ciphers in the Real World*. John Wiley & Sons, Inc.. Hoboken. New Jersey.

[10] Ege Gulcan, Aydin Aysu, and Patrick Schaumont. 2015. *Flexible and Compact Hardware Architecture for the SIMON Block Cipher.*Bradley Department of ECE. USA.

[11] Poschmann, Axel York.2009. *Lightweight Cryptography Engineering for a Pervasive World.* Germany: Ruhr-University Bochum.

[12] Mouha, N. (2012). *Automated Techniques for Hash Function and Block Cipher Cryptanalysis.* Belgium: Khatolieke Universiteit Leuven.

[13] Ralph Merkle. "One way hash functions and DES". In Gilles Brassard, editor, Advances in cryptology: CRYPTO 89, volume 435 of Lecture Notes in Computer Science, pages 428-446. Springer-Verlag, 1989.