Indonesian Journal of Electrical Engineering and Computer Science
Vol. 10, No. 3, June 2018, 1244~1250
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v10.i3.pp1244-1250

Security of a New Cryptographic Hash Function - Titanium

Abdullah Nazeeh Saleh[1], Mohammad A. Al-Ahmad[2]
[1,2]Computer Science Department, College of Basic Education. Public Authority for Applied Education and Training, Kuwait City, Kuwait

Article Info

Article history:

Received Dec 19, 2017
Revised Jan 20, 2018
Accepted Mar 11, 2018

Keywords:

Cryptanalysis
Cryptography
Hashfunction
Preimage
Sponge

ABSTRACT

This paper introduces the security analysis of Titanium hash function that uses SF block cipher and follows sponge construction. A brief description of the sponge function and the design choice of Titanium are introduced. Basic security criteria of random function have been presented and studied on Titanium and then, differential cryptanalysis on Titanium has been performed and showed the resistance of it on the most recent differential attacks. A table of security discussions finalizes the paper and describes the complexity of Titanium on brute force cryptanalysis.

Copyright © 2018 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Computer Science Department. College of Basic Education.
Public Authority for Applied Education and Training.
Kuwait City, Kuwait State
E-mail: malahmads@yahoo.com

1. INTRODUCTION

Hash functions are one-way functions used for mapping variable input size and produce fixed length output digest. It is a powerful algorithm to verify data integrity over peers. There are many hash functions, such as MD5[1], SHA1[2] and Double-A[3]. Many hash functions acted as a random oracle for a time being. However, the revolution of computer processors enhanced the attacks on such algorithms. The concerns of hash function security are its resistance to the basic security criteria; preimage, second preimage, collision and length extensions.

Attackers try to create a scenario to break one of the security criteria by compromising and the analyzing hash states. Thus, designers' goal is building high confusing and defusing to create what so called random oracle.

The basic security criteria of hashes is its resistance to preimage, second-preimage, collision and recently length extensions.

Titanium is a new constructed sponge hash function that uses 512bit SF block cipher[4]. SF is a block cipher that takes 512 plaintext input, 512bit key and applies four operations on the input to produce 512bit output ciphertext. Titanium takes variable length input and produces fixed output digest 512bit.

2. RESEARCH METHODOLOGY

2.1 Sponge Function Overview

Sponge is one of the hash function construction. There are some constructions used for building hash function algorithem such as, Merkle–Damgård construction. It has issues with the digest length as its security is depending on that length. Sponge construction has been introduced by Keccak team[5-6]. It aims to split the security level of the algorithm from the digest length. Sponge construction has three main phases; Absorbing phase, Squeezing phase and the truncation phase.

2.2 Inner State

Message input goes through several iterated operations inside the blender. Each operation produces different output forming in S-box. Each S-box is a state which contains the binary pattern of the algorithm result. The states in the middle of the blender operations called inner states. It is the intermediate chaining values that is formed from the last operation performed on the pattern.

$$P = M||P + 1 + Zeros + Mx \quad (1)$$

Length padding rule has been implemented on Titanium. Adding prefixes or suffixes to the message will not create collisions with length padding. Assuming message length for two messages are same, then the binary pattern will be different. Adding bits to the input will affect the message binary and padding bits. Then, different input.

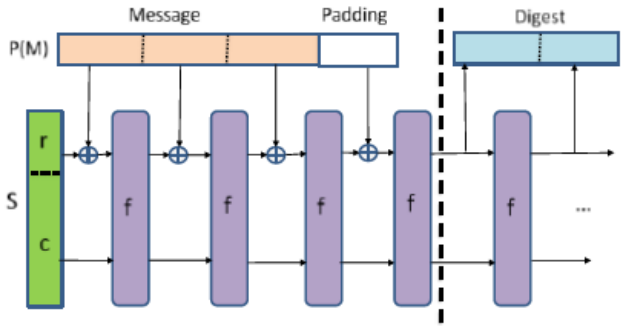

Figure 1. Sponge construction

2.4 Absorbing Phase

r-bit message blocks are inserted to the blender by XORing it with the first r-bits of the state[Figure1].

2.5 Cipher

F cipher [1] is processing over four operations; sub-byte, Convert row, shifting and add round key.

Sub-Byte.

Data elements is sub-byted over 576bit S-boxes. Sub byte operation properties remove the linear characteristics. Therefore, linear cryptanalysis is not applicable on Titanium S-boxes. Moreover, it increases the diffusion and confusion so, studying the linearity effectiveness of differentials is out of complexity scope and does not create an advantage to the attacker.

Convert Row Round.

In this stage, Titanium data element is blended with each other's, preparing it to the next stage. After sub-byte round, convert row round blends the bits, increasing diffusion and confusion such that keeping the properties of small differences in input is obscure.

2.6 Cryptanalysis

Preimage.

Hash functions should be one-way property such that knowing the original message from the digest is not possible with complexity lower than 2^c. There are many ways to break this property such as giving prefixes to the message or going backwards through intermediate chaining values reaching to the mother state then the original message or even with brute force attack. Preimage is to obtain the original state from a given digest[Figure2].

Titanium sponge hash function has 1024-bit capacity and bitrate of 576bit. Since the capacity is the security parameter for sponge construction and its security is split from the digest length [5], the minimum complexity for Titanium against preimage attack is 2^{2c}

Collisions.

Collision is to find different input that leads to the same digest [7]. Collision resistance itself is a general criterion, so there are many ways that attackers use to obtain collisions in the hash function such as finding collisions in intermediate chaining values by applying different scenarios to establish the attacks. The minimum complexity required for random oracle is 2^c. Attackers can break the complexity to half by using birthday theory in probability science[Figure3]. In simple, it could be by surrounding all probability statics for the digest. For instance, a classroom with twelve students. One student should share the same birthday with a colleague. By some probability calculations, the complexity might be broken to the half.

Second Preimage.

Second preimage is the advances of collision attack. It is to find the second message from a given digest and known first message with its hash value[Figure4] [7].

H (M_0) → 0a5d1f18c84b0c145f588a60121da7
H (M_1) → 0a5d1f18c84b0c145f588a60121da7
Attackers try to find M_1

Figure 2. Second Preimage

Length extension.

Length extension is one of the security criteria for hash functions. Hash functions can be used as Message Authentication Codes. H(Secret||Message). Therefore, any weakness in the hash structure will threat the MAC and affect the server files validation [9].

In this case, server calculates the message digest and determines if it is a valid request or not. Theoretically, attackers may forge modified request without knowing the secret that the server uses by appending some data to the message and server still sees it as a valid request (2).

$$h(M||P||M`||P`) \quad (2)$$

Since length extension attacks depend on finding collisions in the internal state, Titanium iterates on 24 times and each operation updates the whole state. Furthermore, changing one bit will change at least half of the state bites and the attacker does not know which part has been truncated.

2.7 Advanced Security analysis

The basic security criteria for hash functions are preimage, second preimage, collision and length extension (Used with MACs). The basic security claims for all of criteria should be at least 2^c. Attackers create a scenario to break one or more of those criteria or reduce the complexity of algorithm, whether it is a theoretical or a practical way.

Multi-collision attack.

Cascading hashes appeared in the PhD thesis of B. Preneel [9]. It is to build a concreted hash digest from two independent hash algorithms. It increases the security level with affecting the total cost of implementation (3).

$$(h1(Message0)||h2(Message1)) \quad (3)$$

Joux [11] proved that cascading hashes does not make difference. The complexity of it remains as if it is only one hash algorithm. Joux [11] found collisions with message's blocks by exhausted search using pre-computed data structure to compare all message's pairs to obtain four collisions (Collision finding machine) such that giving initial value that will produces two blocks of the message (4) [Figure5].

$$f\ (initial\ Value, Block0) = f(Initial\ Value, B0`) \quad (4)$$

The attack is based on finding collisions at intermediate chaining values between the internal states of the message pairs. Titanium has a capacity of 1024bit and updates each state after each operation. Considering birthday theory, the complexity of Titanium against remains 2^c.

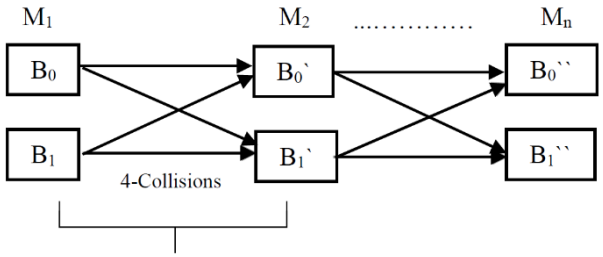

Figure 3. Multi-Collision attack

Herding Attack.

Herding hashes is the advances of Multi-collision attack by using brute-force to create a tree of data[12]. Its idea is to create an array of data structure which is a pre-computed tree for intermediate values by using brute-force. Then, run exhaustive search for internal states that collide with one or more data structure values. After the collision, adding short prefixes to the string is possible with approved validation.

Titanium follows sponge construction and uses SF cipher. The digest is truncated and the truncated part is unknown to the attacker. Furthermore, initial value is same for all inputs. Changes in inputs affect first state then the whole inner states.

By using brute-force, the complexity of Titanium remains at minimum 2^c with the consideration of birthday theory.

2.8 Distinguishers:

Distinguishers is used widely to break security algorithms as it has many techniques to use. It is the study of the relationship between inputs, keys and the outputs to disclose full of the key or part of it. Distinguishers' cryptanalysis aims to break one or more of the hash function security criteria (Preimage – Second preimage – Collision – length extension) through particular cryptanalysis, such as differential cryptanalysis.

Differentials cryptanalysis.

Differentials is the study of the relationship between inputs and outputs. It is aiming to trace the function and where it does a particular behavior such that exploiting that vulnerability and disclose the key or part of the key [14]. It is based on known plaintext-ciphertext cryptanalysis which is a pair of messages that has a particular statistical properties. Attackers apply their differential attacks using different scenarios and techniques such as, slide attack, rotational and truncated differentials. Generally, for Titanium, the total cost of generating pair of messages that has that particular statistical properties is 2^{2c}.

Slide Attack.

Slide attack is known plaintext chiphertext attack. However, it does not use brute force attack to generate the pairs. It depends on what so called, slid pairs. The given variables for the attacker is the message (P_0), chiphertext (C_0) of the P_0 and the assumed message (P_1). Attacker pretends that P_1 equals R_1 of P_1 then f_4 of p_0 should equal R_4 of P_1. After that, attacker make some analysis to disclose the key used between f_4 and C_1. If attacker got the corresponding key, applying the same key with P_0 and the key will produce f_1. If f_1 equals P_1, then the pair is a good pair and considered as slid pair as shown below[Figure6] [12].

Slide attack is efficient with algorithm that uses one key for all rounds and the output of all rounds is known for the attacker. However, Titanium updates its state each round and its states do not present any biases to each other. Using XORing between states makes the states take the diffusion and the confusion properties. Furthermore, the output of Titanium is truncated and the attacker does not know which part has been truncated from the digest. Using brute force attack, the complexity of generating slid pair will depends totally on known plaintext attack which requires 2^{2c} possibilities. By considering birthday theory to establish the attack, the complexity of generating slid pair remains 2^c.

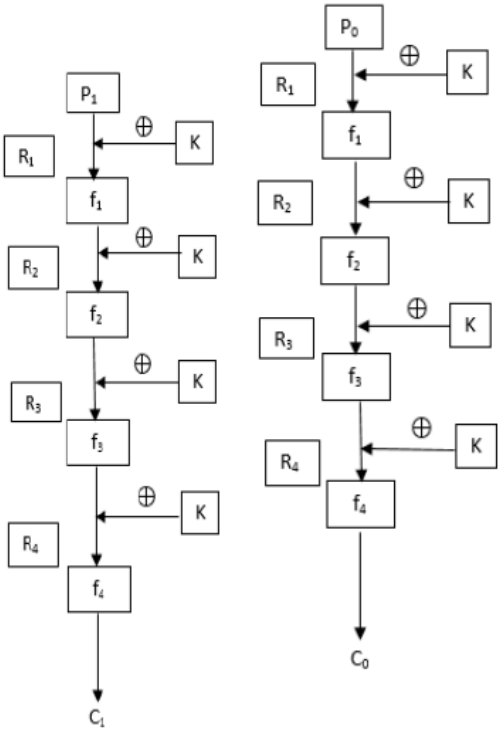

Figure 4. Slide cryptanalysis

Rotational cryptanalysis

It is the analysis that relies on ARX [Modular addition, Rotation and XOR]. Rotations can be obtained by rotating the corresponding word. Rotational cryptanalysis can be established if the bits are friendly to rotate property. However, Titanium does not follow ARX and uses constant in its operation. IVs are same for all messages and capacity remains with a fixed value (zero) [15].

Truncated differential cryptanalysis

It is the cryptanalysis on the differences in inputs and outputs to discover the key or part of it. Truncated differentials relies on known plaintext ciphertext attack. It studies the behavior of the function and tracing it to the stage that the function makes a different behavior hoping to find statistical patterns in Sboxes distribution. Attacker should obtain plaintext and the corresponding ciphertext. Once the attacker gets the statistical property, then pairs called differentials [16].

Titanium has a constant value (C, IV) for all messages and finding the required pairs needs 2^{2c} possibilities. Assuming that the attacker is able to find the pairs with less work ($<2^{c}$), the digest is truncated and attacker does not know which part has been truncated.

Square attack

Square or integral attack is a differential attack based on known plaintext ciphertext attack [17]. It was first applied on block ciphers. However, the technique here is to find the corresponding differences in the block rather than several bits. It exploits the property of one-way S-box. Its pairs should have constants in the pairs' blocks plus variables and then attack could be established with those studied variables and considered as integral pairs.

Titanium has a capacity of 1024bit and never affect the output. Bitrate values of Titanium are changing after each operation and round. Furthermore, the digest is truncated and the full digest is obscure.

Linear cryptanlysis

Linear cryptanalysis is efficient with algorithm that uses ARX [Add – Rotate – XOR]. In this attack, attacker tries to obtain known plaintext ciphertext pairs with linearity proportion of ½ by some XORs operation and statistical studies. It depends on the zeros and ones distribution in the state[Figure7] [18].

Titanium has a capacity of 1024bit which forces attacker to generate 2^{2c} pairs by using brute force attack. Moreover, S-boxes used in Titanium are non-linearity property. Assuming the attacker succeeds in applying the linear on Sboxes somehow, the total cost of establishing the attack is 2^{2c}.

$$I = (I_1, I_2, I_m)$$
$$O = (O_1, O_2, O_m)$$
$$I_1 \oplus I_3 \oplus I_4 \oplus O_2 \oplus O_4 \oplus O_5 = 0$$

Figure 5. Linear pairs

3. DISCUSSIONS

Table 1 is a discussion for Titanium on any desired digest length with different attacks and security criteria. The complexities are the required cost to establish the attack using brute force attack technique.

Table 1. Discussions

Function	Collision	Prei-mage	S-preimage	Distinguishers
Titanium-256 R.Sponge-256	2^{256}	2^{512}	2^{512}	2^{512}
Titanium-512 R.Sponge-512	2^{512}	2^{1024}	2^{1024}	2^{1024}
Titanium-n R.sponge-n	$2^{n/2}$	2^{2c}	2^{2c}	2^{2c}

4. CONCLUSION

Titanium hash function has been analyzed. It shows a resistance of 22c against the studied attacks. Its construction and cipher fortified the algorithm by surrounding it with high diffusion and confusion with taking its performance of the algorithm in the consideration. Using bigger capacity increases hash complexities. However, bigger capacity means higher executive costs on modern CPUs. 1024bit capacity is a reasonable size. The security claims of it fulfill random sponge claims which is the ideal hash function.

REFERENCES

[1] R. Rivest, The MD5 Message-Digest Algorithm. April 1992.
[2] Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini, Yarik Markov. The first collision for full SHA-1
[3] Mohammad AlAhmad, Abdullah Issa, Abdullah Alsaleh, "Double-A - A Salsa20 like - The Design". *The 4th conference of Advanced Computer Science Applications and Technologies (ACSAT), 2015 International Conference on*, IEEE Xplore
[4] A New Block Cipher for Network Security, Kripa, Megha R Kamat, Meghana, Swati D Pai & Mr. Vasanth Nayak.*Inperial Jornal of Interdisciplinary Research (IJIR)*, 2016
[5] Guido Bertoni, Joan Daemen, Michael Peeters and Gilles Van Assche. Keccak sponge function family main document. http://keccak.noekeon.org/Keccak-main-2.1.pdf/, 2010
[6] Sponge Functions. Guido Bertoni1, Joan Daemen1, Micha¨el Peeters2, and Gilles Van. Assche1. gro.noekeon@noekeon.org.1 STMicroelectronics. 2 NXP Semiconductors
[7] Xiaoyun Wang, Dengguo Feng, Xuejia Lai, Hongbo Yu, "Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD", July 27, 2008.
[8] P. Rogaway, T. Shrimpton, "Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance", February 12, 2004
[9] Danilo Gligoroski, Length Extension Attack on Narrow-Pipe SHA-3 Candidates, Springer, 2010
[10] B. Preneel. "Analysis and design of cryptographic hash functions". PhD thesis, Katholieke University Leuven, January 1993.
[11] A. Joux. "Multicollisions in iterated hash functions. Application to cascaded constructions". In M. K. Franklin, editor, CRYPTO, volume 3152 of Lecture Notes in Computer Science, pages 306–316. Springer, 2004.
[12] John Kelsy & Tadayoshi Kohno, Herding Hash Functions and the Nostradamus Attack, January2006
[13] Michael Tunstall, *Practical complexity differential cryptanalysis and fault analysis of AES*, Springer, 2011
[14] Takanori Isobe, Toshihiro Ohigashi, Masakatu Morii, "Slide Cryptanalysis of Lightweight Stream Cipher RAKAPOSHI", *Springer*, 2012
[15] Dmitry Khovratovich, Ivica Nikolic, Rotational Cryptanalysis of ARX, 2010

[16] Takuma KoyamaLei WangYu SasakiKazuo SakiyamaKazuo Ohta, New Truncated Differential Cryptanalysis on 3D Block Cipher
[17] Lars KnudsenDavid Wagner. *Integral Cryptanalysis*, Springer, 2002
[18] Joo Yeon Cho, *Linear Cryptanalysis of Reduced-Round PRESENT*. Springer, 2

BIOGRAPHIES OF AUTHORS

Abdullah Nazeeh Saleh
Abdullah Nazeeh Saleh received his bachelor degree in Education, Computer from Public Authority for Applied Education and Training – PAAET, Kuwait State in 2016. He is a Master degree student, Computer Science – International Islamic University of Malaysia, IIUM and working for Bank Boubyan – Kuwait as I.T. Service Desk Engineer. Abdullah is interested in cryptography researching, developing and has published papers on cryptography topics.

Mohammad Abdulateef AlAhmad
Mohammad Abdulateef AlAhmad received his bachelor degree in computer engineering from university of the pacific in 2002, his master in computer engineering from Gulf university in Bahrain in 2011, and his PhD degree in computer science from international Islamic University Malaysia (IIUM) in 2015. His research area is information security which focuses on cryptographic algorithms and protocols. My favourite specific research topics are designing and analysis of hash functions, cryptocurrency and cryptography in general. My favorite hash functions are Gear, Double A and Titanium cryptographic hash functions.