New Way to Construct Cryptographic Hash Function

Yong WANG

hellowy@126.com

([1]Guangxi Key Laboratory of Trusted Software; [2]*School of Computer Science and Engineering, Guilin University Of Electronic Technology , Guilin, Guangxi,* 541004*, China*)

Abstract : In this paper, a new way to construct cryptographic hash function is given. The cryptographic hash function is generalized to uncertain function which has various specific function forms. When computing hash value, the specific form of the function is determined by the message, but the codebreaker cannot know the message, and hence cannot know the specific form of random function. This provides a new kind of one-wayness, the one-wayness of the specific function makes the breaking of hash is very difficult because in most cryptographic analysis of hash function, the function should be known and fixed. As fixed function is just a special case of uncertain function, when the function is uncertain, we obviously have more choices and can choose more secure function.

Keywords: hash function; uncertain; one-wayness; cryptography

I. Introduction

A hash function is any algorithm that maps data of a variable length to data of a fixed length. The data to be encoded are often called the message, and the hash value is sometimes called message digest or simply digest. A cryptographic hash function is a hash function that has four main properties: 1) it is easy to compute the hash value for any given message; 2) it is infeasible to generate a message that has a given hash; 3) it is infeasible to modify a message without changing the hash; 4) it is infeasible to find two different messages with the same hash. Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MAC), and other forms of authentication. Hash functions nowadays have fixed structure and function, this provides a convenient for the analysis of the hash function. With the progress of the hash analysis technology in recent years, some attacks on hash function are very effective. E. Biham and R.Chen give near complete collisions of SHA-0[1]. A. Joux found a collision for SHA-0[2]. In the 2004 international conference in cryptography, Wang Xiaoyun announced collision of a series of Hash functions, including MD4 [3], MD5 [4], and RIPEMD HAVAL - 128, and RIPEMD. Wang Xiaoyun puts forward a new Hash function analysis technology for MDx series. In 2005, Wang Xiaoyun gave collision attack of MD5 [4], SHA - 0 [5], SHA - 1[6] in a short time. These attack technologies gave a challenge to the existing Hash functions. The collision attacks against MD5 have improved so much that it takes just a few seconds on a regular computer. This promoted the study of the development of the new Hash algorithm. In this paper, uncertain function is used to design hash algorithm based on the idea of multiple uncertainty which suggests adding more uncertain factors into cryptosystem [7].

II. New Way to Construct cryptographic hash algorithm

In order to lead in more uncertainty to the hash, we introduce the conception of uncertain function, the function is uncertain and there is a set of function $\{f_1, f_2, f_3, ..., f_n\}$ as the specific form of uncertain function. Suppose f_i is a well designed cryptographic hash and m represents the message. There is another function

$A=S(m)$,

A determines which specific form is used for computing the currently message m, simplistically, we can suppose A=i, and then hash value

$H= f_i(m) = f_{S(m)}(m)$.

To the sender, the message m is known and hence he can easily know which function is used, but to the codebreaker, the function is unknown and the codebreaker just knows that the function belongs to the set, but doesn't know which specific form is used.

Function is unknown to codebreaker, it seems the above hash function violate Kerckhoffs's assumption, but in fact it doesn't. The uncertain function is public and hence can be standardized like most modern cryptographic algorithms, so it can be widely used. The uncertain function can be analyzed, assessed and improved by any cryptanalytic expert so that it can avoid flaw and back door. The security of the uncertain function is not dependent on the secrecy of the system or software. Though the function is unknown to codebreaker, but it is known to the receiver and the sender who knows the message, and receiver and sender don't need to consult and share the specific form before communication. The above hash system or software can be shared by anyone including the codebreaker and doesn't inconvenience the correspondents, so the uncertain hash system follows the essential requirements of Kerckhoffs's assumption well.

III.Security analysis

Uncertain function is a generalization of certain function. From the angle of optimization, as certain function is included by uncertain function, so we can find more secure hash function in a wider range of uncertain function theoretically.

In most cryptographic analysis, knowledge of algorithm is a necessary known condition. To uncertain hash function, most modern cryptographic analysis to hash function is invalid. In the above case, due to the specific form of function is unknown, the cryptanalyst cannot get the basic necessary condition of cryptanalysis.

According to the above design, one who computes the hash function value can easily get the specific form of hash function, but for the codebreaker only knows the hash values, he has no effective way to confirm the specific form of hash function. The nowadays precondition of breaking hash that the function is known and fixed is mismatched. There are more uncertain factors to the codebreaker and the codebreaker has no traditional way to break hash. For the constructed hash function, given the hash value, there are two uncertain factors to the codebreaker: the specific form of function and the message (input of the function). Specific form of function is decided by the message, but this relationship of specific form and message is very difficult to use. The reason is as the following: Cryptosystem is based on complex computation. Hash function has many steps or rounds, the computation of hash produces many intermediate parameters. Usually for a well-designed hash function,

given the hash value H, it is hard to compute the message m by one-step, the codebreaker should use intermediate parameters to break, so to the codebreaker, when given hash value, the specific form of function and the intermediate parameters is both unknown.

The codebreaker may try to divide and conquer, we can respectively discuss:

A) Confirm and try every message, and then the specific form can be known. In this way the cryptanalysis is an exhaustive attack. To attack hash, a traditional brute-force method based on exhaustive search need a lot of computing power or a lot of time to complete. Any well-designed hash function should resist exhaustive attack.

B) Confirm the specific form A_i, and then try to get the value of m_j. Under this case, even to one specific form A_i, we can find the cryptanalysis is more complex than traditional hash function. For the message m should meet simultaneously the following conditions that A=S(m) and H= f_A(m), but to the traditional function, the message m should just meet the condition H= f (m).

In cryptography, a collision attack on a cryptographic hash tries to find two inputs producing the same hash value, i.e. find two different messages m_1 and m_2 such that hash(m_1) = hash(m_2).

Collision attack resistance: To above hash function, two different messages generally get different specific form and that does not meet the condition that required in modern collision attacks, as they require the function is fixed and the same for different messages. When we try to modify the message or the middle parameters to get a collision, the specific form of function is changed too for the above uncertain function. Xiaoyun WANG's discovery about differential cryptanalysis of hash is very successfully used to break a series of hash function. The message modification technology and bit-tracking technology are used to break a series of hash functions and these technologies require that the hash function is fixed. To uncertain function, when the message is modified, the specific form of function is modified and the hypothesis that hash function is fixed is broken and the modification is invalid; analogously, for different messages, the specific forms of function are different, and hence structure of function is different, bit of the middle parameters or the message is hard to track; so these technologies are hard to implement to break the above hash of uncertain function. Even the codebreaker can successfully select the two different messages they have the same specific form, that gives the messages more restriction and they are more difficult to fit the limiting condition to get a collision.

Algebraic attack resistance:To the above uncertain function, given the message, the function can be expressed by mathematics ways, but just given the hash value, the function cannot be expressed by direct mathematics ways, so the algebraic attacks and similar cryptanalysis are difficult to uncertain hash function.

In cryptography, a preimage attack on cryptographic hash functions tries to find a message that has a specific hash value. A cryptographic hash function should resist attacks on its preimage.

Preimage (first-preimage) attack resistance: To the above function, we can use the message m to confirm the specific form of function by computing A=S(m), and hence compute the hash value H= f_i (m) = $f_{S(m)}$ (m), but give hash value H, the specific form of function is unknown, and it is more difficult to compute m than the certain hash function.

Second-preimage attack resistance: It requires it is computationally infeasible to find any second input which has the same output as any specified input, i.e., given x, to find a second preimage $x' \neq x$ such that h(x) = h(x′). There are two ways to implement second-preimage attack: A) This attack can use just hash value to break and get a message just like first-preimage attack, just need to confirm the message is

other than x. As discussed above, the above constructed hash function is more secure; B) The codebreaker may try to use x to get another preimage, for fixed and the same function, the second preimage x' and the first preimage x may have involvement so that it can be used to find the second preimage x'. But to uncertain function, different preimages usually have different function, it is hard to find the relationship of the two preimage x' and x.

Resistance of side-channel attack is based on information gained from the physical implementation to traditional function. To side-channel attack, uncertain function is double-edged sword. On one hand, uncertain function gives more uncertain to the codebreaker, on the other hand , the different specific form of function may have different physical indices, and hence may reveal the information of specific form of function from side-channel. So to uncertain function, the cipher designer should avoid this danger, so the design of specific form of function should stay the same in amount of calculation, time, energy and other physical indices.

Resistance of some attacks is mostly dependent on the length of hash value, such as birthday attack, brute force attack, rainbow table attack.

As is discussed above, uncertain hash function is more secure than the traditional certain hash function from angles of most hash cryptanalysis except side-channel attack, birthday attack, brute force attack, rainbow table attack. If the specific form of function is well-designed, uncertain hash function can be more secure than the traditional certain hash function to side-channel attack.

IV. Outlook

In this paper, the conception of uncertain function is proposed to generalize the conception of function. It may be used in many fields about math. Information is things used to eliminate the uncertainty from the angle of information theory. For the cipher designer, the more uncertain the hash function is to the codebreaker, the more secure the function is. Uncertain function can be used to enhance the uncertainty and security. In this paper, new one-wayness is given to enhance the security of hash function. This can be used to construct more secure symmetric cryptosystem. One-wayness is very important in many fields of cryptography, the new one-wayness of the specific form of function may give us new way to design other cryptographic algorithms. The inverse use of uncertain function provides a new method to enhance computational complexity. In traditional cryptosystem, the designer should construct a difficult problem to solve an unknown number or some unknown numbers, for hash function, given the hash value, it is a difficult problem to confirm the message, in this paper, it is difficult to confirm both the message and the specific form, that is to say , a difficult problem is constructed to solve both unknown number and unknown function. It may be more difficult to solve unknown function than unknown number. Similar difficult problems may be used in encryption algorithm.

V. Conclusion

Uncertain function is a generalization of certain function, hash function based on uncertain function has new characters and brings new one-wayness to enhance the security of hash function. Compared with the traditional certain hash function, uncertain hash function is more secure. This paper just briefly gives a new way to construct cryptographic hash function and doesn’t involve the concrete design of

specific form of the function. There are many other details to be defined and optimized. The uncertain function can be made up of a series of uncertain unit. This can reduce the work of design specific form of the function. As a new field, there are many problems to be researched, for example, how to reduce the additional calculation of computing A=S(m), how to avoid leaking the specific form of function, new cryptanalysis and the defense measure.

Acknowledgment

This research was supported by Guangxi Key Laboratory of Trusted Software (No: KX201316).

Reference

[1]. E.Biham, R.Chen. Near-collisions of SHA-0, Advances in Cryptology, CRYPTO'2004, LNCS 3152, 290-305, Springer-Verlag, 2004

[2]. A.Joux. Collision for SHA-0, Rump Session of CRYPTO'04, 2004

[3]. Xiaoyun W, Xuejia Lai, Dengguo Feng. Cryptanalysis of the Hash Functions MD4 and RIPEMD; EUROCRYPT 2005, LNCS 3494:1-18.

[4]. Xiaoyun W, Hongbo Yu. How to break MDS and other Hash Functions, EUROCRYPT 2005, LNCS 3494:.19-35

[5]. Xiaoyun Wang, Hongbo Yu. Efficient collision search attacks on SHA-0, Crypto 2005, LNCS 3621:1-16.

[6]. Xiaoyun Wang, Hongbo Yu, Finding collisions in the Full SHA-1;Crypto 2005, LNCS 3621:17-36

[7]. Yong Wang，study on new cryptosystem of multiple uncertainty，network information security，2012. 06: 82-84