A New Modified 512-bit Approach for MD5 Algorithm

Denial Smith[1],Sonal Bhati[2]
Victoria University Melbourne, Australia[1]
Shekhawati Engineering College
Rajasthani Technical University Rajasthan[2]
denialsmith1970@gmail.com[1]

ABSTRACT

As the continuous development of computer network technology and rapid popularization of Internet application, ecommerce and e-government businesses are used more and more widely. However, at the time that these applications bring great convenience to our work and lives, they also bring increasingly serious security problems. Identity authentication is an important method to ensure safety of various e-commerce activities, e-government business information and internet information. Certificate based digital signature authentication and password authentication are most common at present. But traditional password authentication with basic mode of user name and password authentication faces many security problems .

Network Security & Cryptography is a concept to protect network and data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Data Security is a challenging issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The rapid development in information technology, the secure transmission of confidential data herewith gets a great deal of attention. The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized user for malicious purpose. Therefore, it is necessary to apply effective encryption/decryption methods to enhance data security.

Key Words

MD5 Algorithm; Hash Function;

1. INTRODUCTION

HASH FUNCTION AND MD5 ALGORITHM

Hash function compresses a piece of information with random length by hash algorithm into fixed length value, which is called information abstraction. An information abstract generated from two pieces of different plain code is the so called "collision". The requirements for safe Hash function include: first, two pieces of different plain code generate the same information abstract which should not be calculated and is called collision; second, a certain information abstract cannot be calculated through the other plain information generating the same abstract, which means the initial state cannot be deduced by the results. The so call "cannot be calculated" means that it is too expensive to get the results through the algorithm. Thus, Hush function usually contains two obvious features: first, no matter how long of the plain code information, the information abstract with certain length after calculating; second, if only the plain code information has any change, no matter how small the change is, the corresponding information abstract will be totally different. Thus, it is usually called "digital finger print",which could distinguish identities and ensure the unique and integrity of plain code information and the main effect is password authentication. MD5 algorithm is one of the most common Hash function.

Its basic principle is to process the input information divided groups by 512 bits, and each group divided into 16 sub-groups with 32 bits. After a series of processing, the algorithm output Composed by 4 groups with 32 bits, and cascade this 4 groups will generate a hash value with 128 bits. In the process of MD5 algorithm, fill information first to make its length 64 less than the multiple numbers of 512. The filling method is to attach a 1 and millions of 0, and add an information length before filling indicated by binary system with 64 bits. These two steps are to make the information length be the integer multiple of 512, and ensure the difference after different information filling.

2. EXISTING ALGOTITHM LIMITATION

MD5 is an irreversible transformation transforming a set of data of any length into a hash value of 128-bit length and it is a consecutive processing method. Before operation, it first fills data to be processed, and adds 64-bit binary digits to the end of data representing the bit length of the original data. After filling, the bit length of data which is being processed becomes a multiple of 512. Then the data are divided into groups of 512 bits and computations are performed on each group orderly. The input of the first group operation is a 128-bit initial value; the input of the next group operation is a 128-bit output of the previous group operation. The 128-bit output of the last group operation is the MD5 hash value of the whole data. The key of MD5 algorithm is to perform 4 rounds of hash operation on the data packets of 512 bits. The processing logic is shown in Fig. 2.

3. MODIFIED MD5 ALGORITHM

MD5algorithm is co-invented by Rivets in MIT Computer Science Laboratory and RSA Data Security Company. MD5 is a non-reversible encryption algorithm [3]. It is widely applied in many aspects, including digital signature, encryption of information in a database and encryption of communication information. It makes large amounts of information to be compressed into a confidential format before signing the private key by digital signature soft (that is, any length byte string is transformed into a certain length of big integer).A brief description of new modified MD5 algorithm as follows: MD5algorithm divides plaintext input into blocks each which has512-bit, and each block is again divided into sixteen 32-bitmessage words, after a series of processing, the outputs of the algorithm consist of eight 32-bit message words. After these eight 32-bit message words are cascaded, the algorithm generates a 128-bit hash value which is the required cipher text. Specific steps are as follows [11,
12, 13]:
In the single phase of multiphase encryption is described as multiple encryptions where at each cycle different encryption key is used. In this encryption technique, decryption will be performed in reverse order. In multiphase encryption, such processes will be repeated number of times to enhance the complexity in encryption/decryption as well as security of data. Cryptographic algorithms and key sizes have been selected for consistency and to ensure adequate cryptographic strength for Personal Identity Verification (PIV) applications. Multiphase encryption may reduce the problem of key management in the existing technology of Personal Identity Verification (PIV) due to use of different encryption algorithms with fixed size keys instead of large number of variable length key .

3.1 Adding -bit

A hash function computes a fixed length output called the message digest from an input message of various lengths. The MD5 message digest algorithm [1], developed by Ron Rivest at MIT, accepts a message input of various lengths and produces a 128-bit hash code. It has been one of the most widely-used hash algorithms. However, it has been indicated in [2] that there is a security threat in the algorithm. Furthermore, a 128-bit hash output may not offer sufficient security protection in the near future.
To provide higher security protection, MD5-512 has been proposed by Dobbertin, Bosselaers and Preneel [2]. MD5-512 accepts the same input format as that of MD5, and produces a 512-bit output.
It is easy to find that the structures of the two algorithms are quite similar. It follows that they can be combined together to give one hardware design that can perform the two hash functions. This approach has the following advantages. Firstly, the unified design is a resource-efficient implementation when different hash algorithms are needed in applications. Applications can switch to either algorithm based on different requirements. Second, since MD5 is still the most widely-used hash algorithm, upgrading the current implementation in the future to MD5-512 is much easier with a unified hardware architecture.
Motivated by these observations, in this paper we develop a unified architecture for MD5 and MD5-512.Comparison with other unified architectures indicates that the proposed architecture is area-efficient.
First, the input message is padded and divided into data blocks of length 512 bits. Each data block is treated as 16 32-bit words. The algorithms iteratively processes each data block. For the first data block, an initial value is used to compute an intermediate result. The intermediate result, called the chaining variable, is then updated according to the input data block and the previous result. After all iterations are done, the final chaining variable is the hash value congruent to 448 modulo 512 (length≡448 mod 512). The padding consists of a single 1-bit followed by the necessary number of 0-bits.

3.2 Padding the length of data

A 64-bit representation of the length on bits of the original message is appended to the result of above step. It is present by two 32- bitdigits. At this time, the length of message is filled to a multiple of 512.

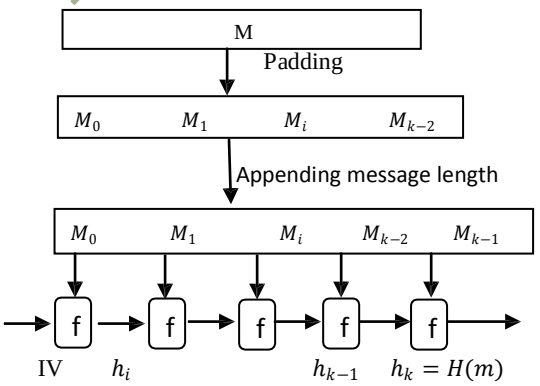

Figure 1: Working principle of an iterated hash function

3.3 Initialize MD5 Standard parameters

Eight 32-bit integers A, B,C,D,E,F,G,H are called chaining variables,
used to calculate the message digest, are initialized by hexadecimal number
A=0x01234567
B=0x89abcdef
C=0xfedcba98
D=0x76543210
E=0x12ac2375
F=0x3b341042
G=0x5f62b97c
H=0x4ba763ed

3.4 Bit operation functions

We define eight bit operation functions J, K, L, M, N, O, P
and Q respectively, in which x, y, z are three 32-bit

integers. The operation is as follows:

$J(x,y,z) = (x \wedge y) \vee ((\neg x) \wedge z)$ ……..…1

$K(x,y,z) = (x \wedge z) \vee (y \wedge (\neg z))$……..2

$L(x,y,z) = x \oplus y \oplus z$..……..3

$M(x, y, z) = y \oplus (x \vee (\neg z))$…. ……..4

$N(x,y,z) = (x \wedge y) \vee ((\neg x) \wedge z)$ ……..…5

$O(x,y,z) = x \oplus y \oplus z$……..……..6

$P(x,y,z) = (x \wedge y) \oplus (y \wedge z) \vee (z \wedge x)$..……..7

$Q(x, y, z) = x \oplus y \oplus z$ …….…. ……..8

In eight functions, if the corresponding bits of x, y and z are independent and uniform, then each bit Of the results should be independent and uniform as well.

4. RESULTS AND CONCLUSIONS

This MD5 algorithm is for the 512 bit message transfer and also with the high security and Stream controlled transfer logic. This algorithm can be used in sending messages for 3G, 4G network. This can also be used for 5G network for which the work has been started. Here we are using 128 bit algorithm and using that as a basic element and create a application for 512 bit messages.

The output would always is of 512bit message. In this way the secret information (e.g. passwords) can be shared with the peer. There is one more application of this algorithm is Message Authentication Code (MAC). This is an integrity check mechanism based on cryptographic hash functions using a secret key. Typically, message authentication codes are used between two parties that share a secret key in order to validate information transmitted between these parties. In SCTP (Stream controlled transfer protocol), it is used by an endpoint to validate the State Cookie information that is returned from the peer in the COOKIE ECHO chunk.

An Application of MD5 algorithm is implemented for the stream controlled transfer messages in the network. This would be a high security algorithm for data transfer in mobile networking with stream controlled logic. There may a vast number of applications for this algorithm in data transfer in

3.4 Bit operation functions implementation

The algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be

"compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.

The MD5 algorithm is designed to be quite fast on 32-bit machines. In addition, the MD5 algorithm does not require any large substitutiontables; the algorithm can be coded quite compactly.

various types of networks. (512, 768 …) like SHAs by extending the block size of compression functions or increasing number of them.

The MD5 algorithm is an extension of the MD4 message-digest algorithm [1,2]. MD5 is slightly slower than MD4, but is more "conservative" in design. MD5 was designed because it was felt that MD4 was perhaps being adopted for use more quickly than justified by the existing critical review; because MD4 was designed to be exceptionally fast, it is "at the edge" in terms of risking successful cryptanalytic attack. MD5 backs off a bit, giving up a little in speed for a much greater likelihood of ultimate security. It incorporates some suggestions made by various reviewers, and contains additional optimizations. The MD5 algorithm is being placed in the public domain for review and possible adoption as a standard.

5. REFERENCE

[1] R. Rivest, "The MD5 Message-Digest Algorithm," RFC 1321, Apr. 1992.

[2] H. Dobbertin, A. Bosselaers and B. Preneel, "RIPEMD-160: A Strengthened Version of RIPEMD, Fast Software Encryption," LNCS 1039, pp. 71-92, Springer-Verlag, 1996.

[3] W. Stallings, Cryptography and Network Security, 2nd ed.,Now York: Prentice-Hall, 1997.

[4] S. Dominikus, "A hardware implementation of MD4-family hash algorithms," Proc. 9th Int. Conf. on Electronics, Circuits and Systems, vol. 3, pp. 1143-1146, 2002.

[5] A UNIFIED ARCHITECTURE OF MD5 AND RIPEMD-160 HASH ALGORITHMS Chiu-Wah Ng, Tung-Sang Ng and Kun-Wah Yip Department of Electrical & Electronic Engineering, The University of Hong Kong Pokfulam Road, Hong Kong

[6] Multi-stage Pipelining MD5 Implementations on FPGA with Data Forwarding, Anh Tuan Hoang, Katsuhiro Yamazaki and Shigeru Oyanagi, Ritsumeikan University, 1-1-1 Noji Higashi, Kusatsu, Shiga 525-8577, Japan

[7] Efficient Implementation for MD5-RC4 Encryption Changxin Li1, Hongwei Wu2, Shifeng Chen1, Xiaochao Li2* and Donghui Guo1,2
1. Dept. of Physics, Xiamen University, Fujian 361005, China
2. Dept. of Electronic Engineering, Xiamen University, Fujian 361005, China

[8] High Throughput Implementation of MD5 Algorithm on GPU Guang Hu, Department of Electron and Information, Huazhong University of Science and Technology, Wuhan, China huguang@mail.hust.edu.cn, Jianhua Ma, Faculty of Computer and Information Sciences, Hosei University, Tokyo 184-8584, Japan, jianhua@hosei.ac.jp Benxiong Huang, Department of Electron and Information, Huazhong University of Science and Technology, Wuhan, China, huangbx@mail.hust.edu.cn

[9] New Modified 256-bit MD5 Algorithm with SHA Compression Function
Alok Kumar Kasgar, Jitendra Agrawal, Santosh Sahu, School of IT School of IT School of IT Rajiv Gandhi Technical University Rajiv Gandhi Technical University Rajiv Gandhi Technical University Bhopal (M.P.) Bhopal (M.P.) Bhopal (M.P.)