International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor (2018): 7.426

Enhancing Security and Speed of Sha-192 with Higher Avalanche

Sushama Ingale[1], Arun Jhapate[2]

[1]Department of Computer Science and Engineering, SIRTS, Bhopal, (MP), India

[2]Professor, Department of Computer Science and Engineering, SIRTS, Bhopal, (MP), India

Abstract: ***In today's world, security is the main issue over internet during transmission of data. Integrity is one of the main factors to guarantee the protection over data. There are many hash algorithms which ensure the integrity. Secure Hash Algorithm can be a capable hashing technique.SHA-3 is the most up to date and efficient Secure Hash Algorithm. In this paper we propose a new approach which produce 192 bit message digest with more secure and high avalanche effect.***

1. Introduction

Cryptographic Hash Functions are important building blocks in computer security. They offer message Integrity that is a security that the receiver is receiving the same message that was sent by dispatcher and has not been customized by any assailant during the broadcast of message. Hash functions are the mathematical functions that take arbitrary length input and produce a small output of fixed size [2]. This output is recognized as message digest or hash code or hash result or simply hash. Hash function produces a fixed size message digest of a known message; this message digest is delighted as a signature of that message. Hash function has the following properties [9].

1) It is a one way function means it is easy to calculate MD from M but it is impossible to calculate M from MD.
2) It should be difficult to find to such messages M1 and M2 which generates same message digest i.e. HF(M1) ≠ HF(M2).

A cryptographic hash function is used to guarantee the integrity of the transmitted data or stored data. Sometimes it is also called digest of a message. There are many algorithms deliberated to execute the hash function. MD-2, MD-4, MD-5, SHA-0, SHA-1 and SHA-2, RIPMID, HAVAL etc, are the best known algorithms for message digest. After this many researchers have also projected their own algorithms for the same such as SHA-192[3].

2. Hash Functions Families

MD-2
It is a cryptographic hash algorithm which produced a message digest of 128 bits. It was published in august 1989. It takes 18 rounds of its compression function to generate a 128 bit digest. [9]

In 2004, MD2 was shown to be exposed to a preimage assault with time complexity equivalent to 2104 applications of the compression function (Muller, 2004). The author of MD2 concludes, "MD2 can no longer be considered a secure one-way hash function".

In 2008, MD2 has further improvements on a preimage attack with time complexity of 273 compression function evaluations.

In 2009, MD2 was shown to be vulnerable to a collision attack with time complexity of 263.3 compression function evaluations.

MD-4
It is another cryptographic hash algorithm, generates a fixed 128 bits message digest. It takes 48 rounds of its compression function. It was published in 1990 [9]. A collision attack published in 2007 can find collisions for full MD4 in less than 2 hash operations.

MD-5
MD-5 generates a message digest of fixed 128 bits. It takes 64 rounds. It was published in 1992. [6] A 2013 attack by Xie Tao, Fanbao Liu, and Dengguo Feng breaks MD5 collision resistance in 218 times.

SHA-0
The Secure Hash Algorithm is cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS), SHA-0 belongs from SHA family; it is another cryptographic hash algorithm generates a message digest of fixed 160 bits. It takes 80 rounds. In 2004, cryptanalysts attack has been found by Bihamet. Al breaks SHA-0 collision resistance at 241 [3].

SHA-1
SHA-1 generates a message digest of 160 bits. It takes 80 rounds and was published in 1995. It is the most widely used algorithm for integrity. Reason for its popularity among existing algorithms is its time efficiency and its robustness. [2] Later on, a 2011 attack by Marc Stevens can produce hash collisions with a complexity of 261 operations.

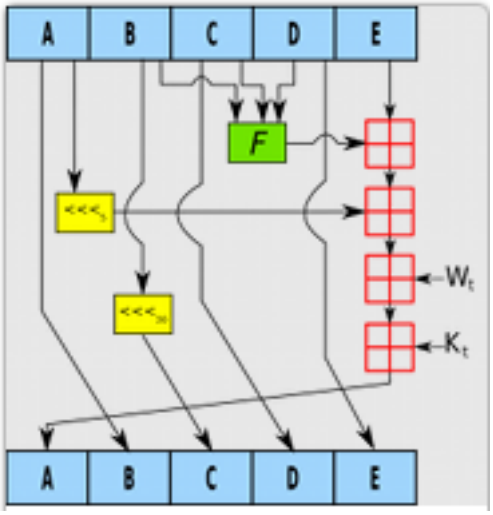


Figure 1: Operation on SHA-1

3. Related Work

Piyush Garg, Namita Tiwari focuses on general observation of SHA algorithms and the security enhancement of existing one due some changes. They observed that SHA-160 and SHA-192 are better in respective field. SHA-192 algorithm is more secure in terms of the number of brute force attacks needed to break it and SHA-160 is fast when compared to the other secure hash algorithms.[5]

Kamlesh kumar Raghuvanshi Purnima Khurana Purnima Bindal: They found that almost all the integrity algorithms have proven breakable except SHA-2 but it is not time efficient. Many researchers have proposed their own algorithms but none of them are time efficient as SHA-1 and also there are chances of improving the internal strength of these algorithms. [4].

Sandhya Verma and G. S. Prajapati they observe that almost all the integrity algorithms have proven breakable except SHA-2 but it is not time efficient. SHA-1 hashing algorithm in terms of the number of brute force attacks needed to break it and moreover it is fast when compared to the other secure hash algorithms. Many researchers have proposed their own algorithms but none of them are time efficient as SHA1 and also there are chances of improving the internal strength of these algorithms. [3].

4. Propose Work

The weakness in SHA family is that two different inputs will produce the same output. There is a need to have a good diffusion so that the output in each round will be spread out and not to be equal with the same output in the next coming stages. In this dissertation a hash algorithm has been presented which increases the security, modified SHA-192 is introduced in this paper having a message digest of length 192 bits. An improved message expansion mechanism (IME), shifting of variables and addition of variables, is used which provide an additional security against the differential attack as best properties of MD5 and SHA-192 are combined.

The weakness in SHA family is that two different inputs will produce the same output. There is a need to have a good diffusion so that the output in each round will be spread out and not to be equal with the same output in the next coming stages. In this dissertation a hash algorithm has been presented which increases the security, modified SHA-192 is introduced in this paper having a message digest of length 192 bits. An improved message expansion mechanism (IME), shifting of variables and addition of variables, is used which provide an additional security against the differential attack as best properties of MD5 and SHA-192 are combined.

I have proposed a new hash algorithm that undergoes a significant change in the elementary function of the secure hash algorithm and also gives us a message digest of length 192 bits with larger bit difference. The proposed SHA-192 uses the padding algorithm, breaking the message into 512 blocks and adding the length as a 64 bit number at end. In order to increase the security aspects of the algorithm message digest should be increased.

The processing step depends upon expanded message block and compression function. In order to increase the security aspects of the algorithm the number message digest should be increased.

1. Padding and appending the message: The purpose of padding is to ensure that the padded message is multiple of 512.If the length of the message M, is L bits it is append the bit 1 to the end of the message followed by k zero bits, where k is smallest, non negative solution to the equation $L+1+k \equiv 448 \bmod 512$. Now, append the 64 bits block that is equal to the number L written in binary.

2. Divide the input into 512 bit blocks: Divide the input message into blocks, each of length 512 bits, i.e. cut M into sequence of 512 bit blocks M[1], M[2]…..M[N].

3. Initialize chaining variables: Now,12 chaining variables A through F are initialised.Before the hash function begins, the initial hash value H0 must be set. The hash is 192 bits used to hold the intermediate and final results the hash can be represented as twelve 32 bit words registers A1, A2, B1,**B2**, C1,C2, D1, D2, E1,E2, F1,F2.
A1=67452301
A2=EFCDAB8
B1=98BADCF
B2=10325476
C1=C3D2E1F0
C2=40385172.
D1=82FECDEK
D2=AHJIDETV
E1=875RTBCD
E2=ANMJH679
F1=57DEFUNT
F2=ASGJH235

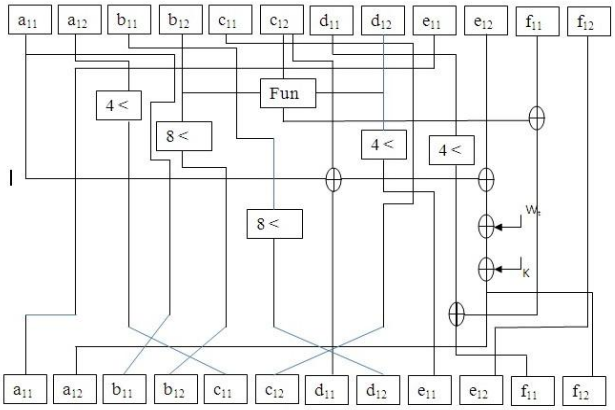


Figure 1: Proposed SHA-192 step function

5. Result

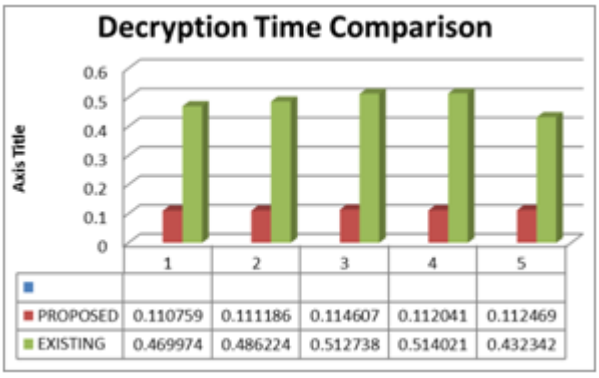
The projected work has been improved the efficiency and results of the security. These things are verified based on following parameters:

1) Decryption Time
2) Avalanche Effect

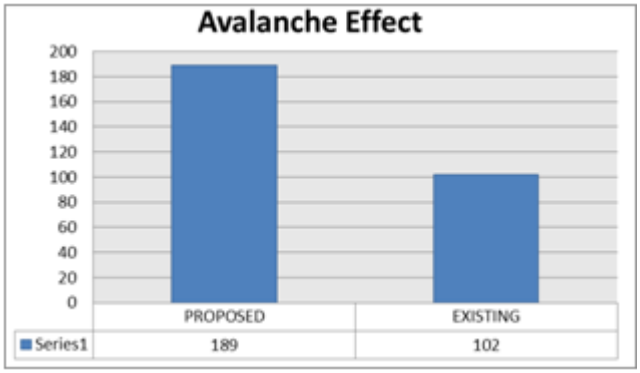
The system which is used to perform and estimate this proposed work over accessible work is as follows:

Table 2: Comparison of time

S. No.	Proposed	Existing
1	0.110759	0.469974
2	0.111186	0.486224
3	0.114607	0.512738
4	0.112041	0.514021
5	0.112469	0.432342



Graph 1: Comparison of time



Graph 2: Comparison Avalanche Effect

6. Conclusion

In this paper we proposed a system which provide the batter security and speed from previous system with higher avalanche effect.

References

[1] Harshvardhan Tiwari and Dr. Krishna Asawa, "A Secure Hash Function MD-192 With Modified Message Expansion" (IJCSIS) International Journal of Computer Science and Information Security, ISSN 1947-5500 ,Vol. VII , No. II, FEB2010.

[2] R.L. Rivest. "The MD5 Message Digest Algorithm" RFC 1321, 1992 [7] Florent Chabaud, Antoine Joux, "Differential collisions in SHA-0,"Advances in Cryptology-CRYPTO'98, LNCS 1462, Springer-Verlag, 1998.

[3] Sandhya Verma and G. S. Prajapati ," A Survey of Cryptographic Hash Algorithms and Issues" International Journal of Computer Security & Source Code Analysis (IJCSSCA), 2015, Vol1, Issue3, ISSN (O): 2454-5651

[4] Kamlesh kumar, Raghuvanshi Purnima Khurana and Purnima Bindal "Study and Comparative Analysis of Different Hash Algorithm" Journal of Engineering Computers & Applied Sciences(JECAS) ISSN No: 2319-5606 Volume 3, No.9, September 2014.

[5] Piyush Garg, and Namita Tiwari, "Performance Analysis of SHA Algorithms (SHA-1 and SHA-192): A Review" International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 2, Issue 3, June 2012.

[6] Thulasimani Lakshmanan and Madheswaran Muthusamy , "A Novel Secure Hash Algorithm for Public Key Digital Signature Schemes" The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012.

[7] Garbita Gupta and Sanjay Sharma, "Enhanced SHA-192 Algorithm with Larger Bit Difference" IEEE International Conference on Communication Systems and Network Technologies, DOI 10.1109/CSNT.2013.42.

[8] Richa Purohit, Upendra Mishra and Abhay Bansal, "A Survey on Recent Cryptographic hash Function Designs" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), ISSN 2278-6856, Volume 2, Issue 1 January - February 2013.

[9] William Stallings, "Cryptography and Network Security: Principles and Practice. Third edition, Prentice Hall.2003.

[10] L.Thulasimani and M.Madheswaran "Security and Robustness Enhancement of Existing Hash Algorithm" IEEE International Conference on Signal Processing Systems 2009.

[11] Harshvardhan Tiwari and Dr. Krishna Asawa "A Secure Hash Function MD-192 With Modified Message Expansion" (IJCSIS) International Journal of Computer Science and Information Security, Vol. VII, No. II, FEB 2010 .

[12] P.P Charles & P.L Shari, "Security in Computing: 4th edition", Prentice-Hall, lnc., 2008. [5] William Stallings," Cryptography and Network security,

Principles and practice", Prentice Hall of India, 3E, 2005.

[13] Florent Chabaud, Antoine Joux, "Differential collisions in SHA-0," Advances in Cryptology-CRYPTO'98, LNCS 1462, Springer-Verlag, 1998. [10] Eli Biham, Rafi Chen, Antoine Joux, Patrick Carribault, Christophe Lemuet, William Jalby, "Collision in SHA-0 and Reduced SHA-1," Advances in Cryptology-EUROCRYPT 2005, LNCS 3494, SpringerVerlag,2005.