Security and Authentication Architecture of block cipher using Mathematical operation and one-way hash function

[1]CH. Suneetha
Associate Professor
In Mathematics
GITAM University
Visakhapatnam, India

[2] D. Sravana Kumar
Associate Professor
in Physics
Dr.V.S.K Govt Degree college
Visakhapatnam, India

[3]P. Sirisha
Faculty in Mathematics
Indian Maritime University
Visakhapatnam, India

[4]KM.Sandeep
Dept. of Computer Science
GITAM University Visakhapatnam, India

Abstract - Extensive growth of telecommunication network provides easy and quick techniques of communicating the information. Rapid development of information technology has given the scope to huge range of new possibilities of internet hacking. Solution to the security problems expanded the field of cryptography. The present paper describes a block cipher mechanism for message confidentiality and authentication using simple arithmetic, logical operations and one-way cryptographic hash functions in two different stages. Agreed upon primary or Master key is used to generate number of sub keys for encrypting different message blocks to extend the lifetime of the master key using some permutation function.

Key words*: Arithmetic operation, Encryption, Decryption, one-way hash function.*

I. INTRODUCTION:

The security of the symmetric cryptosystem depends on the strength of the algorithm and the key. Both the cryptographic algorithm and the key must be so secure to withstand against all types of brute force attacks. In the history of cryptography confidentiality was given the main role trusting that authentication is automatically achieved. As the threat of attacks is ever expanding a good cipher should have the quality confidentiality as well as authentication.

A. Arithmetic Operation Least Common Multiplier

Divisibility rule often encounters in cryptography is a rule of finding whether the given integer is divisible by a fixed divisor. In mathematics factorization decomposes a number into product of factors where the original number is retained by multiplying the products. Least Common Multiplier of two numbers (a, b) is the smallest integer that is multiples of both a and b.

1) Fundamental Theorem on Arithmetic

Any positive integer n greater than 1 can be uniquely expressed as
$n = p_1^{e_1} X p_2^{e_2} X p_3^{e_3} \ldots\ldots X p_K^{e_K}$
Where $p_1, p_2 \ldots p_k$ are primes .and $e_1, e_2 \ldots e_k$ are positive integers.
Theorem: If a, b are non zero integers then there is a unique positive integer m such that a/m and b/m. If c is an integer such that a/c and b/c then m/c.

Theorem: For two integers a and b LCM (a,b) = b if a/b. For three integers a, b, c if a/c , b/c then LCM (a, b)/c
Theorem: If two non-zero integers a, b have factorizations then

$$\text{LCM (a, b)} = p_1^{mn\,(a1,b1)} x\; p_2^{mn\,(a2,b2)} x \ldots\ldots p_k^{mn\,(ak,,bk)}$$

Theorem: If a,b,c are three positive integers then LCM (a,b,c) = LCM [LCM(a,b),c] = LCM [a, LCM(b,c)]

B. Cryptographic Hash Function:

A function that maps variable-length input into a fixed output is called Hash Function. The output is called hash value or message digest. A hash function used for security applications is called cryptographic hash function h = H (M).
H: $D_v \rightarrow R_F$ where D_v is the domain of variable length and R_F is the range of fixed length.

C. Properties of Cryptographic Hash Functions

A good cryptographic hash function should have the following properties to resist all types of active

and passive attacks [1,2]

- Pre-Image Resistant: For the given hash value it is difficult to find the message m such that h = hash (m).i.e., the function should be a one-way function.
- Second Pre-Image Resistant: For given hash value h it is in feasible to find a function y such that h = H(y) computationally.
- Collision Resistant: For two different messages m_1, m_2 it is impossible to find H (m_1) = H (m_2) [3,8] . In present days most widely used cryptographic hash functions are M D5 and SHA - 1.

D. Applications of cryptographic hash functions

Cryptographic hash function is most adaptable algorithm having many applications. Generally cryptographic hash are divided into two types keyed- hash functions and unkeyed-hash functions.

E. Message Authentication Code (MAC)

Keyed hash function is referred to as Message Authentication Code (MAC). Message Authentication Code (MAC) is a technique of verifying the integrity of the message. This assures the received data is exactly as sent. In this mechanism the hash code of the secret key is encrypted to achieve the required authentication [4,5]. The message and the concatenated hash code of the secret key is encrypted to attain the required authentication as well as confidentiality .

F. Hash Message Authenticated Code (HMAC)

Most commonly used MAC construction is HMAC[6,7]. A Message Authenticated Code that uses cryptographic hash functions such as MD 5, SHA-1and secret key is Hash Message Authentication Code (HMAC).
HMAC (K,M) = H [($K^+ \oplus$ opad) ||H[($K^+ \oplus$ ipad) ||M]] Where K^+ is the derived key by padding K to the right extra zeros to the input block size ipad is inner padding of the bits and opad is outer padding of the bits. $\oplus$ represents exclusive OR operation.

G. Nested construction of Message Authentication Code (NMAC)

It is a hash function that uses two keys. The message is concatenated with the one key and again hash function is applied on the output with the second key. If K_1, K_2 are two keys then the Message Authentication Code is
NMAC (K_1,K_2, M)= $h_{k_1}(H_{K_2}(M))$

H. Digital Signature

In case of digital signature the message digest is encrypted with the entity's private key. The security of the digital signature using hash functions is based on the rigidity of finding the collision [11,12,13]. To attain both confidentiality and digital signature it is more advisable to encrypt the message plus private-key encrypted hash code. Besides these applications cryptographic hash functions are used to learn intrusion detection and virus detection also.

I. Rekeying Technique

One of the major factors in symmetric cryptography is key management which involves key generation, life time of the key, storage. Rather than using the agreed upon master key directly for encryption/decryption it is secure and safe to generate the sub key for each data block from the master key by using an agreed upon permutation and all the new sub keys are combined together to form the new master key used for subsequent communications[9,10].

II. Proposed Method

A. Symbols and Abbreviations used

P^n --- n^{th} plain text block of I stage encryption , n takes 1,2,3,……
M^n --- n^{th} plain text block of II stage encryption , n takes 1,2,3,……
P_l^n ----- l^{th} character of the n^{th} plain text block of I stage. l represents the length of the block equal to the length of the hash value of the agreed upon hash algorithm.
M_l^n ----- l^{th} character of the n^{th} plain text block of II stage. l represents the length of the block equal to the length of the hash value of the agreed upon hash algorithm.
$C^{n(I)}$ --- n^{th} cipher block of I stage, n takes 1,2,3,……
$C^{nR(I)}$---Residue part of n^{th} cipher block of I stage n takes 1,2,3…….
$C^{n(II)}$ --- n^{th} cipher block of II stage, n takes 1,2,3,……
$C_l^{n(I)}$ ----- l^{th} character of the n^{th} cipher block of the I stage n = 1,2,3……. ,l the length of the block
$C_l^{nR(I)}$ -----Residue part of l^{th} charater of the n^{th} block of the I stage n = 1,2,3…… and l the length of the block.
$C_l^{n(II)}$ ----- l^{th} character of the n^{th} cipher block of the II stage n = 1,2,3……. ,l the length of the Block
$K^{n(I)}$ --- Key for encrypting the n^{th} block of first

stage , n takes 1,2,3,…… consisting of decimal numbers whose length is equal to the length of the agreed upon hash algorithm

$K^{n(II)}$ --- Key for encrypting the n^{th} block of second stage , n takes 1,2,3,…… consisting of decimal numbers whose length is equal to the length of the agreed upon hash algorithm

$K_l^{n(I)}$ ----- l^{th} decimal number of the n^{th} block key for first stage

$K_l^{n(II)}$ ----- l^{th} decimal number of the n^{th} block key for second stage

Before communicating the messages the sender and receiver agree upon to use the random hash function from the group of present available hash functions and the key consisting of decimal numbers equal to the length of the hash value of the agreed upon hash algorithm say l either in person or using some other key exchange protocols. This agreed upon key is primary key or master key K = $[K_1, K_2, K_3 \dots \dots . K_l]$

The plain text is encrypted in blocks at two stages with different keys. The key for each block is generated from the master key in some agreed upon way. Each block is encrypted in two stages, first stage using simple arithmetic operation Least Common Multiplier of numbers and the second stage using one-way hash function. The plain text length may not be the multiples of the length of the hash value. In such a case pseudo or dummy characters may be padded for the last block. The plain text is divided into blocks of length equal to the hash value of the hash algorithm e.g:32, 64,128,256 or 512. The arbitrary plain text characters are coded to decimal equivalents using ASCII code table and is divided into blocks $P^1P^2 \dots P^n$ each of length equal to the length of the agreed upon hash function say l. The plain text length always may not be the multiples of l. So, for the last block dummy characters may be padded to complete the block length.

B. I Stage Encryption

Consider the first plain text block P^1 of length l, consisting of the decimal numbers

$$P^1=[P_1^1 P_2^1 \dots . P_l^1]$$

The sub key $K^{1(I)}$for encrypting the first block plain text is master key itself. $K^{1(I)}=[K_1^{1(I)} K_2^{1(I)} \dots . K_l^{1(I)}]$

The first number P_1^1 is encrypted as $C_1^{1(I)}$

$C_1^{1(I)}$= LCM $[K_2^{1(I)} \dots . K_l^{1(I)}]+K_1^{1(I)} + P_1^1$

The second number P_2^1 is encrypted as $C_2^{1(I)}$

$C_2^{1(I)}$= LCM $[[K_1^{1(I)} \dots . K_l^{1(I)}]+K_2^{1(I)} + P_2^1$.

.

.

.

$C_l^{1(I)}$ = LCM $[K_1^1 \dots . K_{l-1}^1]+ K_l^1$ + *where* $C_l^{1(I)}$ represents the I stage encryption of P_l^1 which is a decimal number. The decimal number $C^{1(I)} = C_1^{1(I)}, C_2^{1(I)}, \dots . C_l^{1(I)}$ are adjusted to mod 128 is divided into two parts the integer part and the residue part.e.g.,5669_{mod128}=37.

i.e., 5669 = (128*44)+37.Here the integer part is 44 and the residue part is 37.The residual parts of all the numbers $C^{1R(I)}= C_1^{1R(I)}, C_2^{1R(I)}, \dots C_l^{1R(I)}$ is the first cipher block of the first stage.

C. Key Generation for Subsequent Blocks:

The master key is K= K^1 = $[K_1, K_2, K_3 \dots K_l]$ where$K = K_1, K_2, K_3 \dots \dots . K_l$ are decimal numbers. The first cipher block of the first stage is $C^{1(I)} = C_1^{1(I)}, C_2^{1(I)}, \dots \dots C_l^{1(I)}$. The Key for second data block of the first stage K^2 = $[K_1^2 K_2^2 \dots . K_l^2]$ is generated by concatenating $C^{1(I)}$ and the master key K using XOR operation.

$K^{2(I)} = C^{1R(I)} \oplus K$

i.e., $K_1^{2(I)} = C_1^{1R(I)} \oplus K_1^{1(I)}$,

$K_2^{2(I)} = C_2^{1(I)} \oplus K_2^{(I)}$, ……

In general,

$$K_l^{n(I)} = C_l^{(n-1)R(I)} \oplus K_l^{n-1(I)}$$

The decimal equivalents of the second plaintext block $P^2=[P_1^2 P_2^2 \dots . P_l^2]$ is encrypted in the same way as the first block using the mathematical operation Least Common Multiplier with the key $K^{2(I)}$ to get $C^{2(I)} = C_1^{2(I)}, C_2^{2(I)}, \dots \dots C_l^{2(I)}$.Then all the decimal numbers are adjusted to mod 128 to get the second cipher block $C^{2R(I)} = C_1^{2R(I)}, C_2^{2R(I)}, \dots \dots C_l^{2R(I)}$.All the plaintext blocks $P^3, P^4 \dots \dots P^n$ are encrypted in the same way with the keys $K^{3(I)}, K^{4(I)} \dots \dots K^{n(I)}$ generated by concatenating the master key with the preceding cipher block by XOR operation. The decimal numbers of all the cipher blocks are adjusted to mod 128 to obtain the first stage cipher blocks $C^{3R(I)} \dots . C^{nR(I)}$. The integer parts of all the number of each block when adjusted to mod 128 are $I^1=[I_1^1 I_2^1 \dots . I_l^1]$, $I^2=[I_1^2 I_2^2 \dots . I_l^2]$,…. $I^n=[I_1^n I_2^n \dots . I_l^n]$,

D. *II Stage Encryption:*

All the cipher blocks of the first stage $C^{1R(I)}$,$C^{2R(I)}$,$C^{3R(I)}$ … $C^{nR(I)}$ are reversed to constitute the input i.e., the plain text for the second stage encryption.

$M^1= [C_l^{1R(I)}, C_{l-1}^{1R(I)} \dots C_2^{1R(I)}, C_1^{1R(I)}]$

$= [M_l^{1(I)}, M_{l-1}^{1(I)} \dots M_2^{1(I)}, M_1^{1(I)}]$

$M^2 = [C_l^{2R(I)}, C_{l-1}^{2R(I)} \dots C_2^{2R(I)}, C_1^{2R(I)}]$

$= [M_l^{2(I)}, M_{l-1}^{2(I)} \dots M_2^{2(I)}, M_1^{2(I)}]$ ……..

$M^n = [C_l^{nR(I)}, C_{l-1}^{nR(I)} \dots C_2^{nR(I)}, C_1^{nR(I)}]$

$= [M_l^{n(I)} M_{l-1}^{n(I)} \dots M_2^{n(I)}, M_1^{n(I)}]$

Consider the first block M^1 and the agreed upon master key K. The key for first block encryption of the second stage is master key $K=K^{1(II)}= [K_1^{1(II)} K_2^{1(II)} \dots . K_l^{1(II)}]$ itself. The hash value of the key $K^{1(II)}$ of agreed hash function is determined and logical XOR operation is performed between the binary equivalents of each decimal number of M^1 and binary equivalents of each value of $H[K^{1(II)}]$.

$$C^{1(II)} = M^1 \oplus H[K^{1(II)}].$$

The keys for encrypting the subsequent blocks are generated from the same key generation process from the master key by concatenation process as described in C.

$K^{2(II)} = C^{1(II)} \oplus K^{1(II)}$,

$K^{3(II)} = C^{2(II)} \oplus K^{2(II)}$,…….

$K^{n(II)} = C^{(n-1)(II)} \oplus K^{(n-1)(II)}$,

The key $K_2^{1(II)}$ is padded to the first cipher block of second stage $C^{1(II)}$ and agreed hash value is determined. The second block M^2 is encrypted as

$C^{2(II)} = M^2 \oplus [H[C^{1(II)} // K^{2(II)}]$. In general

$C^{n(II)} = M^n \oplus [H[C^{n(II)} // K^{n(II)}]$

All the two staged encrypted blocks $C^{1(II)}$, $C^{2(II)}$, ……, $C^{n(II)}$ consisting of decimal numbers are coded to equivalent text characters using ASCII code table and communicated to the receiver through the public channel as the cipher text C. The integer parts of all the blocks when adjusted to mod 128 I^1, I^2,…….. I^n at the first stage are also sent to the receiver in a separate channel as a string I of integers. In addition the sender appends the secret key to the integer part and finds the hash value of the agreed hash algorithm and tags this value both to the cipher text and to the integer string which acts as Message Authentication Code or Cryptographic Checksum. MAC = $H [I^1 I^2 \dots\dots I^n // K]$

III. Decryption:

The receiver after receiving the cipher text C and the integer string I first verifies the hash value appended to the cipher text and the integer string is same or not. Then the receiver compares the calculated MAC value to the received MAC value to assure the authentication and non corruption of the file. After authenticating the received cipher text C and the integer string I divides the cipher text and integer string into blocks $C^{1(II)}$, $C^{2(II)}$, ……, $C^{n(II)}$ and I^1, I^2,…….. I^n each of length equal to the length of the hash value of the agreed hash function.

A. I stage Decryption:

The present cipher proposed here is symmetric cipher. Decryption starts from the first cipher block $C^{1(II)}$. The key for decrypting the first block is master key (agreed key) $K^{1(II)}= [K_1^{1(II)} K_2^{1(II)} \dots . K_l^{1(II)}]$ itself. The first cipher block $C^{1(II)}$ is decrypted as

$$M^1 = C^{1(II)} \oplus H[K^{1(II)}]$$

The keys for decryption of subsequent blocks are generated by the agreed upon procedure as described in section C, $K^{2(II)} = C^{1(II)} \oplus K^{1(II)}$,

$K^{3(II)} = C^{2(II)} \oplus K^{2(II)}$,……..

$K^{n(II)} = C^{(n-1)(II)} \oplus K^{(n-1)(II)}$,

The second block $C^{2(II)}$ is decrypted as

$M^2 = C^{2(II)} \oplus H[C^{1(II)} // K^{2(II)}]$

. In general $M^n = C^{n(II)} \oplus H[C^{(n-1)(II)} // K^{n(II)}]$

B. II Stage Decryption

In second stage the first stage decipher blocks are again decrypted using the arithmetic operation least common multiplier. All the decipher blocks of the first stage decryption M^1, M^2,…… M^n are reversed to constitute the input i.e., the cipher text blocks for the second stage decryption $C^{1R(I)}, C^{2R(I)}, \dots \dots . C^{nR(I)}$ Here I^1, I^2,……. I^n are the integer parts and $C^{1R(I)}$, $C^{2R(I)}$, $C^{3R(I)}$ …. $C^{nR(I)}$, the decimal numbers which are residue parts when adjusted to mod 128 in the first stage encryption. Consider the first residue block $C^{1R(I)} = [C_1^{1R(I)}, C_2^{1R(I)}, \dots\dots C_{l-1}^{1R(I)}, C_l^{1R(I)}]$ and the first integer string $I^1=[I_1^1, I_{2,\dots.} I_l^1]$. The key for decrypting of first block of the second stage

decryption K^1 is master itself. $K^{1(I)}=[K_1^{1(I)}K_2^{1(I)} \ldots K_l^{1(I)}]$ .The original numbers of the first block are obtained as

$C^{1(I)}=128*I^1+C^{1R(I)}$

i.e., $C_1^{1(I)}=128*I_1^1+C_1^{1R(I)}$

$C_2^{1(I)}=128*I_2^1+C_2^{1R(I)}$

……..

$C_l^{1(I)}=128*I_l^1+C_l^{1R(I)}$

Similarly original numbers of all the blocks are obtained as

$C^{2(I)}=128*I^2+C^{2R(I)}$ ..... $C^{n(I)}=128*I^n+C^{nR(I)}$

Then the decimal numbers of first plain text block $P^1=[P_1{}^1,P_2{}^1,\ldots P_l{}^1]$ are obtained as

$P_1{}^1= C_1{}^{1(I)}$-LCM $(K_2{}^1,K_3{}^1,\ldots K_l{}^1)$-$K_1{}^1$

$P_2{}^1= C_2{}^{1(I)}$-LCM$(K_1{}^1,K_3{}^1,\ldots K_l{}^1)$-$K_2{}^1$

.

.

$P_l{}^1=C_1{}^{1(I)}$-LCM$(K_1{}^1,K_2{}^1,\ldots K_{l-1}{}^1)$-$K_l{}^1$

Same decryption procedure is applied to all the cipher blocks in the second stage to obtain the plain text blocks $P^2,P^3\ldots P^n$. All the decimal numbers are coded to equivalent text characters using ASCII code table to get the original message.

IV. Example:

Before communicating the messages both the entities agree upon to use MD5 hash algorithm for encryption whose hash value is 32 bit length. Also they agree upon to use 32 decimal numbers (equal to the length of the hash value of MD5 algorithm) to act as the secret key for their communication that acts as the master key

Master key is [32 62 51 33 88 126 95 79 81 64 84 9 63 58 27 69 43 29 61 37 48 90 36 85 72 96 34 92 16 73 17 14]

Consider the message ANTIDISESTABLISHMENTARIANISM@@@ @PSEUDOPSEUDOHYPOPARATHYROIDISM @@. This text message is divided into two blocks each of length 32 characters (equal to the length of the hash value of MD5 algorithm).

ANTIDISESTABLISHMENTARIANISM@@@ @

PSEUDOPSEUDOHYPOPARATHYROIDISM@ @

Consider the first block [ANTIDISESTABLISHMENTARIANISM@@@ @].

The first stage cipher for the first block using simple mathematical operation Least Common Multiplier is [(space)LG(‘BSrTdtXBSH(0M8(SPACE)H80p0X XhDLEHDLEDLE].

The first stage cipher for the second block by using simple mathematical operation with different key that is generated from master key and first block cipher of the first stage is [+uiSO,u-RS*9NULNULOESC+BELDC3n7Ntb] OOANMs>1N]

After the first stage encryption of the two blocks, the blocks are reversed to constitute the input for the second stage encryption.

The second stage cipher for the first block using hash function and XOR is [ESCDC3FSYNd8m[R9w01I,5K3-EHTVrd[xEN QiBF&]

The second stage second cipher of the second block is [C4IrIDFEBUgtA8nDC3BEL(DC2CSOHSO:*RS DC1#y(HTox&]

V. Cryptanalysis and conclusions:

The main characteristic feature that differentiates one encryption from the other is the security of the data against all types of attacks, speed and efficiency. In the present paper a new encryption technique using simple arithmetic operation least common multiplier and one way ash function. The principal intention behind the proposed technique is to implement and achieve better security using simple arithmetic operation. In this encryption scheme data is encrypted in blocks. Encryption keys are different for different blocks. The key for first block is master key itself. The keys for second and subsequent blocks are generated by concatenating the master key with the preceding cipher blocks. This technique has an advantage that even if a single sub key is broken all the other are safe. Conventional encryption algorithms involve arithmetic operations on integers like greatest common divisors, modular arithmetic and number theory. Usage of simple one-way hash function does not provide the required security for the algorithm. Linear cryptanalysis is a viable attack against one-way hash function. Security of the algorithm depends on both the one-way hash function and the key. In addition the hash function should be collision resistant. Since the key is secret between the participating entities the cipher is strong against collision attack. After the first stage encryption all the cipher blocks are reversed to contribute the input for the second stage. Previous cipher block is concatenated with the present block key except for the first block. Due to the reversal of the cipher blocks at the second stage and concatenation process the present designed cipher has achieved a good avalanche effect the most desirable property of a good encryption algorithm.

VI. References :

[1] Bart PRENEEL, "Analysis and Design of Cryptographic Hash Functions," Doctoral dissertation, February 2003

[2] Y. Zheng, T. Matsumoto, and H. Imai, "Structural properties of one-way hash functions," Advances in Cryptology, Proc. Crypto'90, LNCS 537 , S. Vanstone,Ed., Springer-Verlag, 1991, pp. 285–302.

[3] B. den. Boer, A. Bosselaers. Collisions for the compression function of MD5, Advances in Cryptology, Eurocrypt'93 Proceedings, Springer-Verlag, 1994.

[4] Mihir Bellare, Joe Kilian, Phillip Rogaway, "The Security of the Cipher Block Chaining Message Authentication Code", Journal of Computer and System Sciences, 61-362 – 399 , 2000.

[5] M Bellare, R Canetti, H Krawczyk, "Keying hash functions for message authentication", Crypto, 1996 - Springer

[6] John Black, Phillip Rogaway, and Tom Shrimpton, "Black box analysis of the block-cipher-based hash-functions constructions from PGV" Proc. of CRYPTO'02, Lecture Notes in Computer Science 2442, Springer, pp. 320–335, 2002.

[7] Magnus Daum and Stefan Lucks, "Attacking hash functions by poisoned messages," EUROCRYPT rump session, 2005. Available from www.cits.rub.de/MD5Collisions/

[8] Daniel R. Simon, "Finding collisions on a one-way street: Can secure hash functions be based on general assumptions?" Proc. of EUROCRYPT'98, Lecture Notes in Computer Science 1403, Springer, pp. 334–345, 1998. Available from research. microsoft.com/crypto/dansimon/me.html

[9] Areej Omar Baalghusun, Olfa Fahad Abusalem, Zahra Abbas Al Abbas, Jayaprakash Kar, "Authenticated Key Agreement Protocols: A Comparative Study, Journal of Information Security, 2015, 6, 51-58

[10] Abdalla, M and M.Bellare,2000. "Increasing the lifetime of a key: A comparative analysis for the security of rekeying techniques" proceeding of Asiacrypt2000,ser LNCC,t.okamoto,Ed,vol,1976,springer verlag

[11] A text book of Applied Cryptography by Bruce Schneier, John Wiley & Sons

[12] ISO/IEC 9797, "Information technology Data cryptographic techniques – Data integrity mechanisms using a cryptographic check function employing a block cipher algorithm," 1993

[13] Elena Andreeva, Bart Mennink, and Bart Preneel, "Security Reductions of the Second Round SHA-3 Candidates. In ISC '11, volume 6531 of LNCS, pages 39{53. Springer-Verlag, 2011.

[14] Ilya Mironov,Hash functions:Theory,attacks and applications,Microsoft Research,Silicon Valley Campus,2005.

[15] Antoine Joux,"Multicollisions in iterated hash functions. Application to cascaded constructions", Proc.of CRYPTO 2004, LNCS 3152, Springer, pp.306-316, 2004.