A Combined Method for Confidentiality, Integrity, Availability and Authentication (CMCIAA)

Neeta Wadhwa, Syed Zeeshan Hussain and S.A.M Rizvi

Abstract **---This paper introduces a single method that ensures the Confidentiality, Integrity, Availability and Authentication of the message to be transmitted. Message is encrypted by the latest symmetric encryption standard called AES (Advanced Encryption Standard). A new method for calculating MAC (Message Authentication Code) based on the shared secret key used in AES, is proposed that proves the message integrity and authentication. The proposed method consists of very simple steps, therefore would have lesser overhead and low complexity, as compared to the standard algorithms of calculating MAC. So this method can be used to achieve all the main goals of Cryptography by a single mean.**

Index Terms **--- Authentication, Confidentiality, Encryption, Integrity, MAC.**

I. INTRODUCTION

In today's Information age, reliance on the Internet become the need for exchanging information of all kinds. Information travelling on the Internet is accessible to all so its security is one of the foremost concerns of the digital world.

A. Cryptography

It is an art and science of secret writing. The message to be transmitted (called as plaintext) is first converted into an unintelligible form (called as ciphertext) by the means of cryptographic methods and then it is transmitted on the computer networks. The receiver got the ciphertext and converted it into the plaintext by the means of same cryptographic methods in the reverse manner [1].This way the only sender and receiver can read the original message and no one can intercept it on the way while transmission.

B. Concept Of MAC (Message Authentication Code)

MAC is a keyed hash function. They take the variable length message as input and produce the fixed size hash for all messages of different lengths [2]. It is used to verify the integrity and authentication of the message. The security of hash functions is determined by the size of hash they produced. The best known attack against these functions, the "birthday attack", can find a pair of messages having a same hash value with a work factor of 2n/2 approximately.

C. Goals of Cryptography

The main goals of cryptography are [1, 2]:

Confidentiality: The message could be read only by the intended recipients, this is the first goal of cryptography.

Integrity: The message should reach the intended receiver exactly same as the sender sends, no alteration could be done during the transit.

Authentication: It proves that the sender is the original sender means an eavesdropper could not pose himself as the sender.

Availability: All the 3 goals are the requirement of secure digital communication but the process of achieving these goals should not hinder the performance of the applications. Thus, it means these processes should have overhead (in terms of speed and memory) as low as possible.

The rest of the paper is organized as follows: Section 2 describes the related studies. The new method is described in the Section 3. Section 4 discusses the complexity analysis of the proposed method. Finally, conclusion and future work is given in the Section 5.

II. RELATED STUDY

Many combined methods have been introduced to achieve one or the other goals of cryptography like:

A new combined encryption and lossless compression algorithm for the encryption of large images is proposed in [3]. The crypto-compression scheme used in the new method is based on a cascade of Radon projection [4] which enables fast encryption of a large amount of digital data. The proposed method also takes advantage of the Mojette transform [5] properties that can easily be included in distributed storage architecture.

A new algorithm is proposed that provides security against chosen - plaintext [6]. The basic idea behind the new method is to use the original message itself as a time-varying key. Thus, in contrast to the traditional key

Manuscript received March 23, 2013; revised April 07, 2013.

N. Wadhwa, Research Scholar in Department of Computer Science, Jamia Millia Islamia, New Delhi, India and Assistant Professor in Department of Computer Science and Engineering, Echelon Institute of Technology, Faridabad, India. (phone: 09289410042; email: neeta.088@gmail.com).

Dr. S. Z. Hussain is with the Department of Computer Science, Jamia Millia Islamia, New Delhi, India (email: szhussain@rediffmail.com)

Dr. S. A. M Rizvi is with the Department of Computer Science, Jamia Millia Islamia, New Delhi, India (email: samsam_rizvi@yahoo.com)

algorithms, one of the keys in the algorithm presented depends on the message itself. Two encryption matrices are generated by means of Singular Value Decomposition (SVD) [7, 8], using a portion of the message. And then one of the key is calculated.

These new techniques work on speed v/s security tradeoff of the encryption algorithms. The present work introduces a new method that may achieve all the goals (Confidentiality, Integrity, Authentication, Availability) of cryptography by satisfying the speed v/s security tradeoff.

III. PROPOSED METHOD [CMCIAA]

AES is a Non-Feistel symmetric cipher. It encrypts 128 bit block size with 128/192/256 bit key for 10/12/14 rounds. The complete specification of AES encryption scheme is given in [9, 10, 11].

The proposed method uses AES for encryption. As, AES is a symmetric cipher, the sender and receiver have to share the secret key 'K' of 128 bit prior to the communication.

A. At Sender Side

1. The plaintext message 'M' is divided into 128 bit blocks P1, P2, P3……Pn. Padding of 0's or 1's should be done to make the plaintext as an exact multiple of 128.
2. The current date and time in 128 bit format is appended as the last block of plaintext (Pn+1).
3. The plaintext blocks P1, P2, P3…….Pn, Pn+1 are encrypted by AES using 128 bit key 'K' and converted in to C1,C2,C3…..Cn, Cn+1.
4. 128 bit P1 is divided in to four 32bit words W1, W2, W3 and W4.
5. a. W1 * T mod 2^{32} results in W1'.
   b. W2 * D mod 2^{32} results in W2'.
   c. W3 * RotShift $_{24}$(W4) mod 2^{32} results in W3'.
   d. W4 * RotShift $_{24}$ (W3) mod 2^{32} results in W4'.

W1 is multiplied by current time (T) mod 2^{32}, W2 is multiplied by current date (D) mod 2^{32}, W3 is multiplied by RotShift $_{24}$(W4) mod 2^{32} and W4 is multiplied by RotShift $_{24}$(W3) mod 2^{32}.

Where **RotShift $_{24}$(W) mod 2^{32} = RotateRight 'W' by 24bits $\oplus$ LeftShift 'W' by 24 bits.**

6. Calculate W1' $\boxplus$ W3'= V1 mod 2^{32} and W2' $\boxplus$ W4' = V2 mod 2^{32}.
7. H (P1) = V1 $\boxplus$ V2 $\boxplus$ K [first 32 bits] mod 2^{32}.
8. Similarly, H(P2), H(P3)……H(Pn) of 32 bit each is calculated . So H $_K$ (M) = H(P1), H(P2), H(P3)……H(Pn).
9. The sender sends, H_K (M) ||E $_K$ (M), Hash, H_K (M) and Ciphertext, C= E_K (M) = C1, C2, C3…… Cn+1 to the receiver.

B. At Receiver Side

1. Receiver got E_K (M) and H_K (M) as Cipher text and Hash of the original message M.
2. Receiver first decrypts the message with the shared key 'K' and deduce plaintext P = D $_K$ (M).
3. After decryption he got the date and time at which the sender did the encryption, at the end of the message.
4. Then the same steps 4 to 8 (of sender side) are followed to calculate the H' $_K$ (M) at the receiver side.
5. Verify H $_K$ (M) = H' $_K$ (M). If they are same, it proves the integrity of the message means the message is not altered on the way. And receiver got the same message as the sender sends.

C. Flowchart of Proposed Method

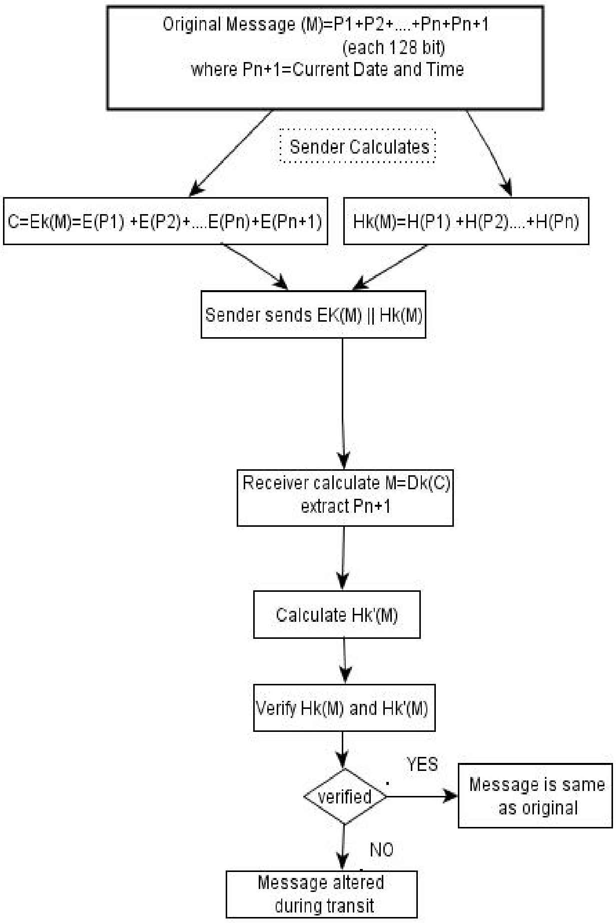
Original Message (M)=P1+P2+....+Pn+Pn+1
(each 128 bit)
where Pn+1=Current Date and Time
Sender Calculates
C=Ek(M)=E(P1) +E(P2)+....E(Pn)+E(Pn+1)
Hk(M)=H(P1) +H(P2)....+H(Pn)
Sender sends EK(M) || Hk(M)
Receiver calculate M=Dk(C)
extract Pn+1
Calculate Hk'(M)
Verify Hk(M) and Hk'(M)
verified
YES
Message is same as original
NO
Message altered during transit

Fig 1: Flowchart of Proposed Method

Here E: Encryption Algorithm AES -128
K: 128bit shared secret key between sender and receiver.
H: Proposed MAC algorithm.

D. Flowchart of proposed MAC Algorithm

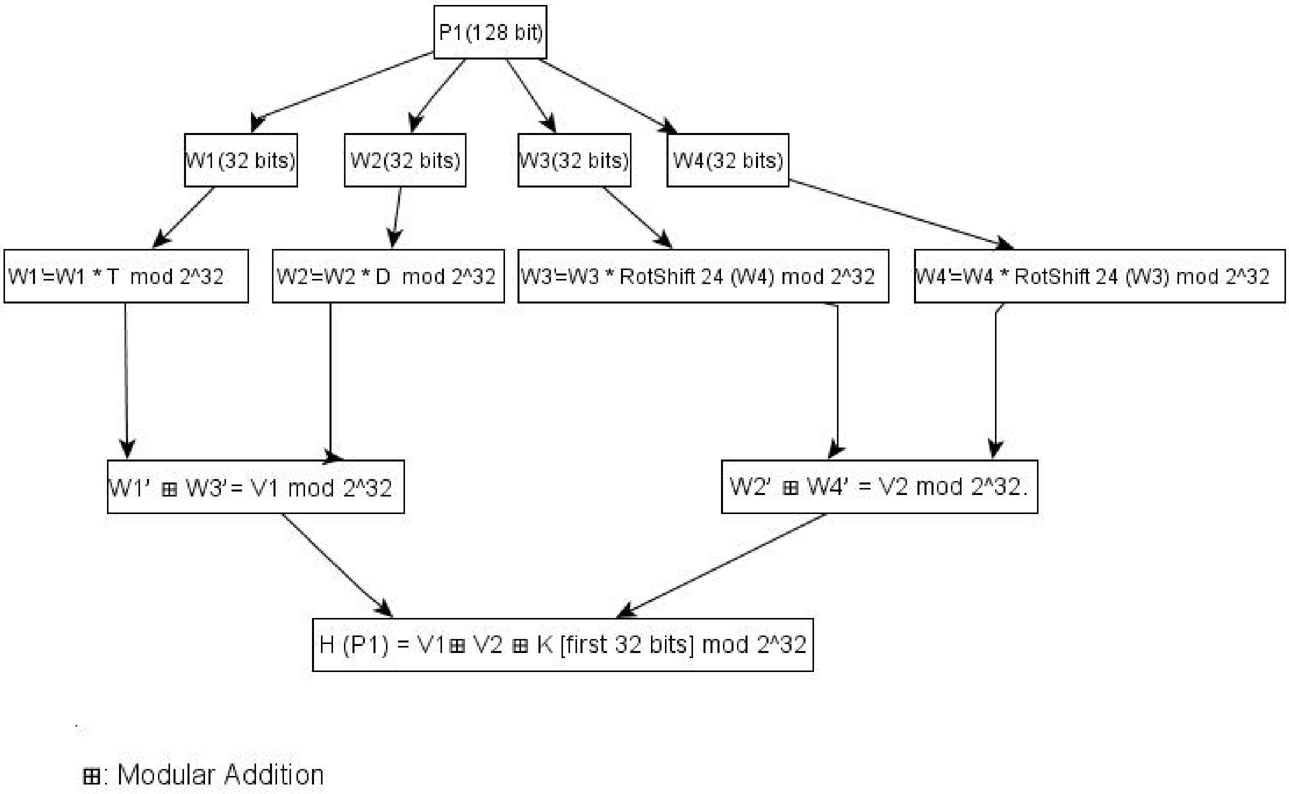

Fig 2: Flowchart of Proposed MAC algorithm

Here D and T: Date and Time at which encryption is done.
Similarly, H(P2), H(P3)….H(Pn) are calculated and Hk(M) = H(P1) + H(P2)+ H(P3)+….+H(Pn).

IV. COMPLEXITY ANALYSIS OF PROPOSED ALGORITHM

AES is a block cipher and it encrypts the same block size every time so its computational complexity is constant. The cryptographic complexity analysis of encryption algorithms is done on the concept that how much effort is required to break the algorithm as algorithms are public their security lies in the secret key. So complexity of an encryption algorithm is based on their key size like AES has complexity of 2^{128}, as its key size is 128 bits.

Similarly, cryptographic complexity analysis of Hash algorithms is based on the size of the output they produced. The hash produced by **CMCIAA**, is always 1/4th of the length of the original message. It is in contrast with the standard MAC algorithms as they always produce the hash of fixed length, does not matter what is the length of the original messages. So, cryptographic complexity analysis of **CMCIAA** is based on the size of the message for which it is producing hash. Longer the message, more secure the hash produced. Moreover, users have to share the single secret key for encryption and authentication both.

The proposed method uses random data (date and time) while producing MAC of the given message. This feature can make it more resistant to collision attacks and pre-image attacks.

V. CONCLUSION AND FUTURE WORK

The proposed method may be used to achieve all the main goals of cryptography by a single mean. **CMCIAA** consists of very simple steps with no rounds as compared to the standard hash and MAC algorithms. It would definitely have low overhead, so the objective of availability would be achieved. Encryption is done with the latest secure encryption standard AES, so Confidentiality is assured. **CMCIAA** produces hash of the message by using shared secret key, it is a keyed hash algorithm, so integrity and authentication goals are also achieved.

The proposed method will be implemented and its speed v/s security analysis will be done by performing various experiments in the next paper.

REFERENCES

[1] Bruce Schneier, **Applied Cryptography: Protocols, Algorithms, and Source Code in C** , John Wiley & Sons, 1996.

[2] B. Schneier, *Practical Cryptography,* Wiley, 2003.

[3] Zou Jian-cheng, Tie Xiao-yun, "Arnold transformation of digital image with two- dimensions and its periodicity", Journal of North China , University of Technology, 2000, pp. 12-15.

[4] F. Autrusseau, B. Parrein, and M. Servieres, "Lossless compression based on a discrete and exact radon transform: A preliminary study," in *ICASSP*, 2006, pp. 466 – 468.

[5] F. Autrusseau, J. P. Guedon and Y. Bizais, "Watermarking and cryptographic schemes for medical imaging," in *SPIE Medical Imaging*, 2003, pp. 532–105.

[6] Chung-Ping Wu and C. C. Jay Kuo, "Design of integrated multimedia Compression and encryption systems," IEEE Transactions on Multimedia, vol. *7,* no. 5, 2005, pp. 828–839.

[7] S. H. Jensen, P. C. Hansen, S. D. Hansen, and J. Aa. Sre̍nsen, "Reduction of broad-band noise in speech by truncated qsvd," IEEE Transactions on Speech and Audio Processing, vol. 46, no. 6, 1995, pp.1737–1741.

[8] P. C. Hansen and S. H. Jensen, "FIR filter representations of reduce-rank noise reduction," *IEEE* Transactions on Signal Processing, vol. 46, 1998, pp. 1737–1741.

[9] Daemen J, Knudsen LR, Rijmen V, " The block cipher SQUARE. Fast Software Encryption, Proc. Fourth International Workshop, 1997 LNCS 1267, Springer- Verlag: 149-165.

[10] Daemen J, RijmenV (1999) AES Proposal: Rijndael. First Advanced Encryption Standard (AES) Candidate Conference, National Institute of Standards and Technology (NIST). http://csrc.nist.gov/encyprtion/aes/rijndael/. Accessed July 2012

[11] FIPS 197 (2001) , Advanced Encryption Standard (AES). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. Accessed July 2012