A SECURE DIGITAL SIGNATURE SCHEME WITH FAULT TOLERANCE BASED ON THE IMPROVED RSA SYSTEM

H. Elkamchouchi[1], Heba G. Mohamed[2], Fatma Ahmed[3] and Dalia H. ElKamchouchi[4]

[1]Dept. of Electrical engineering, Faculty of Engineering, Alexandria University, helkamchouchi@ieee.org
[2]Dept. of Electrical engineering, Arab Academy for Science and Technology (AAST), heba.g.mohamed@gmail.com
[3]Dept. of Electrical engineering, Faculty of Engineering, Alexandria University, moonyally@yahoo.com
[4]Dept. of Electrical engineering, Faculty of Engineering, Alexandria University, Daliakamsh@yahoo.com

ABSTRACT

Fault tolerance and data security are two important issues in modern communication systems. In this paper, we propose a secure and efficient digital signature scheme with fault tolerance based on the improved RSA system. The proposed scheme for the RSA cryptosystem contains three prime numbers and overcome several attacks possible on RSA. By using the Chinese Reminder Theorem (CRT) the proposed scheme has a speed improvement on the RSA decryption side and it provides high security also.

KEYWORDS

Digital Signature, Fault tolerance, RSA Cryptosystem, Security Analysis

1. INTRODUCTION

Digital signature schemes with fault tolerance make it possible for error detections and corrections during the processes of data computations and transmissions. Recently, Zhang, in 1999 [1] Lee and Tsai, in 2003[2] have respectively proposed two efficient fault-tolerant schemes based on the RSA cryptosystem. Both of them can efficiently check the sender's identity and keep the confidentiality of the transmitted document. Furthermore, they can detect the errors and correct them. However, these schemes have a common weakness in security, that is, different messages may easily be computed that have the same signature. Thus, a valid signature could be reused in another document.

The vulnerability of Zhang's scheme was pointed out by Iuon-Chang Lei et. Al [3], i.e. a pernicious client could produce an alternate message with the same signature by permuting the rows or columns in the original message matrix *X*. They suggested a new method; this is certainly

Natarajan Meghanathan et al. (Eds) : ICAIT, CRYPIS, NC, ITCSE-2016
pp. 35–44, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.60704

improved of Zhang's scheme in which the original message matrix is multiplied by two prime matrices with the same length of the original message. Next for the resulting matrix hash value is calculated to determine which digital signature it is. Afterwards, the checksum calculated for each row and column is inserted at the end of the original matrix. The hash value is appended to the last position of the matrix. The resulting (m+1) × (n+1) matrix is converted into ciphertext and sent to the desired user. They showed that a pernicious client cannot forge a valid message with the same signature by permuting the rows and columns in the matrix.

In 2013, Shreenath Acharya, Sunaina Kotekar and Seema S Joshi [4] have improved the mechanism of Iuon-Chang Lei et. Al with providing extra security by making use of transpose matrix based on the RSA. If a malicious looks into the message he will find it difficult to understand or calculate checksum/ hash value, thus it will confuse the malicious. To keep the confidentiality of the data that transfers over a public network R. Rivest et. al [5] have proposed RSA technique as a public key cryptosystems. According to the proposed scheme, the sender can use the receiver's public key to encrypt a message and the receiver can use his secret key to decrypt the encrypted message. Also, they conveyed that a message can be signed with the secret key of the sender and the signature can be verified by any receiver using the sender's public key. As a result the RSA technique is useful in keeping the confidentiality of the transmitted message, verifying the integrity of the received message, and to prove the sender's identity.

In 2014, [6] Nikita Somani and Dharmendra Mangal have proposed a new security scheme for the RSA cryptosystem contains three prime numbers and overcome several attacks possible on RSA. The new scheme has a speed improvement on the RSA decryption side by using the Chinese Reminder Theorem (CRT). This paper addresses a secure and efficient digital signature scheme with fault tolerance based on the improved RSA system. The remaining parts of this paper are organized as follows: In Section 2, we elaborate Improved of Zhang's scheme. Next, we discuss the improved of the standard RSA in Section 3. In Section 4, we proposed our scheme. We analyze the security properties and common attacks of our proposed scheme in Section 5. Finally, in Section 6, we give our conclusion.

2. IMPROVED VERSION OF ZHANG'S SCHEME

Improved version of Zhang's digital signature scheme [4] with fault tolerance is based on the RSA cryptography. In the RSA cryptography, each user provides a public key (e, N) and a secret key d, where N is the product of two large prime numbers p and q such that $N = p \times q$, and the public key e and secret key d must satisfy the equation $d = e^{-1}(p-1)(q-1)$. Let (e_A, N_A) and (e_B, N_B) be the public keys of user A and user B, d_A and d_B are their secret keys. Moreover, assume $N_A \neq N_B$ and the length of N_A and N_B are the same for simplification. An improved algorithm is as shown. Here the original message matrix is not directly encrypted. But the transpose of the message matrix is taken and then encrypted. As observed in the result part though anyone tries to decrypt the message it is not the clear message line by line. Suppose that user B wants to send a message X to user A,

Algorithm 1:

Step1: User B sends an n×m message matrix to X user A:

$$X = \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1m} \\ x_{21} & x_{22} & \cdots & x_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \dots & x_{nm} \end{pmatrix}$$

Where $x_{ij}, 1 \le i \le n, 1 \le j \le m,$ is a message block which has the same length as N_A and N_B

Step 2: Now we take the transpose of the original matrix:

$$T = \begin{pmatrix} t_{11} & t_{12} & \dots & t_{1n} \\ t_{21} & t_{22} & \cdots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t_{m1} & t_{m2} & \dots & t_{mn} \end{pmatrix} = \begin{pmatrix} x_{11} & x_{21} & \dots & x_{n1} \\ x_{12} & x_{22} & \cdots & x_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{1m} & x_{2m} & \dots & x_{nm} \end{pmatrix}$$

Step 3: User B then creates two prime number matrix P and Q as follows:

$$P = \begin{pmatrix} p_1 & p_2 & \dots & p_n \\ p_1 & p_2 & \cdots & p_n \\ \vdots & \vdots & \ddots & \vdots \\ p_1 & p_2 & \dots & p_n \end{pmatrix} \quad , \quad Q = \begin{pmatrix} q_1 & q_1 & \dots & q_1 \\ q_2 & q_2 & \cdots & q_2 \\ \vdots & \vdots & \ddots & \vdots \\ q_m & q_m & \dots & q_m \end{pmatrix}$$

Where matrix P and Q both have the same dimensions with the message matrix T, which is a (m × n) matrix.

Step 4: The sender *B computes* a new message matrix $\bar{X}$ which is the entry-wise product of the matrix T, *P* and *Q:*

$$\bar{T} = \begin{pmatrix} t_{11} & t_{12} & \dots & t_{1n} \\ t_{21} & t_{22} & \cdots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t_{m1} & t_{m2} & \dots & t_{mn} \end{pmatrix} \begin{pmatrix} p_1 & p_2 & \dots & p_n \\ p_1 & p_2 & \cdots & p_n \\ \vdots & \vdots & \ddots & \vdots \\ p_1 & p_2 & \dots & p_n \end{pmatrix} \begin{pmatrix} q_1 & q_1 & \dots & q_1 \\ q_2 & q_2 & \cdots & q_2 \\ \vdots & \vdots & \ddots & \vdots \\ q_m & q_m & \dots & q_m \end{pmatrix}$$

$$= \begin{pmatrix} t_{11} \times p_1 \times q_1 & t_{12} \times p_2 \times q_1 & \dots & t_{1n} \times p_n \times q_m \\ t_{21} \times p_1 \times q_2 & t_{22} \times p_2 \times q_2 & \cdots & t_{2n} \times p_n \times q_m \\ \vdots & \vdots & \ddots & \vdots \\ t_{m1} \times p_1 \times q_m & t_{m2} \times p_2 \times q_m & \dots & t_{mn} \times p_n \times q_m \end{pmatrix}$$

$$= \begin{pmatrix} \bar{t}_{11} & \bar{t}_{12} & \dots & \bar{t}_{1n} \\ \bar{t}_{21} & \bar{t}_{22} & \cdots & \bar{t}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{t}_{m1} & \bar{t}_{m2} & \dots & \bar{t}_{mn} \end{pmatrix}$$

Step 5: For the message matrix $\bar{T}$, the sender B now constructs an (n+1)*(m+1) matrix T_h as follows:

$$T_h = \begin{pmatrix} \bar{t}_{11} & \bar{t}_{12} & \dots & \bar{t}_{1n} & T_1 \\ \bar{t}_{21} & \bar{t}_{22} & \cdots & \bar{t}_{2n} & T_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \bar{t}_{m1} & \bar{t}_{m2} & \cdots & \bar{t}_{mn} & T_m \\ T_1 & T_2 & \cdots & T_n & h \end{pmatrix}$$

Where,

$$T_i = \prod_{j=1}^{n} t_{ij} * p_j \bmod N_B \text{ , for } 1 \le i \le m \text{ , } T_j = \prod_{i=1}^{m} t_{ij} * q_i \bmod N_B \text{ , for } 1 \le j \le n \text{ and}$$

$$h = \prod_{j=1}^{n} \left(\prod_{i=1}^{m} t_{ij} \bmod N_B \right) \bmod N_B$$

Step 6: The sender B computes an (n+1)*(m+1) ciphered matrix as follows:

$$C_h = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} & c_1 \\ c_{21} & c_{22} & \cdots & c_{2n} & c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} & c_m \\ c_1 & c_2 & \cdots & c_n & h_c \end{pmatrix}$$

Where,

$c_{ij} = \bar{t}_{ij}^{\,e_A} mod\ N_A$, $C_i = T_i^{\,e_A} mod\ N_A$, $C_j = T_j^{\,e_A} mod\ N_A$, $h_c = h^{d_B} mod\ N_B$, *for all* $1 \le i \le n, 1 \le j \le m$

Note that T_i and T_j are the checksums and C_i and C_j are the ciphered checksums.

Step 7: The receiver A uses his/her secret key d_A to decrypt C_h and obtains decrypted message as follows:

$$\bar{T}_h = \begin{pmatrix} \bar{t}_{11} & \bar{t}_{12} & \cdots & \bar{t}_{1n} & \bar{T}_1 \\ \bar{t}_{21} & \bar{t}_{22} & \cdots & \bar{t}_{2n} & \bar{T}_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \bar{t}_{m1} & \bar{t}_{m2} & \cdots & \bar{t}_{mn} & \bar{T}_m \\ \bar{T}_1 & \bar{T}_2 & \cdots & \bar{T}_m & \bar{h} \end{pmatrix}$$

Step 8: Now the receiver A verify the checksum to check the following:

$$\bar{T}_i = \prod_{j=1}^{n} \bar{t}_{ij} * p_j \bmod N_B \text{ , for } 1 \le i \le m$$

$$\bar{T}_j = \prod_{i=1}^{m} \bar{t}_{ij} * q_i \bmod N_B \text{ , for } 1 \le j \le n$$

$$\bar{h} = \prod_{j=1}^{n} \left(\prod_{i=1}^{m} \bar{t}_{ij} \bmod N_B \right) \bmod N_B$$

If the verifications are positive, then the receiver believes that the message was not altered during the transmission. Otherwise, there are some errors in the decrypted message.

Step 9: Then user *A* can detect the error by the following two equations

$$\bar{T}_k \neq \prod_{j=1}^{n} \bar{t}_{ij} * p_j \bmod N_B \text{ , for } 1 \le i \le m$$

$$\bar{T}_l \neq \prod_{i=1}^{m} \bar{t}_{ij} * q_i \, mod N_B \, , for \; 1 \leq j \leq n$$

Assuming that the error occurs in the message block $\bar{t}_{kl}$ then, user *A* can correct the error by computing one of the following equations:

$$\bar{t}_{kl} = \bar{T}_k \times \left(\prod_{j=1, j \neq l}^{n} \bar{t}_{kj} \right)^{-1} mod \; N_B$$

$$\bar{t}_{kl} = \bar{T}_l \times \left(\prod_{i=1, i \neq k}^{n} \bar{t}_{il} \right)^{-1} mod \; N_B$$

Step 10: The receiver A takes the transpose of the matrix which will result in message as follows:

$$X_h = \begin{pmatrix} \bar{t}_{11} & \bar{t}_{21} & \cdots & \bar{t}_{m1} \\ \bar{t}_{12} & \bar{t}_{22} & \cdots & \bar{t}_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{t}_{1n} & \bar{t}_{2n} & \cdots & \bar{t}_{mn} \end{pmatrix} = \begin{pmatrix} \bar{x}_{11} & \bar{x}_{12} & \cdots & \bar{x}_{1m} \\ \bar{x}_{21} & \bar{x}_{22} & \cdots & \bar{x}_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{x}_{n1} & \bar{x}_{n2} & \cdots & \bar{x}_{nm} \end{pmatrix}$$

3. IMPROVEMENTS OVER THE STANDARD RSA

The improved RSA scheme provides an enhancement of the Hamami and Aldariseh [7] method by improving the speed on the RSA decryption side and also provides the security by avoiding some attacks possible on RSA. If the same message is encrypted more than one time it will look different every time by using the random number k. The general idea of the improved scheme is to use the Key generation algorithm of Hamami and Aldariseh method and proposed a scheme for encryption and decryption algorithm. The existence of three prime numbers, the difficulty of analysis of variable n must be increases and the key generation time must be reduces. The algorithm for the proposed scheme is as follows:

3.1 Key Generation for Improved RSA Scheme

To generate the key using three prime numbers, user B should do the following:

a) Generate three large prime numbers p, q, and s.
b) Calculate $n = p \times q \times s \;\; and \;\; \varphi(n) = (p-1)(q-1)(s-1)$.
c) Select *e* such that $(e, \varphi(n))$are relatively co-prime.
d) Get the value of d by using $ed \; mod \; \varphi(n) = 1$.
e) Find $d_p = d \; mod(p-1), d_q = d \; mod(q-1), \;\; d_s = d \; mod(s-1)$.
f) Public Key $K_u < e, n >$ and Private Key $K_r < d, p, q, s, d_p, \; d_q, \; d_s >$.

3.2 Encryption Algorithm

To encrypt the message M user A should do the following:
User A should obtained the public key of user B <e, n>

a) Represent the message M as an integer form in interval [0 to n-1].
b) Select k as a random integer $GCD(k, n) = 1$ and 1< k < n-1.
c) Compute C1=$k^e \; mod \; n$.

d) Compute C2=$M^e k \ mod \ n$.
e) Send the cipher text values (C1, C2) to user A

3.3 Decryption Algorithm

On decryption process the concept of RSA is used with CRT. To recover the message from cipher text C2 user A should do the following:

a) Calculate $C_p = C1 \ mod \ p, \ \ C_q = C1 \ mod \ q, \ C_s = C1 \ mod \ s$ and then calculate $k_p = {C_p}^{d_p} \ mod \ p, k_q = {C_q}^{d_q} \ mod \ q \ \ and \ k_s = {C_s}^{d_s} \ mod \ s.$
b) By using the formula calculate k
$k = [\ k_p.(qs)^{(p-1)} \ mod \ n + \ k_p.(ps)^{(q-1)} \ mod \ n + \ k_s.(pq)^{(s-1)} \ mod \ n].$
c) By using the Euclidean algorithm, calculate the value of the unique integer
$t * k \ mod \ n = 1$ and 1< t < n.
d) Then compute M^e, C2*t = (M^e.k)*t = (M^e) k*t = $M^e \ mod \ n$.
e) For getting the value of message M should do the following steps
First calculate $\grave{C}_p = M^e \ mod \ p, \ \grave{C}_q = M^e \ mod \ q, \grave{C}_s = M^e \ mod \ s$ and then calculate $M_p = \grave{C}_p \ mod \ p, M_q = \grave{C}_q \ mod \ q \ , M_s = \grave{C}_s \ mod \ s.$
f) Finally, recover the message M by using the following formula:
$M = [\ M_p.(qs)^{(p-1)} \ mod \ n + \ M_p.(ps)^{(q-1)} \ mod \ n + \ M_s.(pq)^{(s-1)} \ mod \ n].$

4. PROPOSED SCHEME

We propose a secure and efficient digital signature scheme with fault tolerance based on the improved RSA system. In the RSA cryptography, each user provides a public key (*e*, *N)* and a secret key *d,* where *N* is the product of three large prime numbers $p, q \ and \ s$ such that $N = p \times q \times s$, and the public key *e* and secret key *d* must satisfy the equation $d = e^{-1}(p-1)(q-1)(s-1)$.

Algorithm 2:
Step 1to5: Same as Algorithm 1
Step 6: Compute the following ciphertext matrix:
a) Select k as a random integer $GCD(k, N_B) = 1$ and 1< k < $N_B - 1$.
b) Compute C1 = $k^{e_A} \ mod \ N_A$.
c) Compute C2 = ${T_h}^{e_A} k \ mod \ N_A$.

$$C2 \ = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} & c_1 \\ c_{21} & c_{22} & \dots & c_{2n} & c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_{m1} & c_{m2} & \dots & c_{mn} & c_m \\ c_1 & c_2 & \dots & c_n & h_c \end{pmatrix} * k$$

Where,
$c_{ij} = \bar{t}_{ij}^{\ e_A} \ mod \ N_A, \ C_i = {T_i}^{e_A} mod \ N_A, C_j = {T_j}^{e_A} \ mod \ N_A, \ \ h_c = h^{d_B} mod \ N_B,$
for all $1 \le i \le n, 1 \le j \le m$
d) Send the cipher text values (C1, C2) to user A

Step 7: To recover the message T_h from cipher text C2 user A should do the following:

a) Calculate $C_p = C1 \ mod \ p, \quad C_q = C1 \ mod \ q, \ C_s = C1 \ mod \ s$ and then calculate

$k_p = {C_p}^{d_p} \bmod p, k_q = {C_q}^{d_q} \bmod q \ \text{and} \ k_s = {C_s}^{d_s} \bmod s.$

b) By using the formula calculate k
$k = [\, k_p.(qs)^{(p-1)} \bmod N_A + k_p.(ps)^{(q-1)} \bmod N_A + k_s.(pq)^{(s-1)} \bmod N_A \,].$

c) By using the Euclidean algorithm, calculate the value of the unique integer t, $t * k \bmod N_A = 1$ and $1< t <N_A$.

d) Then compute ${T_h}^{e_A}$, C2*t = (${T_h}^{e_A}$.k)*t = (${T_h}^{e_A}$) k*t = ${T_h}^{e_A} \bmod N_A$.

e) For getting the value of message M should do the following steps
First calculate $\dot{C}_p = {T_h}^{e_A} \bmod p$, $\dot{C}_q = {T_h}^{e_A} \bmod q$, $\dot{C}_s = {T_h}^{e_A} \bmod s$ and then calculate $T_p = \dot{C}_p \bmod p, T_q = \dot{C}_q \bmod q\ , T_s = \dot{C}_s \bmod s.$

f) Finally, recover the message T_h by using the following formula:
$T_h = [\, T_p.(qs)^{(p-1)} \bmod N_A + T_p.(ps)^{(q-1)} \bmod N_A + T_s.(pq)^{(s-1)} \bmod N_A].$

$$\bar{T}_h = \begin{pmatrix} \bar{t}_{11} & \bar{t}_{12} & \cdots & \bar{t}_{1n} & \bar{T}_1 \\ \bar{t}_{21} & \bar{t}_{22} & \cdots & \bar{t}_{2n} & \bar{T}_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \bar{t}_{m1} & \bar{t}_{m2} & \cdots & \bar{t}_{mn} & \bar{T}_m \\ \bar{T}_1 & \bar{T}_2 & \cdots & \bar{T}_m & \bar{h} \end{pmatrix}$$

Step 8: Now the receiver A verify the checksum to check the following:

$$\bar{T}_i = \prod_{j=1}^{n} \bar{t}_{ij} * p_j \bmod N_B\ , for\ 1 \le i \le m$$

$$\bar{T}_j = \prod_{i=1}^{m} \bar{t}_{ij} * q_i \bmod N_B\ , for\ 1 \le j \le n$$

$$\bar{h} = \prod_{j=1}^{n} \left(\prod_{i=1}^{m} \bar{t}_{ij} \bmod N_B \right) \bmod N_B$$

If the verifications are positive, then the receiver believes that the message was not altered during the transmission.

Step 9: The receiver A takes the transpose of the matrix which will result in message as follows:

$$\bar{X} = \begin{pmatrix} \bar{t}_{11} & \bar{t}_{21} & \cdots & \bar{t}_{m1} \\ \bar{t}_{12} & \bar{t}_{22} & \cdots & \bar{t}_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{t}_{1n} & \bar{t}_{2n} & \cdots & \bar{t}_{mn} \end{pmatrix} = \begin{pmatrix} \bar{x}_{11} & \bar{x}_{12} & \cdots & \bar{x}_{1m} \\ \bar{x}_{21} & \bar{x}_{22} & \cdots & \bar{x}_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{x}_{n1} & \bar{x}_{n2} & \cdots & \bar{x}_{nm} \end{pmatrix}$$

5. SECURITY ANALYSIS

The proposed scheme further provides extra security and speed improvements by making use of transpose matrix and improve the decryption side of RSA. If an intruder appearance into the message he can realize it difficult to know or calculate checksum/ hash value therefore it'll confuse the intruder. Hence this is often a really smart solution for eavesdropping drawback.
Next, we show that our scheme is heuristically secured by considering the following attacks [8].

Common Modulus Attack: The common modulus attack (CMA) [8] can be occurred by using the same modulus n, when the same message X is encrypted twice and by that attack one can retrieve the message X algorithm. The CMA is applicable in Iuon-Chang Lei et. al [3] scheme method because it uses the encryption and decryption as same as original RSA. In the proposed scheme using a unique integer k by that there are two cipheretext generated and it appears to be impractical to apply that attack on proposed scheme.

Chosen Cipher Text Attack: Chosen-cipher text attack (CCA) [9] is possible in RSA due to the multiplicative property of the modular arithmetic [10] following by RSA. That means product of the two cipher texts is equal to the encryption of the product of the corresponding plaintexts. The CCA is applicable in both original RSA algorithm, and in the proposed one, but by applying CCA on the proposed scheme for getting the value of message X, it appears to be complex and more time consuming as compared to the original RSA algorithm.

Timing Attack: An attacker can determine the value of the private key by maintaining the track of how much time a computer takes to decrypt the encrypted message this because of Timing attack that occurs at RSA implementation Kocher [11]. Timing attack is applicable in majority digital signature fault tolerant schemes based on original RSA algorithm because by measuring the time for encryption and decryption, and time for key generation one can determine the value of the secrete key exponent d, but in the proposed scheme by using a random unique integer k in both the encryption and decryption process makes it difficult to distinguish between the time for public key e or private key d and the time for k.

Known Plain-Text Attack: If the attacker has known some quantity of plaintext and corresponding ciphertext, this will refer to known-plaintext attack [12]. The known-plaintext attack deals with the some known plaintext corresponding to the ciphertext and it is applicable in the digital signature with fault tolerance based on the original RSA algorithm. But it seems to be impractical in the proposed scheme because here, generating the two ciphertexts for the one particular plaintext and if it is applicable to the proposed scheme, it is very difficult to get the value of particular plaintext by applying these attacks.

6. CONCLUSION

The proposed scheme described in the paper is an attempt to provide a speed improvement on the decryption side of digital signature scheme fault tolerance based on improving the RSA algorithm using the concept of the Chinese remainder theorem. The algorithm for the proposed scheme can protect us from several common attacks. Further, it provides extra security measures by making use of transpose matrix of the original message.

REFERENCES

[1] C.N. Zhang, “Integrated Approach for Fault Tolerance and Digital Signature in RSA,” IEEE Proceedings-Computers & Digital Techniques, vol. 146, no. 3, pp. 151-159, 1999

[2] N. Lee and W. Tsai, “Efficient Fault-tolerant Scheme basd on the RSA system,” IEEE Proceedings – Computer and Digital Techniques, vol. 150, no. 1, pp. 17-20, 2003.

[3] Iuon-Chang Lin and Hsing-Lei Wang, “An Improved Digital Signature Scheme with Fault Tolerance in RSA”, Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. IEEE, 2010

[4] Shreenath Acharya, Sunaina Kotekar, Seema S Joshi, Shradda Shetty and Supreetha Lobo,” Implementing Digital Signature based Secured Card System for Online Transactions”, International Journal of Computer Applications 65(24):27-32, March 2013.

[5] R. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-key Cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.

[6] Nikita Somani and Dharmendra Mangal, “An Improved RSA Cryptographic System”, International Journal of Computer Applications 105(16):18-22, November 2014.

[7] A. H. Al-Hamami and I. A. Aldariseh, "Enhanced Method for RSA Cryptosystem Algorithm," IEEE International Conference on Advanced Computer Science Applications and Technologies, pp. 402-408, 2012.

[8] D. Boneh, "Twenty Years of Attacks on the RSA Cryptosystem," Notices of the AMS, vol. 46, no. 2, pp. 203-213, 1999.

[9] Y. Desmedt and A. M. Odlyzko, "A Chosentext Attack on RSA Cryptosystem and some Discrete Logarithm Schemes," Advances in Cryptology CRYPTO ’85, vol. 218, pp. 5116-521, 1986.

[10] R. Kumar, "Security Analysis and Implementation of an Improved Cch2 Proxy Multi-Signature Scheme," International journal of computer network and Information security, vol. 4, pp. 46-54, 2014.

[11] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," Advances in Cryptology-CRYPTO '96, pp. 104-113, 1996.

[12] R. C. Merkle, "Secure Communications over Insecure Channels," Communications of the ACM, vol. 21, no. 4, pp. 294-299, 1978.

AUTHORS

H. Elkamchouchi obtained his B.Sc Electrical Communication Engineering - Excellent with First Class Honors - Faculty of Engineering – Alexandria University - June 1966, Master Communications Engineering (specialization accurate: antennas and propagation) Faculty of Engineering – Alexandria University - September 1969, B.Sc of Science in Applied Mathematics - Excellent with honors - Britain's Royal College of Science - University of London - England - August 1970, Doctor Communications Engineering (specialization accurate: antennas and propagation) - Faculty of Engineering - Alexandria University - March 1972. He work Professor Emeritus, Faculty of Engineering, Alexandria University from September 2003 until now.

Heba Gaber held a Masters' of science in Electrical Engineering from Faculty of Engineering, Arab Academy for Science and Technology. She works on Arab Academy for Science and Technology. She studies for Ph.D. in Electrical Engineering from Faculty of Engineering, Alexandria University.

Fatma Ahmed held a Masters' of science in Electrical Engineering from Faculty of Engineering, Alexandria University. She works on Alexandria Higher Institute of Engineering and Technology. She Held a Ph.D. in Electrical Engineering from Faculty of Engineering, Alexandria University.

Dalia ElKamchouchi held a Masters' of science in Electrical Engineering from Faculty of Engineering, Alexandria University. She works on Alexandria Higher Institute of Engineering and Technology. She Held a Ph.D. in Electrical Engineering from Faculty of Engineering, Alexandria University.