International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 2, April 2020, pp. 1430~1437
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i2.pp1430-1437

A new RSA public key encryption scheme with chaotic maps

Nedal Tahat[1], Ashraf A. Tahat[2], Maysam Abu-Dalu[3], Ramzi B. Albadarneh[4], Alaa E. Abdallah[5],Obaida M. Al-Hazaimeh[6]
[1,3,4]Department of Mathematics, the Hashemite University, Jordan
[2]Department of Communications Engineering, Princess Sumaya University for Technology, Jordan
[5]Faculty of Prince Al-Hussein Bin Abdullah II for Information Technology, the Hashemite University, Jordan
[6]Department of Computer Science and Information Technology, Al-Balqa Applied University, Jordan

Article Info

Article history:

Received Jun 26, 2019
Revised Oct 5, 2019
Accepted Oct 17, 2019

Keywords:

Chaotic maps
Cryptanalysis
Cryptography
Public key cryptography
RSA

ABSTRACT

Public key cryptography has received great attention in the field of information exchange through insecure channels. In this paper, we combine the Dependent-RSA (DRSA) and chaotic maps (CM) to get a new secure cryptosystem, which depends on both integer factorization and chaotic maps discrete logarithm (CMDL). Using this new system, the scammer has to go through two levels of reverse engineering, concurrently, so as to perform the recovery of original text from the cipher-text has been received. Thus, this new system is supposed to be more sophisticated and more secure than other systems. We prove that our new cryptosystem does not increase the overhead in performing the encryption process or the decryption process considering that it requires minimum operations in both. We show that this new cryptosystem is more efficient in terms of performance compared with other encryption systems, which makes it more suitable for nodes with limited computational ability.

Corresponding Author:

Nedal Tahat,
Department of Mathematics,
The Hashemite University, Zarqa 13133, Jordan.
Email: nedal@hu.edu.jo

1. INTRODUCTION

Cryptography is defined as the set of protocols and procedures that are necessary for secure communications in the existence of third parties. Cryptography is divided into two basic types: private key encryption, and public key encryption. In the former, a specific key (i.e., private key) has to be known by the sender and receiver to be able to encrypt and decrypt messages. This means that a secure channel in private key encryption is required to share the key. In reality, it is not easy to attain such secure channel. Diffie and Hellman [1] introduced Public Key Cryptography (PKC), which solves the drawback of private key cryptography; A single number theoretic cryptographic assumptions, on which many public key encryption protocols are based on (i.e., discrete logarithm, or factoring a large composite number) [1-2]. The security of a given protocol depends mostly on the cryptographic assumptions. If these assumptions can be hacked easily, then the cryptosystem will not be secure anymore [3]. Several cryptographic protocols try to enhance the system security by adding extra multiple hard problems that need to be solved simultaneously. Unlike protocols that depend on a single hard problem, these extra hard problems will definitely make the whole system more secure.

The first key distribution protocol, which is based on two different assumptions, was proposed in 1988 by K.S. McCurley [4]. This protocol was inefficient, because it was very hard to select module p and q to achieve similar difficulty for these two assumptions. To maintain acceptable efficiency L, Harn et al. [5] proposed a cryptosystem protocol that was based on two distinct cryptographic assumptions: Discrete Logarithm (DL), and Factoring (FAC). This new protocol has improved the security, while maintaining

the implementation efficiency. Later, many other cryptosystem protocols were proposed [6-9], most of which are based on combining two problems such DL and FAC, Elliptic Curve Discrete Logarithm (ECDL), Knapsack problem, and many more. Some of these protocols achieve the optimal goal, which is an efficient secure system. In this paper, we propose a crypto-system protocol that is based on both of chaotic maps and factorization problems. The new protocol improves the overall security, and needs a lower number of operations in both of the encryption and decryption processes. Therefore, the proposed crypto-system is more practical for realistic applications. The fashion into which the rest of this paper is arranged into is as follows: In Section 2, we briefly introduce the necessary mathematical framework used in the paper. In the section 3, the new proposed encryption scheme is introduced. In Sections 4, 5 and 6, we analyze the security and efficiency of the proposed scheme. We finally conclude in Section 7.

2. CHAOTIC MAPS

Chaotic theory has been heavily used in designing secure communication protocols since the 1990s [10-15], while chaotic maps have been utilized in the design of symmetric encryption protocols in [16-19]. Designing a chaotic map setting is usually difficult, but generally creates secure and efficient protocols. That is because chaotic map-based protocols have low computational costs when compared with other modular exponential computing based protocols or protocols that are based on scalar multiplication on elliptic curves.

2.1. Chebyshev maps

A map of a Chebyshev polynomial, $T_p: R \to R$ of degree p, can be defined with the subsequent recurrent relation [20]:

$$T_{p+1}(x) = 2xT_p(x) - T_{p-1}(x), \quad (1)$$

with $T_0(x) = 1$, and $T_1(x) = x$, the headmost Chebyshev polynomials are,

$$T_2(x) = 2x^2 - 1, \quad (2)$$

$$T_3T_3(x) = 4x^3 - 3x, \quad (3)$$

$$T_4(x) = 8x^4 - 8x^2 + 1` \quad (4)$$

A significant property of Chebyshev polynomials is the semi-group property:

$$T_r(T_s(x)) = T_{rs}(x) \quad (5)$$

An instant sequel of the above property is that Chebyshev polynomials under composition commute, i.e., $T_s(T_r) = T_r(T_s)$. Under the action of the map $T_p: T_p([-1,1]) = [-1,1]$, the interval $[-1,1]$ is invariable. Thus, a Chebyshev polynomial confined to the interval $[-1,1]$ will be the prominent chaotic map for all $p > 1$. It has a unique invariant measure $(x)dx = \frac{dx}{\pi\sqrt{1-x^2}}$, which is absolutely continuous with positive Lyapunov exponent $\lambda = Inp$. The Chebyshev map, for, $p = 2$, reduces to the familiar logistic map. Two presumably intractable problems related to Chebyshev polynomials [21] are:

Definition 1. Chaotic maps discrete logarithm (CMDL) problem: Given a random number $x \in \mathbb{Z}_p^*$, and an element $y \in \mathbb{Z}_p$, the task of the CMDL problem is to find an integer r such that $y = T_r(x)(mod\ p)$.

Definition 2. Chaotic maps Diffie–Hellman (CMDH) problem: Given a random number $x \in \mathbb{Z}_p^*$, and two elements, $T_r(x)$ and $T_s(x)$, for unknown values r and s , the task of the CMDH problem is to compute $T_{rs}(x)$.

2.2. Public-key encryption with Chebyshev polynomial

System based on chaotic theory is usually defined on real numbers. In fact, any encryption algorithm, which utilizes chaotic maps, upon its implementation on a computer (e.g., finite-state machine), it turns into a transformation onto itself from a finite set. Because floating-point has a wide dynamic rage, its implementation seems applicable for software implementation of Chebyshev polynomials. Nevertheless, floating-point cannot be used in public-key encryption for the following reasons:

- There is no uniform distribution for floating-point numbers, on the real axis, over any given interval. Moreover, there is an existence of redundant number representations in floating-point arithmetic caused by normalized calculations. As the same real signal value is represented by some floating-point numbers [22].

- There is a restriction on the message length because a Chebyshev polynomial is a non-invertible. In [23], the public key encryption protocol uses Chebyshev polynomials. This algorithm can be explained as follows: Let a large integer set s be generated by Thomas, then let a number $x \in [-1, 1]$ be generated randomly, and let $T_s(x)$ be computed. Thomas's public key is $(x, T_s(x))$, his private key is s. Bob denotes the message as number $\in [-1, 1]$, then creates a large integer r and calculates $T_r(x)$, $T_{rs}(x) = T_r(T_s(x))$, and $X = MT_{rs}(x)$. Bob relays the cipher-text $c = (T_r(x), X)$ to Thomas. To recover plain-text $M$from c, Thomas utilizes the private key s to compute $T_{rs}(x) = T_r(T_s(x))$, and recovers the text M by calculating $M = X / T_{rs}(x)$. Let l_s, l_r, l_M be the lengths (in bits) of s, r and M, respectively, and let N-bit precision arithmetic be employed in the algorithm software implementation. Then $l_M \leq N - l_s - l_r$ [12, 23].
- When floating-point representation is used to implement chaotic maps, it is hard to implement tools for the purpose of analysing the structure of the periodicity of the periodic orbits. Furthermore, there is no hope in establishing a link between the number and chaos theory.

2.3. Modified Chebyshev polynomials

The following map will be used to show an ElGamal and RSA public-key algorithms to Chebyshev maps: T_p: $\{0,1, \ldots, N-1\} \rightarrow$: $\{0,1, \ldots, N-1\}$ defined as $y = T_p(x) (\mathrm{mod}\, N)$, where x and N are integers. We will call $y = T_p(x) (\mathrm{mod}\, N)$ as modified Chebyshev polynomial. This can replace the power in both algorithms of ElGamal and RSA public-key, if and only if, substitution is possible under composition, and their orbits period can be computed. The properties of the modified Chebyshev polynomials are shown in the following theorems:

Theorem 2.3.1 Modified Chebyshev polynomials commute under composition, that is,

$$T_p(T_q(x) \bmod N) = T_{pq}(x) (\mathrm{mod}\, N) \quad (6)$$

Theorem 2.3.2 Let N be an odd prime and let $x \in \mathbb{Z}$ such that $0 \leq x < N$. Then the period of the sequence $T_n(x)$ ($mod\ N$) for $n = 01,2, \ldots$, is a divisor of $N^2 - 1$.

3. THE PROPOSED PUBLIC KEY ENCRYPTION

We propose in this section our new protocol, which is based on chaotic maps and factoring problems. The new protocol comprises three parts: key generation, encryption, and decryption.

3.1. Key generation

In general, it is assumed that it is desired to join the proposed crypto-system as entity *A*. For key generation purposes, the creation of a public and a private key requires performing a set of processes. We describe these processes in the following steps:

Steps 1: Select two large random primes p and q of almost same size.
Steps 2: Compute $n = pq$ and $\varphi = (p^2 - 1)(q^2 - 1)$.
Steps 3: Choose a random integer e, $1 < e < \varphi(n)$ such that $\gcd(e, \varphi(n)) = 1$.
Steps 4: Calculate the unique integer d, $1 < e < \varphi(n)$, such that $ed \equiv 1 \pmod{\varphi(n)}$.
Steps 5: Choose two random integers a, b such that $0 \leq a, b \leq \varphi(n) - 1$.
Steps 6: Choose $\alpha, \beta \in \mathbb{Z}_n^*$ and compute.

$$y_1 = T_{a^2}(\alpha) (\mathrm{mod}\, n)$$
$$y_2 = T_{b^2}(\beta) (\mathrm{mod}\, n)$$

The public key of $\mathcal{A}$ is $(n, e, y_1, y_2, \alpha, \beta)$ and the corresponding private key is (p, q, a, b, d).

3.2. Encryption

Encryption algorithms are normally involved in the cryptographic process. Many iterations that include substitutions and transformations are performed in these algorithms on original data (known as plaintext). This is done so as to make the process of identifying the data by a hacker or intruder complicated [24]. In this paper, we consider the plaintext space as $\mathbb{Z}_n$. Assume that a user $\mathcal{B}$ wishes to send a message $m \in \mathbb{Z}_n$ to $\mathcal{A}$ using $\mathcal{A}$'s public key. Then $\mathcal{B}$ has to carry-out the following steps:

Steps 1: Select $r \in \mathbb{Z}_n^*$ and find $s_1 = T_e(r) (\mathrm{mod}\, n)$.
Steps 2: Generate two random non-negative integers $c, t \in \mathbb{Z}_n$ and compute:

$$s_2 = T_c(\alpha) (\mathrm{mod}\, n)$$
$$s_3 = T_t(\beta) (\mathrm{mod}\, n)$$

Steps 3: Compute $s_4 = m\,T_c(y_1)T_t(y_2)T_e(r+1) \pmod n$.
Then, $\mathcal{B}$ send to $\mathcal{A}$ the encrypted message(s_1, s_2, s_3, s_4)

3.3. Decryption

Generally, the process of decryption is reversing all operations carried-out to perform the encryption [25]. It entails transforming the encrypted data back to the original form in order to allow the receiver to understand it. In this paper, to recover the message m from(s_1, s_2, s_3, s_4), $\mathcal{A}$ should carry-out the following:

Steps 1: Compute $r = T_d(s_1) \pmod n$.
Steps 2: Compute $R = s_4 T_e^{-1}(r+1) \pmod n$.
Steps 3: Compute $T_{a^{\varphi(n)+2}}(s_2) \bmod n = T_{a^2}(s_2) \bmod n = T_{a^2}T_c(\alpha) = T_c(y_1) \pmod n$.
Steps 4: Compute $T_{b^{\varphi(n)+2}}(s_3) \bmod n = T_{b^2}(s_3) \bmod n = T_{b^2}T_t(\beta) = T_t(y_2) \pmod n$.
Steps 5: Compute $m = R\ T_c^{-1}(y_1)\ T_t^{-1}(y_2) \pmod n$.

To achieve a successful decryption process, the accuracy cannot be compromised in performing decryption.

Theorem: If the initialization and encryption algorithms are executed correctly, then it is guaranteed to get the original text by using the decryption algorithm.

Proof: From the relation $R\ T_c^{-1}(y_1)\ T_t^{-1}(y_2)(mod\ n) = m$, we have

$$T_c^{-1}(y_1)\ T_t^{-1}(y_2) = s_4 T_e^{-1}(r+1)\ T_c^{-1}(y_1)\ T_t^{-1}(y_2)$$

$$= \frac{s_4 T_e^{-1}(r+1)}{T_c(y_1)T_t(y_2)}$$

$$= \frac{m\,T_c(y_1)T_t(y_2)T_e(r+1)\,T_e^{-1}(r+1)}{T_c(y_1)T_t(y_2)}$$

$$= m \pmod n. \tag{7}$$

Note that, in RSA key generation, the two integers e and d are called, respectively, the encryption exponent, and the decryption exponent. While n is called the modulus. It was shown in Section 3.2 that $T_1(x) \equiv x(\bmod p)$. By the same argument,

$$T_d(T_e(x)) \equiv T_{de}(x) \equiv T_{1+k\varphi}(x) \equiv T_1(x) \equiv x(\bmod q) \tag{8}$$

Lastely, since p and q are distinct primes, the Chinese remainder theorem may be use to show that:

$$T_d(T_e(x)) \equiv T_{de}(x) \equiv T_{1+k\varphi}(x) \equiv T_1(x) \equiv x(\bmod n) \tag{9}$$

4. EXAMPLE

To illustrate the impact of the proposed scheme, we have used artificially small parameters into a representative example as follows:

- Key generation: The user $\mathcal{A}$choose $\mathrm{p} = 13, \mathrm{q} = 17$ and compute $\mathrm{n} = 221$, $\varphi = 43384$. $\mathcal{A}$ selects a random integer $\mathrm{e} = 317$, and find the unique integer,

$$\mathrm{d} \equiv \mathrm{e}^{-1} \bmod \varphi \equiv (317)^{-1} \bmod 43384 \equiv 12821 \tag{10}$$

$\mathcal{A}$ Chooses two random integers $\mathrm{a} = 211$ and $\mathrm{b} = 311$ such that $0 \le \mathrm{a}, \mathrm{b} \le \varphi(\mathrm{n}) - 1$, and he also chooses$\alpha = 107, \beta = 179 \in \mathbb{Z}_{\mathrm{n}}^*$ and computes:

$$\mathrm{y}_1 = \mathrm{T}_{(211)^2}(107) \equiv \mathrm{T}_{100}(107) \bmod (221) = 199 \tag{11}$$

$$\mathrm{y}_2 = \mathrm{T}_{(311)^2}(179) = \mathrm{T}_{144}(179) \bmod (221) = 18 \tag{12}$$

Then, the user $\mathcal{A}$ public key is $(\mathrm{n}, \mathrm{e}, \mathrm{y}_1, \mathrm{y}_2, \alpha, \beta)$, and $(\mathrm{p}, \mathrm{q}, \mathrm{a}, \mathrm{b}, \mathrm{d})$ represents the corresponding private key.

- Encryption: To encrypt a message m = 155. $\mathcal{B}$ chooses r = 173 ∈ $\mathbb{Z}_n^*$ and compute:

$$s_1 = T_{317}(173) \bmod 221 = 31 \quad (13)$$

A user $\mathcal{B}$ chooses two random non-negative integers c = 127, t = 123 ∈ $\mathbb{Z}_n$ and computes:

$$s_2 = T_{127}(107) \bmod (221) = 72 \quad (14)$$

$$s_3 = T_{123}(179) \bmod (221) = 135 \quad (15)$$

$$s_4 = 155\ T_{127}(199) T_{123}(18) T_{317}(174) \quad (16)$$

$$= 155\ (199)(69)(23) (\bmod 221) = 178 \quad (17)$$

$\mathcal{B}$ sends to $\mathcal{A}$ the encrypted message (s_1, s_2, s_3, s_4).

- Decryption: To recover the message m from (s_1, s_2, s_3, s_4), $\mathcal{A}$ computes:

$$r = T_{12821}(31) (\bmod\ 221) = 173 \quad (18)$$

$$R = 178\ (T_{317}(174))^{-1} \bmod 221 = 75 \quad (19)$$

$$T_{a^{\varphi(n)+2}}(s_2) \bmod n = T_c(y_1) (\bmod n) = 199 \quad (20)$$

$$T_{b^{\varphi(n)+2}}(s_3) \bmod n = T_t(y_2) (\bmod n) = 69 \quad (21)$$

$$m = 75\ (199)^{-1}(69)^{-1} \bmod 221 = 75\ (10)(205) \bmod 221 = 155 \quad (22)$$

5. SECURITY

The proposed crypto-system' security is found on factoring and chaotic map. To depict the heuristic security at our scheme, a collection of common attacks were considered in the following:

Attack 1: Assume that an attacker desires to recover all secret values (p, q, a, b, d), utilizing all accessible system information. In this scenario, the attacker has to conduct factoring and chaotic maps solutions. S/he needs to find the primes of n for factoring, which can usually be solved using the number field sieve method [9]. Nevertheless, the size of modulus n influences this method, and computationally cannot factor an integer of size 1024-bit and above. If the two prime numbers p and q are chosen well, it will definitely increase the resistance of the scheme to attack by the special-purpose factorization algorithms. For chaotic maps to find a and b from $y_1 = T_{a^2}(\alpha) (\bmod n)$ and $y_2 = T_{b^2}(\beta) (\bmod n)$, and if the same level of security is used over primes, then the attacker has to solve integer factorization problem and chaotic map. Also, the integers c and t must be large to prevent exhaustive search attack. One obvious encryption practice is to use different parameters k, c and t for different messages, because if a sender used the same parameters for encryption of two message say m_1 and m_2, then s/he would obtain $s_4 = m\, T_c(y_1) T_t(y_2) T_e(r+1) \pmod n$ and $s'_4 = m\, T_c(y_1) T_t(y_2) T_e(r+1) \pmod n$. So, from the relation $m_2 = s'_4\, s_4 m_1$, an attacker who knows the message m_1 can recover m_2. Note, the new proposed algorithm is randomized, parameters k, c and t are randomly chosen by the sender. Also, it can be proved that an attacker cannot find the cipher text of $m_1 m_2$ even if he knows the corresponding ciphertext of messages m_1 and m_2.

Attack 2: If the attacker manages to factor the modulus n, then, he can use p and q to calculate the value $r = T_d(s_1) (\bmod n)$ and $R = s_4 T_e^{-1}(r+1) (\bmod n) = m T_c(y_1) T_t(y_2) (\bmod n)$. To recover the message m from $m T_c(y_1) T_t(y_2) (\bmod n)$, he has to find c and t. And that is the computationally infeasible assumption of the chaotic maps.

Attack 3: Assume that the attacker is able to solve the chaotic maps problem, and thus obtain the integers a^2 and b^2. Then, he will know $T_{a^2}(s_2) \bmod n = T_{a^2} T_c(\alpha) = T_c(y_1) (\bmod n)$ and $T_{b^2}(s_3) \bmod n = T_{b^2} T_t(\beta) = T_t(y_2)$, which is not enough to recover the message. The attacker still has to compute $r = T_d(s_1) (\bmod n)$ to find $R = s_4 T_e^{-1}(r+1) (\bmod n)$, and since the factorization of n is not known, it is infeasible to computationally compute d.

Attack 4: Now, let us assume that an oracle $\mathcal{O}$ which can break the proposed scheme exists (i.e., the corresponding cipher-text is obtained through $\mathcal{O}$ from the message). Now, we can show the security of the proposed scheme by the following the theorem.

Theorem: If there exists an oracle that is able to break the suggested scheme, then it is also able to break the DRSA and CM.

Proof: If $a = 0 = b$, then $y_1 = T_{a^2}(\alpha) = 1 = T_{b^2}(\beta)$ and so to be a particular case of the proposed scheme is satisfied by the dependent RSA crypto-system. Therefore, if an oracle exists such that it is capable of breaking the proposed scheme, then it is capable also of breaking the dependent RSA scheme.

Assume that there is an oracle $\mathcal{O}$ that is capable of breaking the proposed scheme. We will show that $\mathcal{O}$ can also break CM. Given that (p, g, y) is the public key and assume that a is the private key of the CM, with $y = T_a(g) (\text{mod } p)$ Assume that a cipher text, (C, D) was captured by an attacker, which is encrypted by the CM scheme, and s/he desires to recover the original message m. So, there is a $z \in \{0, \dots, p-2\}$ such that $C = T_g(z) \ (\text{mod } p)$ and $D = mT_z(y) (\text{mod } p)$. First, s/he selects a prime q such that $q \nmid D$ and finds $n = pq$. Secondly, s/he selects integers $\alpha, y_1, C_1, D_1 \in \{1, \dots, n-1\}$ such that:

$$\alpha \equiv g \ (mod\ p), \qquad \alpha \equiv 1 \ (mod\ q), \tag{23}$$

$$y_1 \equiv y \ (mod\ p), \qquad y_1 \equiv 1 \ (mod\ q), \tag{24}$$

$$C_1 \equiv C \ (mod\ p), \qquad C_1 \equiv 1 \ (mod\ q), \tag{25}$$

$$D_1 \equiv D \ (mod\ p), \qquad D_1 \equiv 1 \ (mod\ q), \tag{26}$$

Since, $T_a(\alpha) = y \ (\text{mod } p)$ and $T_a(\alpha) = 1 \ (\text{mod } q)$, then $T_a(\alpha) = y_1 (\text{mod } n)$. Similarly, $T_z(\alpha) = C_1 \ (\text{mod } n)$. Consider $M \in \{1, \dots, n-1\}$ such that $M \equiv m \ (mod\ p)$ and $M \equiv 1 \ (\text{mod } q)$, then $D_1 \equiv M\, T_z(y_1) (\text{mod n})$. Once more, choose $\beta \in \mathbb{Z}_n^*, b \in \{0, \dots, \varphi(n) - 1\}$ and compute $y_2 \equiv T_b(\beta) (mod\ n)$. So, $(n, e = 1, \alpha, \beta, y_1 = T_a(\alpha), y_2 = T_b(\beta))$ is the public key and $(p, q, d = 1, a, b)$ is the private key of the proposed scheme. Given the oracle $\mathcal{O}$ could break the proposed scheme, therefore, from the cipher text $(1, C_1 = T_z(\alpha), C_2 = T_0(\beta), C_3 = 2\, M\, T_z(y_1) T_0(y_2) = 2D_1) \ (\text{mod } n)$, one can recover M and hence m.

6. PERFORMANCE EVALUATION

In this section, evaluation of the new proposed scheme performance in terms of computational complexity and communication costs is carried-out. The notations which are used in this paper are listed and defined in Table 1. Table 2 shows taht the total computational complexity that is required by the proposed scheme is $10T_{ch} + 6T_{mul} + 3T_{inv}$, which is equivalent to merely 1.8s. It shows that it is much faster than other schemes. From the obtained results in Table 2, it is clear that the proposed scheme based on chaotic maps and factoring problems has beaten the trivial DRSA and QER schemes in series. It is also more efficient than the trivial use of the DRSA and ELGamal schemes in series.

Table 1. Notations of the performance analyze

T_{exp}	time for executing a modular exponentiation operation	$1T_{exp} \approx 5.37s$
T_{mul}	time for modular multiplication operation	$1T_{mul} \approx 0.00207s$
T_{ch}	time for executing a Chebyshev chaotic map operation	$1T_{ch} \approx 0.172s$
T_{sr}	time complexity for performing a modular square computation	$1T_{sr} \approx 0.00414s$
T_{inv}	time complexity for evaluating a modular inverse computation	$T_{inv} \approx 10T_{mul} \approx 0.0207s$

Table 2. A Comparison between the new proposed schemes with two other schemes in terms of computational complexity

Scheme	Encryption	Decryption	Total (in *seconds*)	Hard Problems
Goswami et al. [9]	$6T_{exp} + 3T_{mul}$	$4T_{exp} + 3T_{mul} + 3T_{inv}$	44.77	DL, FAC
Poulakis [8]	$6T_{exp} + 4T_{mul}$	$3T_{exp} + 2T_{mul} + 2T_{inv}$	48.37	DL, FAC
Proposed Scheme	$6T_{ch} + 3T_{mul}$	$4T_{ch} + 3T_{mul} + 3T_{inv}$	1.8	FAC, CMDL

7. CONCLUSION

In conclusion, this paper proposed a new crypto-system based on integer factorization and chaotic maps discrete logarithm (CMDL) problems. The new crypto-system has enhanced the overall security when compared with other major public key crypto-systems algorithms. The suggested scheme needs minimum number of operations performed in the encryption and decryption algorithms, which makes it very efficient. We have proved that the new proposed scheme demands a much lower computational cost than other schemes. We have proved that our scheme is robust against several attacks. Hence, our proposed scheme is as secure as RSA algorithm.

REFERENCES

[1] T. EIGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms Advances in Cryptology," in *Proc. of CRYPTO 84*, pp. 10-18, 1985.
[2] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, vol. 21, pp. 120-126, 1978.
[3] O. M. A. AI-Hazaimeh, "Design of a New Block Cipher Algorithm," *Network and Complex Systems, ISSN*, pp. 2225-0603, 2013.
[4] K. S. McCurley, "A Key Distribution System Equivalent to Factoring," *Journal of cryptology*, vol. 1, pp. 95-105, 1988.
[5] L. Harn and S. Yang, "ID-Based Cryptographic Schemes for User Identification, Digital Signature, and Key Distribution," *IEEE Journal on Selected Areas in Communications*, vol. 11, pp. 757-760, 1993.
[6] Z. Shao, "Signature Schemes Based on Factoring and Discrete Logarithms," *IEE Proceedings-Computers and Digital Techniques*, vol. 145, pp. 33-36, 1998.
[7] R. Guo, Q. Wen, Z. Jin, and H. Zhang, "Pairing Based Elliptic Curve Encryption Scheme with Hybrid Problems in Smart House," in *2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP)*, pp. 64-68, 2013.
[8] D. Poulakis, "A Public Key Encryption Scheme Based on Factoring and Discrete Logarithm," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 12, pp. 745-752, 2009.
[9] P. Goswami, M. M. Singh, and B. Bhuyan, "A New Public Key Scheme Based on Integer Factorization and Discrete Logarithm," *Palestine Journal of Mathematics*, vol. 6, 2017.
[10] F. Dachselt and W. Schwarz, "Chaos and Cryptography," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, pp. 1498-1509, 2001.
[11] J. Fridrich, "Symmetric Ciphers Based on Two-Dimensional Chaotic Maps," *International Journal of Bifurcation and chaos*, vol. 8, pp. 1259-1284, 1998.
[12] L. Kocarev, Z. Tasev, and J. Makraduli, "Public-Key Encryption and Digital-Signature Schemes using Chaotic Maps," in *16th European Conference on Circuits Theory and Design, ECCTD*, 2003.
[13] L. M. Pecora and T. L. Carroll, "Driving Systems with Chaotic Signals," *Physical Review A*, vol. 44, p. 2374, 1991.
[14] K.-w. Wong, "A Fast Chaotic Cryptographic Scheme with Dynamic Look-Up Table," *Physics Letters A*, vol. 298, pp. 238-242, 2002.
[15] O. M. Al-Hazaimeh, M. F. Al-Jamal, N. Alhindawi, and A. Omari, "Image Encryption Algorithm Based on Lorenz Chaotic Map with Dynamic Secret Keys," *Neural Computing and Applications*, pp. 1-11, 2017.
[16] G. Chen, Y. Mao, and C. K. Chui, "A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps," *Chaos, Solitons & Fractals*, vol. 21, pp. 749-761, 2004.
[17] L. J. Sheu, "A Speech Encryption using Fractional Chaotic Systems," *Nonlinear dynamics*, vol. 65, pp. 103-108, 2011.
[18] X. Wang, X. Wang, J. Zhao, and Z. Zhang, "Chaotic Encryption Algorithm Based on Alternant of Stream Cipher and Block Cipher," *Nonlinear Dynamics*, vol. 63, pp. 587-597, 2011.
[19] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A Chaotic Image Encryption Algorithm Based on Perceptron Model," *Nonlinear Dynamics*, vol. 62, pp. 615-621, 2010.
[20] L. Kocarev, J. Makraduli, and P. Amato, "Public-Key Encryption Based on Chebyshev Polynomials," *Circuits, Systems and Signal Processing*, vol. 24, pp. 497-517, 2005.
[21] S. H. Islam, "Provably Secure Dynamic Identity-Based Three-Factor Password Authentication Scheme using Extended Chaotic Maps," *Nonlinear Dynamics*, vol. 78, pp. 2261-2276, 2014.
[22] K. DE, "The Art of Computer Programming, vol. 1," *Reading, Addison-Wesley*, 1969.
[23] L. Kocarev and Z. Tasev, "Public-Key Encryption Based on Chebyshev Maps," in *Proceedings-IEEE International Symposium on Circuits and Systems, ISCAS'03*, Bangkok, Thailand, vol. 3, pp. 28-31, 2003.
[24] O. M. A. Al-Hazaimeh, "Increase The Security Level For Real-Time Application using New Key Management Solution," *International Journal of Computer Science Issues (IJCSI)*, vol. 9, pp. 240, 2012.
[25] O. M. Al-hazaimeh, "A Novel Encryption Scheme for Digital Image-Based on One Dimensional Logistic Map," *Computer and Information Science*, vol. 7, pp. 65, 2014.

BIOGRAPHIES OF AUTHORS

Nedal Tahat received his BSc in Mathematics at Yarmouk University, Jordan in 1994, and MSc in Pure Mathematics at Al al-Bayt University, Jordan, in 1998. He is a PhD candidate in Applied Number Theory (Cryptography) from National University of Malaysia (UKM) in 2010. He is an Associate Professor at Department Mathematics, Hashemite University. His main research interests are cryptology and number theory. He has published more than 35 papers, authored/coauthored, and more than 15 refereed journal and conference papers.

Ashraf A. Tahat is an Associate Professor in the Department of Communications Engineering at Princess Sumaya University for Technology (PSUT) and the Vice-Chairman of IEEE Jordan Section. Dr. Tahat earned his B.Sc. and M.Sc. degrees in Electrical Engineering from the Illinois Institute of Technology (IllinoisTech), Chicago, USA, where he also received a Ph.D. in 2002, with a focus on communications and signal processing. Dr. Tahat joined PSUT in 2005 and served as the Head of the department of Communications Eng. from 2010 to 2012. He was also a Visiting Professor with McGill University, Montreal, Canada, in the Department of ECE, conducting research on modern communications systems (2012-2013). From 2002 to 2003, he was an Adjunct Professor at IllinoisTech, Chicago, USA.

Maysam Abu-Dalu received the B.Sc. degree in mathematics from Jordan University of Science and Technology, Jordan, in 2005, the M.Sc. degree in Pure Mathematics from Jordan University of Science and Technology, in 2008. She is an Assistant Lecturer at Department Mathematics, Hashemite University.

Ramzi B. Albadarneh received his BSc in Mathematics at Al al-Bayt University, Jordan in 2000, and MSc in Pure Mathematics at Al al-Bayt University, Jordan, in 2003. He is a PhD candidate in Applied Mathematics (Numerical Analysis) from University of Jordan in 2009. He is an Associate Professor at Department Mathematics, The Hashemite University. His main research interests are Numerical solution of differential equation and finite difference method. He has published more than 9 papers, authored/coauthored, and more than 9 refereed journal and conference papers.

Alaa E. Abdallah is currently an Assistant Professor in the Department of Computer Science at the Hashemite University (HU), Jordan. He received his PhD in Computer Science from Concordia University in 2008, where he worked on routing algorithms for mobile ad hoc networks. He received his BS from Yarmouk University, Jordan and MS from the University of Jordan in 2000 and 2004, respectively. Prior to joining HU, he was a network researcher at consulting private company in Montreal (2008–2011). His current research interests include routing protocols for ad hoc networks, parallel and distributed systems, and multimedia security.