Development of a New Chaotic Maps Cryptosystem with Quadratic Residue Problem

https://doi.org/10.3991/ijoe.v18i11.29563

Nedal Tahat(✉), Rania Shaqbou'a, Maysam Abu-Dalu, Ala Qadomi
Faculty of Science, The Hashemite University, Zarqa, Jordan
nedal@hu.edu.jo

Abstract—A new fast public key cryptosystem is proposed, which is based on two dissimilar number-theoretic hard problems, namely the simultaneous chaotic maps (CM) problem and quadratic residue (QR) problem. The adversary has to solve the two hard problems simultaneously to recover the plaintext according to their knowledge about the public keys and the cipher-text. Cryptographic quadratic residue and chaotic system are employed to enhance the security of our cryptosystem scheme. The encryption, and decryption are discussed in details. Several security attacks are proposed to illustrate the system shield through chaotic maps and quadratic residue problems. The performance analysis of the proposed scheme show a much improved performance over existing techniques.

Keywords—public key cryptography, quadratic residue, chaotic maps, cryptosystem

1 Introduction

Diffie and Hellman (1976) [1] were the first to propose the idea of transmitting secret message between two communicating parties; a sender and a receiver in an insecure channel (with the presence of attackers). Their idea (is called cryptosystem) consists of these following properties:

- The sender first encrypts the message using receiver's public key and sends the encrypted message to the receiver
- The receiver who possesses the secret key can decrypt and read the original message
- The security of the system is depends on the underlying hard problems in computational number theory
- Knowing only the public key of receiver, the attacker is not able to read the message since he has no information about the corresponding secret key unfortunately, they did not develop any such system. The first realization was developed by Rivest et al. (1978) [2] and is called RSA cryptosystem after their first names. The security of RSA is based on the hardness of solving factoring problem (FAC). Informally, if the attacker manages to solve FAC, the underlying system will no longer be secure. With the proper selection of parameters, no one is able to break the novel RSA system. Rabin (1979) [3] designed a new cryptosystem whose security is depends heavily on

residuosity problem (RES). His system relies on the difficulty of finding prime divisors of a given large composite integer as in RSA. However, no concrete relationship between the hardness of solving FAC and RES is found. Six years later, Elgamal (1985) [4] proposed his new cryptosystem based on Discrete Logarithm Problem (DLP). Later, Koblitz (1987) [5] and Miller (1986) [6] independently proposed the use of elliptic curve in cryptosystems. Their security lies on the so-called Elliptic Curve Discrete Logarithm Problem (ECDLP). Their systems are more efficient than previous systems since the size of the main parameter is only 160-bits. Many such systems were then been developed [7, 8]. One common feature of these schemes is that the security of the systems is based on a single hard problem. If one day in a near future an attacker solves the hard problem, the underlying system will no longer be secure. Thus to overcome this disadvantage, many designers are proposing cryptosystems based on two hard problems [9-11]. If the attacker find a solution to one of these hard problem the system stays secure as the problem is still hard to solve. It is impossible for the attacker to solve the two problem simultaneously.

A chaotic map-based image encryption algorithm was originally suggested in 1989 [12]. Lately, there has been an expanding activity in this field as a few methods were presented within the research art [13-17]. The chaotic map-based public cryptosystems require least computational complexity in comparison with that is needed by public cryptosystems that rely on modular exponential computing, or scalar multiplication on elliptic curves. Therefore, in this study, we created a new hybrid mode based cryptosystem using chaotic map and quadratic residue problems. With the greater level of security confirmed, we showed that the performance of the scheme requires a few time complexity unit operations in both encryption and decryption algorithms, which makes the system implementable for real world applications.

The remainder of this paper is organized as follows. We provide the necessary theory and properties of the extended chaotic maps and some notation in Section 2.Then, we propose new chaotic maps cryptosystem with quadratic residue problem in Section 3. In Section 4, security analysis and performance analysis are discussed, followed by numerical simulation are discussed in Section 5. Finally, we draw our conclusion in Section 6.

2 Preliminaries

In this section, we briefly introduce the basic concept of Chebyshev chaotic map [13, 17-24] and the factorization problem [3**]** and its related mathematical properties.

2.1 Chebyshev chaotic map

The structure of the Chebyshev polynomials is reviewed in Figure 1[25].

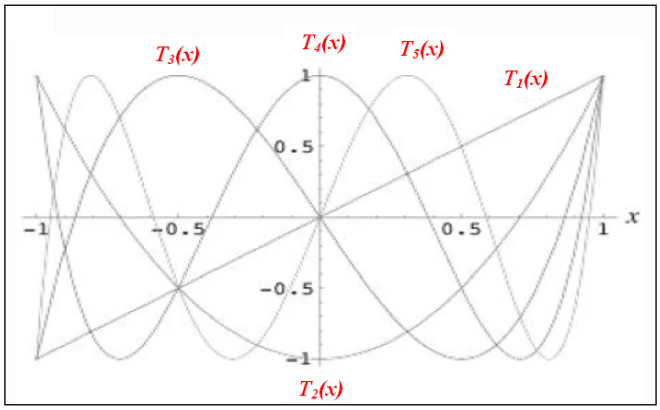

Fig. 1. Chebyshev polynomials structure

Let n be an integer and x be a variable with the interval $[-1,1]$. The Chebyshev polynomial $T_n(x) : [-1,1] \longrightarrow [-1,1]$ is defined as:

$$T_n(x) = \cos(n \cos^{-1}(x)) \tag{1}$$

and the Chebyshev polynomial map $T_n(x) : \mathbb{R} \longrightarrow \mathbb{R}$ of degree n is defined by the recurrent relation:

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)\,;\; n \geq 2 \tag{2}$$

where $T_0(x) = 1, T_1(x) = x$. Some Chebyshev polynomials are $T_2(x) = 2x^2 - 1$, $T_3(x) = 4x^3 - 3x$, $T_4(x) = 8x^4 - 8x^2 + 1$ and $T_5(x) = 16x^5 - 20x^3 + 5x$.

From (2), we get a matrix equation:

$$\begin{bmatrix} T_a(x) \\ T_{a+1}(x) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 2x \end{bmatrix} \begin{bmatrix} T_{a-1}(x) \\ T_a(x) \end{bmatrix} \tag{3}$$

and by manipulating the index, we obtain:

$$\begin{bmatrix} T_{a-1}(x) \\ T_a(x) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 2x \end{bmatrix} \begin{bmatrix} T_{a-2}(x) \\ T_{a-1}(x) \end{bmatrix} \tag{4}$$

Combining the above equations, we next get

$$\begin{bmatrix} T_a(x) \\ T_{a+1}(x) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 2x \end{bmatrix}^a \begin{bmatrix} T_0(x) \\ T_1(x) \end{bmatrix} \tag{5}$$

Where $T_0(x) = 1, T_1(x) = x$.

The Chebyshev polynomial also has the following two interesting properties:

- The semi-group property

$$\begin{aligned} T_r\big(T_s(x)\big) &= cos\big(rcos(s\, cos^{-1}(x))\big) \\ &= \cos\,(rscos^{-1}(x)) \end{aligned}$$

$$= T_{sr}(x)$$
$$= T_s\big(T_r(x)\big) \quad (7)$$

where r and s are positive integers and $x \in [-1,1]$.

- The chaotic property

The Chebyshev map $T_a(x)$; $\big[-1,1 \longrightarrow [-1,1]\big]$ of degree $a > 1$ is a chaotic map with invariant density $f^*(x) = \frac{1}{\pi\sqrt{1-x^2}}$ for positive Lyapunov exponent $\lambda = Ln(a) > 0$. The Chebyshev map, for, p=2, reduces to the familiar logistic map.

An immediate consequence of this property is that Chebyshev polynomials commute under composition:

$$T_r\big(T_s(x)\big) = T_s(T_r(x))$$

In order to improve the security of Chebyshev polynomials, Zhang [21] proved that the semi-group property holds for Chebyshev polynomials defined on the interval $(-\infty, \infty)$. The enhanced Chebyshev polynomials are expressed in the following form;

$$T_n(x) = \big(2xT_{n-1}(x) - T_{n-2}(x)\big) \pmod p \quad (8)$$

where $n \geq 2, x \in (-\infty, \infty)$, and p is a large prime number. Obviously, one has:

$$T_{rs}(x) = T_r\big(T_s(x)\big) = T_s\big(T_r(x)\big) \pmod p \quad (9)$$

Theorem 1. [13] Let $f(M) = t^2 - 2Mt + 1$ and α, β be two roots of $f(M)$. If $M = \frac{1}{2}(\alpha + \beta)$, in this case, the number of possible solutions is met by:

$$T_a(M) = \frac{\left(M+\sqrt{M^2-1}\right)^a + \left(M-\sqrt{M^2-1}\right)^a}{2} \pmod p \quad (10)$$

Theorem 2. [13] If a and b are two positive integers and $a > b$, then we obtain that:

$$2T_a(M).T_b(M) = T_{a+b}(M) + T_{a-b}(M) \quad (11)$$

Theorem 3. [13] If $a = b + c$ and p is a prime (i.e., large number), we obtain that:

$$[T_a(M)]^2 + [T_b(M)]^2 + [T_c(M)]^2 = 2T_a(M)T_b(M)T_c(M) + 1 \pmod p \quad (12)$$

Lemma 1. [13] Let the elements of a finite field are g and h , i.e. if $g + g^{-1} = h + h^{-1}$then $g = h$ or $g = h^{-1}$.

Lemma 2. [13] For any $g \in GF(p)$ and $y = g^t$ for some integer t, we can find an integer $M \in GF(p)$ and then construct a chaotic maps sequence $\{T_a(M)\}$, in polynomial time such that:

$$\frac{1}{2}(y + y^{-1}) = T_t(M) \in T_a(M) \quad (13)$$

Lemma 3. [13] Let p, n and α are the same as earlier; and G is the group formed by the combination of these three. To obtain the value of v such that $a = T_{v^2(mod\ n)}(\alpha)\ mod\ p$, where a is given and $a \in G$, one must solve both the chaotic maps problem in G and the factorization of n.

Theorem 4. The discrete logarithm problem over $GF(p)$ can be solved in polynomial time if a method AL can be used to solve the chaotic mapping problem over$GF(p)$.

2.2 The factorization problem

The factorization problem is how to find two large numbers p and q given a coposite number n that is the product of the two numbers p and q. While finding large prime numbers is a relatively easy task, the problem of factoring the product of two such numbers is considered to be computationally difficult if the primes are carefully selected. Rivest et al. [2] developed the RSA public-key cryptosystem based on the difficulty of this problem. While the factorization problem has received some attention over many years from many mathematicians, it is only in the past 20 years that significant progress has been made towards its resolution. Since, the invention of the RSA cryptosystem in 1978 inspired many mathematicians to study the problem. Additionally, high-speed computers became available for the implementation and testing of sophisticated algorithms. The RSA Problem is now more than a quarter century old [28]. The robust simplicity of the problem has led to several observations over the years, some yielding attacks, others avoiding them. Digital signature and Public-key encryption schemes have been developed whose power is derived from the RSA Problem. The question now is how much the security of the RSA Problem depends on factoring, and as with any hard problem in cryptography, whether any methods more robust than those currently available for solving the problem will ever be found.

- **Definition 1:** (FAC problem) Let n be a large composite integer with $n = rs$ where r and s are two large strong primes of 512-bits. Then find the primes r or s.
- **Definition 2:** (QR problem) Let p, q are two strong primes of large size and γ is an integer. Then, compute γ such that $\gamma \equiv \beta^2 \bmod pq$.

2.3 Computational problem

To prove the security of our proposed cryptosystem, we present some important mathematical properties of Chebyshev chaotic maps as follows.

a) Semi-group property: Given $x \in [-1,1]$,

$$T_r\big(T_s(x)\big) = \cos\Big(r\cos^{-1}\big(s\cos^{-1}(x)\big)\Big) = \cos\big(rs\cos^{-1}(x)\big) = T_{sr}(x) = T_s(T_r(x))$$

b) Chaotic maps problem: If two elements x and y are given, the task of the discrete logarithm problem is to find integers s, such that $T_s(x) = y$.

c) If three elements x, $T_r(x)$, and $T_s(x)$, are given, the task of the Diffie-Hellman problem is to compute elements $T_{rs}(x)$.

3 The new cryptosystem

Let us recall first the following notations and parameters we will use before introducing the new scheme.

- Let p be a large prime and n is a factor of p−1 that is the product of two safe primes $\overline{p}$ and $\overline{q}$, i.e., $n = \overline{p}\,\overline{q}$.
- Let α is an element in $GF(p)$ and the order of α is n, and G is the multiplicative group generated by α. Note that the two large primes $\overline{p}$ and $\overline{q}$, are kept secret for all users in the system.

3.1 Key generation phase

- Choose randomly an integer $x < n$ such that $\gcd(x, n) = 1$
- Compute the number

$$y = T_x(\alpha) \text{ m } (mod\ p) \tag{14}$$

The public key is given by y and can be accessed in the public directory and the secret key is given by x and only known to the legal receiver. Also only the receiver knows the primes factorization of n.

3.2 Algorithm for encryption

Get the original message, $m \in [0, n-1]$. The sender encrypts his message as follows before sends receiver a pair (v_1, v_2).

- Select a random an integer $1 < r < n$ such that $\gcd(r, n) = 1$
- Compute

$$v_1 \equiv (m^2 \,.T_r(y)\ mod\ p)\ mod\ n \tag{15}$$

- Evaluate

$$v_2 \equiv T_r(\alpha) \bmod p \tag{16}$$

In the original ElGamal, (1985) cryptosystem we compute the number v_1 in Eq. 1a without squaring the original message. In our scheme, we need this as we implementing the Rabin, (1979) cryptosystem for QR-like scheme.

3.3 Algorithm for decryption

The receiver decrypts the obtained encrypted message (v_1, v_2) as below:

- Compute the following

$$v_1\ (T_x(v_2)\ mod\ p)^{-1} \equiv m^2\ mod\ n \tag{17}$$

- The receiver uses the known technique (Rabin, 1979) to extract the original message m from m^2 and this can be done since he knows the prime factorization of n.

Theorem 1. If the algorithms of initialization and encryption run smoothly then the decryption of the encrypted message in decryption is correct.

Proof: equation (17) in decryption is true for all encrypted messages (v_1, v_2) since:

$$\begin{aligned} v_1\,(T_x(v_2)\ mod\ p)^{-1} &= \frac{v_1}{T_x(v_2)} \\ &= \frac{(m^2\,.T_r(y)\ mod\ p)\ mod\ n}{T_x(T_r(\alpha))} \\ &= \frac{m^2\,.T_r\ T_x(\alpha)}{T_{xr}(\alpha)} \\ &= \frac{m^2\ T_{xr}(\alpha)}{T_{xr}(\alpha)} \\ &= m^2\ mod\ n \end{aligned}$$

4 Security analysis and performance analysis

In this section, we will prove that the security of our proposed cryptosystem is computationally related to quadratic residue and chaotic maps assumption. In addition, we demonstrate that the proposed scheme is sound and correct. Some possible attack are discussed to show that the proposed technique is secure. Finally, the performance is evaluated and compared with some other related works.

4.1 Security analysis

We show that our scheme is heuristically secure by considering the following three most common attacks.

Direct attack. Adv wishes to obtain all secret keys using all information available from the system.

Particularly, he wants to find the 3-tuples $(x, \bar{p}, \bar{q})$. In this case, Adv needs to solve QR and chaotic map . For QR, he needs to find the primes of n and the best way to factorize the modulus $n = \bar{p}\bar{q}$ is by using the number field sieve method (Lenstra *et al*., 1993). However, this method is just dependent on the size of modulus n and it is computationally infeasible to factor an integer of size 1024-bit and above. The primes p and q also must be well-chosen that they are must be strong primes (Gordon, 1984). This could resist the scheme from the special-purpose factorization algorithms attack. For chaotic maps, to resist various attacks, one should maintain the same security level for the chaotic maps over primes.

Quadratic residue attack. Assume that the Adv has successfully solves the QR assumption so that he knows the primes p and q. He also learns the following equation:

$$v_1 \equiv m^2\,.T_r(y) \equiv m^2 T_{xr}(\alpha)$$

From the equation, to recover the original message, m he has to remove the term $T_{xr}(\alpha)$ from v_1. he needs to find rx which is the assumption of the computational chaotic maps and this is computationally infeasible

Chaotic maps attack. Assume that the Adv is able to solve the chaotic map problem and thus obtain the secret integer x. He then knows that $T_x(v_2) = T_{rx}(\alpha)\ mod\ p$ and tries to recover the original message m from the equation $v_1 \equiv m^2 . T_r(y) = v_1 \equiv m^2 . T_{rx}(\alpha)$. Upon knowing the secret x, he manages to remove the term $T_{rx}(\alpha)$ from v_1 to obtain m^2. Unfortunately, to get m from m^2 he must know the secret primes p and $q$but this is impossible since the FAC is computationally infeasible.

Efficiency performance. Compared to RSA and ECC, Chebyshev polynomial computation problem offers smaller key sizes, and faster computation, as well as saving in memory, energy and bandwidth. In our proposed protocol, no modular exponentiation and scalar multiplication on elliptic curves are needed. However, Wang [22] proposed several methods to solve the Chebyshev polynomial computation problem. For convenience, some notations for operations involved and their equivalent in seconds are given and defined as follows [24-27].

- T_{exp} is the time in seconds for executing a modular exponentiation operation, $1T_{exp} \approx 5.37s$
- T_{mul} is the time for modular multiplication operation, $1T_{mul} \approx 0.00207s$
- T_{ch} is the time for executing a Chebyshev chaotic map operation, $1T_{ch} \approx 0.172$
- T_{inv} is the time complexity for evaluating a modular inverse computation, $T_{inv} \approx 10T_{mul} \approx 0.0207s$.

We next compare in Table 1, our proposal with the schemes based on hybrid problems (Abdoul and Ahmed, 2013; Ismail and Hijazi, 2011). In Table 1, the total computational complexity required by the proposed scheme is $6T_{mul} + 3T_{ch} + T_{inv}$ which is equivalent to merely 0.54912s and is far better than what other schemes have to offer.

Thus, we conclude that the proposed scheme based on chaotic maps and factoring problems is more efficient than the schemes based on DLP, QR and FAC problems.

Table 1. Comparison of two schemes in term of computational complexity

Scheme	Encryption	Decryption	Total (in seconds)	Hard problems
Ismail et al. (2011)	$2T_{exp} + 2T_{mul}$	$T_{exp} + 4T_{mul}$	16.12242	DLP ,QR
Abdoul and Ahmed (2013)	$2T_{exp} + 7T_{mul}$	$T_{exp} + 5T_{mul} + T_{inv}$	16.14105	DLP, FAC
Our scheme	$3T_{mul} + 2T_{ch}$	$3T_{mul} + T_{ch} + T_{inv}$	0.54912	Chaotic map, QR

5 Numerical simulation of the cryptosystem

Suppose we want to cipher a message $m = 442$ with our scheme. Let's consider $\bar{p} = 23, \bar{q} = 31$ and $p = 1427$, the modulus $n = \bar{p}\,\bar{q} = 713$ and n is a factor of $p - 1$. We choose the numbers $x = 113$ and $\alpha = 12$ with order 713 such that $12^{713} = 1 \pmod{1427}$, then compute the public key,

$$y = T_x(\alpha) = T_{113}(12) = 1354(\text{mod } 1427)$$

Thus our public key and secret key of the scheme are (713,12,1354) and (23,31,113) respectively. To encrypt the message $m = 442$, the sender selects $r = 137$ and computes and sends the receiver.

$$\begin{aligned} v_1 = m^2 \,.T_r(y) &\equiv 442^2(\, T_{137}(1354) \bmod 1427) \\ &\equiv 2 \times 683 \,(\text{mod } 713) \\ &\equiv 653 \,(\text{mod } 713) \text{ and} \end{aligned}$$

$$v_2 = T_{137}(12) = 500 \,(\text{mod } 1427)$$

The receiver recovers the original message as below:

$$v_1 \,(T_x(v_2)\, mod\, p)^{-1} \equiv m^2 \bmod n$$

$$\begin{aligned} v_1 \,(T_x(v_2) \bmod p)^{-1} \bmod n &\equiv 653 \,(T_{113}(500) \bmod 1427)^{-1} \\ &\equiv 653 \,(683)^{-1} \bmod 713 \\ &\equiv 653 \times 404 \bmod 713 \\ &\equiv 2 \bmod 713 \end{aligned}$$

$$m^2 \bmod n \equiv 442^2 \bmod 713 \equiv 2 \bmod 713$$

The receiver extract the original message m from $m^2 \equiv 2 \bmod 713$.

$$m \equiv (2)^{\frac{1}{2}} \bmod 713 \equiv 442$$

6 Conclusion

In this paper, a new cryptosystem based on chaotic maps and quadratic residue problems has been proposed. The cryptosystem based on multiple cryptographic assumptions offers a greater security level than that schemes based on a single cryptographic assumption. By the introducing chaotic maps into the field, the proposed scheme promises to bring in far better performance than cryptosystems based on DL and FAC problems. Compared with previous schemes, the proposed scheme demands a much lower computation cost, providing excellent security, reliability, and efficiency.

7 References

[1] Authors Diffie, W. and M.E. Hellman, (1976), "New directions in cryptography", IEEE Trans. Inform. Theory, Vol.22, pp. 644-654. https://doi.org/10.1109/TIT.1976.1055638

[2] Rivest, R.L., A. Shamir and L. Adleman, (1978), "A method for obtaining digital signatures and publickeyCryptosystems," Mag. Commun. ACM, 21: 120- 126. https://doi.org/10.1016/0898-1221(79)90039-7

[3] Rabin, M.O., (1979)," Digitalized signatures and publickey functions as intractable as factorization", Technical Report, Massachusetts Institute of Technology Cambridge, MA.

[4] Elgamal, T., (1985)," A public key cryptosystem and a signature scheme based on discrete logarithms",IEEE Trans. Inform. Theory, Vol. 31, pp.469-472. https://doi.org/10.1109/TIT.1985.1057074
[5] Koblitz, N., (1987)," Elliptic curve cryptosystems", Math. Comput., 48: 203-209. https://doi.org/10.1090/S0025-5718-1987-0866109-5
[6] Miller, V.S., (1986)," Use of elliptic curves in cryptography", Adv. Cryptol., 218: 417-426. https://doi.org/10.1007/3-540-39799-X_31
[7] Menezes, A.J., (1993)," Elliptic Curve Public Key Cryptosystems", 1st Edn., Springer, Boston, ISBN: 0792393686, pp. 144. https://doi.org/10.1007/978-1-4615-3198-2_1
[8] Rabah, K., (2005)," Elliptic curve elgamal encryption and signature schemes", Inform. Technol. J., 13 pp. 299-306. https://doi.org/10.3923/itj.2005.299.306
[9] Baocang, W. and H. Yupu, (2005)," Public key cryptosystem based on two cryptographic assumptions", IEE Proc. Commun., 152: 861-865. https://doi.org/10.1049/ip-com: 20045278
[10] Elkamchouchi, H.M., M.E. Nasr and R. Esmail, (2004)," New public key techniques based on double discrete logarithm problem", Proceeding of the 21st National Radio Science Conference, Mar. 16-18, IEEE Xplore Press, pp: 1-9. https://doi.org/10.1109/NRSC.2004.239775
[11] Ismail, E.S. and M.S. Hijazi, (2011)," New cryptosystem using multiple cryptographic assumptions", J. Comput. Sci., 7: 1765-1769. https://doi.org/10.3844/jcssp.2011.1765.1769
[12] Boneh, D., Franklin, M. (2001), "Identity-Based Encryption from the Weil Pairing", Proceedings of Crypto, LNCS2139, pp.213-229. https://doi.org/10.1007/3-540-44647-8_13
[13] Chain, K. Kuo, C. (2013), "A new digital signature scheme based on chaotic maps, Nonlinear Dyn., Vol.74, pp.1003-1012. https://doi.org/10.1007/s11071-013-1018-1
[14] Chen, W., Quan, C., Tay, C.J. (2009), "Optical color image encryption based on Arnold transform and interference method", Optics Communications, Vol.282, No.18, pp. 3680-3685. https://doi.org/10.1016/j.optcom.2009.06.014
[15] Li, X., Zhao, D. Zhao. (2010), "Optical color image encryption with redefined fractional Hartley transform", International Journal for Light and Electron Optics, Vol.121, No. 7, pp. 673-677. https://doi.org/10.1016/j.ijleo.2008.10.008
[16] Martin, K., Lukac, R., Plataniotis, N. K. (2005), "Efficient encryption of wavelet-based coded color images", Pattern Recognition, Vol.38, No.7, pp.1111-1115. https://doi.org/10.1016/j.patcog.2005.01.002
[17] Tay, J. C., Quan, C., Chen, W., Fu, Y. (2010), "Color image encryption based on interference and virtual optics, Optics Laser Technology, Vol.42, No.2, pp. 409-415. https://doi.org/10.1016/j.optlastec.2009.08.016
[18] Liu, Y., Xue, K. (2016), "An improved secure and efficient password and chaos-based two party key agreement protocol", Nonlinear Dync, Vol. 84, No. 2, PP. 549-557. https://doi.org/10.1007/s11071-015-2506-2
[19] Yoon, J. E (2012), "Efficiency and security problems of anonymous key agreement protocol based on chaotic maps", Commun Nonlinear Sci. Numer. Simul, Vol.17, No. 7, pp. 2735-2740. https://doi.org/10.1016/j.cnsns.2011.11.010
[20] Nedal Tahat, Ashraf A. Tahat, Ramzi B. Albadarneh and Talal A.Edwan, (2020) ," Design of Identity-Based Blind Signature Scheme UponChaotic Maps", *International journal of online and biomedical engineering* , Vol. 16, No. 5,pp. 104-117. https://doi.org/10.3991/ijoe.v16i05.13809
[21] Zhang, F., Chen, X. (2005), "Cryptanalysis of Huang-Chang partially blind signature scheme, Journal of Systems and Software, Vol 76, No. 3, pp. 323-325. https://doi.org/10.1016/j.jss.2004.07.249
[22] Wang, X., Wang, X., Zhao, J. (2011)," Chaotic encryption algorithm based alternant of stream cipher and block cipher", *Nonlinear Dyn.* 63, pp.587-597. https://doi.org/10.1007/s11071-010-9821-4

[23] Gura, N., Patel, A.,Wander, A., Eberle H., and Shantz, S. C. Comparison elliptic curve cryptography and RSA on 8-bit CPUs. *Lect Notes Comput Sci*, 3156, 119-132, (2004). https://doi.org/10.1007/978-3-540-28632-5_9

[24] Hong, S. M., Oh, S. Y. and Yoon, H (1996)," New modular multiplication algorithms for fast exponentiation", *Lect Notes Comput Sci*, 1070, 166-177. https://doi.org/10.1007/3-540-68339-9_15

[25] Abdoul Aziz Ciss and Ahmed Youssef, (2013)," A Factoring and discrete logarithm based cryptosystem", Int. J. Contemp. Math. Sciences, Vol. 8, no. 11, pp.511 – 517. https://doi.org/10.12988/ijcms.2013.13050

[26] Nedal T., Emad, A. (2018)," Hybrid publicly verifiable authenticated encryption scheme based on chaotic naps and factoring problems", Journal *of Applied Security Research,* Vol,13. No3, pp. 304-314. https://doi.org/10.1080/19361610.2018.1463135

[27] Nedal T., Alomari, K., Obaida, A., Mohammad, A. (2020)," An efficient self-certified multi-proxy signature scheme based on elliptic curve discrete logarithm problem", *Journal of Discrete Mathematical Sciences and Cryptography.* https://doi.org/10.1080/09720529.2020.1734293

[28] John, a., Victor, S., Paul, Z. (2000), "factorization in Z[x]: the searching phase, ACM, 291-276.

8

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 of Mathematics, Faculty of Science, The Hashemite University, P.O Box 330127, Zarqa 13133, Jordan. His main research interests are cryptology and number theory. He has published more than 50 papers, authored/coauthored, and more than 20 refereed journal and conference papers.

Rania Shaqbou'a, She received the B.Sc. degree in mathematics from Yarmouk University, Jordan, in 1999, the M.Sc. degree in Pure Mathematics from University of Jordan, IN 2005. She is an Assistant Lecturer at Department of Mathematics, Faculty of Science, The Hashemite University, P.O Box 330127, Zarqa 13133, Jordan.

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 of Mathematics, Faculty of Science, The Hashemite University, P.O Box 330127, Zarqa 13133, Jordan.

Ala Qaomi received her M.Sc. in Applied Mathematics from the University of Jordan, Jordan, and a B.Sc. in Mathematics from the Hashemite University, Jordan. Her research interests are in the areas of Functional analysis and applied analysis and dynamic systems. She is currently an instructor at the Department of Mathematics, Faculty of Science, The Hashemite University, P.O Box 330127, Zarqa 13133, Jordan.

Article submitted 2022-01-17. Resubmitted 2022-05-15. Final acceptance 2022-06-01. Final version published as submitted by the authors.