Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/130115

A New Digital Signature Scheme Based on Chaotic Maps and Quadratic Residue Problems

Nedal Tahat[1,*] *and Mohammad S. Hijazi*[2]

[1] Department of Mathematics, Faculty of Sciences, The Hashemite University, Zarqa 13133, Jordan
[2] Department of Mathematics, College of Arts and Sciences Tabarjal, Jouf University, KSA.

Received: 2 Oct. 2018, Revised: 27 Nov. 2018, Accepted: 2 Dec. 2018
Published online: 1 Jan. 2019

Abstract: Securing electronic signature gives the contracting parties, especially the consumer, safety and security, which positively reflects on trade exchange. Digital-signature algorithms can be categorized based on the type of security suppositions, for example discrete logarithm, factorization of hard-problems, and elliptic-curve cryptography, which are all currently believed to be unsolvable in a reasonable time period. In recent years, a variety of chaotic cryptographic schemes have been proposed. The idea of chaotic systems with applications to cryptography has received a great deal of attention from researchers from a variety of disciplines. Therefore, in this paper, we propose a new signature scheme based on two hard number theoretic problems, Chaotic Maps (CM) and Quadratic Residue (QR). Our performance analysis shows that compared, to other associated schemes, our scheme not only improves the efficiency level but also ensures security . We also give a proof that the security of the proposed scheme can protect against the known key attacks.

Keywords: Digital signature, chaotic maps,quadratic residue problem, Cryptosystem

1 Introduction

Digital signatures are very important tools to implement secure and correct signs. Today, traditional physical signature is out-dated. Communications between partners of a company is a significant issue that must be secure. Digital signature provides suitable background for sending secure messages using different schemes. Digital signatures belong to the most important applications of technology in modern cryptography and information security. After many years of evolution, digital signature technologies are already mature and have already been widely applied in electronic commerce. For digital signature algorithms, we can categorize them into two groups according to their security suppositions. One is a digital signature scheme based on a single assumption, such as discrete logarithm, factorization of hard-problems, or elliptic curve cryptography. To improve the security of signature schemes, many other schemes were developed based on two hard problems: FAC and DLP [1,2,3,4,5,6,7]. However, several authors have also shown these schemes to be flawed [8,9,10,11]. Furthermore,there are many signatures schemes based on two problems [12,13,14,15] , but these schemes need high computational complexity. Therefore, for the enhancement of system security, the adoption of the digital signature algorithm based on multiple assumptions is very important. In this paper, we propose a digital signature scheme based on chaotic maps and quadratic residue problems.

The first chaotic image encryption algorithm was first proposed by Matthews [16]. There is a growing interest in this area and several approaches have been proposed [17,18,19,20,21,23,24,25,26] a novel key-agreement protocol based on chaotic maps. In their scheme, the semi-group property of the Chebyshev chaotic map was used to establish the session key. Hwang et al.[22] proposed a secure group-key-agreement protocol based on chaotic hash that utilised the chaotic hash functions. Recently, Chain and Kuo [13] developed a secure and efficient signature scheme based on chaotic maps and factorization problems. Their scheme was the first scheme based on chaotic maps and factorization problems. Unfortunately, their scheme requires many keys for signing and verifying signatures.

In this paper, we proposed a new signature scheme based on chaotic maps and quadratic residue problems. Compared with the signature scheme based on modular

[*] Corresponding author e-mail: nedal@hu.edu.jo

exponentiation and scalar multiplication on elliptic curve, our proposed scheme is more efficient.

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 a new signature scheme in Section 3. In Section 4,the security properties of the proposed scheme are discussed, followed by the performance are discussed in Section 5. Finally, we draw our conclusion in Section 6.

2 Preliminary Knowledge

In this section, we briefly introduce the basic concept of Chebyshev chaotic map and its related mathematical properties [13,26,18].

2.1 Chepyshev Chaotic Map

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

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

Chebyshev polynomial map $T_n : R \longrightarrow R$ of degree n is defined by the following recurrent relation :

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

Where $n \geq 2$, $T_0(x) = 1$, $T_1(x) = x$. Some of the other Chebyshev polynomial are $T_2(x) = 2x^2 - 1$, $T_3(x) = 4x^3 - 3x$, $T_4(x) = 8x^4 - 8x^2 + 1$, $T_5(x) = 16x^5 - 20x^3 + 5x$.

The Chebyshev polynomial has the following two interesting properties:

- The semi-group property:

$$\begin{aligned} T_r(T_s(x)) &= \cos\left(r\cos\left(s\cos^{-1}(x)\right)\right) \\ &= \cos\left(rs\cos^{-1}(x)\right) \\ &= T_{sr}(x) \\ &= T_s(T_r(x)). \end{aligned} \tag{3}$$

Where r and s are positive integers numbers and $x \in [-1,1]$

- The chaotic property:

The Chebyshev map $T_a(x) = [-1,1] \longrightarrow [-1,1]$ of degree $a > 1$ is a chaotic map with invariant density $f*(x) = \frac{1}{\pi\sqrt{1-x^2}}$ for positive Lyapunov exponent $\lambda = ln(a) > 0$. In order to improve this property, Zhang [29] proved that the semi-group property holds for Chebyshev polynomials defined on the interval $(-\infty,\infty)$ as follows:

$$T_a(x) = 2xT_{a-1}(x) - T_{a-2}(x) \pmod p \tag{4}$$

Where $a \geq 2$, $x \in (-\infty,\infty)$, and p is a large prime number. Therefore, the property

$$T_r(T_s(x)) = T_{sr}(x) = T_s(T_r(x)) \pmod p$$

And the semi group property also holds. The extended Chebyshev polynomials still commute under composition.

2.2 Computational Problems

To prove the security of the proposed scheme, we present some important mathematical properties of Chebyshev chaotic map as follows:

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

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

3 The proposed digital signature scheme

In this section, a new signature scheme based on chaotic maps problem is proposed. The proposed signature scheme involves the one-to-one interactions between a signer and a verifier to execute the system initialization phase, the key generation phase, the signature generation phase, and the signature verification phase, described as follows.

3.1 System Initialization Phase.

The parameters used in our scheme are described as follows:

- $h(.)$ is a strong one-way hash function whose output is an integer of which the length is t-bit. Here, we assume $t = 128$ as the output length of the standard hash function.
- 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.

3.2 Key Generation Phase

In this phase, we do the following steps.

- –Select randomly a private key $x \in Z_n^*$ such that $gcd(x,n) = 1$
- –Calculate a corresponding public key which is certified by certificate authority $y = T_{x^2}(\alpha)$

The signer publishes his public keys as (p,n,y,α) and keeps his corresponding private keys as $(x,\bar{p},\bar{q})$

3.3 Signature Generation Phase

To create a signature for the message $m, 1 < m < n$, the signer first hashes the message to obtain $h(m)$. Next, the signer randomly chooses a secret integer $r, 1 < r < n$ such that $\gcd(r,n) = 1$. The signer does the following steps.

- –Computes $K = T_{r^2}(\alpha)(\text{mod} p)$ and $\gamma^2 \equiv xr(\text{mod} n)$.
- –Solve $\gamma^2 h(m) \equiv x^2 K^2 + \gamma^2 s\,(\text{mod} n)$ for s.

Then the original signer publishes (K,γ,s) as the signature of the message m.

3.4 Signature Verification Phase.

Verifier confirms the validity of the signature (K,γ,s) by testing the following equation whether it holds

$$[T_{\gamma^2 h(m)}(\alpha)]^2 + [T_{K^2}(y)]^2 + [T_{\gamma^2 s}(\alpha)]^2 \equiv$$

$$2T_{\gamma^2 h(m)}(\alpha) T_{K^2}(y) T_{\gamma^2 s}(\alpha) + 1(\text{mod} p) \qquad (5)$$

Theorem 3.1 Following the applied protocol, then the verification in the signature verification phase is correct.

Proof. With knowledge of the signer public key y and the signature (K,γ,s) of message M, the verifier is able to authenticate the message M. From Theorem 2.3 :

$$[T_a(M)]^2 + [T_b(M)]^2 + [T_c(M)]^2 \equiv$$

$$2T_a(M) T_b(M) T_c(M) + 1(\text{mod} p)$$

Let $a = \gamma^2 h(M)$, $b = K^2 x^2$, and $c = \gamma^2 s$, we evaluate the following equation

$$\begin{aligned} & [T_{\gamma^2 h(m)}(\alpha)]^2 + [T_{K^2}(y)]^2 + [T_{\gamma^2 s}(\alpha)]^2 \\ = & [T_{\gamma^2 h(m)}(\alpha)]^2 + [T_{K^2} T_{x^2}(\alpha)]^2 + [T_{\gamma^2 s}(\alpha)]^2 \\ = & [T_{\gamma^2 h(m)}(\alpha)]^2 + [T_{K^2 x^2}(\alpha)]^2 + [T_{\gamma^2 s}(\alpha)]^2 \\ = & 2T_{\gamma^2 h(m)}(\alpha) T_{K^2 x^2}(\alpha) T_{\gamma^2 s}(\alpha) + 1(\text{mod} p) \\ = & 2T_{\gamma^2 h(m)}(\alpha) T_{K^2}(y) T_{\gamma^2 s}(\alpha) + 1(\text{mod} p) \end{aligned}$$

If Eq. (5) holds, then the receiver is ensured that the message is indeed signed by the signer. Otherwise, the signature is invalid.

4 Security analysis

It is apparent that the security of this scheme relies on the difficulty of finding (K,γ,s) such that Eq. (5) holds when message M is given and the signer's secret keys are unknown. Before we attempt some possible attacks on our scheme, we first discuss the computational relationship between chaotic maps and the discrete logarithm problem and then analyze some basic crypto analysis problems which are related to the proposed scheme [13].

Theorem 4.1 Let $f(M) = t^2 - 2Mt + 1$ and α, β be two roots of $f(M)$. If $M = \frac{1}{2}(\alpha + \beta)$, then the number of solutions satisfy

$$T_a(M) = \frac{\left(M + \sqrt{M^2 - 1}\right)^a + \left(M - \sqrt{M^2 - 1}\right)^a}{2} \ (\text{mod } p).$$

Theorem 4.2 If a and b are two positive integers and $a > b$, then

$$2T_a(M).T_b(M) = T_{a+b}(M) + T_{a-b}(M) \qquad (6)$$

Theorem 4.3 If $a = b + c$ and p is a large prime number, then

$$(2T_a(M)\ T_b(M)\ T_c(M) + 1)\ (\text{mod } p) \qquad (7)$$

$$= \left([T_a(M)]^2 + [T_b(M)]^2 + [T_c(M)]^2\right) (\text{mod } p)$$

Lemma 4.1 Let g and h be elements of a finite field ,i.e. if $g + g^{-1} = h + h^{-1}$ then $g = h$ or $g = h^{-1}$

Lemma 4.2 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 $\{T_a(M)\}$ such that $\frac{1}{2}\left(y + y^{-1}\right) = T_t(M) \in T_a(M)$ in polynomial time.

Theorem 4.4 If an algorithm AL can be used to solve the chaotic maps problem over $GF(p)$, then AL can be used to solve the discrete logarithm problem over $GF(p)$ in polynomial time.

Lemma 4.3 Let p, n and α be defined as above and G be the group generated by α. To find v such that $a = T_{v^2(\text{mod } n)}(\alpha)$ mod p , where a is given and $a \in G$, one must solve both chaotic maps problem in G and the QR of n.

Now, we discuss some possible attacks on our signature scheme. Note of the possible attacks can be used to break the proposed scheme if solving both chaotic maps problem and QR is feasible.

Attack 1. Adv wishes to obtain secret key x using all information that is available from the system. In this case, Adv needs to solve $y = T_{x^2}(\alpha) mod\, p$ which is clearly infeasible because the difficulty of solving QR and CM. Moreover, all secret integers like $\bar{p}, \bar{q}$ are also hard to be found.

Attack 2. Adv tries to derive the signature (K,γ,s) for a given message M by letting two integers fixed and finding the other one. In this case, Adv randomly selects

(K,γ) or (γ,s) or (K, s) and find s or K or γ respectively such that the following conditions are upheld:.

$$[T_{\gamma^2 h(m)}(\alpha)]^2+[T_{K^2}(y)]^2+[T_{\gamma^2 s}(\alpha)]^2$$

$$=2T_{\gamma^2 h(m)}(\alpha)T_{K^2}(y)T_{\gamma^2 s}(\alpha)+1(\bmod p)$$

For example, say Adv fixes the values (γ,s) and tries to figure out the value of K. then Adv must deal with the problem of finding K from $\xi \in G$

$$\xi^2-2\xi T_{\gamma^2 h(m)}(\alpha)T_{\gamma^2 s}(\alpha)+[T_{\gamma^2 h(m)}(\alpha)]^2+$$

$$[T_{\gamma^2 s}(\alpha)]^2-1=0(\bmod p)$$

Therefore, ξ can be recovered by the following equation:

$$\xi=\frac{2T_{\gamma^2 h(m)}(\alpha)T_{\gamma^2 s}(\alpha)}{2}\pm$$

$$\frac{\sqrt{(2T_{\gamma^2 h(m)}(\alpha)T_{\gamma^2 s}(\alpha))-4([T_{\gamma^2 s}(\alpha)]^2+[T_{\gamma^2 h(m)}(\alpha)]^2-1)}}{2}$$

However, it is infeasible to find K from $\xi=T_{K^2}(y)(\bmod p)$ even if Adv can get ξ from the above Eq. From Lemma 4.3, we can see that this is equivalent to solving both the chaotic maps problem in G and the factorization of n. The rest of two cases go similarly.

Attack 3. It is assumed that Adv is able to solve CM problem. In this case, Adv knows x^2 from $y=T_{x^2}(\alpha)$ but cannot compute s and γ from $\gamma^2 h(m)\equiv x^2K^2+\gamma^2 s\,(\bmod n)$ due to difficulty of breaking QR.

Attack 4. It is assumed that Adv is able to solve QR problem. Thus, Adv knows the prime factorization of n. In this case, Adv knows γ from $\gamma^2=xr\,(\bmod n)$ but still cannot calculate the third component signature, s from $\gamma^2 h(m)\equiv x^2K^2+\gamma^2 s\,(\bmod n)$ because he or she does not knows the value of x and K due to the difficulty of breaking CM.

Attack 5. Adv may also try collecting T valid signature (K_j,γ_j,s_j) on message M_j where $j=1,2,\ldots,t$, and attempts to find the secret key of the signature scheme. In this case, Adv has s equations as follows.

$$\begin{aligned}
\gamma_1^2 h(M_1) &= K_1^2x^2+\gamma_1^2 s_1(\bmod n)\\
\gamma_2^2 h(M_2) &= K_2^2x^2+\gamma_2^2 s_2(\bmod n)\\
&\vdots\\
\gamma_t^2 h(M_t) &= K_t^2x^2+\gamma_t^2 s_t(\bmod n)
\end{aligned}$$

In the above t equation, there are $(3t+1)$ variables i.e. (K_j,γ_j,s_j) and x, where $j=1,2,\ldots,t$, all of which is unknown by Adv. Hence, x remains hard to be obtained as Adv generates an infinite number of solutions for the above system of equations and cannot figure out which one is correct.

5 Performance evaluation

In this section, we evaluate the performance of our scheme and compare it with other related authentication schemes. It is generally known that most of the mobile devices have limited power resources and computing capability. Therefore, one of the most important concerns of design authentication scheme in mobile environment is power consumption (including computation cost and communication cost). Compared to RSA and ECC, Chebyshev polynomial computation problem offers smaller key sizes, faster computation. In our proposed authentication scheme, there is no time-consuming modular exponentiation and scalar multiplication on elliptic curves needed. Since exclusive OR operation requires extremely small computational cost, we neglect its computation cost. For the convenience of evaluating the computational cost, we define some notations as follows.T_h: time required to compute hash function,$T_h\approx 0.0005ms$, which is negligible; T_{ch}: time required to compute extended chaotic function, $T_{ch}\approx 0.032ms$; T_{exp}: time required to compute exponentiation function, $T_{exp}\approx 5.37s$; T_{mul}: time required to compute multiplication function, $T_{mul}\approx 0.00207ms$;T_{sqr}: time complexity for executing the modular square root computation, $T_{sqr}\approx 0.0041ms$ and T_{inv}: time required to compute inverse function, $T_{inv}\approx 0.0207ms$ [27,28].

In Table 1, we summarize the efficiency comparisons among our proposed scheme and other previous digital signature schemes in terms of computational complexity and the execution time. From Table 1, we can see that the computation cost of our scheme is lower than that of Ismail et al. and Chiou schemes on three phases. Therefore, our proposed scheme is the most efficient one compared to the other two related schemes in terms of overall computation costs, and it can be claimed that the execution time of the proposed scheme is suitable for different real-life applications, including medical care systems.

6 Conclusion

In this paper, we proposed a new digital signature scheme. The security of our scheme is based on chaotic maps and quadratic residue problems. Several possible attacks have also been considered. In addition, the performance comparison for the proposed scheme in relation to the other studies has been analyzed, and we conclude that the proposed scheme properly considers the efficiency and robustness.

References

[1] S. Hwang, C. Yang,and F. Tzeng, Improved digital signature scheme based on factoring and discrete logarithms, Journal

Table 1: Performance comparisons among the proposed scheme and other related schemes

Phases/Schemes	The proposed scheme	Ismail et al's scheme [15]	Chiou's [14] scheme
Key generation phase	$3T_{ch}+T_{sqr}$	$T_{exp}+Tsqr$	$T_{exp}+T_{inv}$
Signature generation phase	$T_{ch}+4T_{sqr}$ $+4T_{mul}$	$T_{exp}+4T_{sqr}$ $+2T_{mul}$	$3T_{exp}+2T_{mul}$ $2T_{sqr}$
Signature verification phase	$6T_{sqr}+6T_{ch}$ $+4T_{mul}$	$3T_{exp}+3T_{sqr}$ $+T_{sqr}$	$4T_{exp}+T_{mul}$
Total costs	$10T_{ch}+8T_{mul}$ $+11T_{sqr}$	$5T_{exp}+2T_{mul}$ $+8T_{sqr}$	$8T_{exp}+Tinv$ $3T_{mul}+3T_{sqr}$
Execution time(ms)	0.32386	27.050534	42.9993
Type of based hard problem	CH and QR	DL and QR	DL and FAC

of Discrete Mathematical Sciences and Cryptography, Vol.5, No.2, pp.151-155(2002)

[2] F. Pon, H. Lu, and B. Jeng, Meta-He digital signature schemes based on factoring and discrete logarithms, Applied Mathematics and Computation, Vol.165, No.1, pp.171-176(2005)

[3] F. Tzeng, Y. Yang and S. Hwang, A new digital signature scheme based on factorings and discrete logarithms, International Journal of Computer Mathematics, Vol.18, No.1, pp 9-14(2004).

[4] L. Harn, Public-key cryptosystem design based on factoring and discrete logarithms, IEE Proceedings Computers and Digital Techniques, Vol. 141, No.3, pp.193-195(1994).

[5] N. Lee and T. Hwang, Modified Harn signature scheme based on factoring and discrete logarithms, IEE Proceeding of Computers Digital Techniques, Vol.143, No.3, pp.196-198(1996).

[6] J. Li and G. Xiao, Remarks on new signature scheme based on two hard problems, Electronics Letters, Vol.34, No.25, pp.2401-2402(1998).

[7] Z. Shao, Digital signature schemes based on factoring and discrete logarithms, Electronics Letters, Vol.38, No.24, pp.1518-1519(2002).

[8] H. He, Digital signature schemes based on factoring and discrete logarithms ,Electronics Letters, Vol.37, No.4, pp.220-222(2001)

[9] S. Hung, Cryptanalysis of a digital signature scheme based on factoring and discrete logarithms. Proceedings of the National Computer Symposium, Taipei, Taiwan, F043-F045,(2001).

[10] H. Qian, F. Cao and H. Bao, Cryptanalysis of LiTzeng Hwang improved signature schemes based on factoring and discrete logarithms, Applied Mathematics and Computation, Vol.166, No.3, pp.501-505(2005)

[11] C. Wang, H. Lin and C. Chang, Signature scheme based on two hard problems simultaneously, Proceedings of the 17th International Conference on Advanced Information Networking and Application (AINA), Xian, China, pp.557-560(2003)

[12] E. Ismail, N. Tahat and R. Ahmad, A New Digital Signature Scheme Based on Factoring and Discrete Logarithms, Journal of Mathematics and Statistics Vol.4, No.4, pp.222-225(2008).

[13] K. Chain, and C. Kuo,A new digital signature scheme based on chaotic maps. Nonlinear Dynamics, Vol.24, No.4, pp.1003-1012(2013).

[14] S. Chiou, Novel digital signature schemes based on factoring and discrete logarithms, International Journal of Security and Its Applications, Vol.10, No.3, pp.295-310(2016).

[15] E. Ismail and N. Tahat, A New signature scheme based on multiple hard number theoretic problems, International Scholarly Research Notices, Vol.2011, Article ID 231649, 3 pages,(2011).

[16] R. Matthews, On the derivation of a chaotic encryption algorithm, Cryptologia,Vol.13, No.1, pp.29-41 (1989)

[17] X. Li and D. Zhao, Optical color image encryption with redefined fractional Hartley transform, International Journal for Light and Electron Optics, Vol.121, No.7, pp.673-677(2010)

[18] J. Tay, C. Quan, W. Chen and Y. Fu, Color image encryption based on interference and virtual optics, Optics and Laser Technology, Vol.42, No.2, pp.409 -415(2010).

[19] W. Chen, C. Quan and J. Tay, Optical color image encryption based on Arnold transform and interference method, Optics Communications, Vol.282, No.18, pp.3680-3685(2009).

[20] K. Martin, R. Lukac and N. Plataniotis, Efficient encryption of wavelet-based coded color images, Pattern Recognition, Vol. 38, No.7, pp.1111-1115(2005).

[21] D. Xiao, F. Liao and J. Deng, A novel key agreement protocol based on chaotic maps, Journal of Information Sciences, Vol.177, No.4, pp. 1136-1142(2007).

[22] S. Hwang, C. Yang and F. Tzeng, Improved digital signature scheme based on factoring and discrete logarithms, Journal

of Discrete Mathematical Sciences and Cryptography, Vol.5, No.2, pp. 151- 155(2002).

[23] J. Niu and Y. Wang, An anonymous key agreement protocol based on chaotic maps, Journal of Communications in Nonlinear Science and Numerical Simulation, Vol.16, No.4, pp.1986-1992(2011).

[24] Y. Wang and F. Zhao, An improved key agreement protocol based on chaos, Journal of Communications in Nonlinear Science and Numerical Simulation, Vol.15, No.12, pp.4052-4057(2010).

[25] D. Xiao, F. Liao and W. Wong, An efficient entire chaos-based scheme for deniable authentication, Journal of Chaos, Solitons and Fractals, Vol.23, No.4, pp.1327-1331(2005).

[26] J. Yoon and S. Jeon, An efficient and secure Diffie-Hellman key agreement protocol based on Chebyshev chaotic map, Journal of Communications in Nonlinear Science and Numerical Simulation, Vol.16, No.6, pp.2383- 2389(2011).

[27] L. Bakrawy, N. Ghali, A. Hassanien and Th. Kim, A fast and secure one-way hash function, Compututer and Information Science, Vol.259, pp.85-93 (2011).

[28] L. Xiong, N. Jianwei, K. Saru, H. Sk, W. Fan, K. Muhammad and K. Ashok, A novel chaotic maps-based user authentication and key agreement protocol for multi-sever environments with provable security, Wireless Pers Communication, Vol.89, No.2, pp.569-597(2016).

[29] L. Zhang, Cryptanalysis of the public key encryption based on multiple chaotic systems, Chaos Solitons Fractals, Vol.37, No.3, pp.669-674 (2008)

Nedal Tahat He received the B.Sc. degree in mathematics from Yarmouk University, Jordan, in 1994, the M.Sc. degree in Pure Mathematics from Al al-Bayt University,Jordan, in 1998, and the Ph.D. degree 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.

Mohammad Saleh Hijazi is an assistant professor and head of the mathematics department in the college of arts and sciences in Jouf University since 2014 until present. He got his phd in mathematics from University Kebengsaan Malasya (UKM) in 2013. The PhD dissertation is about cryptography, design new cryptosystem and digital signature schemes based on multiple hard problems based on number theory and algebra. He also holds a M.Sc degree in Mathematics from Yarmouk University -Jordan, 2004 and B.Sc in Mathematics Yarmouk University-Jordan Very 2000