Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 3, pp. 1059–1071
DOI : 10.47974/JDMSC-1823

A novel chaotic map partially blind signature scheme based on quadratic residue problems

Mohammad Alaroud
Department of Mathematics
Faculty of Arts and Science
Amman Arab University
Amman 11953
Jordan

Nedal Tahat *
Department of Mathematics
Faculty of Sciences
The Hashemite University
Zarqa
Jordan

A. K. Alomari
Department of Mathematics
Faculty of Science
Yarmouk University
Irbid
Jordan

Obaida M. Al-hazaimeh
Department of Computer Science
Al-Balqa Applied University
Jordan

This article has been corrected with minor changes. These changes do not impact the academic content of the article.

* *E-mail:* **nedal@hu.edu.jo**

Abstract

A Novel Partially Blind Signature Scheme (PBSS) Using Quadratic Residue (QR) and Chaotic Map (CM) Issues. To avoid the signer learning the contents of the message, the user can use a blind signature to acquire their consent. Yet, there remains situations where additional information relevant to the signature should be recorded by the signer. This supports the implementation of the concept "partially blind signature,"which provides moreaccess to information within the signed message. Scholars are increasingly interested in developing electronic signature techniques based on mathematical problems because of the growing emphasis on the relevance of security and efficiency in this field. In this work, we combine aspects of cryptography with those of chaotic systems (CS) to offer a technique with low computational requirements. Intractability of the quadratic residue issue and the discrete logarithm of Chebyshev polynomials are crucial to the scheme's security. Through a comparison of performance metrics based on two challenging challenges, the research findings indicate that the proposed approach boasts Reduced communication expenditure compared to existing techniques in the literature. This work represents a pioneering effort as it introduces a novel chaotic map-based partially blind signature method and the quadratic residue problem, marking a first-of-its-kind contribution in this field.

Subject Classification: *94A62; 11T71.*

Keywords: *Quadratic residue, Chaotic maps, Digital signature, Cryptography.*

1. Introduction

The blind digital signature was first proposed by Chaum (1983) [1] and Chaum[2] to protect the privacy of e-cash users. To use one of these signatures, the signer must be able to put their name to a document without reading it beforehand. In addition, the signer should not have the ability to tell when or for whom the paper was signed if he ever sees the signature pair (despite verifying the signature's validity). To resolve the contradiction between the anonymity and controllability of blind signatures, Abe and Fujisaki [3]introduced the notion of partially blind signature in 1996.The signed message is separated into two sections when using a partially blind signature; the first portion contains information that is known to both the signer and the recipient, such as the signed message's scope. Part two is the message itself, which will be confidential while it is being signed. This approach not only ensures the signer's anonymity, but also gives them some say over the information included in the signature itself. All existing blind signature techniques [4-10]are built on solutions to a single hard problem, such as factoring or discrete logarithm or elliptic curve discrete logarithm problems.

Using the quadratic residue problem, Chun-I et al. (1998) [11]suggested a largely blind technique in which neither modular exponentiations nor inverse computations are done by the signatories being requested. For signature requesters or users, the computation load is decreased by about 98% under a

1024-bit modulus with the blind signature approaches proposed by Chun-I et al. (1998), but not for the signer. Users of smart cards and mobile signature requesters would benefit greatly from their strategy.While the partially blind signature system suggested by Hwang et al. (2002)[12] is secure, it does not guarantee anonymity. After that, Huang et al. (2004) [13]Developed a novel, efficient partially blind signature scheme using discrete logarithm and the Chinese remainder theorem. However, Zhang and Chen (2005) [14] demonstrated that their schemewas insecure because an eavesdropper could strip the signer's signature of any embedded public common information and acquired a partially blind signature with a special public information.There has been a recent proposal of a new partially blind signature scheme by Tahat et al. [15] that uses factoring, discrete logarithm problems, and a chaotic map. However, the performance of this scheme greatly exceeds that of the proposed scheme, and the primary cause for such variance is the fact it requires few operations.Back in 1989 [16], the first algorithm for encrypting images using chaotic maps was proposed [16]. Several methods have been proposed in recent years[10, 12, 17-23], indicating an increasing interest in this field of study. Chaotic map public cryptosystems have much lower computational costs than public cryptosystems based on modular exponential computing or scalar multiplication on elliptic curves[24]. As a result, in this research, we will suggest a novel chaotic map and factoring problem–based partially blind signature system. As a result of the minimized number of operations, the proposed method outperforms earlier partially blind signature schemes relying on two challenging problems by a significant margin. Here are the remaining sections of this paper: In Section 2, we will explore the history of extended chaotic maps, describe them in detail, and talk about two related computational issues. The suggestion for partially blind signatures will be introduced in Section 3. An extensive analysis of the proposed scheme's performance will be presented in Section 4. Performance comparisons will be shown in Section 5, and the paper will be concluded in Section 6.

2. Related materials

In this section, we will illustrate some basic elliptic curve tools and define the two underlying hard problems QRP and CMP.

2.1 *Chebyshev chaotic transforms*

We analyzed the operatory of Chebyshev sequential polynomials (CSP; see[25]for details).CSP $T_\delta(\mu)$ is a polynomial of n-degree in the variants μ. Let $\mu \in [-1,1]$ be the version, and let n be an integer. Briefly, CSP stated as:

$$T_n(\mu) = cos\big(n\ cos^{-1}(\mu)\big), T_0(\mu) = 1, T_1(\mu) = \mu$$

$$T_n(\mu) = 2\mu T_{n-1}(\mu) - T_{n-2}(\mu); n \geq 2$$

Here, we have a representation of the functional $\cos^{-1}(\mu)$ and $\cos(\mu)$ as $cos^{-1}: [-1,1] \longrightarrow [0,\pi]$and $cos: R \longrightarrow [-1,1]$. Chaotic properties and semi-group properties are the two most prominent characteristics of CSP [23-27].

1. The chaotic possessions: CSP transformation defined as $T_\delta: [-1,1] \longrightarrow [-1,1]$ with degree $> 1$is a chaotic transform connected to the functional (invariant density) $f^*(\mu) = \frac{1}{\left(\pi\sqrt{1-\mu^2}\right)}$
2. The properties of the so-called semi-group satisfy the following equalities:
$$T_\sigma(T_\rho(\mu)) = \cos(\sigma cos^{-1}(\cos(\rho\, cos^{-1}(\mu)))) = \cos(\sigma\rho\, cos^{-1}(\mu)) = T_{\rho\sigma}(\mu) = T_\rho(T_\sigma(\mu)),$$
where ρ and σ are positive integer and$\mu \in [-1,1]$.

Two tests are available for Chebyshev polynomials that take into account their handling in polynomial time.

1. The goal of the discrete logarithm problem is to determine two integers s for a given pair of elements x and y.such that $T_s(x) = y$.
2. In order to address the problem of Diffie-Hellman, it is imperative to calculate the elements$x$, $T_r(x)$, and $T_s(y)$, to compute elements $T_{rs}(x)$. Assume p is not a prime number. Any positive integer a satisfying $\gcd(a,p) = 1$ (i.e., a co-prime to p) is said to be a quadratic residue mod p if and only if there exists a positive integer x such that the congruence $x^2 \equiv a\ mod\ p$. However, if it is not a quadratic residue mod p, we say that an is quadratic. The characteristic function of the quadratic residues mod p was first introduced by Legendre to make it easier to study their properties. Legendre's symbol $\left(\frac{*}{p}\right)$is defined as follows: for any integer a,
$$\left(\frac{a}{p}\right) = \begin{cases} 1\,, & \text{if } a \text{ is a quadratic residue } (\text{mod } p), \\ -1, & \text{if } a \text{ is a quadratic non} - \text{residue } (\text{mod } p) \text{ and}, \\ 0, & \text{if } p \text{ divides } a \end{cases}$$
3. Let p, q be large, strong prime, and y be a positive integer. This is called QRP. Find the value of y, such that $y \equiv \beta^2\ (mod\ pq)$.

3. The proposed scheme for partially blind signatures

In order to describe our new partially blind signature scheme, analyze its security, and discuss its performance in terms of both efficiency and speed, we will need the following throughout the article: A large number, denoted as "p," and another number "n" are both factors of *(p-1)*. Here, *(p-1)* is the result of multiplying two safe prime numbers, "p" and "q," where n is calculated as $n = p * q$. ψ represents an element in the finite field GF(P) whose order modulo p is n. Additionally, "G" represents the multiplicative group that is generated by ψ.. If we take $t = 128$, then the output of the cryptographic hash function h(.) will be t-bits in length. Please take note that the system hides the large prime numbers $\bar{p}$ and $\bar{q}$.

3.1 *Generating keys*

For the signing process, the integer "e" is selected from the set $\mathbb{Z}_n^*$ with $\text{ggcd}(e,n)=1$ and computes "d" as integer like as $ed \equiv 1 \pmod{\varphi(n)}$.Then, after drawing an integer b at random from $\mathbb{Z}_n^*$, you must compute

$$w = T_{v^4}(\psi)(mod\ p\ ).$$

(w,n,p) and (v,p,q) denote the system's public and private keys, respectively.

3.2 *Algotithm for signing message*

The message-signing algorithm for our scheme is described in this section. In order to sign a message, the signer must first identify the message's m, and then calculate its hash value, $h(m)$. There are two stages to the signing algorithm: the request and the signature extraction stage.

3.1.1 Requesting

Let's pretend that party A needs to have a message signed $h(m)$. First, he needs to alert the signer, and then he must:

- Select an integer $r \in \mathbb{Z}_n^*$by signer and compute$\hat{k} = T_{r^4}(\psi)(mod\ p)$
- The signer must then verify$\text{gcd}(\hat{k}, n) = 1$. If this condition is not met, the signer sends $\hat{k}$ to the requester A.
- Upon receiving $\hat{k}$ from requester A, the signer verifies whether $\text{ggcd}(\hat{k}, n) = 1$ and formats "c" as specified. Thus, requester A and the signer share "c" as an input.
- Furthermore, Requester A chooses two factors to be blinded at random $\alpha, \beta \in \mathbb{Z}_n^*$ and computes $k = T_{\beta^4}(\hat{k}) \pmod{p}$ then verify whether $\text{gcd}(k, n) = 1$. If not, he reverts to the previous step of choosing a new potential blinding factor. Otherwise, he computes $\delta = \alpha^{-1}h(m)\ \hat{k}k^{-1} \pmod{n}$ and notifies the signer by sending (δ, c).

3.1.2 Extraction and signature

This is the blind signature of the signer for message$h(m)$:

- The signer computes and sends$\hat{s} \equiv \delta\ rv^{-1}\hat{k}\ c \pmod{n}$to requester A
- Requester A computes and sends$\lambda \equiv \alpha\ \hat{s}^2 k^2 \hat{k}^{-2}\ \beta \pmod{n}$to the signer
- The signer computes and sends$\hat{u} \equiv \lambda^2 \pmod{n}$ to the requester A
- The requester A computes$\xi \equiv \hat{u}(\hat{s}^{-1})^2 \pmod{n}$. Then the signature is given by$(c,\ k, \xi)$.

3.2 *Algorithm for verifying signature*

Everyone can confirmthe validity of the resulted signature using verifying equation below. If its holds, receiver can convince that the message was signed by the original or legal signer. The requester accept the signature $(c,\ k, \xi)$ if

$$T_{\xi^2}(w) = T_{h(m)^4 k^4 c^4}(k) \pmod{p}$$

Theorem 1: *If* $(c,\ k, \xi)$ *is a novel partially blind signature scheme's signature for "m", then*

$$T_{\xi^2}(w) = T_{h(m)^4k^4c^4(mod\ n)}(k)(\text{mod } p)$$

Proof: Note that, $\xi^2 = (\hat{u}(\hat{s})^{-2})^2$

$$= \lambda^4(\hat{s})^{-4}$$
$$= \left(\alpha^4\hat{s}^8k^8\hat{k}^{-8}\beta^4\right)\hat{s}^{-4}$$
$$= \alpha^4\hat{s}^4k^8\hat{k}^{-8}\beta^4$$
$$= (\alpha^4.v^{-4}r^4\delta^4c^4)k^8\hat{k}^{-8}\beta^4$$
$$= \left(\alpha^4.v^{-4}r^4\alpha^{-4}h(m)^4\hat{k}^4c^4\hat{k}^4\right)k^8\hat{k}^{-8}\beta^4$$
$$= v^{-4}r^4h(m)^4k^4\beta^4c^4(\text{mod } n)$$

And thus $T_{\xi^2}(w) = T_{v^{-4}r^4h(m)^4k^4\beta^4c^4(\text{mod } n)}(T_{v^4}(\psi))$

$$= T_{v^{-4}r^4h(m)^4k^4\beta^4c^4v^4(\text{mod } n)}(\psi)$$
$$= T_{r^4h(m)^4k^4\beta^4c^4(\text{mod } n)}(\psi)$$
$$= T_{h(m)^4k^4c^4(\text{mod } n)}T_{r^4\beta^4(\text{mod } n)}(\psi)$$
$$= T_{h(m)^4k^4c^4(\text{mod } n)}T_{\beta^4(\text{mod } n)}T_{r^4}(\psi)$$
$$= T_{h(m)^4k^4c^4(\text{mod } n)}T_{\beta^4(\text{mod } n)}\ (\hat{k})$$
$$= T_{h(m)^4k^4c^4(\text{mod } n)}(k)(\text{mod } p$$

which means that m can be signed using $(c,\ k, \xi)$. As a result, our proposed protocol offers a form of blind signature verification.

4. Security analysis

Some of the security features of our partially blind signature scheme are discussed here. The following conditions must be met by any secure partially blind signature scheme:

4.1 *Condition of partial blindness*

Requesters and signer of PBSSs have worked together to establish a standard format for communicating about partial-blindness properties. During the verification of signature process, the requester cannot alter or **omit** the embedded information. The requester in the proposed scheme provides the common information c and the blinded data to the signer, who then calculates and sends the requested value of$\hat{s} \equiv \delta\ rv^{-1}\hat{k}\ c\ (\text{mod } n)$. The requester calculates $\hat{s}$. if he is able to modify or delete the shared data from the corresponding signature$(c,\ k, \xi)$. However, determining the secret key v presents a significant challenge. In addition, the requester must provide λ to the signer (i.e., blinded), who afterwards calculates and returns the requested $\hat{u}$ to the requester. QRP is hard to solve, so the requester is stuck with $\hat{u} \equiv \lambda^2(\text{mod } n)$.Therefore, in PBSS, the requester is unable to falsify the unblinded

portion by manipulating or removing "c" and "$\widehat{u}$" from signature (c, k, ξ) of message $h(m)$.

4.2 *Randomization*

To implement the proposed scheme, the signer will blindly send the requester $\hat{k} = T_{r^4}(\psi)(\text{mod } p)$, where r is a random factor. The requester then sends to the signer, who in turn sends back the following: $\hat{s} \equiv \delta\, r v^{-1} \hat{k}\, c \pmod{n}$. Removal of r from $\hat{s}$ would require deriving $v$from $w = T_{v^4}(\psi)(\text{mod } p)$, a clearly infeasible difficulty of solving the CM and QR problems. Thus, requester A cannot eliminate message randomness under the proposed scheme, corresponding signature$(c,\ k, \xi)$.

4.3 *Unlink ability*

During each instance i of the protocol, the signer can keep a log of the message passed between the requester and themselves (δ_i, λ_i) thanks to the unlink ability property. The pair (δ_i, λ_i) represents the signer's perspective on protocol instance i. The resulting theorem is as follows:

Theorem 2: *Giving a signature* $(c,\ k, \xi)$ *produced by PBSS, the signer can derive* (α_i', β_i') *for every* (δ_i, λ_i) *such that:*

$$\delta_i = (\alpha_i')^{-1} h(m) \hat{k} k^{-1} (\text{mod } n)$$
$$\lambda_i \equiv \alpha_i' \hat{s}^2 k^2 \hat{k}^{-2} \beta_i' (\text{mod } n)$$

Proof: From $\delta_i = (\alpha_i')^{-1} h(m) \hat{k} k^{-1} (\text{mod } n)$, we have that $\alpha_i' \equiv \delta_i'\, h(m)\ \hat{k} k^{-1} (\text{mod } n)$ and from $\lambda_i \equiv \alpha_i' \hat{s}^2 k^2 \hat{k}^{-2} \beta_i' (\text{mod } n)$ we obtain $\beta_i' \equiv (\alpha_i')^{-1}\ \hat{k}^2 k^{-2} \hat{s}^{-2} s_i (\text{mod } n)$

Based on these inferences, the signer can calculate α_i', β_i' for each and every record. Therefore, the signer can consistently ascertain the two blinding factors (α_i', β_i') for each transmitted record $(\delta_i, \lambda_i)$when provided with a signature$(c,\ k, \xi)$ generated by PBSS.This indicates that the signer has lost track of the connection between the signature and the instance of the signing process to which it belongs. Therefore, the unlink ability property is met by our method.

4.4 *Unforgeability*

Solving the QR problem and the discrete logarithm problem associated with Chebyshev polynomials is known for its considerable computational difficulty, these two problems form the basis of our scheme's security. Below are some of the possible routes an adversary Adv could take to forge a signature.

Attack 1: Adv makes several attempts to forge signatures using various methods. Using all of the data at their disposal, Adv hopes to deduce the secret key v. Given the complexity of CM and QR problems, it is obvious that solving $w = T_{v^{4(mod\ n)}}(\psi)(mod\ p)$ is impossible for Adv.

Attack 2: By fixing two integers and trying to determine the third, Adv attempts to derive the signature $(c, k, \xi)$for a given message $h(m)$.For example, Advselects c and k and tries to figure out the value of ξsuch that $T_{\xi^2}(w) = T_{h(m)^4k^4c^4}(k) \pmod p$.To do this, Adv firstpicks at random an integers c, k and computes $\tau = T_{h(m)^4k^4c^4}(k)$. Finally he solves $\tau = T_{\xi^2}(w) \bmod p$for u but can only find ξif both QRP and CM are breakable. Next, he may choose (ξ, k) and try to find c. He computes $\mu = T_{\xi^2}(w) \pmod p$ and $\omega = T_{h(m)^4k^4c^4}(k) \pmod p$. Then he finds c from $T_{c^4}(\omega) \pmod p$ but only successful if both problems solvable.

Attack 3: To uncover the scheme's secret keys, Adv may also collect t valid on message $m_j$jwhere $j = 1,2, \dots t$. The equations for Adv in this case are as follows:

$$v^4\xi_1^4 = c_1^4\, h(m_1)\beta_1^4 r_1^4 k_1^4 \pmod n$$
$$v^4\xi_2^4 = c_2^4\, h(m_2)\beta_2^4 r_2^4 k_2^4 \pmod n$$
$$\vdots$$
$$v^4\xi_t^4 = c_t^4\, h(m_t)\beta_t^4 r_t^4 k_t^4 \pmod n$$

The above t equations contain $(2t + 1)$ unknown variables: v, r_j and β_j. Given that Adv can producethere exists an infinite number of solutions to the system of equations described above, but it is impossible to discern which one is the correct solution, v remains difficult to detect.

Attack 4: For the sake of argument, let's say that Adv can figure out CM. Adv here knows v^4, but he is unable to locate b because of the QRP problem. Hence cannot find $\lambda, \hat{s}$and $\hat{u}$, he cannot compute $\xi = \hat{u}(\hat{s}^{-1})^2 \pmod n$and fails to generate the signature(c, k, ξ).

Attack 5: Let's pretend can figure out QRP. This means that he is familiar with the prime factors of $n, \bar{p},$ and $\bar{q}$. The lack of information v, he is unable to compute s and $\xi = \hat{u}(\hat{s}^{-1})^2 \pmod n \pmod n$, so unable to generate (c, k, ξ) as signature.

5. Performance comparison

Here, the target method is comparedto recently presented methods, such as those presented by Tahat et al.[15] and Tahat el at [26]. Costs of data storage, data transfer, and computation have all been considered when discussing the effectiveness of the proposed work. Table 1 displays some used notations in quantitative comparisons. Costs associated with both the signing and verification processes have been considered in the analysis of performance. The relative estimation notations are listed in Table 2. The relations between $T_{exp}, T_{chaotic}, T_{mul}, T_{inv}, T_{sqr}$ and with respect to $T_{hash} \approx 0.32\, ms$ has been established in [27–36].Table 3 displays the relationships between the aforementioned notations, all of which have been used in the proposed work.

Table 2 displays a ranking of the metrics according to their computational complexity;

$$T_{hash} \approx T_{chaotic} < T_{mul} < T_{inv} < T_{exp}$$

Table 1
Notations used in quantitative comparisons.

Sr. No.	Notation	Meaning
1	T_{exp}	Group modular exponentiation execution time
2	$T_{chaotic}$	The duration of a chaotic map's execution
3	T_{mul}	Modular multiplication time
4	T_{hash}	One-way hash execution time
5	T_{sqr}	Modular square computation time
6	T_{inv}	Inverse modular operating time

Table 2
Relationships among notations

Sr. No.	Relationships among notations
1	$T_{hash} \approx T_{chaotic}$
2	$T_{mul} \approx 2.5\, T_{hash}$
3	$T_{inv} \approx 7.5 T_{hash}$
4	$T_{sqr} \approx 5 T_{hash}$
5	$T_{exp} \approx 600 T_{hash}$

Table 3
Quantitative analysis of signing and verification computational costs

Schemes/Stages	Signing stage	Verification stage	Total (ms)
The Scheme in [15]	$2T_{exp} + 2T_{chaotic} + 5T_{inv} + T_{hash} + 12T_{mul}$	$2T_{exp} + 6T_{chaotic} + 9T_{mul}$	794.16
The Scheme in [26]	$5T_{exp} + 4T_{inv} + T_{hash} + 13T_{mul}$	$4T_{exp} + T_{hash} + T_{mul}$	1749.44
Proposed PBSS	$2T_{chaotic} + 4T_{inv} + T_{hash} + 29T_{mul}$	$2T_{chaotic} + 16T_{mul} + T_{hash}$	47.52

In Table 3, we compare the computational complexity and runtime of our proposed scheme to those of other existing digital signature schemes. Table 3 demonstrates that compared to Tahat et al. [15], Tahat et al. [26], our scheme has a lower computation cost. Instead of taking 794.16 ms[15] or 1749.44 ms[26], our method only takes 47.52 ms.

6. Conclusion

Here, we provide a partially blind signature scheme that takes the problem of factoring and chaotic maps as its foundation. The security of the proposed scheme relies on the fact that both the quadratic residue and the discrete logarithm of Chebyshev polynomials are unsolvable. The inherent nature of Chebyshev polynomials means that the proposed scheme uses fewer bits and has a lower computation cost than partially blind signature schemes. Our suggested scheme is more applicable because it provides superior safety, dependability, and efficiency in real-world scenarios.

References

[1] D. Chaum, "Blind signatures for untraceable payments," in *Advances in cryptology*, pp. 199-203 (1983).

[2] D. Chaum, "Blind signature system," in *Advances in cryptology*, pp. 153-153 (1984).

[3] M. Abe and E. Fujisaki, "How to date blind signatures," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 244-251 (1996).

[4] C.-I. Fan, W.-K. Chen, and Y.-S. Yeh, "Randomization enhanced Chaum's blind signature scheme," *Computer Communications,* vol. 23, pp. 1677-1680 (2000).

[5] C.-I. Fan and C.-L. Lei, "Cryptanalysis on improved user efficient blind signatures," *Electronics Letters,* vol. 37, p. 1 (2001).

[6] K. Nyberg and R. A. Rueppel, "A new signature scheme based on the DSA giving message recovery," in *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pp. 58-61 (1993).

[7] T. Okamoto and K. Ohta, "Universal electronic cash," in *Annual international cryptology conference*, pp. 324-337 (1992).

[8] O. Al-Hazaimeh, M. Al-Jamal, M. Bawaneh, N. Alhindawi, and B. Hamdoni, "A new image encryption scheme using dual chaotic map synchronization," *International Arab Journal of Information Technology,* vol. 18, pp. 95-102 (2021).

[9] O. M. Al-Hazaimeh, "A new dynamic speech encryption algorithm based on Lorenz chaotic map over internet protocol," *International Journal of Electrical & Computer Engineering (2088-8708),* vol. 10 (2020).

[10] O. M. Al-Hazaimeh, "A new speech encryption algorithm based on dual shuffling Hénon chaotic map," *International Journal of Electrical and Computer Engineering (IJECE),* vol. 11, pp. 2203-2210 (2021).

[11] C.-I. Fan and C.-L. Lei, "Low-computation partially blind signatures for electronic cash," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences,* vol. 81, pp. 818-824 (1998).

[12] K. Chain and W.-C. Kuo, "A new digital signature scheme based on chaotic maps," *Nonlinear dynamics,* vol. 74, pp. 1003-1012 (2013).

[13] H.-F. Huang and C.-C. Chang, "A new design of efficient partially blind signature scheme," *Journal of Systems and Software,* vol. 73, pp. 397-403 (2004).

[14] F. Zhang and X. Chen, "Cryptanalysis of Huang–Chang partially blind signature scheme," *Journal of Systems and Software,* vol. 76, pp. 323-325 (2005).

[15] N. Tahat, S. Shatnawi, and E. S. Ismail, "A new partially blind signature based on factoring and discrete logarithms," *Journal of Mathematics and Statistics,* vol. 4, p. 124 (2008).

[16] R. Matthews, "On the derivation of a "chaotic" encryption algorithm," *Cryptologia,* vol. 13, pp. 29-42 (1989).

[17] W. Chen, C. Quan, and C. Tay, "Optical color image encryption based on Arnold transform and interference method," *Optics communications,* vol. 282, pp. 3680-3685 (2009).

[18] X. Li and D. Zhao, "Optical color image encryption with redefined fractional Hartley transform," *Optik,* vol. 121, pp. 673-677 (2010).

[19] K. Martin, R. Lukac, and K. N. Plataniotis, "Efficient encryption of wavelet-based coded color images," *Pattern Recognition,* vol. 38, pp. 1111-1115 (2005).

[20] C. J. Tay, C. Quan, W. Chen, and Y. Fu, "Color image encryption based on interference and virtual optics," *Optics & Laser Technology,* vol. 42, pp. 409-415 (2010).

[21] O. M. Al-Hazaimeh, M. F. Al-Jamal, A. Alomari, M. J. Bawaneh, and N. Tahat, "Image encryption using anti-synchronisation and Bogdanov transformation map," *International Journal of Computing Science and Mathematics,* vol. 15, pp. 43-59 (2022).

[22] N. Tahat, A. Alomari, A. Al–Freedi, O. M. Al-Hazaimeh, and M. F. Al–Jamal, "An efficient identity-based cryptographic model for Che-

byhev chaotic map and integer factoring based cryptosystem," *Journal of Applied Security Research,* vol. 14, pp. 257-269 (2019).

[23] N. Tahat, A. Alomari, O. M. Al-Hazaimeh, and M. F. Al-Jamal, "An efficient self-certified multi-proxy signature scheme based on elliptic curve discrete logarithm problem," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 23, pp. 935-948 (2020).

[24] O. M. Al-Hazaimeh, A. A. Abu-Ein, M. M. Al-Nawashi, and N. Y. Gharaibeh, "Chaotic based multimedia encryption: a survey for network and internet security," *Bulletin of Electrical Engineering and Informatics,* vol. 11, pp. 2151-2159 (2022).

[25] J. M. D. H. C. Polynomials, "Chapman & Hall," *CRC Boca Raton Florida* (2003).

[26] N. Tahat, E. S. Ismail, and A. Alomari, "Partially blind signature scheme based on chaotic maps and factoring problems," *Italian Journal of Pure and Applied Mathematics,* vol. 165 (2018).

[27] P. Bergamo, P. D'Arco, A. De Santis, and L. Kocarev, "Security of public-key cryptosystems based on Chebyshev polynomials," *IEEE Transactions on Circuits and Systems I: Regular Papers,* vol. 52, pp. 1382-1393 (2005).

[28] S. Han and E. Chang, "Chaotic map based key agreement with/out clock synchronization," *Chaos, Solitons & Fractals,* vol. 39, pp. 1283-1289 (2009).

[29] N. Tahat, A. A. Tahat, M. Abu-Dalu, R. B. Albadarneh, A. E. Abdallah, and O. M. Al-Hazaimeh, "A new RSA public key encryption scheme with chaotic maps," *International Journal of Electrical & Computer Engineering* (2088-8708), vol. 10 (2020).

[30] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems," *Chaos, Solitons & Fractals,* vol. 37, pp. 669-674 (2008).

[31] F. Chen, X. Liao, K.-w. Wong, Q. Han, and Y. Li, "Period distribution analysis of some linear maps," *Communications in Nonlinear Science and Numerical Simulation,* vol. 17, pp. 3848-3856 (2012).

[32] M. H. Ibrahim, S. Kumari, A. K. Das, M. Wazid, and V. Odelu, "Secure anonymous mutual authentication for star two-tier wireless body area networks," *Computer methods and programs in biomedicine,* vol. 135, pp. 37-50 (2016).

[33] Nedal Tahat, Mohd Taib Shatnawi, Safaa Shatnawi, O. Y. Ababneh & Obaida M. Al-Hazaimeh. A signature algorithm based on chaotic maps and factoring problems, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:8, 2783-2794 (2022), DOI: 10.1080/09720529.2022.2101601.

[34] Manoj Kumar Chande, Cheng-Chi Lee & Chun-Ta Li. Cryptanalysis and improvement of a ECDLP based proxy blind signature scheme, *Journal of Discrete Mathematical Sciences and Cryptography*, 21:1, 23-34 (2018), DOI: 10.1080/09720529.2017.1390845.

[35] A. Shakiba. Security analysis for chaotic maps-based mutual authentication and key agreement using smart cards for wireless networks, *Journal of Information and Optimization Sciences*, 40:3, 725-750 (2019), DOI: 10.1080/02522667.2018.1470752.

[36] O. M. Al-Hazaimeh and A. Ma'moun, "Vehicle To Vehicle and Vehicle To Ground Communication-Speech Encryption Algorithm," in *2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, pp. 1-4 (2023).

Received January, 2023