PARTIALLY BLIND SIGNATURE SCHEME BASED ON CHAOTIC MAPS AND FACTORING PROBLEMS

Nedal Tahat*
Department of Mathematics
Faculty of Sciences
The Hashemite University
Zarqa 13133
Jordan
nedal@hu.edu.jo

E.S. Ismail
School of Mathematical Science
Faculty of Sciences and Technology
Universiti Kebangsaan Malaysia
43600 Bangi, Selangor
Malaysia
esbi@ukm.edu.my

A.K. Alomari
Department of Mathematics
Faculty of Science
Yarmouk University
211-63 Irbid
Jordan
abdomari2008@yahoo.com

Abstract. Due to the importance of security and efficiency of electronic signatures schemes, there is an increase in interest among scholars to develop such schemes based on mathematical problems to be more secure and efficient. In this paper, we propose a scheme with a low computation cost based on both cryptographic and chaotic system characteristics. The security of the scheme depends upon the intractability of the factorization problem and discrete logarithm of Chebyshev polynomials. The performance comparison demonstrated that the proposed scheme has a lower communication cost than the existing schemes in the literature, such as the one proposed by Tahat et al. To the best of our knowledge, this is the first time a partially blind signature scheme based on chaotic maps and factoring problem has been proposed.
Keywords: chaotic maps, digital signature, factorization, partially blind signature.

1. Introduction

The concept of blind digital signature was introduced by Chaum (1983) [4] and Chaum (1984) [5] to enable spender anonymity in electronic cash system. Such

∗. Corresponding author

signatures require a signer to be able to sign a document without knowing its contents. Moreover, should the signer ever see the document signature pair, he should not be able to determine when or for whom it was signed (although he can verify that the signature is indeed valid). In order to solve the contradiction between the blind signatures' anonymity and controllability, in 1996, Abe and Fujisaki [1] proposed the concept of partially blind signature. Partially blind signatures will divide the signed message into two parts; one of which is public information that is agreed by the signer and the user, for example, the scope of the signed message. The other part is the message which is kept blind as it waits for a signature. Not only does this scheme protect the privacy of the users, it also allows the signer to control parts of the contents of the signature. All developed blind signature schemes in the literature are designed based on a single hard problem such as factoring, discrete logarithm or elliptic curve discrete logarithm problems [4,5,7,8,16,17]. Chun-I et al. (1998) [9] proposed a partially blind scheme based on quadratic residue problem, in which there are no modular exponentiations or inverse computations performed by the signature requesters. Compared to the blind signature schemes proposed in the literature, Chun-I et al. (1998) reduced the number of computations for the signature requesters or users by nearly 98% under a 1024 -bit modulus, but it does not decrease the computation load for the signer. Their scheme is especially suitable for mobile signature requester and smart-card users. Hwang et al. (2002) [10] has shown, however, that it does not meet the untraceability property of a blind signature. Huang et al. (2004) [11] then proposed a new efficient partially blind signature scheme based on discrete logarithm and the Chinese remainder theorem, but unfortunately Zhang and Chen (2005) [22] later showed that their scheme is not secure, as any malicious requester can remove the embedded public common information from the signer's signature and obtain a partially blind signature with a special public information. Recently, Tahat et al. [18] proposed a new partially blind signature scheme based on factoring and discrete logarithm problems.

The first chaotic map-based image encryption algorithm was proposed in 1989 [15]. Recently, there is a growing interest in this area as several approaches have been proposed in the literature [3,6,12,14,19]. The computational costs of chaotic map-based public cryptosystems are very low compared to public cryptosystems based on modular exponential computing or scalar multiplication on elliptic curves. Hence, in this paper, we will propose a new partially blind signature scheme based on chaotic map and factoring problems. The proposed scheme is much more efficient than previous partially blind signature schemes based on two hard problems due to the decreased number of operations.

The remainder of this paper is organized as follows. Section 2 will describe the theory and properties of the extended chaotic maps and two computational problems. In Section 3, the partially blind signature will be proposed. Security requirements will be described in Section 4. In Section 5, we will present the

performance evaluation of the proposed scheme. A numerical example will be given in Section 6. Finally, Section 7 will conclude the paper.

2. Preliminary knowledge

In this section, we briefly introduce the basic concept of Chebyshev chaotic map and its related mathematical properties [13, 21].

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

$$T_n(x) = \cos(n \cos^{-1}(x)\ ). \tag{2.1}$$

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

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x), \tag{2.2}$$

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 [3, 13, 21]:

• The semi-group property:

$$\begin{aligned} T_r(T_s(x)) &= \cos(r\cos(s\ \cos^{-1}(x)\ )) = \cos(rs\ \cos^{-1}(x)\ ) \\ &= T_{sr}(x) = T_s(T_r(x)), \end{aligned} \tag{2.3}$$

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 [23] proved that the semi-group property holds for Chebyshev polynomials defined on the interval $(-\infty, \infty)$ as follows:

$$T_a(x) = 2xT_{a-1}(x) - T_{a-2}(x)(\text{mod } p), \tag{2.4}$$

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

$$T_r(T_s(x)) = T_{sr}(x) = T_s(T_r(x))(\text{mod } p),$$

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

Theorem 2.1. *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*

$$T_a(M) = \frac{(M + \sqrt{M^2 - 1})^a + (M - \sqrt{M^2 - 1})^a}{2} \pmod{p}.$$

Theorem 2.2. *If a and b are two positive integers and $a > b$, then*

$$2T_a(M).T_b(M) = T_{a+b}(M) + T_{a-b}(M). \tag{2.5}$$

Theorem 2.3. *If $a = b + c$ and p is a large prime number, then*

$$\begin{aligned} &(2T_a(M)\ T_b(M)\ T_c(M) + 1) \pmod{p} \\ &= ([T_a(M)]^2 + [T_b(M)]^2 + [T_c(M)]^2) \pmod{p}. \end{aligned} \tag{2.6}$$

Lemma 2.4. *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 2.5. *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 $\frac{1}{2}(y + y^{-1}) = T_t(M) \in T_a(M)$ in polynomial time.*

Theorem 2.6. *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 2.7. *Let p, n and α be defined as above and G be the group generated by α. To find v such that $a = T_{v^2 (mod\ n)}(\alpha)$ mod p , where a is given and $a \in G$, one must solve both chaotic maps problem in G and the factorization of n.*

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 is to compute elements $T_{rs}(x)$

3. The proposed partially blind signature scheme

Throughout the article, we need the following tools to describe our new partially blind signature scheme and to discuss its security analysis and efficiency performances: A large number p and n is a factor of $p-1$ that is the product of two safe primes $\overline{p}$ and $\overline{q}$ i.e., $n = \overline{pq}$. β is an element in $GF(p)$ whose order modulo p is n, and G is the multiplicative group generated by β. A cryptographic hash function $h(.)$ where the output is $t-$bit length and assume $t = 128$. Note that the two large primes $\overline{p}$ and $\overline{q}$ are kept secret in the system.

3.1 Generating Keys

The signer pick randomly an integer e from $\mathbb{Z}_n^*$ such that $\gcd(e, n) = 1$. Computes an integer d such that $ed \equiv 1(\text{mod } \varphi(n))$. Next select at random an integer x and compute $z = T_x(\beta)$. Here the public and secret keys of the system are given by $(n,\ z)$ and (d, x) respectively.

3.2 Requesting

Suppose requester A wants to obtain a signature on message, $h(m)$. Firstly, he must notify the signer and then:

1. The signer select an integer $r < n$ such that $\gcd(r, n) = 1$ and compute $\hat{t} = T_r(\beta)(\text{mod}p)$.
2. Then, the signer check that $\gcd(\hat{t}, n) = 1$. If this not the case, he/she send $\hat{t}$ to the requester A.
3. After receiving $\hat{t}$, requester A checks if $\gcd(\hat{t}, n) = 1$ and prepares the common information c, according to a pre-defined format. Hence, the value c is a common input of both the requester A and the signer.
4. Requester A also randomly selects two blinding factors $u \in \mathbb{Z}_n^*$, $v \in \mathbb{Z}_n^*$ and compute

$$t = T_{(u+v)}(\hat{t})(\text{mod } p) \tag{3.1}$$

and checks whether $\gcd(t, n) = 1$. If this is not case, he goes back to select another blinding factor. Otherwise, he computes $\mu \equiv u^{-1}h(m)\hat{t}\ t^{-1}\ (\text{mod } n)$ and sends $(\mu,\ c)$ to the signer.

3.3 Signing and extraction

The signer signs blindly the message $h(m)$ as follows:

The signer signs blindly the message $h(m)$ as follows

1. The signer computes and sends

$$\hat{k} \equiv (\mu\ x\ c\ r^{-1} + \hat{t}\ )(\text{mod } n) \tag{3.2}$$

to requester A.

2. Requester A computes and sends

$$k \equiv \hat{k}^{-e}(\ \hat{k}\ t\ \hat{t}^{-1}\ u + v\ t)(\text{mod } n)$$

to the signer.

3. The signer computes and sends

$$\hat{R} \equiv (r\ k)^d \pmod{n} \tag{3.3}$$

to the requester A.

4. The requester A computes

$$R \equiv \hat{R}\ \hat{k} (\mathrm{mod}\ n). \tag{3.4}$$

Then the signature is given by (c, t, R).

The following theorem shows that if a signature (c, t, R) of a message m is produced by the proposed partially blind signature scheme, then it satisfies

$$\begin{aligned} &\left[T_{R^e (mod\ n)}(\beta)\right]^2 + \left[T_{h(m)c\ (mod\ n)}(z)\right]^2 + [T_t(t)]^2 \\ &= (2T_{R^e}(\beta) T_{h(m)c}(z)\ T_t(t) + 1)(\mathrm{mod}\ p). \end{aligned} \tag{3.5}$$

Theorem 3.1. *If (c, t, R) is a signature of the message m produced by a proposed new partially blind signature scheme, then*

$$\begin{aligned} &\left[T_{R^e (mod\ n)}(\beta)\right]^2 + \left[T_{h(m)c\ (mod\ n)}(z)\right]^2 + [T_t(t)]^2 \\ &= (2T_{R^e}(\beta) T_{h(m)c}(z)\ T_t(t) + 1)(\mathrm{mod}\ p). \end{aligned}$$

Proof. We have to show that the signature (c, t, R) satisfies:

$$\begin{aligned} &R^e (mod\ n) \equiv (\hat{R}\ \hat{k})^e \equiv (r^d k^d\ \hat{k})^e \equiv r\ k\ \hat{k}^e \\ &\equiv r\hat{k}^{-e}(\hat{k}\ t\ \hat{t}^{-1}\ u + v\ t)\ \hat{k}^e\ \equiv r(\hat{k}\ t\ \hat{t}^{-1}\ u + v\ t) \\ &\equiv r((\mu\ x\ c\ r^{-1} + \hat{t})t\ \hat{t}^{-1}\ u + vt) \equiv ((\mu\ x\ c\ + \hat{t}r)t\ \hat{t}^{-1}\ u + vt) \\ &\equiv (((u^{-1}h(m)\hat{t}\ t^{-1}\ )\ x\ c\ + \hat{t}r)t\ \hat{t}^{-1}\ u + vtr) \equiv (h(m)xc + tur + vtr)(\mathrm{mod}\ n), \end{aligned}$$

and thus

$$\begin{aligned} &\left[T_{R^e (mod\ n)}(\beta)\right]^2 + \left[T_{h(m)c\ (mod\ n)}(z)\right]^2 + [T_t(t)]^2 \\ &= \left[T_{((h(m)xc+tur+vtr))}(\beta)\right]^2 + \left[T_{h(m)c\ (mod\ n)} T_x(\beta)\right]^2 + \left[T_t T_{(u+v)}(T_r(\beta))\right]^2 \\ &= \left[T_{(h(m)xc+tur+vtr)}(\beta)\right]^2 + \left[T_{h(m)xc}(\beta)\right]^2 + [T_{tur+tvr}(\beta)]^2. \end{aligned}$$

Let $a = h(m)xc + tur + vtr, b = h(m)xc$, $l = tur + tvr$ and $a = b + l$

$$\begin{aligned} &\left[T_{(h(m)xc+tur+vtr)}(\beta)\right]^2 + \left[T_{h(m)xc}(\beta)\right]^2 + [T_{tur+tvr}(\beta)]^2 \\ &= 2T_{(h(m)xc+tur+vtr)}(\beta) T_{h(m)xc}(\beta) T_{tur+tvr}(\beta) + 1 \\ &= (2T_{R^e}(\beta) T_{h(m)c}(z)\ T_t(t) + 1)(\mathrm{mod}\ p), \end{aligned}$$

which means (c, t, R) is a valid signature of m. Therefore, our proposed protocol provides a partially blind signature scheme.

4. Security analysis

In this section, we discuss some security properties of our partially blind signature scheme. A secure partially blind signature scheme should satisfy the following requirements.

4.1 Partial blindness

The partial blindness of all signatures issued by the signer contains a clear common information c according to the predefined format negotiated and agreed by both the requester and the signer. The requester is unable to change or remove the embedded information c while keeping the verification of signature successful. In the proposed scheme, the requester has to submit the blinded data σ to the signer, and then the signer computes and sends σ to the signer, and then the signer computes and sends $\hat{k} \equiv (\mu\ x\ c\ r^{-1} + \hat{t})(\text{mod } n)$. However, it is difficult to derive the secret key x. Also the signature-requester has to submit the blinded data k to the signer then the signer computes and sends $\hat{R}$ to the requester. The signature-requester cannot change or remove $\hat{R} \equiv r^d k^d \pmod{n}$ because it is difficult to derive the secret key d. Hence, in the proposed scheme, the signature-requester cannot change or remove the c and $\hat{R}$ from the corresponding signature (c, t, R), of message m to forge the unblinded part of the signature.

4.2 Randomization

In the proposed scheme, the signer randomizes the blinded data using the random factor r before signing it in the signing phase. In the requesting phase, the signer selects an integer r and sends such that $\hat{t} = T_r(\beta)(\text{mod } p)$ and submit $\hat{t}$ to the requester. Then the requester A sends μ to the signer and the signer returns $\hat{k} \equiv (\mu\ x\ c\ r^{-1} + \hat{t})(\text{mod } n)$ to the requester A. If the requester A tries to remove r from $\hat{k} \equiv (\mu\ x\ c\ r^{-1} + \hat{t})(\text{mod } n)$ and $\hat{R} \equiv r^d k^d \pmod{n}$, then he has to derive x and d which are clearly infeasible difficulty of solving chaotic maps and factoring problem. Hence, in the proposed scheme, the requester A cannot remove the random r from the corresponding signature(c, t, R) of message m

4.3 Unlinkability

For every instance, the signer can record the transmitted messages (μ_i, k_i) between the signature-requester and the signer during the instance i of the protocol. The pair (μ_i, k_i) is usually referred to as the *view* of the signer to the instance i of the protocol. Thus, we have the following theorem:

Theorem 4.1. *Giving a signature (c, t, R) produced by the proposed scheme, the signer can derive $(\acute{u}_i,\ \acute{v}_i)$ for every (μ_i, k_i) such that*

$$\mu_i \equiv (\acute{u}_i)^{-1} h(m) \hat{t}\ t^{-1}\ (mod\ n)\ \ and\ \ k_i \equiv \hat{k}^{-e}(\hat{k}\ t\ \hat{t}^{-1}\ \acute{u}_i + \acute{v}_i\ t)(mod\ n).$$

Proof. $\mu_i \equiv (\acute{u}_i)^{-1} h(m)\hat{t}\ t^{-1} \pmod{n}$, we have that:

$$\mu_i \acute{u}_i \equiv h(m)\hat{t}\ t^{-1} \pmod{n}$$
$$\acute{u}_i \equiv \mu_i^{-1} h(m)\hat{t}\ t^{-1} \pmod{n}.$$

If $k_i \equiv \hat{k}^{-e}(\hat{k}\ t\ \hat{t}^{-1}\ \acute{u}_i + \acute{v}_i\ t) \pmod{n}$, then we have the following derivations:

$$\hat{k}^e \equiv (\hat{k}\ t\ \hat{t}^{-1}\ \acute{u}_i + \acute{v}_i\ t) \pmod{n},$$
$$\acute{v}_i\ t \equiv (k_i \hat{k}^e - \hat{k}\ t\ \hat{t}^{-1}\ \acute{u}_i) \pmod{n},$$
$$\acute{v}_i\ \equiv (k_i \hat{k}^e - \hat{k}\ t\ \hat{t}^{-1}\ \acute{u}_i) t^{-1} \pmod{n}.$$

According to the above derivations, the signer can derive $\acute{u}_i$, $\acute{v}_i$ for every record (μ_i, k_i). Hence, giving a signature (c, t, R) produced by the proposed scheme, the signer can always derive the two blinding factors (μ_i, k_i) for every transmitted record (μ_i, k_i). This implies that the signer is unable to find the link between the signer and its corresponding signing process instance. Thus, our scheme satisfies the unlinkability property.

4.4 Unforgeability

The security of our scheme is based on the difficulty of solving the factoring problem and discrete logarithm problem of Chebyshev polynomials. The adversary Adv may try to derive a forged signature using different ways, as shown below.

Attack 1: Adv tries to derive the signature (c, t, R) for a given message m by letting one integer fixed or two and finding the other one.

In this case, Adv randomly fixes either $(c, t), (c, R)$ or (t, R) to find R, t or c respectively to satisfy

$$\left[T_{R^e (mod\ n)}(\beta)\right]^2 + \left[T_{h(m)c\ (mod\ n)}(z)\right]^2 + \left[T_t(t)\right]^2$$
$$= (2T_{R^e}(\beta) T_{h(m)c}(z)\ T_t(t) + 1) \pmod{p}$$

as difficult chaotic maps problems and factorization, simultaneously.

Case 1. Say Adv fixes the value (c, t) and tries to figure out the value R.
Adv then needs to solve the following equations that can be reduced from Eq.(3.5)

$$\psi^2 - 2\psi T_{h(m)c}(z)\ T_t(t) + \left[T_{h(m)c\ (mod\ n)}(z)\right]^2 + \left[T_t(t)\right]^2 - 1 = 0\ (mod\ p)$$

Therefore, ψ can be recover by the following equation:

$$\psi = \frac{2T_{h(m)c}(z)\ T_t(t)}{2} \pm \frac{\sqrt{(2T_{h(m)c}(z)\ T_t(t))^2 - 4(\left[T_{h(m)c\ (mod\ n)}(z)\right]^2 + \left[T_t(t)\right]^2 - 1)}}{2}. \tag{4.1}$$

However, it is infeasible to fin y from $\psi \equiv T_{R^e(mod\ n)}(\beta)\ mod\ p$ even if he can get ψ from Eq.(4.1)

From Lemma 1, we can see that this is equivalent to solving the chaotic maps problem in G and factorization of n.

Case 2. Say Adv fixes the value (c, R) and tries to figure out the value t.

Then his task is more difficult than Instance 1 because he must find t from η, where

$$\begin{aligned} &\eta^2 - 2\eta T_{h(m)c}(z) T_{R^e(mod\ n)}(\beta) \\ &+ \left[T_{h(m)c\ (mod\ n)}(z)\right]^2 + \left[T_{R^e(mod\ n)}(\beta)\right]^2 - 1 = 0\ (mod\ p). \end{aligned} \tag{4.2}$$

Lemma 1 indicates that this is at least as difficult solving the chaotic maps problems and factorization of n.

Case 3. Say Adv fixes the value (t, R) and tries to figure out the value c.

Then his task is more difficult than Case 1, since he must compute c from

$$\xi^2 - 2\xi T_{R^e}(\beta)\ T_t(t) + \left[T_{R^e(mod\ n)}(\beta)\right]^2 + \left[T_t(t)\right]^2 - 1 = 0\ (mod\ p).$$

Lemma 1 indicates that is at least as hard as solving the chaotic maps problem in G and the factorization n.

Case 4. If Adv randomly chooses one of variable from (c, t, R) , and he wishes to derive the other two variables such that Eq.(2.5), Eq. (2.6), Eq. (3.1) and Eq. (3.5) are upheld, his task is at least as difficult as that of case (1), (2), (3). Furthermore, there is no simpler method than solving the chaotic maps problem in G and the factorization of n.

In the following two attacks, we assume that one the factoring or chaotic maps problems are solvable. The idea is to show that Adv still has to solve the other problem in order to obtain all the secret information.

Attack 2. It is assumed that Ad is able to solve chaotic maps problem. In this case, Adv know x and can generate or calculate the numbers $\hat{k}$ and k. Unfortunately, he does not know d and cannot compute $\hat{R} \equiv r^d k^d \pmod{n}$ and $R \equiv \hat{R}\ \hat{k} \pmod{n}$, then fails to produce the signature(c, t, R).

Attack 3. It is assumed that Ad is able to solve factoring problem, which means he knows the prime factorization of n i.e. $\overline{p}$ and $\overline{q}$ and can find the number d. However, he cannot compute $\hat{k}$, since no information on x is available, hence he cannot compute $R \equiv \hat{R}\ \hat{k}$. Thus fails to produce the signature (c, t, R).

Attack 4. Adv may also try collecting s valid signature (c_j, t_j, R_j) on message M_j where $j = 1, 2, \ldots, s$,and attempts to find the secret keys of the

signature scheme. In this case, Adv has s equations as follows.

$$\begin{aligned} R_1^e &= h(M_1)c_1x + t_1u_1r_1 + t_1v_1r_1 \pmod{n} \\ R_2^e &= h(M_2)c_2x + t_2u_2r_2 + t_2v_2r_2 \pmod{n} \\ &\vdots \\ R_s^e &= h(M_s)c_sx + t_su_sr_s + t_sv_sr_s \pmod{n}. \end{aligned}$$

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

Adv wishes to obtain secret keys (x, d) using all information that is available from the system. In this case, Adv needs to solve $ed \equiv 1 (\text{mod } \varphi(n))$ and $z = T_x(\beta) (\text{mod } p)$ respectively for d and x which are clearly infeasible because the difficulty of solving factoring and chaotic map problems.

5. Performance analysis

Compared to other public key cryptosystems, Chebyshev polynomial computation problem offers smaller key sizes, faster computation as well as memory, energy and bandwidth savings. The computational complexity of ECC is very high, but compared to the ECC encryption algorithm, chaotic maps encryption algorithm avoids scalar multiplication and modular exponentiation computations, effectively improving the efficiency. For the convenience of evaluating the computational cost, we define some notations as follows -T_h: time required to compute hash function,$T_h \approx 0.0005s$; T_C: time required to compute extended chaotic function, $T_C \approx 0.032s$; T_{exp}: time required to compute exponentiation function, $T_{exp} \approx 5.37s$; T_m: time required to compute multiplication function, $T_m \approx 0.00207s$; and T_{inv}: time required to compute inverse function, $T_{inv} \approx 0.0207s$ [2,20].

Table 1 shows the comparison of computational cost between the proposed scheme and the scheme in [18]. We can see that the proposed scheme is more efficient than the scheme in [18]. Our scheme requires only 21.87146 s, while their scheme needs 48.44278 s.

6. Numerical simulation of the scheme

Assume that a signer wishes to sign a hashed message $h(m) = 402$, such that only the intended party can validate the resulting signature

The scheme's set up is done by a signer, with $\overline{p} = 47$, $\overline{q} = 59$, $n = \overline{p}\,\overline{q} = 2773$, $p = 11093$, $\varphi(n) = (\overline{p}-1)(\overline{q}-1) = 2668$, $e = 17$, $d \equiv e^{-1} \equiv 17^{-1} \equiv 157 (\text{mod } 2668)$, $x = 27$, $\beta = 100$, $z = T_{27}(100) (\text{mod } 11093) = 1034$ and the common information $c = 332$.

Table 1: Performance comparisons among our scheme and scheme in [18]

Phases	The proposed scheme		The scheme in [18]	
	Computation cost	Execution time(s)	Computation cost	Execution time(s)
Requesting	$3T_{exp} + 4T_{mul} + 2T_{inv} + T_h$	16.16018	$2T_c + 3T_{mul} + 2T_{inv} + T_h$	0.11202
Singing and Extraction	$2T_{exp} + 9T_{mul} + 2T_{inv}$	10.8003	$2T_{exp} + 10T_{mul} + 3T_{inv}$	10.8228
verification	$4T_{exp} + T_{mul} + T_h$	21.48257	$2T_{exp} + 2T_{mul} + 6T_c + T_h$	10.93664
Total costs	$9T_{exp} + 14T_{mul} + 2T_h + 4T_{inv}$	48.44278	$4T_{exp} + 15T_{mul} + 8T_c + 2T_h + 5T_{inv}$	21.87146

Requesting: A signer select an integer $r = 2551$ such that $\gcd(2551,\ 2773) = 1$ then computes and send $\hat{t} = T_{2551}(100)(\text{mod } 11093) = 8875$ to the requester. The requester then randomly selects two blinding factors $u = 2331,\ v = 2526$ and computes

$$t = T_{(2331+2526)}(8875) \text{ (mod } 11093) \equiv 3292(\text{mod } 11093),$$
$$\mu \equiv u^{-1}h(m)\hat{t}\ t^{-1} \equiv (1123)(402)(8875)(1293)(\text{mod}2773) \equiv 567$$

Then the requester sends $(567,\ 332)$ to the signer.

Signing and extraction:

The signer computes and sends $\hat{k} = (567{\times}27{\times}332{\times}687{+}8875\ )(\text{mod } 2773) \equiv 1869$ to the requester, whose next calculates

$$k \equiv 1118(1869 \times 3292 \times 793 \times 2331 + 2526 \times 3292) \text{ (mod } 2773) \equiv 34 \text{ (mod } 2773)$$

and sends it to the signer. The signer computes and sends

$$\hat{R} \equiv (34 \times 2551)^{157}(\text{mod } 2773) \equiv 2336(\text{mod } 2773)$$

to the requester.

The requester computes $R \equiv 2336 \times 1869(\text{mod } 2773) \equiv 1282 \text{ (mod } 2773)$. Then the signature is given by $(c, t, R) = (332, 3292, 1282)$. Now the recipient obtain a signature as $(332, 3292, 1282)$ and accept this signature since

$$[T_{R^e}(\beta)]^2 + \left[T_{h(m)c}\ (z)\right]^2 + [T_t(t)]^2(mod\ p) \equiv$$
$$(10741)^2 + (6483)^2 + (8448)^2(\text{mod } 11093) \equiv 7228 \quad (\text{mod } 11093)$$
$$(2T_{R^e}(\beta)T_{h(m)c}(z)\ T_t(t) + 1)(\text{mod } p) \equiv$$
$$(2 \times 10741 \times 6483 \times 8448 + 1)(\text{mod } 11093) \equiv 7228 \quad (\text{mod } 11093)$$

7. Conclusion

Based on the difficulty to solve chaotic maps and factoring problems, we proposed a partially blind signature scheme in this paper. In the proposed scheme, the security depends on the intractability of both the integer factorization and discrete logarithms of Chebyshev polynomials. The proposed scheme utilizes a smaller number of bits and lower computation cost due to the inherence of Chebyshev polynomials as compared to its partially blind signature scheme counterparts such as the one proposed by Tahat et al. [18]. Providing excellent security, reliability and efficiency, we believe our proposed scheme is more suitable for practical applications.

References

[1] M. Abe, E. Fujisaki, *How to date blind signatures*, Lecture Notes in Computer Science, 1163 (1996), 244-251.

[2] L. Bakrawy, N. Ghali, A. Hassanien, Th. Kim, *A fast and secure one-way hash function*, Comput and Info Sci., 259 (2011), 85-93.

[3] K. Chain, C. Kuo, *A new digital signature scheme based on chaotic maps,* Nonlinear Dyn., 74 (2013), 1003-1012.

[4] D. Chaum, *Blind signatures for untraceable payments,* Advances in Cryptology-Crypto., 23 (2008), 9-21.

[5] D. Chaum, *Blind signatures system,* Advances in Cryptology-Crypto '83, 1984, 153-156.

[6] W. Chen, C. Quan, C.J. Tay, *Optical color image encryption based on Arnold transform and interference method,* Optics Communications, 282 (2009), 3680-3685.

[7] Fan Chun-I, W.K. Chen, Y.S. Yeh, *Randomization enhanced Chaum's blind signatures scheme,* Computer Communications, (23)(17) (2000), 1677-1680.

[8] Fan Chun-I, Laung Lei-Chin, *Cryptanalysis on improved user efficient blind signature,* Electronic Letters, (48) (177) (2001), 203-209.

[9] Chun-I Fan, Luang Lei-Chin, *Low-computation partially blind signatures for electronic cash,* IEICE Transaction on Fundamentals, (E81-A) (5) (1998), 818-824.

[10] M.S. Hwang, C.C. Lee, Y.C. Lai, *Traceability on low computation partially blind signatures for electronic cash*, IEICE Transaction on Fundamental, (E85-A) (2002), 1181-1182.

[11] H.F. Huang, C.C. Chang, *A new design of efficient partially blind signature scheme*, Journal of Systems and Software, (73)(3) (2004), 397-403.

[12] X. Li, D. Zhao, *Optical color image encryption with redefined fractional Hartley transform*, Int. J. for Light and Electron. Optics, (121) (7) (2010), 673-677.

[13] Y. Liu, K. Xue, *An improved secure and efficient password and chaos-based two party key agreement protocol*, Nonlinear Dync., (84) (2) (2016), 549557.

[14] K. Martin, R. Lukac, K.N. Plataniotis, *Efficient encryption of wavelet-based coded color images,* Pattern Recognition, (38) (7)(2005), 1111-1115.

[15] R. Matthews, *On the derivation of a chaotic encryption algorithm,* Cryptologia, (13) (1) (1989), 29-42.

[16] K. Nyberg, R.A. Rueppel, *A new signature scheme based on DSA giving message recovery,* In 1^{st} ACM Conference on Computer and Communication security, 1993, 58-61.

[17] T. Okamoto, K. Ohta, *Universal electronic cash,* Advances in Cryptology-Crypto '91. LNCS 576, (1991), 324-337.

[18] N. M.F. Tahat, M.S. Shatnawi, S.E. Ismail, *A new partially blind signature based on factoring and discrete logarithm problem*, Journal of Mathematics and Statistic, (4) (2) (2008), 124-129.

[19] C.J. Tay, C. Quan, W. Chen, Y. Fu, *Color image encryption based on interference and virtual optics*, Optics & Laser Technology, (42)(2)(2010), 409-415.

[20] L. Xiong, N. Jianwei, K. Saru, H.I. Sk, W. Fan, K.K. Muhammad, and K.D. Ashok, *A novel chaotic maps-based user authentication and key agreement protocol for multi-sever environments with provable security,* Wireless Pers Commun., (89)(2)(2016), 569-597.

[21] E.J. Yoon, *Efficiency and security problems of anonymous key agreement protocol based on chaotic maps*, Commun Nonlinear Sci. Numer. Simul., (17) (7) (2012), 2735-2740.

[22] F. Zhang, X. Chen, *Cryptanalysis of Huang-Chang partially blind signature scheme*, Journal of Systems and Software, (76) (3) (2005), 323-325.

[23] L. Zhang, *Cryptanalysis of the public key encryption based on multiple chaotic systems*, Chaos Solitons Fractals, (37) (3) (2008), 669-674.

Accepted: 21.12.2016