Design of Identity-Based Blind Signature Scheme Upon Chaotic Maps

https://doi.org/10.3991/ijoe.v16i05.13809

Nedal Tahat (✉)
The Hashemite University, Zarqa, Jordan
nedal@hu.edu.jo

Ashraf A. Tahat
Princess Sumaya University for Technology, Amman, Jordan

Ramzi B. Albadarneh
The Hashemite University, Zarqa, Jordan

Talal A.Edwan
Princess Sumaya University for Technology, Amman, Jordan

Abstract—Cryptosystems relying on chaotic maps have been presented lately. As a result of inferred and convenient connections amongst the attributes of conventional cryptosystems and chaotic frameworks, the concept of chaotic systems with applications to cryptography has earned much consideration from scientists working in the various domains. Hence, we suggest a novel IDentity-based Blind Signature (ID-BS) based technique in this paper that relies on a pair of hard number theoretic problems, namely, the Chaotic Maps (CM) and FACtoring (FAC) problems. The technique is immune to attacks, in addition to its efficiency in application. Relative to other related schemes, it requires fewer module operations. In summary, our proposed technique is superior to similar schemes within the cryptosystems domain.

Keywords—Identity based, blind signature, chaotic map, factoring problem, digital signature.

1 Introduction

As a consequence of the wide spread and fast expansion of computer and communications networks and their numerous applications, it has become imperative to employ authentication and key agreement protocols for remote users [1]-[3]. These protocols should be able to generate secure session key in addition to being immune known-key attacks and insure secure communications [1]-[3].

The blind signature notion was first introduced by Chaum [4], which entails that it is not necessary for signers to have knowledge of the content of the message, to consequently sign the message. The Blind Signature method relies on the principle that a user can take away the signature of a signer on a desired document without revealing internal

information contained with it [5]. The fundamental aim of the Blind Signature scheme is obtaining the signature from an individual without exposing concealed content retained within that document. The virtue of blind signature is that it may be allowed for the requester to acquire the signature, although the signing party may not be able to draw an association to the document from a signature. If a requester issues a signature pair, an association between both of the pairs of requester and signer cannot be established. Also, unforgeability and untraceability are fulfilled by the blind signature scheme in addition to authentication [5-15]. The IDentity-based Blind Signature (IDBS) method is considered of high value due to the fact that an individual's identity is casually represented by his Public Key (PK). As a practical illustration, in the event that an electronic case disseminated by the bank may be effectively confirmed with the assistance of personal credentials; where this is simply achieved with the assistance of any possible assortment of strings such as bank's name, city, country, and year of the client or business. It is not necessary to communicate with or obtain a bank's key from the PK center. It is still an unresolved issue for approaches based on Integer Factorization Problem (IFP) of RivestShamirAdleman (RSA) techniques to insure security against generic parallel attacks.

The ID-BS approach eliminated the demand for a requester to pursue the public key of the recipient ahead of dispatching an encrypted message. Identity-based cryptography offers a viable helpful substitute technique to traditional Public-Key Infrastructure (PKI) [5, 9]. Several ID-BS approaches have been suggested subsequent to the year 1984 [4], [14- 17], nevertheless, ones arose in 2001, in particular, were able to achieve identity-based encryption [18]. The superiority of the ID-BS approach dwells in simplifying the procedure of key management. In the preceding two years, a few bilinear parings were adapted to different use cases and scenarios in cryptography [19, 20].

A chaotic map-based image encryption algorithm was originally suggested in 1989 [18]. Lately, there has been an expanding activity in this field as a few methods were presented within the research art [22-26]. 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, we will present in this paper a novel ID-BS technique relying on chaotic map and factoring problems. Our proposed scheme is much more efficient than previous ID-BS schemes as a result of the decreased number of operations.

We organize the rest of this paper as follows: we concisely lay-out the ground-work in Section 2. In Section 3, we construe the ID-BS scheme. Section 4 incorporates investigation of the security and computational cost of the presented technique as compared with current schemes. In Section 5, we depict a numerical illustration on our presented ID-BS technique. We finally draw conclusions in Section 6.

2 Preliminaries

We will shortly present the basic notion of Chebyshev chaotic map in addition to its associated mathematical characteristics [22, 26-28].

2.1 Chepyshev chaotic map

Given an integer m, and a variable z on the interval $[-1,1]$. Then, a Chebyshev polynomial $T_m(z): [-1,1] \rightarrow [-1,1]$ is defined as

$$T_m(z) = \cos(m \cos^{-1}(z)) \tag{2.1}$$

Chebyshev polynomial map $T_m: \mathcal{R} \rightarrow \mathcal{R}$ of degree m is defined by the recurrent relation as follows:

$$T_m(z) = 2zT_{m-1}(z) - T_{m-2}(z) \tag{2.2}$$

Where $m \geq 2, T_0(z) = 1, T_1(z) = z$. In addition, a few other Chebyshev polynomials are given as: $T_2(z) = 2z^2 - 1$, $T_3(z) = 4z^3 - 3z$, $T_4(z) = 8z^4 - 8z^2 + 1$,

Two intriguing features of a Chebyshev polynomial are the following [19, 24], [33]:

- The semi-group property [30]:

$$\begin{aligned} T_w(T_t(z)) &= \cos\big(w \cos(t \cos^{-1}(z))\big) \\ &= \cos(wt \cos^{-1}(z)) \\ &= T_{wt}(z) \\ &= T_t(w(x)) \end{aligned} \tag{2.3}$$

In Eq. (2.3), the numbers w and t are positive integers, while $z \in [-1,1]$.

- The chaotic property [30]:

The Chebyshev map $T_m(z) = [-1,1] \longrightarrow [-1,1]$ of degree m ($m > 1$) represents a chaotic map that has an invariant density $f^*(z) = \frac{1}{\pi\sqrt{1-z^2}}$ in conjunction with a positive Lyapunov exponent$= In(m) > 0$

So that to enhance this property, it was shown by Zhang [29] that the semi-group property is fulfilled for Chebyshev polynomials established on the interval $(-\infty, \infty)$ as follows [30]:

$$T_m(z) = 2zT_{m-1}(z) - T_{m-2}(z) (\text{mod } p) \tag{2.4}$$

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

$$T_w(T_t(z)) = T_{tw}(z) = T_t(T_w(z)) (\text{mod } p) \tag{2.5}$$

Also, the semi group property is fulfilled. The extended Chebyshev polynomials retain the characteristic that they commute under composition.

Definition 2. If one is given two elements m and γ , the role of the discrete logarithm problem is to identify integer s , such that $T_s(m) = \gamma$.

Definition 3. If one is given three elements, $T_m(z)$, and $T_s(z)$, the role of the Diffie-Hellman problem is to find element $T_{ms}(z)$.

2.2 Chaotic map problems

Given the integers L and K, and the prime number p , then, the general second-order linear recurrence relation is of the form:

$$L \times T_{m-1}(Z) + K \times T_{m-2}(Z) \text{ (m} \geq 2) \tag{2.6}$$

Where $T_m(Z) \in GF(p)$ for all m

The chaotic maps recurrence relation function [30] is define by Eq.(2.4), accompanied by the initial conditions $T_0(Z) = 1$ and $T_1(Z) = Z$. It can simply be seen that the chaotic maps functions are a particular kind of second-order linear recurrence relation in Eq. (2.6) with $L = 2Z$ and $K = -1$.

Theorem 1. Assume that $f(Z) = C^2 - 2ZC + 1$ with the pair of roots μ, δ . If $Z = \frac{1}{2}(\mu + \delta)$, thus, the number of solutions fulfills [19]

$$T_m(Z) = \frac{\left(Z+\sqrt{Z^2-1}\right)^m + \left(Z-\sqrt{Z^2-1}\right)^m}{2} \text{ (mod } p). \tag{2.7}$$

Theorem 2. Given the two positive integers s and r where $s > r$, hens

$$2T_s(Z).T_r(Z) = T_{s+r}(Z) + T_{s-r}(Z) \tag{2.8}$$

Theorem 3. If $t = r + s$ and p is a large prime number, thus,

$$(2T_t(Z)\ T_r(Z)\ T_s(Z) + 1) \text{ (mod } p) = ([T_t(Z)]^2 + [T_r(Z)]^2 + [T_s(Z)]^2) \text{(mod } p) \tag{2.9}$$

Theorem 4. If it is possible to employ an algorithm to unravel the chaotic maps problem over (p), thus an algorithm may be utilized to solve the discrete logarithm problem over $GF(p)$ in polynomial time [33].

Lemma 1. For any $\alpha \in GF(p)$ and $\mu = \alpha^r$, given an integer, we are able to find an integer $Z \in GF(p)$, where hence create a chaotic maps sequence $\{T_m(Z)\}$ corresponding to $\frac{1}{2}(\mu + \mu^{-1}) = T_s(Z) \in T_m(Z)$ in polynomial time.

Lemma 2. If we define p, N, and β as they were previously defined atop, with G be the group generated by β. In order to identify w according to $c = T_{w^2}(\beta) \text{mod } p$, where c is provided, with $c \in G$. One has to find solution for both of the chaotic maps problem in G and the factorization of n.

2.3 Computational problems and random oracle models

In order to illustrate the security of our presented technique, we outline in the following a few essential mathematical characteristics of Chebyshev chaotic map:

1. If we are provided with a couple of elements x and y, the discrete logarithm problem role is to identify an integer s , that satisfies $T_s(x) = y$.
2. If provided with three elements x, $T_r(x)$, and $T_s(x)$, the role of the Diffie-Hellman problem is to calculate elements $T_{rs}(x)$.

3. Random Oracle Model (**ROM**), where ROM is a security hypothesis, that affords a general framework for the security verification of information. The ROM has a totally a random hash function. If it is assumed that the hash function is able to furnish a wholly random oracle, the model may be treated as the excessive model among the ideal model and instantiation model [30].

3 The Proposed ID-BS Scheme

In the presented ID-based chaotic blind signature technique, ahead of signing of the message *m* by its signer, the message is blinded. When the sign procedure is completed, blind reduction procedure of the signed message is executed by provider of the message. Concurrently, we offer identity parameters via the hash combination of ID and private key *x*. The chaotic signature is computed by utilizing the new hash value. The utilization of chaotic type blind signature is able to successfully avert the difficult procedure of bilinear pairing, and therefore may boost the algorithm effectiveness.

3.1 Requirements

The blind signature normally encompasses measures stated as follows [30]:

1. (Blind Transformation) the message m is transformed into message m' by the Message Provider and is then commissioned to the Message Signer.
2. (Sign) the collected message m' is signed by Message Signer and then the Sig (m') will be sent to the Message Provider.
3. (Blind Reduction) the Sig (m') will be operated on by the Message Provider to form Sig (m).
4. (Verify) to verify the signature, fulfillment of the associated mathematical relationship by the signature is inspected accordingly.

Table 1. Definition of parameters.

Parameter	Definition
$\overline{p}$, $\overline{q}$	a pair of prime random large numbers, where their product will be equal to $n = \overline{p}\ \overline{q}$.
p	a prime number that is large, with n to be a factor of $p - 1$.
α	belongs to $GF(p)$ and it is an element with n as its order modulo p, and α generates the multiplicative group G.
$H_{\circ}(.)$	this is a cryptographic hash function that generates a length t bit outcome (where, $t = 128$ is assumed).
$x, \overline{p}$, $\overline{q}$	private keys.
ID	identity information.
m	original message.
$\acute{m}$	message after blind.
α, λ, k	random number.
y, α , p, n	public keys.
(v, w)	original signature.
(γ, δ)	final signature.

3.2 Initialization phase

We outline the following parameters – see Table 1 – to illustrate our work.

3.3 Generating keys

The private key will be chosen as the result of randomly selecting an integer $x \in \mathbb{Z}_n^*$ by the signer. Chose the ID to be used as the user identity. Pick a cryptographic hash function $H_\circ()$ to compute $H_\circ(x, ID)$. Then the public key is calculated as y:

$$y = T_{H_\circ(x,ID)^2}(\alpha) \ \ mod\ p \tag{3.1}$$

3.4 Signing and extraction

The Signing and extraction steps are as follows:

1. Message signer selects $k \in \mathbb{Z}_n$, calculates v then sends it,

$$v = T_k(\alpha) \ (\text{mod}\ p) \tag{3.2}$$

2. (Blind transformation) randomly chosen by the Message Provider, the blind factor $\lambda \in Z_n$ is used in calculating,

$$m' = m^2\ T_\lambda^{-2}(v) \ \text{mod}\ n \tag{3.3}$$

3. (Sign) utilizing (3.4), w is computed by the Signer to be delivered to Message Provider.

$$m' = (H_\circ(x, ID)^2\ v^4 + k^3\ w^4) \ (\text{mod}\ n) \tag{3.4}$$

4. (Blind Reduction) Message Provider calculates

$$\gamma = v^2\ T_{\lambda^2}(v) \ (\text{mod}\ n) \tag{3.5}$$

$$\delta = \lambda^{-1}\ w^2\ T_\lambda(v) \ \ (\text{mod}\ \ n) \tag{3.6}$$

Then the signature is, (m, γ, δ)

3.5 Signature verification

To authenticate the signature, the verifier inspects equitability of the following identity:

$$[T_{m^2}(\alpha)]^2 + \left[T_{\gamma^2}(y)\right]^2 + [T_{\delta^2}(\gamma)]^2 = 2T_{m^2}(\alpha)\ T_{\gamma^2}(y) T_{\delta^2}(\gamma) + 1 \ (\text{mod}\ p) \tag{3.7}$$

The subsequent theorem may be employed to prove that if a signature (m, γ, δ) of a message *m* is indeed formed by the presented partially blind signature technique.

Theorem 3.1 Granted that a signature(m, γ, δ) of the message *m* formed by the presented ID-BS scheme, then,

$$[T_{m^2}(\alpha)]^2 + \left[T_{\gamma^2}(y)\right]^2 + [T_{\delta^2}(\gamma)]^2 = 2T_{m^2}(\alpha)\, T_{\gamma^2}(y) T_{\delta^2}(\gamma) + 1 \pmod{p} \quad (3.8)$$

Poof. We have to show that the signature (m, γ, δ) satisfies:

$$T_{\gamma^2}(y) = T_{v^4 (T_\lambda(v))^2} T_{H_\circ(x,ID)}(\alpha) = T_{v^4 (T_\lambda(v))^2 (H_\circ(x,ID))^2}(\alpha)$$

$$T_{\delta^2}(\gamma) = T_{\delta^2 v^2}\, T_{\lambda^2}(v)$$

$$= T_{\delta^2}\, T_{k^2}(\alpha)\, T_{\lambda^2} T_k(\alpha)$$

$$= T_{\delta^2 k^3 \lambda^2}\,(\alpha)$$

$$= T_{\lambda^{-2}\, w^4 (T_\lambda(v))^2 k^3 \lambda^2}\,(\alpha)$$

$$= T_{w^4 (T_\lambda(v))^2 k^3}\,(\alpha)$$

Now,

$$[T_{m^2}(\alpha)]^2 + \left[T_{\gamma^2}(y)\right]^2 + [T_{\delta^2}(\gamma)]^2 =$$

$$[T_{m^2}(\alpha)]^2 + \left[T_{v^4 (T_\lambda(v))^2 (H_\circ(x,ID))^2}(\alpha)\right]^2 + \left[\, T_{w^4 (T_\lambda(v))^2 k^3}\,(\alpha)\right]^2$$

Let $t = m^2 (\mathrm{mod}\, n)$, $r = w^4 \left(T_\lambda(v)\right)^2 k^3 \pmod{n}$,
$s = v^4 \left(T_\lambda(v)\right)^2 \left(H_\circ(x,ID)\right)^2 (\mathrm{mod}\, n)$ and $t = r + s \pmod{n}$
By Theorem (3)

$$[T_{m^2}(\alpha)]^2 + \left[T_{\gamma^2}(y)\right]^2 + [T_{\delta^2}(\gamma)]^2 =$$

$$[T_{m^2}(\alpha)]^2 + \left[T_{v^4 (T_\lambda(v))^2 (H_\circ(x,ID))^2}(\alpha)\right]^2 + \left[\, T_{w^4 (T_\lambda(v))^2 k^3}\,(\alpha)\right]^2$$
$$= 2T_{m^2}(\alpha)\, T_{v^4 (T_\lambda(v))^2 (H_\circ(x,ID))^2}(\alpha)\, T_{w^4 (T_\lambda(v))^2 k^3}\,(\alpha) + 1$$

$$= 2T_{m^2}(\alpha)\, T_{\gamma^2}(y) T_{\delta^2}(\gamma) + 1 \pmod{n}$$

Which means (m, γ, δ) is a legitimate signature of *m*. Therefore, our presented method yields a partially blind signature scheme.

4 Analysis of Our Proposed Scheme

4.1 Security analysis

We examine in this section a few security characteristics of our proposed ID-BS scheme. In order for an ID-BS scheme to be secure, it must fulfil the subsequent conditions.

Blindness: The property of blindness shared by all signatures composed by the signer embody an unambiguous shared information, which the message provider and the message signer consented upon. Although, the message provider is incapable of changing or eliminating the enclosed information, whereas retaining the feature of successful signature verification possible. Within our suggested scheme, a message provider is obligated to surrender to the signer the blinded data m, where in-turn the signer calculates and communicates $m' = (H_{\circ}(x, ID)^2\ v^4 + k^3\ w^4)$ to the designated target. If the message provider is capable of victoriously changing or eliminating the v from the associated signature (m, γ, δ), thus s/he calculates w through $m' = (H_{\circ}(x, ID)^2\ v^4 + k^3\ w^4)$. Nevertheless, it is burdensome to deduce the secret key x. Accordingly, in the presented technique, the message provider incapable of changing or removing the v out of the associated signature (m, γ, δ) of message m to imitate the unblinded signature portion.

Randomization: Ahead of signing in the signing step in the presented technique, the blinded data is randomized by the signer via the random element *k*. The signer picks an integer *k*, then communicates it to the recipient. Then, the recipient forwards $m' = m^2\ T_{\lambda}^{-2}(v)$ to the signer, where the signer remits $w^4 \equiv (m' - H_{\circ}(x, ID)^2 v^4)k^{-3}(mod\ n)$ to the message provider. If the message provider tries to remove k from $w^4 \equiv (m' - H_{\circ}(x, ID)^2 v^4)k^{-3}(\mathrm{mod}\ n)$, thereupon s/he must infer x through $y = T_{H_{\circ}(x,ID)^2}(\alpha) \mod p$. Nevertheless, it is burdensome to resolve x due to the fact that deriving it is CM and FAC problems. Thus, within the presented scheme, it is not possible for the message provider to eliminate the random k out of the associated signature (m, γ, δ).

Untraceability: Within this technique, it is inconceivable for Message Signer to figure out the connection among (γ, δ) and (v, w) by computing, where to unravel this problem corresponds to CM and FAC problems [30].

Unforgability: The complexity of unfolding the CM and FAC problems is the basis for the security of our technique. The adversary Adv could attempt to deduce a forged signature employing assorted plans, as depicted subsequently.

Attack 1: For a particular message *m*, Adv contends to unfold the signature (m, γ, δ) through allowing a single integer to be fixed, or fixing two integers, and determining the other. In this scenario, Adv will in random fashion fix either (m, γ), (m, δ) or (γ, δ) accordingly to fulfil,

$$[T_{m^2}(\alpha)]^2 + \left[T_{\gamma^2}(y)\right]^2 + [T_{\delta^2}(\gamma)]^2 = 2T_{m^2}(\alpha)\ T_{\gamma^2}(y) T_{\delta^2}(\gamma) + 1\ (\mathrm{mod}\ p) \tag{4.1}$$

as difficult chaotic maps problems and factorization, simultaneously.

Case 1: Assuming that Adv will fix the elements (m, γ) and attempts to resolve the value δ, consequently Adv is required to unravel the ensuing equations that may be obtained by simplifying the equation,

$$\psi^2 - 2\psi T_{m^2}(\alpha)\, T_{\gamma^2}(y) + [T_{m^2}(\alpha)]^2 + \left[T_{\gamma^2}(y)\right]^2 - 1 \pmod p \tag{4.2}$$

Thus, ψ may be retrieved by the subsequent equation:

$$\psi = \frac{2T_{m^2}(\alpha)\, T_{\gamma^2}(y)}{2} \mp \frac{\sqrt{\left(2T_{m^2}(\alpha)\, T_{\gamma^2}(y)\right)^2 - 4\left(\left[T_{m^2}(\alpha)\right]^2 + \left[T_{\gamma^2}(y)\right]^2 - 1\right)}}{2} \tag{4.3}$$

Although, it is impractical to determine δ using $\psi = T_{\delta^2}(\gamma)$ despite if s/he is able to find ψ from Eq. (4.2).

Lemma (2) indicates that this is slightly as burdensome as unraveling the chaotic maps problems and factorization of *n*.

Case 2: Say Assuming that Adv will fix the elements (m, δ) and attempts to resolve the value γ. At that point, her/his duty is more burdensome than Case1 due to the fact that s/he should find γ through $\eta = T_{\gamma^2}(y)$, wherein:

$$\eta^2 - 2\eta T_{m^2}(\alpha) T_{\delta^2}(\gamma) + [T_{m^2}(\alpha)]^2 + [T_{\delta^2}(\gamma)]^2 - 1 \pmod p \tag{4.4}$$

Lemma (2) indicates that this is slightly as burdensome as unraveling the chaotic maps problems and factorization of *n*.

Case 3: Assuming that Adv will fix the elements (γ, δ) and attempts to resolve the value m. Hence, her/his duty is more burdensome than Case 1, since s/he has to find $\xi = T_{m^2}(\alpha)$ relying on the equation:

$$\xi^2 - 2\xi T_{\gamma^2}(y) T_{\delta^2}(\gamma) + \left[T_{\gamma^2}(y)\right]^2 + [T_{\delta^2}(\gamma)]^2 - 1 \pmod p \tag{4.5}$$

Lemma (2) indicates that this is slightly as burdensome as unraveling the chaotic maps problems and factorization of *n*.

Attack 2: If we presume that Ad manages to figure out the chaotic maps problem, at this point, Adv knows $H_{\circ}^2(x, ID)$. Distressingly, s/he is incapable of computing $w^4 \equiv (m' - H_{\circ}(x, ID)^2 v^4) k^{-3} (mod\ n)$ and $\delta = \lambda^{-1}\, w^2\, T_{\lambda}(v) \mod n$, which will result in failure to create the signature (m, γ, δ).

Attack 3: If we t is assumed that Ad is able to solve factoring problem, which means he knows the prime factorization of n i.e. p and q: However, he cannot compute since no information on $H_{\circ}^2(x, ID)$ is available, hence he cannot compute w and $\gamma = v^2\, T_{\lambda^2}(v)$. Thus, fails to produce the signature (m, γ, δ).

Attack 4: Adv can possibly contend gathering t valid signatures $(m_j, \gamma_j, \delta_j)$ of message M_j, wherein $j = 1,2,3, \ldots, t$, in order to try to bring about the signature scheme secret keys. At this stage, Adv retains a set of equations conforming to:

$$m_1^2 = \left(T_{\lambda_1}(v_1)\right)^2 \left[w_1^4\, k_1^3 + v_1^4 \left(H_{\circ(x,ID)}\right)^2\right] \bmod n$$

$$m_2^2 = \left(T_{\lambda_2}(v_2)\right)^2 \left[w_2^4\, k_2^3 + v_2^4 \left(H_{\circ(x,ID)}\right)^2\right] \bmod n$$

$$m_t^2 = \left(T_t(v_t)\right)^2 \left[w_t^4\, k_t^3 + v_t^4 \left(H_{\circ(x,ID)}\right)^2\right] \bmod n \quad (4.6)$$

The above set of *s* equations contains a number of variables equals to (4*s* + 1) i.e, λ_j, v_j, k_j, w_j, and *x*, in which $j = 1,2,3, \ldots, t$, that are all unknown to the Adv. Hence, x remains hard to be obtained as Adv will generate an infinite number of solutions to the system of equations depicted atop and is incapable of identifying which is factual choice.

4.2 Performance comparison

The Chebyshev polynomial computation problem provides a reduced size key when compared to other public key cryptosystems, in addition to rapid computing, along with bandwidth, memory and energy conservation. The Elliptic-Curve Cryptography (ECC) has large complexity in terms of computations. When assimilated with the encryption algorithm of the ECC method, the encryption algorithm of chaotic maps evades scalar multiplication and modular exponentiation calculations, dramatically enhancing the efficiency. For the sake of facilitating the cost evaluation process of computational requirements, Table 2 defines the notations and Execution time(s) [21, 32].

Table 3 depicts the computational cost comparison of between the proposed scheme and the scheme in [30,31]. It is apparent that the proposed scheme has better efficiency when assimilated with the techniques proposed in [30,31]. Our scheme requires only 0.33249*s*, while their schemes needs 37.6456*s*, and 48.44278*s*, accordingly.

Table 2. Definition of notations and execution times.

Notation	Definition	Execution time(s)
T_h	Required time to compute hash function	$T_h \approx 0.005$s
Texp	Time complexity of an exponentiation	$T_{exp} \approx 5.37$s
Tch	Required time to compute extended chaotic function	$T_{ch} \approx 0.032$s
Tmul	Required time to compute multiplication function	$T_{mul} \approx 0.00207$s
Tinv	Required time to compute inverse function	$T_{inv} \approx 0$: 0207s

Table 3. Performance comparisons among our scheme and schemes in [30,31]

Phases	Message	Message Verification	Total signature	provider	cost
The proposed scheme	Time complexity cost	$T_{ch} + T_h$ $+13T_{mul}$	$3T_{ch}$+ $9T_{mul}$+ $2Tinv$	$3Tch + 8Tmul$	$7Tch + Th$ $+30T_{mul}$ $+2T_{inv}$
	Execution Time(s)	0.0639	0.15603	0.11256	0.33249
The scheme in [30]	Time complexity cost	$Texp + Th$ $+2T_{mul}$	$3T_{exp} + 2T_{inv}$ $+T_{mul}$	$3T_{exp} + T_{mul}$	$7T_{exp} + 2T_{inv}$ $+4T_{mul} + T_h$
	Execution Time(s)	5.379	16 1538	16.1128	37.4656
The Scheme in [31]	Time complexity cost	$2T_{exp} + T_h$ $+2T_{mul}$	$3T_{exp} + 2T_h$ $+11T_{mul}$ $+ 4T_{inv}$	$4T_{exp} + T_h$ $+T_{mul}$	$9T_{exp} + 4T_{inv}$ $+4T_h + 14T_{mul}$
	Execution Time(s)	10.749	16.2256	21.49	48.4618

5 Numerical Simulation of the ID-BS

Suppose that a signer desires to sign an original message m = 322. A signer sets up the scheme with p = 47, q = 59, n = 2773, p = 11093, α = 100 is an element in $GF(p)$ whose order modulo p is n.

5.1 Generating keys

The signer randomly picks an integer $x = 27 \in \mathbb{Z}_n^*$ to be the private key, ID for user identity, calculates $H_\circ(27, ID) = 137$, Then calculates y, is the public key

$$y = T_{137^2(\mathrm{mod}\ 2773)}(100) = T_{2131}(100)(\mathrm{mod}\ 11093) = 980$$

5.2 Signing and extraction

The results of signing and extraction are as follows:

1. Message signer select $k = 2551 \in \mathbb{Z}_n$ calculates v then sends it

$$v = T_{2551}(100)\ \mathrm{mod}\ 11093 = 8875$$

2. (Blind transformation) Message Provider randomly selects $\lambda = 2331 \in \mathbb{Z}_n$ calculate

$$m' = 322^2\ T_{2331}^{-2}(8875)\ \mathrm{mod}\ 2773 = 1083(1895)^{-2}\ \mathrm{mod}\ 2773 = 169$$

3. (Sign) Signer gets w ,and sends to Message Provider.

$$w^4 \equiv (m' - H_\circ(x, ID)^2 v^4)k^{-3}(mod\ n)$$

$$\equiv (169 - 2131(2169))135$$

$$w^4 \equiv 947 \bmod 2773$$

$$w \equiv 133 \bmod 2773 \tag{5.1}$$

(Blind Reduction) Message Provider calculates

$$\gamma = (8875)^2\, T_{(2331)^2 \bmod 2773}(8875) \bmod 2773$$

$$= 1333\ (8422) \bmod 2773$$

$$= 1422$$

$$\delta = (2331)^{-1}\ (133)^2\ T_{2331}(8875)\ \ \bmod\ 2773$$

$$= 1123(1051)(10403) \bmod 2773 = 1883 \tag{5.2}$$

Then the signature is $(322, 1422, 1883)$

5.3 Signature verification

To examine the authentic of the signature, the verifier performs a check of fulfilment of the equality of,

$$[T_{m^2}(\alpha)]^2 + \left[T_{\gamma^2}(y)\right]^2 + [T_{\delta^2}(\gamma)]^2 = 2T_{m^2}(\alpha)\ T_{\gamma^2}(y) T_{\delta^2}(\gamma) + 1\ (\bmod p)$$

$$[T_{m^2}(\alpha)]^2 + \left[T_{\gamma^2}(y)\right]^2 + [T_{\delta^2}(\gamma)]^2 = [1416]^2 + [8074]^2 + [189]^4 (\bmod 11093)$$

$$= 3599$$

$$2T_{m^2}(\alpha)\ T_{\gamma^2}(y) T_{\delta^2}(\gamma) + 1 = 2(189)(8074)(189) + 1\ (\bmod 11093)$$

$$= 3599 \tag{5.3}$$

6 Conclusion

This paper suggested a secure ID-BS technique that relies on the chaotic map and factoring problems. The presented approach utilizes a smaller number of bits and lower computation cost due to the inherence of CM as compared to its ID-BS scheme counterparts presented in the relevant literature. In order to enhance the security of the algorithm under the random oracle model, a hash function was brought-out and employed.

The ability of our scheme to offer superb reliability and security in addition to efficiency renders our presented scheme more suited for rational applications.

7 References

[1] Pavani, V. L. (2018), "A Novel Authentication Mechanism to Prevent Unauthorized Service Access for Mobile Device in Distributed Network", International Journal of Interactive Mobile Technologies (iJIM), Vol 12,No. 8, pp. 4-19, https://doi.org/10.3991/ijim.v12i8.8194.

[2] Hathout, B. B., Ghoniemy S., Ibrahim, O. (2017), "A Modified Cloud-Based CryptographicAgent for Cloud Data, Integrity", International Journal of Interactive Mobile Technologies (iJIM), Vol 11, No 2. pp. 6-23. https://doi.org/10.3991/ijim.v11i2.6553.

[3] Wardhono,W. S., Priandani,N. D., Ananta,M. T. Brata, K. C., Tolle, H. (2018), "End-to-End Privacy Protection for Facebook Mobile Chat based on AES with Multi-Lay ered MD5", International Journal of Interactive Mobile Technologies (iJIM), Vol 12, No 1., pp.160-167. https://doi.org/10.3991/ijim.v12i1.7472.

[4] Chaum, D. (1984), "Blind Signature System", Advances in Cryptology, Proceedings of CRYPTO '83, Santa Barbara, California, USA, August. DBLP, pp. 153-156. https://doi.org/10.1007/978-1-4684-4730-9_14.

[5] Mohammed, E., Emarah, A. E., ElShennawy, Kh. (2000), "A Novel blind signature using Elgamal", IEEE Arab Academy for Science and Technology, pp.189-196.

[6] Shamir, A. (1985), "Identity-based cryptosystems and signature schemes", Advances in cryptology, Vol.196, 47-53. https://doi.org/10.1007/3-540-39568-7_5.

[7] Zhenjie, H., Kefei, C., Yumin, W, (2005) , "Efficient identity-based signatures and blind signatures",Cryptology and Network Security, Vol. 3810, pp. 120-133. https://doi.org/10.1007/11599371_11.

[8] Li, F., Zhang, M., Takagi, T. (2013). "Identity-based partially blind signature in the standard model for electronic cash", Mathematical and Computer Modelling, 58, No. (1-2, 196-203. https://doi.org/10.1016/j.mcm.2012.07.009.

[9] He, D., Chen, J., Zhang, R. (2011), "An efficient identity-based blind signature scheme without bilinear pairings", Computers Electrical Engineering, Vol.37, No.4, pp. 444- 450. https://doi.org/10.1016/j.compeleceng.2011.05.009.

[10] Camenisch, J. L., Piveteau, J. M., Stadler, M. A. (1995), "Blind signatures based on the discrete logarithm problem", Lecture Notes in Computer Science, Vol. 950,428-432. https://doi.org/10.1007/bfb0053458.

[11] Agnew, G. B., Mullin, C. R., Van-stone, S. A. (1990). "Improved digital signature scheme based on discrete exponentiation", Electronics Letters, Vol.26, pp.1024-1025. https://doi.org/10.1049/el:19900663. https://doi.org/10.1016/j.amc.2003.12.008.

[12] Chaum, D. (1982), "Blind signatures for untraceable payments", Advances in Cryptology Crypto82. Springer-Verlag. pp. 199-203. https://doi.org/10.1007/978-1-4757-0602-4_18.

[13] Dolev, D, Dwork, C., Naor, M. (2000), "Non-malleable cryptography. SIAM Journal on Computing, Vol.30, No.2, pp. 391-437. https://doi.org/10.1145/103418.103474. https://doi.org/10.1137/s0097539795291562.

[14] Rupeng, L., Jia, Yu., Guowen, L., Daxing, L. (2007). "A New identity-based blind signature scheme with batch verifications", Multimedia and Ubiquitous Engineering, 2007. MUE'07. International Conference on, pp.1051- 1056. https://doi.org/10.1109/MUE.2007.35.

[15] Jingfeng, S., Juxia, L. (2010), "Identity Based Proxy Blind Signature Scheme Based on DLP",International Conference on Internet Technology and Applications, pp. 1-4. https://doi.org/10.1109/itapp.2010.5566211.
[16] Chen, X. F., Zhang, F. G., Liu, L. S. (2007), "ID-based restrictive partially blind signatures and applications", The Journal of Systems and Software, Vol. 80, No. 2, pp.164-171. https://doi.org/10.1016/j.jss.2006.02.046.
[17] Ming, X., Huang, S. (2010), "Secure Identity-Based Blind Signature Scheme in the Standard Model", Journal of Information Science and Engineering, Vol.26, pp.215-230. https://doi.org/10.6688/JISE.2010.26.1.15
[18] 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.
[19] Chen, Q., Wen, Q., Jin, Z., Ping, Z. (2013), "Secure and Efficient Certificateless Signature and Blind Signature Scheme from Pairings, "Applied Mechanics and Materials, Vol.457, pp.1262-1265. https://doi.org/10.4028/www.scientific.net/amm.457-458.1262.
[20] Ajmath, A.K., gowri, T. (2003), "An ID-based Blind Signature Scheme from Bilinear Pairings",International Journal of Computer Science and Security,Vol. 4, No.1, pp. 98-106. https://doi.org/10.1080/19361610.2016.1211869.
[21] Matthews, R. (1989), "On the derivation of a chaotic encryption algorithm", Cryptologia, Vol.13, No 1, pp.29-42. https://doi.org/10.1080/0161-118991863745.
[22] 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.
[23] 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.
[24] 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.
[25] 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.
[26] 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.
[27] 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.
[28] 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.
[29] 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.
[30] Shuang, W., Hao1, Y, Dongnan, L. (2018), "A new identity based blind signature scheme and its application", IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference, pp.672-676. https://doi.org/10.1109/iaeac.2018.8577730.
[31] Tahat, N., Ismail, E., Ahmad, R. (2009), "A New Blind Signature Scheme Based on Factoring and Discrete Logarithms", International Journal of Cryptology Research, Vol. 1, No.1, pp. 1-9.

[32] Bakrawy, L., Ghali, N., Hassanien, A., Kim, T. (2011), "A fast and secure one-way hash function", Comput and Info Sci., Vol.259, pp.85-93. https://doi.org/10.1007/978-3-642-27189-2_9.

[33] Tahat, N., Abdallah, E. (2018) "Hybrid Publicly Verifiable Authenticated Encryption Scheme Based on Chaotic Maps and Factoring Problems", Journal of Applied Security Research, Vol.13, No.3, pp.304-314. https://doi.org/10.1080/19361610.2018.1463135.

8 Authors

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

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

Ramzi B. Albadarneh received his BSc in mathematics from Al al-Bayt University, Jordan in 2000, MSc in pure mathematics from Al al-Bayt University, Jordan, in 2003, and a PhD in applied mathematics (Numerical Analysis) from The University of Jordan, Jordan in 2009. He is an Associate Professor at the department of mathematics, The Hashemite University. His main research interests are numerical analysis and methods. He has published more than 11 papers, authored/Coauthored, and more than 9 refereed journal and conference papers.

Talal A. Edwan main work has been in analysis of network performance evaluation, protocols and algorithms. He received a BSc in Electronics Engineering with a First Class Honours from Princess Sumaya University for Technology (Jordan) in 2002, MSc in Networks Engineering with Distinction from University of Plymouth (UK) in 2005, and a PhD in Computer Networks from Loughborough University (UK) in 2010. Dr Talal is an Assistant Professor in the Department of Computer Engineering at PSUT since 2012, his research interests are: Computer Networks, Network Congestion Control, and Performance Evaluation of Computer Systems/Networks.

Article submitted 2020-02-17. Resubmitted 2020-03-22. Final acceptance 2020-03-23. Final version published as submitted by the authors.