Chaotic Map and Quadratic Residue Problems-Based Hybrid Signature Scheme

Rania Shaqbou'a* and Nedal Tahat*
The Hashemite University, Zarqa 13133, JORDAN

O. Y. Ababneh†,
Zarqa University, Zarqa, JORDAN

Obaida M. Al-Hazaimeh‡
Al-Balqa Applied University, Irbid, JORDAN

Abstract

The secure electronic signature provides contracting parties, particularly the consumer, with safety and reassurance which has a favorable impact on business transactions due to the strong legal authority supplied by this signature, which is based on a method for its formation. Therefore, researchers are rushing to design safe and performance electronic signature schemes at the same time. We offer a novel signature technique based on two hard number theory issues in this work, Quadratic Residue (QR) and Chaotic Maps (CM). Several fields of study including mathematics, physics, and computer science have taken an interest in chaotic systems as a potential tool for cryptography. Analysis demonstrates that our strategy is more secure and efficient than other connected schemes, compared to other schemes. A proof of the proposed scheme's security against known key attacks is also provided in this article.

Key Words: Chaotic maps, digital signature, quadratic residue problem, crypto-system.

1 Introduction

Secure and correct signings can only be achieved with digital signatures. Today, the traditional physical signature is outdated. Communication between colleagues in an organization is a significant issue that must be addressed securely. With a digital signature, you can send secure messages with a variety of various techniques. Information security and modern cryptography rely heavily on the use of digital signatures. It has been a long time coming, but digital signature technology is now mature and widely used in e-commerce. There are two types of digital signature algorithms based on their security presuppositions. As an example of this, consider discrete logarithm, the factorization of complex problems, or elliptic curve cryptography as methods for digital signature.

Many different techniques based on two difficult challenges have been created in order to increase the security of signature schemes: FAC and DLP [10, 16, 19]. However, several authors have also shown these schemes to be flawed [8, 9, 17]. Furthermore, there are many signature schemes based on two problems [1, 5-6, 12, 24], but these schemes need high computational complexity. As a result, the adoption of a digital signature method based on several assumptions is critical for improving system security. Based on chaotic maps and factoring issues, we have developed a digital signature algorithm. Matthews was the first to suggest a chaotic image encryption scheme [11]. There is an increasing interest in this field, and numerous approaches [3-4, 13-14, 13, 18, 27] have been presented for key-agreement protocol that is based on chaotic maps. Using a Chebyshev chaotic map's semi-group characteristic, they were able to establish the session key. Using chaotic maps and factorization issues, Chain and Kuo [5] have established an efficient and secure signature system. They were the first to use factorization issues and chaotic maps in their algorithm. But the scheme's flaw is that it necessitates a large number of keys for signature verification and signing. Using chaotic maps and factoring difficulties, we create a new signature scheme in this paper. By using an acceptable number of operations for both signature generation and verification, we demonstrate that the new scheme's performance is extremely efficient.

The remaining sections of this work are arranged as: In Section 2, we offer the requisite theory, characteristics, and notation for extended chaotic maps and factoring problems. Then in Section 3, we suggest a new signature technique. In Section 4, the suggested scheme's security and performance analysis aspects are presented. In Section 5, a numerical representation is depicted on our supplied scheme. In Section 6, we finally reach a conclusion.

2 Preliminaries

This section serves as a basic introduction to the Chebyshev chaotic map concept [2-5, 15, 18, 22, 26, 28] and the factorization problem [19] and its related mathematical properties.

* Department of Mathematics, Faculty of Science, P.O Box 330127. Email: nedal@hu.edu.jo.
† Department of Mathematics, Faculty of science.
‡ Department of Computer Science and Information Technology.

2.1 Map of Chebyshev Chaos.

The structure of the Chebyshev polynomials is reviewed in Figure 1 [20].

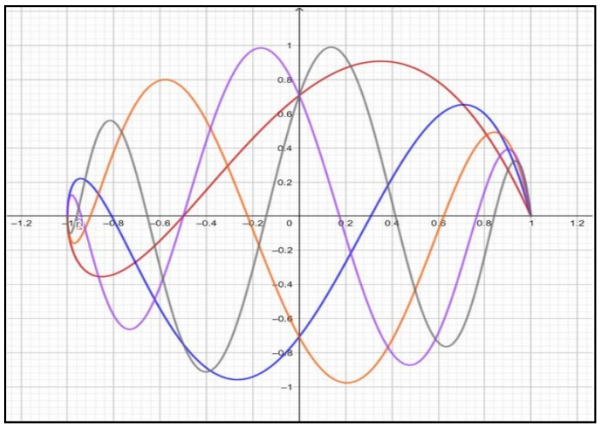

Figure 1: Chebyshev polynomials structure

A variable θ in the range [-1,1] and n is a positive integer. Let

$$T_n(\theta) : [-1,1] \longrightarrow [-1,1]$$

defined as:

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

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

$$T_n(\theta) = 2\theta T_{n-1}(\theta) - T_{n-2}(\theta) \;;\quad n \geq 2 \tag{2}$$

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

From (2), we get a matrix equation

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

the index is manipulated to get the results we want:

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

Combining the above equations, we next get

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

Where $$T_0(\theta) = 1, T_1(\theta) = \theta. \tag{6}$$

In addition, the Chebyshev polynomial possesses the following two intriguing properties:

- The property of a semi-group

$$\begin{aligned} T_r(T_s(\theta)) &= cos(rcos(s\, cos^{-1}(\theta))) \\ &= \cos\,(rscos^{-1}(\theta)) \\ &= T_{sr}(\theta) \\ &= T_s(T_r(\theta)) \end{aligned} \tag{7}$$

where r and s are both positive integers and $\theta \in [-1,1]$

- The property of a chaotic

An invariant density $f^*(\theta) = \frac{1}{\pi\sqrt{1-\theta^2}}$ is found in the Chebyshev map $T_a(\theta)$; $[-1,1 \longrightarrow [-1,1]]$ of degree $a > 1$, for positive Lyapunov exponent $\lambda = Ln(a) > 0$. Logistic maps can be constructed by using the Chebyshev map with *p=2*.

Since this condition holds under composition, the Chebyshev polynomials commute immediately.

$$T_r(T_s(\theta)) = T_s(T_r(\theta))$$

When it comes to Chebyshev polynomials, Zhang [15] has shown that the semi-group property applies for those defined on the interval $(-\infty, \infty)$ in order to make the formulas more secure. Polynomials in this form are called augmented Chebyshev polynomials.

$$T_n(\theta) = \left(2xT_{n-1}(\theta) - T_{n-2}(\theta)\right) (\text{mod } p) \tag{8}$$

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

$$T_r(T_s(\theta))(\theta) = T_r(T_s(\theta)) = T_s(T_r(\theta))(\text{mod } p) \tag{9}$$

Theorem 1. **[14]** Let $f(u) = t^2 - 2ut + 1$ and α, β be two roots of $f(u)$. If u= $\frac{1}{2}(\alpha + \beta)$, in this case, the number of possible solutions is met by:

$$T_a(u) = \frac{(u+\sqrt{u^2-1})^a + (u-\sqrt{u^2-1})^a}{2} (\text{mod } p) \tag{10}$$

Theorem 2. **[14]** If a and b are two positive integers and $a > b$, then we obtain that:

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

Theorem 3. **[14]** If $a = b + c$ and p is a prime (i.e., large number), we obtain that:

$$\begin{aligned} &[T_a(u)]^2 + [T_b(u)]^2 + [T_c(u)]^2 \\ &= 2T_a(u)T_b(u)T_c(u) + 1(\text{mod } p) \end{aligned} \tag{12}$$

Lemma 1. **[14]** Let the elements of a finite field are g and h, i.e., if $g + g^{-1} = h + h^{-1}$then $g = h$ or

$$g = h^{-1}$$

Lemma 2. **[14]** For any $\alpha \in GF(p)$ and $y = \alpha^t$ for some integer t, we can find an integer $u \in GF(p)$ and then construct a chaotic maps sequence $\{T_a(u)\}$, in polynomial time such that

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

Lemma 3. **[14]** Let p, n and α are the same as earlier; and G is the group formed by the combination of these three. To obtain the value of μ such that $a = T_{\mu^2(mod\ n)}(\alpha)\ mod\ p$, where a is given and $a \in G$, one must solve both the chaotic maps problem in G and the factorization of n.

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

2.2 The Factorization Problem.

Finding two huge integers *p* and *q* from a composite number *n*, which is the product of two numbers p and q, is known as the factorization problem. Large prime numbers aren't hard to come by, but factoring the product of two of them is regarded computationally challenging when the primes aren't randomly chosen. The RSA public-key cryptosystem was designed by Rivest et al. [16] because of the difficulties of this challenge. Many mathematicians have worked on the factorization problem for many years, but considerable progress has only been made in the last 20 years. Since the RSA cryptosystem was invented in 1978, several mathematicians have studied the topic in depth. Advanced algorithms could now be implemented and tested on high-performance computers. RSA has now been a problem for more than two decades [25]. More than a few studies on the problem's robustness have yielded attacks, while others evaded them. Based on the RSA problem, digital signatures and public-key encryption techniques have been created. What remains to be seen is how much of the RSA Issue's security is dependent on factoring, and whether, like with every cryptographic hard problem, more robust approaches than those currently available can ever be developed.

Definition 1: (FAC problem). Let n be a large composite integer with $n = rs$ where r and s are two large strong primes of 512-bits. Then find the primes $r$or s.

Definition 2: (QR problem). Let p, q be two strong primes of large size and γ is an integer. Then, compute γ such that $\gamma \equiv \beta^2 \bmod pq$

2.3 Computational Problem.

In order to demonstrate the security of our proposed cryptosystem, we show several essential mathematical features of Chebyshev chaotic maps:

a) The property of Semi-group: Given $\theta \in [-1,1]$,

$$T_r(T_s(\theta)) = \cos\left(r\cos^{-1}(s\cos^{-1}(\theta))\right)$$

$$= \cos\left(rs\cos^{-1}(\theta)\right)$$

$$= T_{sr}(\theta) = T_s(T_r(\theta))$$

b) An integer s must be found such that $T_s(\theta) = y$ in the discrete logarithm problem given as two elements x and y and an associated value for its value in the chaotic map.

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

3 The Proposed Scheme

The following parameters and notations will be used before the new scheme is introduced.

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

3.1 Algorithm for Key Generation.

The following steps are taken during this phase.

- Select randomly integer b
- Compute the corresponding integers k such that
- Compute the corresponding integers K such that $K = T_{b^4}(\alpha)(\ mod\ n)$

The signer publishes his public keys as (p, n, K, α) and keeps his corresponding private keys as $(b, \overline{p}, \overline{q})$

3.2 Algorithm for Signing Message.

Our scheme's message-signing algorithm is presented in this section. Once the signer has decided on m (the message they want to sign), they subsequently compute the hashed value of it *h(r)*. Following are the steps that the signer must do in order to sign *h(r)*.

- Select a random integer $r \in \mathbb{Z}_n^*$
- Compute $L = T_{r^4}(\alpha)\ (mod\ p)$ (14)
- Calculate $S \equiv (h(m)\ b\ r\ L)\ mod\ n$ (15)
- Compute $\lambda \equiv (h(m)b + r\ L)^2\ mod\ n$ (16)

Signing the message *h(r)* is done by the original signer, who creates (L, S, λ).

3.3 Algorithm for Verifying Signature.

After the receiver received the message *h(r)* and signature from signer, he can verify the correctness and validity of the produced signature using the following verifying equation. If it holds, receiver is convinced the message was signed by the actual signer. Now we present the algorithm for verifying signature for our scheme.

- Compute$\gamma \equiv (\lambda^2 + 2S^2 - 4\lambda S)\ mod\ n$ (17)
- Compute

$$W_1 = \left[T_\gamma(\alpha)\right]^2 + \left[T_{h(m)^4 (mod\ n)}(K)\right]^2 + \left[T_{L^4 (mod\ n)}(L)\right]^2 mod\ p \quad (18)$$

- Calculate

$$W_2 = 2T_\gamma(\alpha)T_{h(m)^4 (mod\ n)}(K)\ T_{L^4 (mod\ n)}(L) + 1 \quad (19)$$

Accept the signature $(L, S,\ \lambda)$ as valid if and only if W_1=W_2.

Theorem 1: If the algorithms for generating keys and signing messages are run smoothly then the validation of signature in scheme is correct.

Proof: We have to show that the signature $(L, S,\ \lambda)$ satisfies $W_1 = W_2$. Note that

$$\lambda^2 = h(m)^4 b^4 + r^4 L^4 + 6(h(m) b\ r\ l)^2 + 4(h(m)^2 b^2 + r^2 L^2)\ h(m) b\ r\ L$$

$$= h(m)^4 b^4 + r^4 L^4 + 6S^2 + 4h(m) b\ r\ L(h(m)^2 b^2 + r^2 L^2)$$

$$= h(m)^4 b^4 + r^4 L^4 + 6\ S^2 + 4S(\lambda - 2S)$$

$$= h(m)^4 b^4 + r^4 L^4 6\ S^2 - 2S^2 + 4S\lambda$$

And also we have

$$\gamma \equiv (\lambda^2 + 2S^2 - 4\lambda S)\ mod\ n$$

$$\equiv h(m)^4 b^4 + r^4 L^4 - 2S^2 + 4S\lambda + 2S^2 - 4S\lambda$$

$$\equiv h(m)^4 b^4 + r^4 L^4$$

From Theorem. (3)

$$[T_a(m)]^2 + [T_b(m)]^2 + [T_c(m)]^2 = (2\ T_a(m) T_b(m) T_c(m) + 1)\ (mod\ p)$$

Let $a = h(m)^4 b^4 + r^4 L^4, c = h(m)^4 b^4,\ d = L^4 r^4$

Thus, we obtain

$$W_1 = \left[T_\gamma(\alpha)\right]^2 + \left[T_{h(m)^4 (mod\ n)}(K)\right]^2 + \left[T_{L^4 (mod\ n)}(L)\right]^2$$

$$= \left[T_{h(m)^4 b^4 + r^4 L^4}(\alpha)\right]^2 + \left[T_{h(m)^4 (mod\ n)} T_{b^4}(\alpha)\right]^2 + \left[T_{L^4 (mod\ n)} T_{r^4}(\alpha)\right]^2$$

$$= \left[T_{h(m)^4 b^4 + r^4 L^4}(\alpha)\right]^2 + \left[T_{h(m)^4 b^4 (mod\ n)}(\alpha)\right]^2 + \left[T_{L^4 r^4 (mod\ n)}(\alpha)\right]^2$$

$$= 2\ T_{h(m)^4 b^4 + r^4 L^4}(\alpha) T_{h(m)^4 b^4 (mod\ n)}(\alpha) T_{L^4 r^4 (mod\ n)}(\alpha) + 1$$

$$= 2T_\gamma(\alpha)T_{h(m)^4 (mod\ n)}(K)\ T_{L^4 (mod\ n)}(L) + 1 = W_2$$

4 Performance Analysis and Security Analysis

4.1 Security Analysis

We use heuristic security techniques to evaluate our system. It's done by looking at the various cryptographic attacks on the system by an attacker. The first step is to identify the various types of attacks and then analyze why each one would fail.

Attack 1. Adversary (Adv) wishes to obtain the secret keys of the scheme. In this case, Adv first analyzes (p, n, α) in order to recover the signer's private key b. He needs to solve $w \equiv T_{b^4 (mod\ n)}(\alpha)\ mod\ p$ which are clearly infeasible because the difficulty of solving CM and QR problems.

Attack 2. Adv tries to drive the signature $(L, S,\ \lambda)$ for given message m by letting two integers fixed and finding the other one. In this case, Adv randomly select $(S,\ \lambda)$ or (L, S) or (λ, L) and find L or λ or S respectively such that it satisfies $W_1 = W_2$.

Now say Adv fixes the values $(S,\ \lambda)$ and tries to figure out the value L, then using equations (18 and 19) as a starting point to solve the following equations.

$$\psi^2 - 2\psi T_\gamma(\alpha)T_{h(m)^4 (mod\ n)}(K) + \left[T_\gamma(\alpha)\right]^2 + \left[T_{h(m)^4 (mod\ n)}(K)\right]^2 - 1 = 0$$

As a result, ψ may be found using the following equation:

$$\psi = \frac{T_\gamma(\alpha)T_{h(m)^4 (mod\ n)}(k)}{2} \mp \frac{\sqrt{\left(\psi T_\gamma(\alpha)T_{h(m)^4 (mod\ n)}(K)\right)^2 + 4\left(\left[T_\gamma(\alpha)\right]^2 + \left[T_{h(m)^4 (mod\ n)}(K)\right]^2 - 1\right)}}{2}$$

Even if he can derive ψ from the preceding equation, finding L from $\psi = T_{L^4 (mod\ n)}(L)$ is impossible (i.e., infeasible). We can see from Lemma 1 that this is identical to solving the chaotic maps issue in *G* and factorizing *n*.

Adv may proceed this attack by selecting two integers

$(L,\ \lambda)$ and tries to figure out the value of S. So, since the Adv does not know the value of S, then γ cannot be found because$\gamma \equiv (\lambda^2 + 2S^2 - 4\lambda S)$. Then using equation (14) as a starting point to solve the following equations.

$$\omega^2 - 2\omega T_{h(m)^4(mod\ n)}(K)\ T_{L^4(mod\ n)}(L) + \left[T_{h(m)^4(mod\ n)}(K)\right]^2 + \left[T_{L^4(mod\ n)}(L)\right]^2 - 1 = 0$$

As a result, ω may be found using the following equation:

$$\omega = \frac{T_{L^4}(L)T_{h(m)^4(mod\ n)}(k)}{2} \mp \frac{\sqrt{\left(\omega T_{L^4}(L)T_{h(m)^4(mod\ n)}(K)\right)^2 + 4\left([T_{L^4}(L)]^2 + \left[T_{h(m)^4(mod\ n)}(K)\right]^2 - 1\right)}}{2}$$

Even if he can derive ω from the preceding equation, finding S from $\omega = T_\gamma(\alpha) = T_{(\lambda^2+2S^2-4\lambda S)(mod\ n)}(L)$ is impossible (i.e., infeasible). We can see from Lemma 1 that this is identical to solving the chaotic maps issue in G and factorizing n.

In the latter case also the same problem if the Adv selecting two integers $(L,\ S)$ and tries to figure out the value of λ. So, since the Adv does not know the value of λ, then γ cannot be found because $\gamma \equiv (\lambda^2 + 2S^2 - 4\lambda S)(\mathrm{mod}\ n)$, then using equations (18 and 19) as a starting point to solve the following equations.

Attack 3. Adv may also get a message signature M_j to obtain t a valid signature $(L_j,\ S_j,\ \lambda_j)$where $j = 1,2, \dots, t$ and tries to find the secret signature key. Here are Adv's equations.

$$\lambda_1^2 + 2S_1^2 - 4\lambda_1 S_1 = h(M_1)^4 b^4 + r_1^4 L_1^4\ (\mathrm{mod}\ n)$$

$$\lambda_2^2 + 2S_2^2 - 4\lambda_2 S_2 = h(M_2)^4 b^4 + r_2^4 L_2^4\ (\mathrm{mod}\ n)$$

$$\lambda_t^2 + 2S_t^2 - 4\lambda_t S_t = h(M_t)^4 b^4 + r_t^4 L_t^4\ (\mathrm{mod}\ n)$$

Where $j = 1,2, \dots, t$. The aforementioned t equations have $(t+1)$ variables, which are b and r_j. Because Adv can generate unlimited solutions to the given system of equations, it is impossible to determine which one is accurate.

Attack 4. Assume that Adv is able to solve QRP. That means, he can find the primes $(\bar{p}, \bar{q})$, but still does not know b^4 because the difficulty of solving CMP. Hence cannot obtain $b, s,$ and λ and fails to produce the signature$(L, S,\ \lambda)$.

Attack 5. Assume that Adv is able to solve CMP. That means, he can find the number b^4 but to get b be must face another problem, QRP which is hard to solve. Thus, he cannot compute the values $S \equiv (h(m)\ b\ r\ L)\ mod\ n$ and $\lambda \equiv (h(m)b + r\ L)^2\ (mod\ n)$ and fails to produce the signature $(L, S,\ \lambda)$.

4.2 Efficiency Performance

The Chebyshev polynomial computation problem, compared to RSA and ECC, has lower key sizes, faster computation, and less memory, energy, and bandwidth use. Scalar multiplications of elliptic curve exponentiations are unnecessary in our protocol. There are numerous ways to tackle the Chebyshev polynomial computation problem given by Wang [26]. For ease of reference, several notations for the procedures involved and their equivalent in seconds are supplied and defined as follows [3, 7, 20-21, 25, 28]:

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

Table 1 shows a comparison between our approach and Chiou's system 2016, which is based on hybrid problems. Using the proposed technique, the total computational complexity is $6T_{mul} + 3T_{ch} + T_{inv}$, which is just 0:749 s, significantly less than the other schemes. Using chaotic maps and QR problems, we show that the suggested approach, based on DLP, QR, and FAC problems is more efficient.

5 Numerical Simulation of the Cryptosystem

Let say a signer wishes to sign a hashed message, *h(m)*=4. Let's consider $\bar{p} = 107, \bar{q} = 103$ and $p = 88169$, the modulus $n = \bar{p}\bar{q} = 11021$ and n is a factor of $p - 1$. We choose the numbers $b = 23$ and $\alpha = 55$ with order 11021 such that $55^{11021} = 1\ (\mathrm{mod}\ 88169)$, then compute the public key,

$$K = T_{23^4}(55) = T_{4316}(55) = 48096(\mathrm{mod}\ 88169)$$

Table 1: An evaluation based on their computational complexity-comparison

Scheme	Signature	Verification	Total (Seconds)	Hard Problems
Chiou's Scheme [13]	$3T_{exp} + 2T_{mul} + 2T_{sq}$	$4T_{exp} + T_{mul}$	42.9993	DLP, FAC
Proposed Scheme	$5T_{mul} + T_{ch} + 3T_{sq} + T_h$	$7T_{sq} + 3T_{ch} + T_h + 3T_{mul}$	0.749	Chaotic map, QR

Thus our public key and secret key of the scheme are$(88169,11021,48096,55)$ and 107, 103, 2, respectively. To sign, the signer first chooses at random $r = 13 \in \mathbb{Z}_n^*$ and computes the following:

$$L = T_{13^4}(55)(\text{mod } 88169) = 80445 \text{ (mod } 88169)$$

$$S \equiv 402(13)(23)(80445)(\text{mod } 1102) \equiv 9676 \text{ (mod } 1102)$$

$$\lambda \equiv (402 \times 23 + 13 \times 80445)^2(\text{mod } 1102) \equiv 5257 \text{ (mod } 1102)$$

The signature produces as (L, S, λ) = (88169,1102,525). To test its validity, the verifier calculates the following:

$$\gamma \equiv (\lambda^2 + 2S^2 - 4\lambda S)$$

$$\equiv (5257^2 + 2 \times 9676^2)$$

$$- 4 \times 5257 \times 9676(\text{ mod } 1102)$$

$$\equiv 1317 \text{ (mod } 1102)$$

$$W_1 = \left[T_\gamma(\alpha)\right]^2 + \left[T_{h(m)^4(mod\ n)}(K)\right]^2$$

$$+\left[T_{L^4(mod\ n)}(L)\right]^2\ mod\ p$$

$$W_1 = [T_{1317}(55)]^2 + [T_{528}(55)]^2$$

$$+[T_{789}(55)]^2\ (mod\ 88169)$$

$$W_1 = [73392]^2 + [86390]^2 + [3092]^2$$

$$W_1 = 82254 \text{ (mod } 88169)$$

$$W_2 = 2 \times 73392 \times 86390 \times 3092 + 1$$

$$W_2 = 82254$$

Since W1=W2 then the signature is now validated

6 Conclusion

Based on chaotic maps and quadratic residue problems, we developed a novel signature technique. Using chaotic maps, the proposed system claims to give much improved performance than existing signature schemes based on FAC and DL problems. The proposed strategy has a significantly reduced calculation cost than previous schemes, resulting in enhanced security, dependability, and productivity.

References

[1] O. M. Al-Hazaimeh, "A New Dynamic Speech Encryption Algorithm Based on Lorenz Chaotic Map over Internet Protocol," *International Journal of Electrical and Computer Engineering*, 10(5):4824, 2020.

[2] O. M. Al-hazaimeh, "A New Speech Encryption Algorithm Based on Dual Shuffling Hénon Chaotic Map," *International Journal of Electrical and Computer Engineering (IJECE)*, 11(3):2203-2210, 2021.

[3] O. M. Al-Hazaimeh, A. A. Abu-Ein, K. M. Nahar, and I. S. Al-Qasrawi, "Chaotic Elliptic Map for Speech Encryption," *Indonesian Journal of Electrical Engineering and Computer Science*, 25(2):1103-1114, 2022.

[4] L. Bakrawy, N. Ghali, A. Hassanien and Th. Kim, A Fast and Secure One-Way Hash Function," *Compututer and Information Science*, 259:85-93, 2011.

[5] K. Chain and C. Kuo, "A New Digital Signature Scheme Based on Chaotic Maps," *Nonlinear Dynamics*, 24(4):1003-1012, 2013.

[6] S. Chiou, "Novel Digital Signature Schemes Based on Factoring and Discrete Logarithms," *International Journal of Security and Its Applications*, 10(3):295-310, 2016.

[7] S. Ghassan, "Certificate Revocation Management in VANET," *International Journal of Cyber-Security and Digita,* 1(2):115-121, 2012.

[8] H. He, "Digital Signature Schemes Based on Factoring and Discrete Logarithms," *Electronics Letters*, 37(4):220-222, 2001.

[9] S. Hung, "Cryptanalysis of a Digital Signature Scheme Based on Factoring and Discrete Logarithms," *Proceedings of the National Computer Symposium*, Taipei, Taiwan, F043- F045, 2001.

[10] S. Hwang, C. Yang, and F. Tzeng, "Improved Digital Signature Scheme Based on Factoring and Discrete Logarithms," *Journal of Discrete Mathematical Sciences and Cryptography,* 5(2):151-155, 2022.

[11] E. Ismail and N. Tahat, "A New Signature Scheme Based on Multiple Hard Number Theoretic Problems," *International Scholarly Research Notices*, Article ID 231649, vol. 2011, 3 pages, 2011.

[12] E. Ismail, N. Tahat, and R. Ahmad, "A New Digital Signature Scheme Based on Factoring and Discrete Logarithms*, Journal of Mathematics and Statistics,* 14(4):222-225, 2008.

[13] X. Li and D. Zhao, "Optical Color Image Encryption with Redefined Fractional Hartley Transform," *International Journal for Light and Electron Optics*, 121(7):673- 677, 2010.

[14] R. Matthews, "On the Derivation of a Chaotic Encryption Algorithm," *Cryptologia*, 13(1):29-41, 1989.

[15] A. K. Mohammad, P. M. Himadri, and D. J. Syeda, "Anti-Synchronization Phenomenon of Discrete Chaotic Maps using Linear Transformations," *Journal of Information and Optimization Sciences*, 41(8):1757-1769, 2020.

[16] F. Pon, H. Lu, and B. Jeng, "Meta-He Digital Signature Schemes Based on Factoring and Discrete Logarithms," *Applied Mathematics and Computation*, 65(1):171-176, 2005.

[17] H. Qian, F. Cao, and H. Bao, "Cryptanalysis of LiTzeng Hwang Improved Signature Schemes Based on Factoring and Discrete Logarithms," *Applied*

Mathematics and Computation, 166(3):501-505, 2005.
[18] 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, DOI: 10.1080/02522667.2018.1470752, 2019.
[19] Z. Shao, "Digital Signature Schemes Based on Factoring and Discrete Logarithms," *Electronics Letters*, 38(24):1518-1519, 2002.
[20] N. Tahat, "Convertible Multi-Authenticated Encryption Scheme with Verification Based on Elliptic Curve Discrete Logarithm Problem," *Int. J. Computer Applications in Technology*, 54(3):229-235, 2016.
[21] N. Tahat, A. K. Alomari, A. Al–Freedi, O. M. Al-Hazaimeh, and M. F. Al–Jamal, "An Efficient Identity-Based Cryptographic Model for Chebyhev Chaotic Map and Integer Factoring Based Cryptosystem," *Journal of Applied Security Research*, 14(3):257-269, 2019.
[22] N. Tahat, A. K. 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*, 23(4):935-948, 2020.
[23] J. Tay, C. Quan, W. Chen, and Y. Fu, "Color Image Encryption Based on Interference and Virtual Optics," *Optics and Laser Technology*, 142(2):409-415, 2010.
[24] C. Wang, H. Lin, and C. Chang, "Signature Scheme Based on Two Hard Problems Simultaneously," *Proceedings of the 17th International Conference on Advanced Information Networking and Application (AINA),* Xian, China, pp. 557-560, 2003.
[25] X. Wang, X. Wang, and J. Zhao, "Chaotic Encryption Algorithm Based Alternant of Stream Cipher and Block Cipher," *Nonlinear Dyn*., 63:587-597, 2011.
[26] L. Xiong, N. Jianwei, K. Saru, H. Sk, W. Fan, K. Muhammad, and K. Ashok, "A Novel Chaotic Maps-Based User Authentication and Key Agreement Protocol for Multisever Environments with Provable Security, *Wireless Pers Communication*, 89(2):569-597, 2016.
[27] J. Yoon and S. Jeon, "An Efficient and Secure Diffie-Hellman Key Agreement Protocol Based on Chebyshev Chaotic Map," *Journal of Communications in Nonlinear Science and Numerical Simulation*, 16(6):2383-2389, 2011.
[28] L. Zhang, "Cryptanalysis of the Public Key Encryption Based on Multiple Chaotic Systems," *Chaos Solitons Fractals*, 37(3):669-674, 2008.

Rania Shaqbou'a received the B.Sc. degree in mathematics from Yarmouk University, Jordan, in 1999, the M.Sc. degree in Pure Mathematics from University of Jordan, in 2005. She is an Assistant Lecturer at Department Mathematics, Hashemite University.

Nedal M. Tahat received his BSc in Mathematics at the Yarmouk University, Jordan, in 1994, and MSc in Pure Mathematics at Al al-Bayt University, Jordan, in 1998. He is a PhD candidate in Applied Number Theory (Cryptography) from the National University of Malaysia (UKM), in 2010. He is a Full Professor at the Department Mathematics, Hashemite University. His main research interests are cryptology and number theory. He has published more than 52 papers, authored/co-authored, and more than 15 refereed journal and conference papers. He can be contacted at email: nedal@hu.edu.jo

Osama Ababneh is an Assistant Professor of Applied Mathematics at the Faculty of Science, Mathematics department, Zarqa University, Jordan. In 2005 Ababneh got his first degree in Mathematics at Al-Albyet University and from 2007 to 2010 he carried out further studies in Mathematics (Master and PHD) at UKM University, Malaysia. From 2011 till now he has been an Assistant Professor at the Irbed University and Zarqa university, Jordan. Ababneh is the Editor in Chief of General Letters in Mathematics. Ababneh has more than twenty scientific papers and is a member of scientific committees of various international conferences and an editorial board member of various scientific journals.

Obaida M. Al-Hazaimeh earned a BSc in Computer Science from Jordan's Applied Science University in 2004 and an MSc in Computer Science from Malaysia's University Science Malaysia in 2006. In 2010, he earned a PhD in Network Security (Cryptography) from Malaysia. He is a Full professor at Al-Balqa Applied University's Department of Computer Science and Information Technology. Cryptology, image processing, machine learning, and chaos theory are among his primary research interests. He has published around 51 papers in international refereed publications as an author or co-author. He can be contacted at email: dr_obaida@bau.edu.jo