Received: April 27, 2024. Revised: June 17, 2024.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

2D Henon, Tinkerbell and Tent Sine Chaos Map for Digital Signature System based on Modified Schnorr and Elgamal Schemes

Rusul Mansoor Al-Amri[1] **Rafida M. Elobaid**[2] **Alaa kadhim farhan**[3]* **Wageda Al-sobky**[4]
Hossam E. Ahmed[5,6]

[1]*College of Nursing, University of Al-Ameed Karbala, PO No: 198 Iraq*
[2]*School of Engineering, Applied Science and Technology, Canadian University Dubai, UAE*
[3]*Department of Computer Science, University of Technology, Iraq*
[4]*Benha Faculty of Engineering, Department of Basic Engineering Science, Benha University, Egypt*
[5]*Department of Electrical Engineering, College of Engineering,*
Northern Border University, Arar 91431, Saudi Arabia
[6]*Electrical Engineering Department, Faculty of Engineering, Benha University, Benha, Egypt*
* Corresponding author's Email: Alaa.k.farhan@uotechnology.edu.iq

Abstract: This research presents new proposed algorithms for generating digital signatures. The proposed algorithms based on coupling chaotic maps with Schnorr and Elgamal schemes to obtain the private key. These maps, including 2D henon, 2D tinkerbell, and Tent Sine System, generate a sequence of random iterations, each one is then converted into 256-bit integer to be fit as the private key. The key space is increased (2^{256}) compared to the traditional Schnorr and Elgamal (2^{160}) and there become a wide range of digital signatures corresponding to the random iterations. The key space development increases the security level of the signature scheme which in turn makes it difficult for any adversary to hack the scheme. Also, the results proved that our new algorithm takes less signing and verification time compared to other proposed algorithms. It was proved that our proposed algorithms don't require large number of keys for signing or verification. It is just one private key and another public.

Keywords: 2DHenon map, Tinkerbell map, Tent Sine map, Elgamal digital signature scheme, Schnorr digital signature scheme.

1. Introduction

A mathematical procedure known as a “digital signature” can be employed to guarantee the integrity and authenticity of an email, application software, or digital document [1]. Despite being the digital counterpart of them, it provides significantly greater inherent protection than a printed document or stamped signature. It also attempts to deal with the problem of imitation and espionage in online communication. It can provide evidence of who generated a digital email, purchase, or document, as well as their identity and current status [2]. Participants may also apply it to attest to their free and informed consent. Whitfield Diffie and Martin Hellman established the concept of a digital signature strategy in 1976; however, they only hypothesized that such mechanisms may have arisen based on functions that are trapdoor one-way permutations [3]. The RSA procedure, devised shortly after by Ronald Rivest, Adi Shamir, and Len Adleman, has been used for producing simple digital signatures (albeit only as a demonstration of concept since “uncomplicated RSA signatures are not strong) [4]. The first commercially promoted application programme to enable a digital signature was Lotus Notes 1.0, which was published in 1989 and employed the RSA algorithm [5]. After RSA, multiple digital signature technologies quickly emerged, the earliest of which were Lamport signatures, Merkle signatures (sometimes called “Merkle trees” or “Hash trees) [6], and Rabin signatures [7]. Ronald Rivest, Shafi

Goldwasser, and Silvio Micali were the first to officially lay down the security specifications for digital signature procedures in 1988. The GMR signature system, the first to have demonstrated its ability to safeguard even an existential falsification versus a specific message assault, which is the commonly acknowledged security criterion for signature strategies, has been provided as well. They have established an order of attack scenarios for signature algorithms. Moni Naor and Moti Yung [8] issued the first such strategy, which has not been based on trapdoor functions but instead on a collection of functions with a far weaker prerequisite for one-way permutation. [8].

Digital signatures can offer further reassurance of the evidence regarding the source, sense of self, and legitimacy of an electronic document, as well as acknowledgement of informed permission and approval by a signatory [9], since organizations migrate away from physical documents with ink signatures or authenticity marks. The US Government Printing Office (GPO) produces electronic budgets, private and public legislation, and congressional bills that have digital signatures. Computerised student certificates with digital signatures are being published by universities like Penn State, Stanford and the University of Chicago. In many countries, including the US, they are recognized as legally binding in the same manner as traditional printed paper signatures [10]. In order to create a digital signature, the signing technology—delivers a single-direction hash of the online data that needs to be verified, such email apps [11]. An algorithm generates a fixed-length stream of characters and numbers that is known as a hash. The digital signature creator's secret key is then used to encrypt the hash. The cryptographic hash linked to the digital signature contains more data, including the hashing algorithm [12]. The hash is encoded rather than the complete message or content since a hash method can convert any input into a value of a certain length [13].

This reduces an enormous amount of time because hashing is significantly faster than signing. The value of a hash is not the same as the data it encodes. Any modifications to the data, even if they just affect a single component, will affect the value. This feature enables other users to decode the hash and confirm the accuracy of the contents using the signer's public key [14]. If the decoded hash and another calculated hash of the identical data agree, it is assured that the data was not changed after it was digitally signed [15].

The recipient is aware of the contents of the communication as well as who sent it. If the hash digests for both are different, it could indicate that the signature was made with a secret key that is incompatible with the public key that the signer supplied, or that there is a problem with authentication [16]. Digital signatures can be applied to any message, encrypted or not, as long as the recipient is certain of the sender's identity and that the message was delivered unaltered [17].

The digital signature links the signer and the document together, making it difficult for the signer to maintain that they did not sign anything. This quality is known as non-repudiation. Digital signatures and digital authorizations are not the same thing [18]. A digital certificate is an electronic document that has the licensing CA's digital signature embedded in it. By linking a public key to a specific identity, it is possible to confirm that it belongs to a certain person or entity [19]. Digital signature technology is used by manufacturers to speed up procedures and improve document security. The government, healthcare, manufacturing, financial services, smart contracts, and cryptocurrencies are a few of these industries [20].

The rapid advancement of technology has led to the development of numerous digital signature techniques. The previously mentioned algorithms were all created with the intention of generating digital signatures that were very safe and well-executed.

chaotic structures have been extensively utilized in recent years to create reliable cryptographic techniques [39, 40]. These structures have demonstrated their capacity to erect extremely strong defenses against a variety of threats. Additionally, these structures offer an excellent trade-off between rapidity, safety, and efficiency, which makes them the top choice for secure digital signatures [41]. Randomness and non-periodicity are examples of nonlinear features of chaotic systems, which are produced by their extreme sensitivity to initial states and parameters. The intricacy of the applied chaotic system determines the security of chaotic digital signature systems. Some of its characteristics include being sensitive to factors and having chaotic sequences that are widely scattered, making long-term predictions problematic.

Numerous more schemes were created based on two challenging difficulties to increase the security of signature techniques: FAC as well as DLP [52-57]. Some writers have, nevertheless, also demonstrated the flaws in these methods [58-61]. In addition, there exist numerous signature techniques that rely on two problems [62-65], however these schemes require a high level of computing complexity. As a result, it is crucial to implement the digital signature method based on several assumptions in order to improve system security. We present a digital signature technique for Schnorr and Elgamal schemes in this paper that is based on chaotic maps.

Matthews was the researcher who first presented the first chaotic picture encryption technique [42]. An innovative key-agreement procedure employing chaotic maps and other complex functions, they have been proposed in a number of ways [43-51] in response to the increased interest in this field. The session key in their method was determined by using the semi-group characteristic of the Chebyshev chaotic map. A secure group-key agreement mechanism depending on chaotic hash and utilizing chaotic hash functions was put out by Hwang et al. [22]. A secure and effective signature system built around chaotic maps and factorization difficulties was recently devised by Chain and Kuo [13]. Their plan was the first to use factorization issues and chaotic maps. Regretfully, their scheme needs a large number of keys in order to sign and validate signatures.

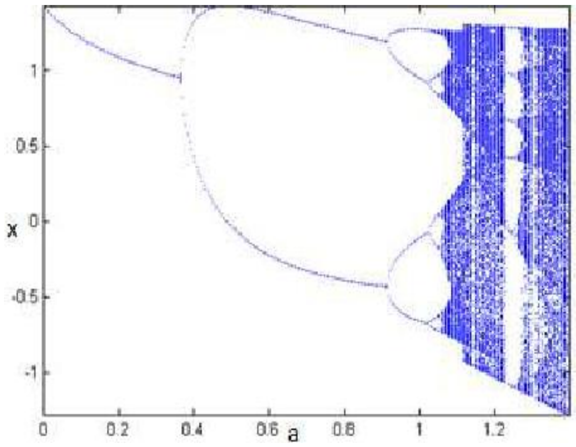
Our contributions propose a new digital signature scheme with new properties suitable for work organization. We integrated chaotic maps with El-Gamal and Schnorr digital signature to improve the security against any attacks. The rest of paper is organized as follows:

In section 2, chaotic maps are explained in general, and the exploited ones are described particularly. In section 3, Schnorr and Elgamal schemes are introduced. The proposed algorithm is explained in section 4. Finally, results of the proposed algorithms and comparison between them and the traditional ones are illustrated in section 5.

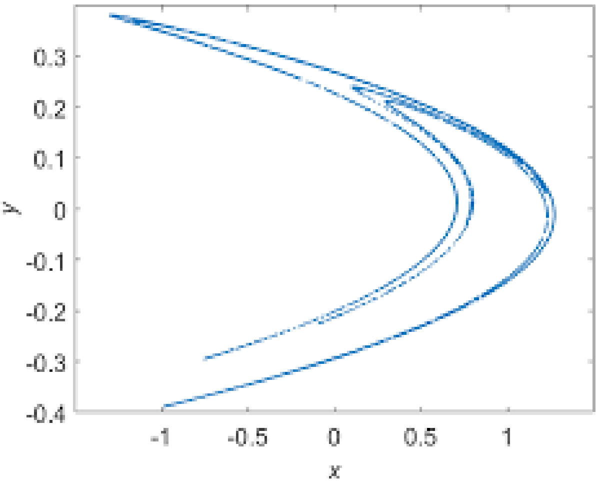
2. Chaotic maps

A chaotic map is a map—more precisely, a growth function—that exhibits some form of mathematical irregularity. A pioneer of the chaos hypothesis was Henri Poincaré. He discovered that there can be non-periodic rotations that are neither always ascending nor getting closer to a fixed point in the 1880s when analysing the three-body issue [21]. Most of the mathematics associated with the chaos hypothesis has been constructed using the continuous replication of straightforward mathematical formulas. Chaotic maps had been expanding continuously up until today. They have worked on an assortment of applications, encompassing robotics, biology, economics, and cryptography [22]. Two types of chaotic systems have been the subject of much research: chaos in one-dimensional (1D) and high-dimensional (HD) dimensions. Examples of classical 1D chaotic structures are duffing maps, henon, and bogdanov maps. The chaotic sequences generated by 1D chaotic maps are less stochastic due to their modest complexity and regularity, which raises several safety problems when handling visual coding. The behavior of chaotic patterns in HD chaotic structures is presumably more unexpected and more suited for visual coding since they have a more complex structure and a wider range of parameters than 1D chaotic systems [23].

Diverse chaotic maps, including 2D henon, 2D tinkerbell and Tent Sine System, have been presented to be utilised in these algorithms. Constructing cryptosystems benefits from the distinctive characteristics of chaotic structures, such as determinacy, ergodicity, and sensitivity to initial conditions, as these attributes are analogous to the confusion and diffusion aspects of an adequate cryptosystem.



(a)



(b)

Figure. 1 Bifurcation diagram and phase diagram of 2D Henon map: (a) bifurcation diagram and (b) phase diagram

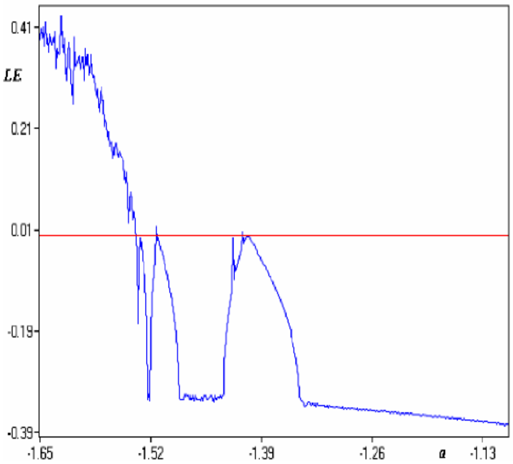
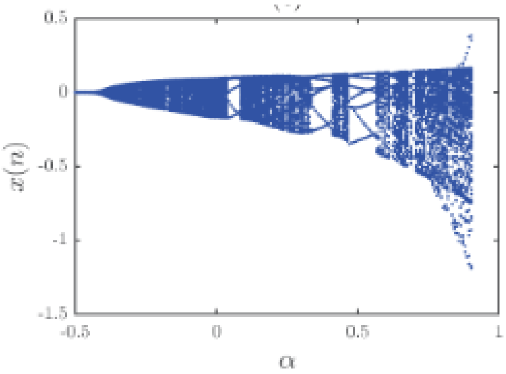
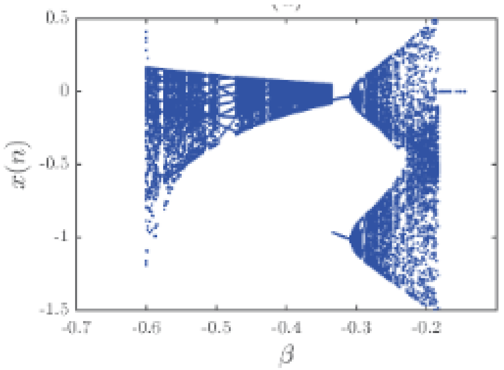


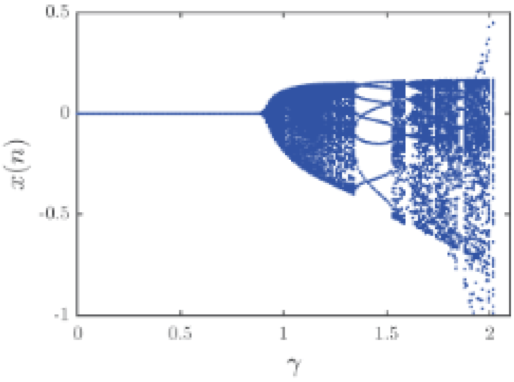
Figure. 2 Henon map lyapunov exponent



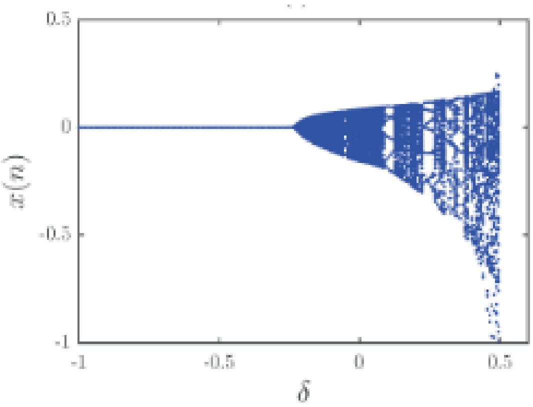
(a)



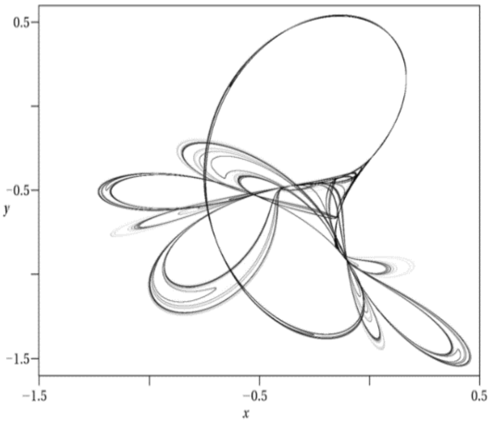
(b)



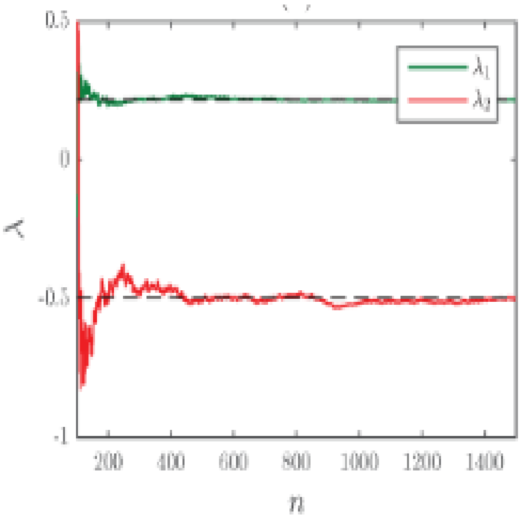
(c)



(d)



(e)



(f)

Figure. 3: (a) Attractor of the Tinkerbell map with (α, β, γ, δ) =(0.9,−0.6013,2,0.5) and initial conditions ($x(0)$,$y(0)$)=(−0.72,−0.64), (b) bifurcation plot with $\alpha\in[-0.5,1]$ as the critical parameter and $\Delta\alpha$=0.0075, (c) bifurcation plot with $\beta\in$ [−0.6, −0.1] as the critical parameter and $\Delta\beta$=0.0025, (d) bifurcation plot with $\gamma\in$ [0,2.1] as the critical parameter and $\Delta\gamma$=0.01, (e) bifurcation plot with $\delta\in$ [−1,0.6] as the critical parameter and $\Delta\delta$=0.008, and (f) estimated Lyapunov exponents ($\lambda 1$, $\lambda 2$) where $\lambda 1\approx 0.2085$ $\lambda 2\approx -0.4925$ for n iterations

2.1 2D henon map

The Hénon map, which is additionally known as the Hénon-Pomeau attractor/map, is a discrete-time nonlinear system in mathematics [24-28]. It can be considered one of the most extensively researched illustrations of chaotic behaviour in structures with dynamics. The aforementioned equations illustrate how the Hénon map transforms a location (x_n, y_n) in the plane to a new location:

$$\begin{gathered}\boldsymbol{X_{n+1} = 1 - a x_n^2 + y_n} \\ \boldsymbol{y_{n+1} = b x_n}\end{gathered} \tag{1}$$

The traditional Hénon map has two parameters, a and b, with values of a = 1.4 and b = 0.3. These values determine the map's dependence. There is a degree of chaos in the Hénon map for the traditional values. The map simplifies to a single-dimensional quadratic map with a maximum Lyapunov exponent of ln (2) = 0.693147181, where the maximum exists for a = 2 and b = 0. A shrinkage that is indefinitely fast in the direction orthogonal to a single-dimensional parabolic attractor is implied by its opposite exponent, which is minus infinity. Figs. 1 and 2 display the 2D Henon map's bifurcation diagram, phase diagram, and Lyapunov exponent, respectively.

2.2 2D Tinkerbell map

A discrete-time nonlinear structure known as the Tinkerbell map is presented by:

$$\begin{gathered}X_{n+1} = x_n^2 - y_n^2 + \alpha x_n + \beta y_n \\ y_{n+1} = 2 x_n y_n + \gamma x_n + \delta y_n\end{gathered} \tag{2}$$

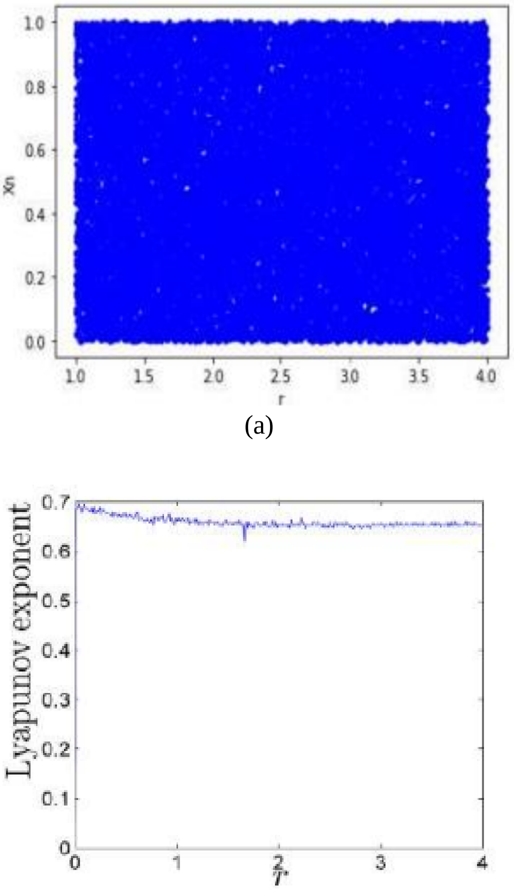
A few regular values for the control parameters α, β, γ and δ are:

- $\alpha = 0.9, \beta = -0.6013, \gamma = 2.0, \delta = 0.50$
- $\alpha = 0.3, \beta = 0.6000, \gamma = 2.0, \delta = 0.27$

Figs. 3 and 4 display the 2D Tinkerbell map's bifurcation diagram, phase diagram, and Lyapunov exponent, respectively [29-32].

2.3 Tent sine system

The tent map shares the same problems as logistic maps: a small chaotic range and non-uniform distribution inside the interval [0, 1]. By merging the tent and sine maps as seed maps, a novel chaotic system known as the tent sine system (TSS) is produced [36]. Its definition is given by formula (3), which combines its two parameters. $x_n \in [0, 1]$ and r ∈ [0, 4]. The TSS possesses ideal chaotic features, as seen in Fig. 6(a). As illustrated in Fig. 6 (b), the LSS and TSS Lyapunov exponents have values greater than zero in the range of r ∈ [0, 4], whereas the LE values of their seed maps are positive within a restricted range.



(a)

(b)

Figure. 4 Dynamical behavior of TSS: (a) bifurcation plot and (b) Lyapunov exponent

$$\boldsymbol{x_{n+1} =} \begin{cases} \boldsymbol{\left(\frac{r x_n}{2} + \frac{(4-r)\sin(\pi x_n)}{4}\right) mod\, 1,\ x_n < 0.5} \\ \boldsymbol{\left(\frac{r(1-x_n)}{2} + \frac{(4-r)\sin(\pi x_n)}{4}\right) mod\, 1,\ x_n \geq 0.5} \end{cases} \tag{3}$$

3. Digital signature algorithms

Digital signature algorithms are numerous. A few of these algorithms, including the Elgamal and Schnorr algorithms, are effective and appropriate for usage in certain applications, such smart contracts, and provide good security and outcomes. [33].

3.1 Schnorr digital signature algorithm

Claus Schnorr stated it in his own words. It is one of the oldest digital signature methodologies and is recognized for its straightforwardness. Security centres on the stubbornness of particular discrete logarithm issues. It provides signatures that are succinct and effective. [34]

A) *Choosing parameters:*

it is thought that the discrete log challenge is hard in the set of generators, G, of prime order, q, where each signatory to the signature technique agrees, and generator g. Usually, Schnorr are allocated to a group. Everyone accepts the encoded hash function $H: \{0,1\}^* \rightarrow \mathbb{Z}_q$, where $\mathbb{Z}_q$ is the set of integers from 0 to $q-1$

B) *generation of Key:*

- From $\mathbb{Z}_q$, a secret signing key, u, is selected. The public key for verification is designated to be $t = g^u \, mod \, q$

C) *Signing*

To put up a sign with a message, :

- From the suitable range, a random integer l is selected at random.
- Declare a parameter w such that it:

$$w = g^l \tag{4}$$

- Afterwards, identify an element z such that:

$$\boldsymbol{z = H(w||M)} \tag{5}$$

where a bit string representing the concatenation symbol, ||, is displayed.

- Suppose

$$\boldsymbol{s = l - uz} \tag{6}$$

Where s gives the value of the signature.

- Two distinct signatures joined are (s, z).
- Bear in mind that , $z \in \mathbb{Z}_q$; if $q < 2^{160}$, then 40 bytes are enough to store the signature illustration.

D) *Verification*

- Let a parameter w_v such that:

$$\boldsymbol{w_v = g^s t^z} \tag{7}$$

- Then suppose.

$$\boldsymbol{z_v = H(w_v||M)} \tag{8}$$

- The signature is authenticated if $z_v = z$.

3.2 Elgamal digital signature algorithm

Elgamal signature methodology has been presented depending on the difficulty of discrete logarithm processing. It was first published in 1985 by Taher Elgamal. [35]

A) *Key generation*

Key development occurs in two stages. Selecting methodological components that other system users can access is the first stage; computing a single key pair for a specific user is the second.

B) *Parameter generation*

- A key length has been chosen N.
- q is a prime number of a length N -bit is selected.
- A cryptographic hash function H with output length L bits is chosen. Only the leftmost bits of the hash output are handled if $L > N$.
- A generator $g < q$ of the multiplicative group of integers z_q^* modulo $q$is chosen.
- (q, g) These are the scheme's constituent parts. Members of the system may have these components in common.

C) *Per-user keys*

- The second step uses a set of elements to estimate the key pair for a particular user:
- An integer u is randomly picked from $\{1, \ldots\ldots, q-2\}$.
- Estimate

$$\boldsymbol{t = g^u \, mod \, q} \tag{9}$$

$u$is the secret key and $t$is the public key.

D) *Signing*

The following code generates a message sign:

- l is picked as a random integer from $\{2, \ldots\ldots, q-2\}$ which relatively prime to $q-1$.
- Estimate a parameter $w$such that:

$$\boldsymbol{w = g^l \mathbf{mod} q} \tag{10}$$

- Estimate the signature value $s$such that:

$$\boldsymbol{s = (H(m) - uw) l^{-1} \mathbf{mod} (q - 1)} \tag{11}$$

- In the uncommon scenario that $s = 0$, you have to start over with a new random l.
- (w, s) is the signature.

E) *Verification*

- Follow these three procedures to determine whether a message's signature is valid.
- Test if $0 < w < q$ and $0 < s < q - 1$.

- The signature is authentic only if $$g^{H(m)} \equiv t^{w} w^{s} \bmod q \quad (12)$$

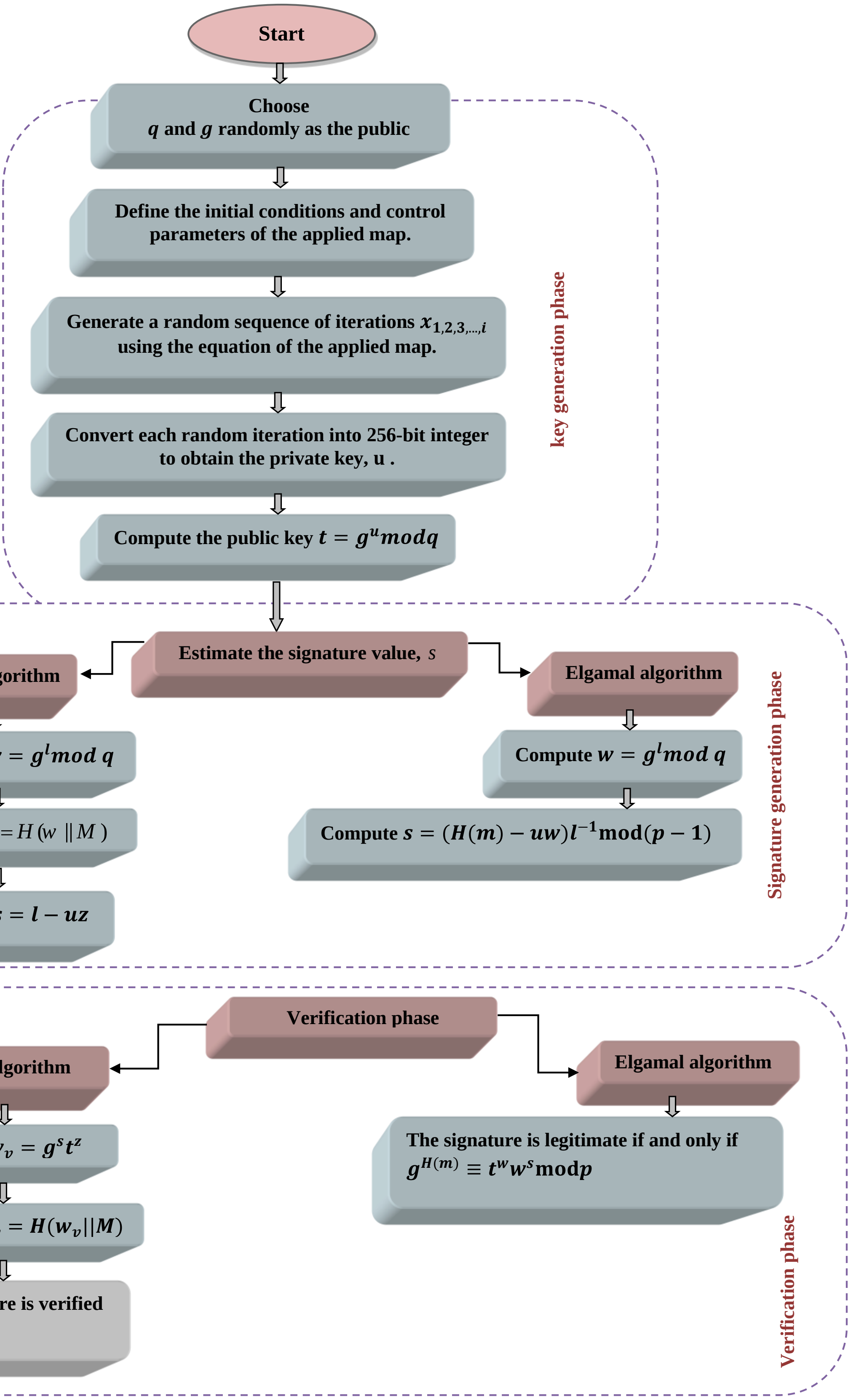


Figure. 5 Flow chart of the proposed algorithm

4. The proposed algorithm

The proposition would mainly modify the process of secret signing key generation. It would utilize the randomness property of the chaotic map to generate large sequence of the private key. A secret signing key, u, is generated as a key sequence using a chaotic map. 2D henon, 2D tinkerbell and Tent Sine System. would be used in this manner. The verification public key is calculated as $t = g^u \mathrm{mod} q$. Signing and verification phase would be the same as described in item 3.1 and 3.2. The flow chart of the proposed algorithm is shown in Fig. 5.

Steps of the proposed algorithm

Input: q , g and l.

Output: The private key, u, and a signature, s ,for each private key.

a. Define the parameters and initial conditions of the map.
b. Generate a random sequence of iterations using the map's equation.
c. Convert each random iteration into 256-bit integer.
d. Generate a signature, s,for each private key u.
e. Verify that each signature is valid.

5. Results and comparisons

Traditional Schnorr and Elgamal algorithms have been used in multiple applications such as smart contracts, healthcare, etc. They have achieved good results, but the private key size hasn't been large (2^{160}) and random enough to achieve the required security. In the proposed algorithms, chaotic maps were employed to generate a random sequence of the private key with larger size (2^{256}). Time for creating the signature and verification was optimized. All conditions, parameters and number of iterations used in all algorithms have been chosen so that no repetition in results could occur. Table 1 shows the applied values in the proposed algorithms, Table 2 shows the results of the proposed algorithms that state that Tent Sine System achieved the best results (speed and large space of output) of all, and Table 3 shows the comparison between the proposed algorithms and the traditional one's results. Table 4 shows the comparison between the proposed algorithms and the other one's results for 100000 message tests. It is proved that our new algorithm achieves the least signing and verification time. Tables 5,6,7,8,9,10 show Schnorr and Elgamal digital signature based on the implemented maps for 100000 messages. These tables prove that our new algorithms don't require a high level of computing complexity and suitable for hardware implementation.

Table 1. Initialization values for the proposed algorithms

Digital signature algorithm	chaotic map	number of iterations	size of the Output	initial conditions period	the range of q
Schnorr	**2D Henon**	100000	256-bit	$x_0 = 0.009$, $y_0 = 0.009$	$[10^{20}, 10^{50}]$
	2D Tinkerbell	20000	256- bit	x_0 = -0.72, y_0 = -0.64	$[10^{20}, 10^{50}]$
	Tent Sine System	2,000,000	256- bit	x_0= 0.231095821	$[10^{20}, 10^{50}]$
Elgamal	**2D Henon**	100000	256- bit	$x_0 = 0.009$, $y_0 = 0.009$	$[10^{20}, 10^{50}]$
	2D Tinkerbell	20000	256- bit	x_0 = -0.72, y_0 = -0.64	$[10^{20}, 10^{50}]$
	Tent Sine System	2,000,000	256- bit	x_0= 0.231095821	$[10^{20}, 10^{50}]$

Table 2. Results of the proposed algorithms

Digital Signature Algorithm	Chaotic Map	Part of the output Sign With "Hello World" Message
Schnorr	**2D Henon**	The Sign is 13168562200547752301863090564508715765876765278996 The Sign is 34984702639951553571740306798409331928656013291907 The Sign is 13410811066797462372767720607460012872086967596791 The Sign is 48637126091968866872910066759369168978897681172744 The Sign is 3573713172372281342518975220840685576358978746420
	2D Tinkerbell	The Sign is 42571814182950694018232358725777067388052811711878 The Sign is 22085085847743319536417062125939732860859904703984 The Sign is 54466351999695445092915957485968437327259315854717 The Sign is 79059165560747490096259118214548750126629817177233 The Sign is 10614265891787828951633456991785927798979679362172
	Tent Sine System	The Sign is 6368865835558097313297469905348897871420327256405 The Sign is 25869041779441335872486111863436388272804412647310 The Sign is 35206197005819375188474348265481393425248508969077 The Sign is 38007937231520285484876041141838111878086034557542 The Sign is 7406828609745575066955786797476717800801324442435
Elgamal	**2D Henon**	The Sign is 65389733047973312481512364041884540900686317030088 The Sign is 74390984048605155256005006317852592132657317630154 The Sign is 17405871285942945051654538687248491252623615053441 The Sign is 38423570228158889935898444806334280733526558665137 The Sign is 57741608140206406112789318266829362097537481538689
	2D Tinkerbell	The Sign is 54161095208154053180256503307073262623719288002975 The Sign is 20848457528616425752810030069767219645052068000660 The Sign is 64915538648446113493814920351607986738703615542690 The Sign is 32196303913745641981233711830911479517995436451470 The Sign is 63915057822151641670227372575368602801626960680497
	Tent Sine System	The Sign is 42728882339421040679326696146869828060693444044492 The Sign is 27856000767517775508957165209340726340911421159160 The Sign is 41760007724853616496528156731387258991947258289291 The Sign is 35884675887264893399988445953706128713667801535572 The Sign is 26186244121890729789228497304376916997498484405180

Table 3. Comparison between the proposed algorithms and the traditional one's results for 100000 message tests

Algorithm	Time of signing(s)	Time of verification(s)	Private key space
Traditional Schnorr	0.00016991869	0.0003609101659	2^{160}
Schnorr based on 2D Henon	0.0000000011	0.0001994507	2^{256}
Schnorr based on 2D Tinkerbell	0.0009989738	0.0029962062	2^{256}
Schnorr based on Tent Sine System	0.0006417499999	0.00055259175	2^{256}
Traditional Elgamal	0.00034725805187	0.0006738269302593	2^{160}
Elgamal based on 2D Henon	0.0156443119	0.0009781853	2^{256}
Elgamal based on 2D Tinkerbell	0.0010154247	0.0019965171	2^{256}
Elgamal based on Tent Sine System	0.00090998991012	0.0008496008053	2^{256}

Table 4. Comparison between algorithms for 224-bit key length

Algorithm	Signature time(ms)	Verification time(ms)	Total time(ms)
Schnorr Scheme	0.1310	1.4503	1.5813
Elgamal Scheme	0.4946	0.2075	0.7021
Schnorr based on 2D Henon	1.0124	1.3421	2.3545
Schnorr based on 2D Tinkerbell	1.3524	1.4565	2.8089
Schnorr based on Tent Sine System	0.4258	0.4365	0.8623
Elgamal based on 2D Henon	1.115	1.213	2.328
Elgamal based on 2D Tinkerbell	1.0047	1.0876	2.0923
Elgamal based on Tent Sine System	0.50041	0.4015	0.90191
Ref [34] structure 1	1.3081	1.4480	2.7561
Ref [34] structure 2	1.3456	1.4634	2.809
Ref [34] structure 3	0.3924	0.2609	0.6533
Ref [34] structure 4	0.5075	0.2538	0.7613
Ref [35]	3,5000	5,2200	40,200
Ref [61]	-	-	4465.38
Ref [62]	-	-	8508.74
Ref [63]	-	-	2344.23
Ref [64]	-	-	1515.03
Ref [65]	-	-	10.31
Ref [66]	-	-	912.19
Ref [67]	-	-	7.29
Ref [68]	-	-	29.570

Table 5. Schnorr Digital signature based on 2D Henon map for 100000 messages

	length of characters	signing time (ms)	verification time (ms)
1	208	0.34567	0.44236
2	416	0.32158	0.3248
3	624	0.33254	0.43325
4	832	0.32156	0.36987
5	1040	0.311254	0.434258
6	1248	0.332455	0.39575
7	1456	0.34258	0.45472
8	1660	0.302458	0.34269
9	1868	0.39875	0.432258
10	2076	0.399587	0.378954

Table 6. Schnorr Digital signature based on 2D Tinkerbell map for 100000 messages

	length of characters	**signing time (ms)**	**verification time (ms)**
1	208	0.35265	0.34263
2	416	0.33415	0.34358
3	624	0.34524	0.33345
4	832	0.42153	0.30125
5	1040	0.44126	0.44254
6	1248	0.310203	0.38457
7	1456	0.34185	0.44987
8	1660	0.31857	0.320147
9	1868	0.341256	0.44427
10	2076	0.410587	0.35687

Table 7. Schnorr Digital signature based on Tent Sine System for 100000 messages

	length of characters	**signing time (ms)**	**verification time (ms)**
1	208	0.331456	0.43982
2	416	0.311528	0.320014
3	624	0.3320542	0.432975
4	832	0.3921506	0.35621
5	1040	0.389112	0.40014
6	1248	0.3432454	0.303244
7	1456	0.34412	0.478512
8	1660	0.30098	0.344420
9	1868	0.39997	0.4310298
10	2076	0.39842	0.300023

Table 8. Elgamal Digital signature based on 2D Henon map for 100000 messages

	length of characters	**signing time (ms)**	**verification time (ms)**
1	208	0.32584	0.45562
2	416	0.3751	0.366325
3	624	0.32147	0.43424
4	832	0.33657	0.37756
5	1040	0.31001	0.45476
6	1248	0.33021	0.300154
7	1456	0.30143	0.455526
8	1660	0.39852	0.35476
9	1868	0.33258	0.4319985
10	2076	0.35672	0.372350

Table 9. Elgamal Digital signature based on 2D Tinkerbell map for 100000 messages

	length of characters	**signing time (ms)**	**verification time (ms)**
1	208	0.39862	0.45466
2	416	0.35247	0.35524
3	624	0.333256	0.43442
4	832	0.31001	0.365547
5	1040	0.30921	0.43224
6	1248	0.330624	0.3775
7	1456	0.310026	0.45322
8	1660	0.33658	0.345470
9	1868	0.37412	0.430022
10	2076	0.39885	0.30715

Table 10. Elgamal Digital signature based on Tent Sine System for 100000 messages

	length of characters	**signing time (ms)**	**verification time (ms)**
1	208	0.33654	0.43625
2	416	0.31147	0.328459
3	624	0.300145	0.400324
4	832	0.322032	0.35542
5	1040	0.310104	0.432322
6	1248	0.396587	0.399856
7	1456	0.362410	0.402422
8	1660	0.33240	0.3756
9	1868	0.38960	0.44426
10	2076	0.3320987	0.321452

6. Conclusion

In this research, chaotic maps were coupled with Schnorr and Elgamal algorithms to enhance the security level through increasing the key space of the secret key and provide unpredictable chaotic behavior. These maps involved 2D henon, 2D tinkerbell and tent sine map. They were employed to generate a random sequence of iterations which then converted into 256-bit integers to be ready for using as the private key. The proposed algorithms were tested for different sizes of parameters and messages. The results of the experiments indicate that the proposed digital signature algorithms provide high security and quality of service. The results of the proposed algorithms stated that the key space became 2^{256} instead of 2^{160} in traditional algorithms. The signing and verification time are less than other proposed algorithms. Also, our proposed algorithms didn't need a large number of keys for signing and verification as in some previous algorithms. The results also proved that the new algorithms don't require a high level of computing complexity. So, our development increases the security level of the digital signature algorithm strengthening it towards brute force attacks without causing time or hardware problems.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

The authors first, fourth and five were responsible for methodology, software, validation, formal analysis, investigation, resources, data curation, writing original draft preparation, writing review and editing, and visualization, while the authors second and third were responsible for supervision and project administration.

References

[1] F. Piper, "An Introduction to Cryptography", *Information Systems Control Journal*, Vol. 6, No. 2003, pp.54-61,2003.

[2] A. M. Mahfouz, A. S. Ismail, H. Nasry, and W. I. Elsobky, "Path Detection for A Moving Target in Wireless Sensor Network Based on Clifford Algebra", In: *Proc. of International Telecommunications Conf (ITC-Egypt)*, pp. 1-5, 2022.

[3] F. Lalem, A. Laouid, M. Kara, M. Al-Khalidi and A. Eleyan, "A novel digital signature scheme for advanced asymmetric encryption techniques", *Journal of Applied Sciences*, Vol. 13, No. 8, pp. 5172, 2023.

[4] A. H. Lone. H, and R. Naaz, "Demystifying cryptography behind blockchains and a vision for post-quantum blockchains", In: *Proc. of IEEE International Conf for Innovation in Technology (INOCON)*, Bangluru, India, pp. 1-6, 2020.

[5] A. Qudratov, and A. Adilov, "ELECTRONIC DIGITAL SIGNATURE", *Journal of Science and Innovation*, Vol. 1, No.7, pp. 668-671,2022.

[6] E. Ferrara, "The history of digital spam", *Journal of Communications of the ACM*, Vol. 62. No. 8, pp. 82-91, 2019.

[7] M. A. Budiman. D. Rachmawati, and R. Utami, "The cryptanalysis of the Rabin public key algorithm using the Fermat factorization method", *Journal of Physics*, Vol. 1235, No. 1, pp. 012084, 2019.

[8] X. Luo, H. Wang, D. Wu, C. Chen, M. Deng, J. Huang, and X. S. Hua, "A survey on deep hashing methods", *ACM Transactions on Knowledge Discovery from Data*, Vol. 17, No. 1, pp. 1-50, 2023.

[9] B. K. Anerjee, and S. Saha, "Blockchain Signatures to Ensure Information Integrity and Non-Repudiation in the Digital Era: A comprehensive study", *International Journal of Computing and Digital Systems*, Vol. 16, No. 1, pp. 1-12,2024.

[10] W. W. Alsobky, H. Saeed, and A. N. Elwakeil, "Different Types of Attacks on Block Ciphers", *International Journal of Recent Technology and Engineering*, Vol. 9, No. 3, pp. 28-31, 2020.

[11] R. Sobti, and G. Geetha, "Cryptographic hash functions: a review", *International Journal of Computer Science Issues (IJCSI)*, Vol. 9, No. 2, pp. 461, 2012.

[12] T. Lakshmanan, and M. Madheswaran, "A novel secure hash algorithm for public key digital signature schemes", *International Arab Journal of Information and Technology*, Vol. 9, No. 3, pp. 262-267, 2012.

[13] A. T. Maolood, A. K. Farhan, W. I. El-Sobky, H. N. Zaky, H. L. Zayed, H. E. Ahmed, and T. O. Diab, "Fast Novel Efficient S-Boxes with Expanded DNA Codes", *Journal of Security and Communication Networks*, Vol. 2023, No. 5767102, pp. 19, 2023.

[14] J. R. Naif, G.H. Abdul, A. K. Farhan3 "Internet of Things Security using New Chaotic System and Lightweight AES", *Journal of AL-Qadisiyah for Computer Science and Mathematics*, Vol. 11, No. 2, pp. 2521-3504, 2019.

[15] A. Kadhim, S. Khalaf, "New Approach for Security Chatting in Real Time", *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, Vol. 4, No. 3, pp. 2278-6856, 2015.

[16] A. Kadhim, and R. M. Mohamed, "Visual cryptography for image depends on RSA & AlGamal algorithms". In: *Proc. of Al Sadeq International Conf. on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, Baghdad, Iraq, pp. 1-6, 2016.

[17] S. A. Jassim and A. K. Farhan, "A survey on stream ciphers for constrained environments". In: *Proc. of 1st Babylon International Conf. on Information Technology and Science (BICITS)*, Babil- IRAQ, pp. 228 -233, 2021.

[18] A. M. Mahfouz, A. S. Ismail, H. Nasry and W. I. Elsobky, “Path Detection for A Moving Target in Wireless Sensor Network Based on Clifford Algebra”, In: *Proc. of International Telecommunications Conf. (ITC-Egypt)*, Egypt, pp. 1-5, 2022.

[19] H. Nasry, A. Abdallah, A. Farhan, H. Ahmed & W. Alsobky, “Multi Chaotic System to Generate Novel S-Box for Image Encryption”, *Journal of Physics*, Vol. 2304, No. 1, pp. 012007, 2022.

[20] R. B. Naik and U. Singh, “A review on applications of chaotic maps in pseudo-random number generators and encryption”, *Journal of Annals of Data Science,* Vol. 11, No. 1, pp. 25-50, 2024.

[21] X. Wang and J. Zhao, “An improved key agreement protocol based on chaos”, *Journal of Communications in Nonlinear Science and Numerical Simulation,* Vol. 15, No. 12, pp. 4052-4057, 2010.

[22] Z. A. Abduljabbar et al., “Provably Secure and Fast Color Image Encryption Algorithm Based on S-Boxes and Hyperchaotic Map”, *IEEE Access,* Vol. 10, No. 2022, pp. 26257-26270, 2022.

[23] H. Saeed, H. E. Ahmed, T. O. Diab, H. L. Zayed, H. N. Zaky, and W I. Elsobky, “Evaluation of the Most Suitable Hyperchaotic Map in S-Box Design Used in Image Encryption”, *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Vol. 5, No. 4, pp. 176-182, 2022.

[24] M. T. Suryadi, Y. Satria and L. N. Prawadika, “An improvement on the chaotic behavior of the Gauss Map for cryptography purposes using the Circle Map combination”, *Journal of Physics*, Vol. 1490, No. 1, pp. 012045, 2020.

[25] C. Li, G. Luo, K. Qin and C. Li, “An image encryption scheme based on chaotic tent map”, *Journal of Nonlinear Dynamics*, Vol.87, No. 2017, pp. 127-133, 2017.

[26] S. Zhu, G. Wang and C. Zhu, “A secure and fast image encryption scheme based on double chaotic S-boxes”, *Journal of Entropy*, Vol. 21, No. 8, pp. 790, 2019.

[27] V. Gelfreich, and D. Turaev, “Arnold diffusion in a priori chaotic symplectic maps”, *Journal of Communications in Mathematical Physics*, Vol. 353, No. 2017, pp.507-547, 2017.

[28] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han and C. Su, “Blockchain-based reliable and efficient certificateless signature for IIoT devices”, *IEEE Transactions on Industrial Informatics*, Vol. 18, No. 10, pp.7059-7067, 2021.

[29] J. A. Alzubi, “Blockchain-based Lamport Merkle digital signature: authentication tool in IoT healthcare”, *Journal of Computer Communications*, Vol. 170, No. 2021, pp. 200-208, 2021.

[30] J. Na, H. Y. Kim, N. Park, and B. Seo, “Comparative Analysis of Schnorr Digital Signature and ECDSA for Efficiency using Private Ethereum Network”, *IEIE Transactions on Smart Processing & Computing*, Vol. 11, No. 3, pp. 231- 239, 2022.

[31] Y. Qin and B. Zhang, “Privacy Preserving Biometrics Image Encryption and Digital Signature Technique Using Arnold and ElGamal”, *Journal of Applied Sciences*, Vol. 13, No. 14, pp. 8117, 2023.

[32] Y. Zhou, L. Bao, C.L.P. Chen, “A new 1D chaotic system for image encryption”, *Journal of Signal Process*, Vol. 97, No. 2014, pp.172-182, 2014.

[33] P. Kuppuswamy. “A New Efficient Digital Signature Scheme Algorithm based on Block cipher”, *IOSR Journal of Computer Engineering*, Vol. 7, No. 1, pp. 47-52, 2012.

[34] N. E. El-meligy, W. I. EL-SOBKY, A. S. MOHRA, A. Y. HASSAN, and T. O. DIAB, “NEW HIDING TECHNIQUE IN DIGITA SIGNATURE BASED ON ZIGZAG TRANSFORM AND CHAOTIC MAPS”, *Journal of Jilin University (Engineering and Technology Edition)*, Vol. 42, No. 9, pp. 1671-5497, 2023.

[35] M. Padmaa, and D. Y. Venkataramani, “ZIG-ZAG PVD—A nontraditional approach”, *International Journal of Computer Applications*, Vol. 5, No. 6, pp. 5-10, 2010.

[36] M. H. Mohamed, W. I. El-Sobky, and S. Hamdy, “Elliptic Curve Digital Signature Algorithm Challenges and Development Stages”, *International journal of Innovative Technology and Exploring Engineering*, Vol. 10, No. 10, pp. 121-128, 2021.

[37] R. Matthews, “On the derivation of a chaotic encryption algorithm”, *Journal of Cryptologia*, Vol.13, No.1, pp.29-41, 1989.

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

[39] A. Dalia S., N. A. Alwan, and NMG Al-Saidi. “Image encryption based on highly sensitive chaotic system”, *AIP Conference Proceedings*, Vol. 2183. No. 1. AIP Publishing, 2019.

[40] N. Hayder, et al. “Image encryption based on local fractional derivative complex logistic map”, *Symmetry*, Vol. 14, No. 9, p. 1874, 2022.

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

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

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

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

[45] S. B. Sadkhan, Al Maliky, *Multidisciplinary perspectives in cryptology and information security*, IGI Global, 2014.

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

[47] N. M. G. Al-Saidi, and M. Rushdan, Md Said. “Improved digital signature protocol using iterated function systems.” *International Journal of Computer Mathematics 88.17 (2011): 3613-3625*.

[48] F. Pon, H. Lu, and B. Jeng, “Meta-He digital signature schemes based on factoring and discrete logarithms”, *Journal of Applied Mathematics and Computation*, Vol. 165, No. 1, pp. 171- 176, 2005.

[49] N. M. G. AL-Saidi, M. RM Said, and A. M. Ahmed. “Efficiency analysis for public key systems based on fractal functions”, *Journal of Computer Science*, Vol. 7, No. 4, p. 526, 2011.

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

[51] N. Lee, and T. Hwang, “Modified Harn signature Scheme based on factoring and discrete logarithms”, *IEE Proceeding of Computers Digital Techniques*, Vol. 143, No. 3, pp. 196-198, 1996.

[52] J. Li, and G. Xiao, “Remarks on new signature scheme based on two hard problems”, *Journal of Electronics Letters*, Vol. 34, No. 25, pp. 2401-2402, 1998.

[53] Z. Shao, “Digital signature schemes based on factoring and discrete logarithms”, *Journal of Electronics Letters*, Vol. 38, No. 24, pp. 1518-1519, 2002.

[54] H. He, “Digital signature schemes based on factoring and discrete logarithms”, *Journal of Electronics Letters*, Vol. 37, No. 4, pp. 220-222, 2001.

[55] G. S. G. N. Anjaneyulu, “A Modified Wei-Hua-He Digital Signature Scheme Based on Factoring and Discrete Logarithm”, *Journal of Symmetry*, Vol. 14, No. 11, p. 2443, 2022.

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

[57] C. Wang, H. Lin, and C. Chang, “Signature scheme based on two hard problems simultaneously”, In: *Proc. of the 17th International Conf. on Advanced Information Networking and Application (AINA)*, Xian, China, pp. 557- 560, 2003.

[58] E. Ismail, N. That, and R. Ahmad, “A New Digital Signature Scheme Based on Factoring and Discrete Logarithms”, *Journal of Mathematics and Statistics*, Vol. 4, No. 4, pp. 222-225, 2008.

[59] K. Chain, and C. Kuo, “A new digital signature scheme based on chaotic maps”, *Journal of Nonlinear Dynamics*, Vol. 24, No. 4, pp. 1003-1012, 2013.

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

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

[62] H. Cui, R. H. Deng, J. K. Liu, X. Yi, and Y. Li, “Server-Aided attribute-based signature with revocation for resource-constrained Industrial-Internet-of-Things devices”, *IEEE Transactions on Industrial Informatics*, Vol. 14, No. 8, pp. 3724-3732, 2018.

[63] M. R. K. Ariffin, *et al*. “A new direction in utilization of chaotic fractal functions for cryptosystems”, *Applications of Chaos and Nonlinear Dynamics in Science and Engineering*, Vol. 2 pp. 233-248, 2012.

[64] L. Shen, J. Ma, X. Liu, F. Wei, and M. Miao, “A secure and efficient ID-Based aggregate signature scheme for wireless sensor networks”, *IEEE Internet Things Journal*, Vol. 4, No. 2, pp. 546-554, 2017.

[65] M. A. Mughal, X. Luo, A. Ullah, S. Ullah, and Z. Mahmood, “A lightweight digital signature-based security scheme for human-centered Internet of Things”, *IEEE Access*, Vol. 6, No. 2018, pp. 31630-31643, 2018.

[66] G. K. Verma, B. B. Singh, N. Kumar, M. S. Obaidat, D. He, and H. Singh, “An efficient and provable certificate-based proxy signature scheme for IIoT environment”, *Information Sciences*, Vol. 518, No. 2020, pp. 142-156, 2020.

[67] J. H. Seo, “Efficient digital signatures from RSA without random oracles”, *Information Sciences*, Vol. 512, pp. 471-480, 2020.

[68] C. Meshram, M. S. Obaidat., J. V. Tembhurne, S. W. Shende, K. W. Kalare, and S. G. Meshram, “A lightweight provably secure digital short-signature technique using extended chaotic maps for human-centered IoT systems”, *IEEE Systems Journal*, Vol. 15, No. 4, pp. 5507-5515, 2020.