International Journal of Analysis and Applications

A Quantum-Corrected Chaotic System for Strengthening Schnorr and Elgamal Signatures to Optimize Key Generation and Performance

Hadeel Moutaz Al-dabbas[1], Ahmed M. Ajaj[1], Nadia M. G. Al-Saidi[2,*], Nawres A. Alwan[2,3], Wageda I. El Sobky[4]

[1]*Department of Islamic Banking and Finance, College of Islamic Sciences, Aliraqia University, Baghdad, Iraq*

[2]*Department of Applied Sciences, University of Technology, Baghdad, 10066 Iraq*

[3]*Department of Computer Systems & Technology, Faculty of Computer Science and Information Technology, Universiti of Malaya, Malaysia*

[4]*Basic Engineering Sciences Department, Benha Faculty of Engineering, Benha University, Banha 13511, Egypt*

**Corresponding author:* Nadia.M.Ghanim@uotechnology.edu.iq

ABSTRACT: This paper aims to improve the performance of Schnorr and Elgamal schemes using the random property of the chaotic maps. After analyzing different chaotic map types, this paper generates a new 1D chaotic system based on sin and logistic maps. After that, we derived a new map with quantum corrections by coupling a kicked quantum system with a harmonic oscillator bath. As the dissipation parameter increases, we observe a period-doubling progression towards classical behavior, along with other intriguing characteristics at intermediate parameter values. Then, this new chaotic system is applied to the Schnorr and Elgamal schemes. Extensive randomness tests were conducted, and the algorithm demonstrated exceptional performance. Following rigorous testing and analysis, the algorithm exhibited impressive signing and verification times of approximately 0.0000799212 (s) and 0.0000100223 (s) for the Schnorr scheme,

Received Oct. 24, 2024

2020 Mathematics Subject Classification. 94A60.

Key words and phrases. chaotic maps; Schnorr digital signature; Elgamal digital signature; quantum system.

https://doi.org/10.28924/2291-8639-23-2025-65

ISSN: 2291-8639

and 0.000029932 (s) and 0.0000399298 (s) for the Elgamal scheme, respectively. These times are notably lower compared to other proposed algorithms. The private key space was expanded to 2^{256} from 2^{160}, further strengthening security. Testing with 100,000 messages of varying lengths confirmed the algorithm's robust performance, making it a viable option for contemporary cryptosystems used in multimedia data exchange.

1. Introduction

A message, software, or digital document can have integrity and authenticity through the use of a mathematical technique called a "digital signature [1]. It gives much more intrinsic security than a paper document or stamped sign, yet it is the digital version of it. Additionally, it aims to address the issue of online communication hacking and impersonation. It can offer proof of the ownership, identity, and status of digital messages, transactions, or documents [2]. They can also be used by signers to confirm informed consent. They are regarded as legally enforceable in many nations, including the United States, in exactly the same manner that conventional handwritten paper signatures are [3]. A single-direction hash of the online data to be confirmed is provided by signing technology, such as an email program, to establish a digital signature [4]. The message and sender's identity are known to the recipient. If both values of hashes differ, either the data has been manipulated or the signature was produced with a secret key that does not match the public key that the signer has provided (an issue with authentication) [5]. Any message, encrypted or not, can employ a digital signature as long as the recipient has assurance of the sender's identity and that the message was transmitted intact [6]. Because the digital signature is distinctive to the document and the signer and links them together, the signer cannot claim not to have signed something. This quality is known as non-repudiation. To strengthen document integrity and streamline procedures, industries adopt digital signature technology. Government, healthcare, manufacturing, financial services, smart contracts, and cryptocurrency are some of these sectors [7].

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 to generate digital signatures that were very safe and well-executed.

chaotic structures have been extensively utilized in recent years to create reliable cryptographic techniques [8-10]. These structures have demonstrated their capacity to erect extremely strong defences 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. 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 schemes were created based on two challenging difficulties to increase the security of signature techniques, which are FAC as well as DLP [11-16]. Some writers have, nevertheless, also demonstrated the flaws in these methods [17-20]. In addition, there exist numerous signature techniques that rely on two problems [21-24], 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 [25]. An innovative key agreement procedure employing chaotic maps has been proposed in several ways [26- 34] 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. [35]. A secure and effective signature system built around chaotic maps and factorization difficulties was recently devised by Chain and Kuo [7]. 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 a new chaotic map with El-Gamal and Schnorr's digital signature to improve the security against any attacks. The rest of this paper is organized as

follows: In section 2, chaotic maps are explained in general, and the new one is described particularly. Also, Schnorr and Elgamal schemes are introduced. The proposed algorithm is explained in the same section. Finally, the results of the proposed algorithms and the comparison between them and the traditional ones are illustrated in section 3.

2. Materials and Methods

2.1. Chaotic maps

A chaotic map refers to a growth function that demonstrates some form of mathematical irregularity [36]. The mathematics associated with the chaos hypothesis has largely been developed through the continuous replication of simple mathematical formulas. Chaotic maps have been continuously expanding and have found applications in various fields including robotics, biology, economics, and cryptography [37]. Extensive research has focused on two types of chaotic systems: one-dimensional (1D) and high-dimensional (HD) chaos. The construction of cryptosystems benefits from the unique characteristics of chaotic structures, such as determinacy, ergodicity, and sensitivity to initial conditions, which are analogous to the confusion and diffusion aspects of a reliable cryptosystem [38]. Therefore, there is a need to develop new chaotic systems that exhibit improved chaotic performance. To achieve this, first, a new 1D chaotic system based on sin and logistic maps is developed. Then, a new map with quantum corrections by coupling a kicked quantum system with a harmonic oscillator bath is derived with superior properties such as time evolution, bifurcation diagram, and Lyapunov exponent [39].

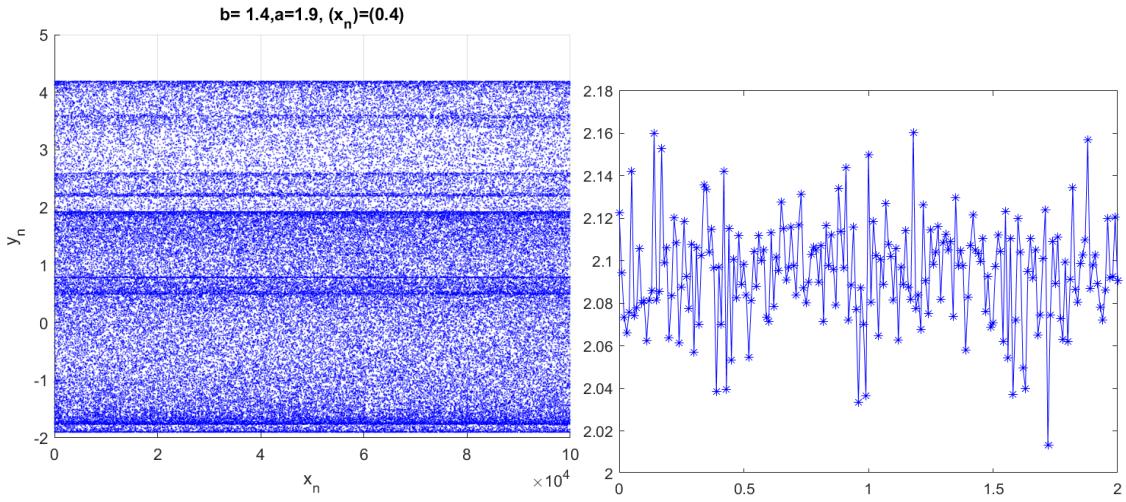
2.1.1. The proposed 1D chaotic system

The logistic and sine maps can be used as seed maps to construct a new chaotic system [40]. Our new chaotic system is defined as

$$x_{n+1} = a\, sin\big(2\, x_n(1 - x_n)\big) + 2a\, e^{-bx_n^2} \tag{1}$$

where x_n is the initial state, a and b are parameters.

The new map behaves chaotically when $x_n \in [0, 10]$, $a = 1.9$ and $b = 1.4$ and its chaotic sequences are distributed uniformly as shown in Figure 1.



(a) (b)

Figure 1. Dynamical behavior of the new map: (a) bifurcation plot; (b) Lyapunov exponent.

2.1.2. Quantum chaotic system

We have used the same approach given in [41] to derive equations of motion for a kicked quantum system coupled to a bath of oscillators, introduce a quasi-continuum model to describe the dissipation from the bath, and then take an expectation value and study the resulting expectation-value map. To investigate this approach first, we have to show that system (1) is dissipative.

To determine whether (1) is dissipative or not, we must examine if the map reduces the volume of phase space over time. First, we need to find the derivative of x_{n+1} with respect to x_n.

Thus, the derivative of (1) is given as:

$$f'(x) = acos\,(2x(1-x)) \cdot (2-4x) - 4abxe^{-bx^2} \tag{2}$$

If $|f'(x)| < 1$ that means map (1) is dissipative because it contracts the phase space.

If $|f'(x)| > 1$ that means map (1) is not dissipative.

From (2) we must choose the values of x, a and b such that to make $f'(x) < 1$, that is led (1) is dissipative. For example, if $x = 0.8, a = 2.3$ and $b = 1.4$. then $f'(x) < 1$. That is mean (1) is dissipative.

To adapt the classical chaotic map into a quantum map based on the approach in [41] we will proceed step by step, beginning with defining the boson annihilation and creation operators $\hat{a}$ and $\hat{a}^{\dagger}$, respectively, which represent the main system of interest with a characteristic frequency ω_0. The boson operators obey the usual equal-time commutation relations: $[\hat{a}, \hat{a}^{\dagger}] = 1, [\hat{b}_{k_1}, \hat{b}_{k_2}^{+}] =$

$\delta_{k_1 k_2}, [\hat{b}_k, \hat{a}] = 0$, etc. Also, the bath of oscillators described by the operators $\hat{b}_k$ and $\hat{b}_k^\dagger$ for each mode k, which interacts with the main system. The coupling constant is denoted by C.

To investigate the impact of quantum correlations, express $\hat{a}$ as $\langle \hat{a} \rangle + \delta \hat{a}$, where $\delta \hat{a}$ signifies a quantum fluctuation around $\langle \hat{a} \rangle$ and has the property $\langle \delta \hat{a} \rangle = 0$. This approach allows us to examine the effects of correlations like $\langle \delta \hat{a} \delta \hat{a} \rangle, \langle \delta \hat{a}^\dagger \delta \hat{a} \rangle$, etc., as the coupling to the bath changes. The Hamiltonian system is defined as;

$$\hat{H} = \hat{H}_{bath} + \hat{H}_{inter} + (\text{Time-dependent Perturbation}) \tag{3}$$

where

$$\hat{H}_{bath} = \hbar \sum_k (\omega_k - \omega_0) \hat{b}_k^\dagger \hat{b}_k \tag{4}$$

is called Bath Oscillators, and

$$\hat{H}_{inter} = \hbar C \sum_k \left(\hat{a}^\dagger \hat{b}_k + \hat{b}_k^\dagger \hat{a} \right) \tag{5}$$

is called interaction term

and time-dependent perturbation is

$$\hbar V(\hat{a}, \hat{a}^\dagger) \sum_n \delta(t - nT) \tag{6}$$

Where $\sum_n \delta(t - nT)$ is discrete-time impulses which represent a series of impulses occurring at regular intervals T.

Where $\hbar$ is plank constant, and $V(\hat{a}, \hat{a}^\dagger)$ is a mimic of the nonlinear function of (1) and T represents the period of the kicks.

Then Eq. (3) will be:

$$\hat{H} = \hbar \sum_k (\omega_k - \omega_0) \hat{b}_k^\dagger \hat{b}_k + \hbar C \sum_k \left(\hat{a}^\dagger \hat{b}_k + \hat{b}_k^\dagger \hat{a} \right) + \hbar V(\hat{a}, \hat{a}^\dagger) \sum_n \delta(t - nT) \tag{7}$$

The non-linear function in (1) needs to be translated into a quantum operator that can be added as a time-dependent perturbation to the Hamiltonian.

Therefore, from (1) we have:

$$a \sin(2x(1 - x)) + 2ae^{-bx^2} \tag{8}$$

we can represent x quantum-mechanically as a function of $\hat{a}$ and $\hat{a}^\dagger$. And we chose to set $x \approx (\hat{a} + \hat{a}^\dagger)$, which represents the position operator in the quantum harmonic oscillator. From the Taylor series we have

$$\sin(\hat{O}) \approx \hat{O} - \frac{\hat{O}^3}{6} + \cdots \tag{9}$$

For the sin part of (1), we get:

$$\sin\left(2(\hat{a} + \hat{a}^\dagger)\left(1 - (\hat{a} + \hat{a}^\dagger)\right)\right) \approx 2(\hat{a} + \hat{a}^\dagger)\left(1 - (\hat{a} + \hat{a}^\dagger)\right) \tag{10}$$

and the exponential part will get; $e^{-b(\hat{a}+\hat{a}^\dagger)^2}$

Then quantum perturbation of non-linear function will be:

$$V(\hat{a},\hat{a}^\dagger) = a\left[2(\hat{a}+\hat{a}^\dagger)\left(1-(\hat{a}+\hat{a}^\dagger)\right)+2e^{-b(\hat{a}+\hat{a}^\dagger)^2}\right] \tag{11}$$

Then Eq. (7) becomes:

$$\hat{H} = \hat{H}_{bath}+\hat{H}_{int}+\hbar a\left[2(\hat{a}+\hat{a}^\dagger)\left(1-(\hat{a}+\hat{a}^\dagger)\right)+2e^{-b(\hat{a}+\hat{a}^\dagger)^2}\right]\sum_n \delta(t-nT) \tag{12}$$

Now the Heisenberg equations of equations of motion, the time evolution of an operator $\hat{O}(t)$ is

$$\dot{\hat{O}}(t) = \frac{i}{\hbar}[\hat{H},\hat{O}(t)]+\frac{\partial\hat{O}}{\partial t} \tag{13}$$

where $[\hat{H},\hat{O}]$ is the commutator of the Hamiltonian $\hat{H}$.

From Eq. (7) derivation each part for $\hat{a}(t)$

$$\frac{i}{\hbar}\left[\hat{H}_{int},\hat{a}(t)\right] = \frac{i}{\hbar}\left[\hbar C\sum_k\ (\hat{a}^\dagger\hat{b}_k+\hat{b}_k^\dagger\hat{a}),\hat{a}(t)\right] \tag{14}$$

Using the commutation relations $\left[\hat{a},\hat{a}^\dagger\right]=1$ and $\left[\hat{a},\hat{b}_k\right]=0$, this simplifies to:

$$-iC\sum_k\ \hat{b}_k(t) \tag{15}$$

Time-dependent Non-linear function $\hat{H}_{nl}(t)$ we have:

$$\begin{aligned}\frac{i}{\hbar}\left[\hat{H}_{nl}(t),\hat{a}(t)\right] &= \frac{i}{\hbar}\left[\hbar V(\hat{a},\hat{a}^\dagger)\sum_n\ \delta(t-nT),\hat{a}(t)\right]\\ &= i\left[\hat{a}(t),V(\hat{a},\hat{a}^\dagger)\right]\sum_n\ \delta(t-nT)\end{aligned} \tag{16}$$

Then we have the time evolution of $\hat{a}(t)$ based on the Heisenberg equation is

$$\dot{\hat{a}}(t) = -iC\sum_k\ \hat{b}_k(t)-i\left[\hat{a},V(\hat{a},\hat{a}^\dagger)\right]\sum_n\ \delta(t-nT) \tag{17}$$

This equation captures the dynamics of $\hat{a}(t)$ due to both its interaction with the bath oscillators and the non-linear, time-dependent perturbation applied at discrete times $t=nT$.

The Heisenberg equation of motion for an operator $\hat{O}$ is given by the commutator relation:

$$\dot{\hat{O}}(t) = \frac{i}{\hbar}[\hat{H},\hat{O}] \tag{18}$$

Then we apply the Heisenberg Equation to $\hat{b}_k(t)$ on Eq. (4) we have:

$$\left[\hat{H}_{\text{bath}},\hat{b}_k\right] = \left[\hbar\sum_j\ \Delta_j\hat{b}_j^\dagger\hat{b}_j,\hat{b}_k\right] = \hbar\sum_j\ \Delta_j\left[\hat{b}_j^\dagger\hat{b}_j,\hat{b}_k\right] \tag{19}$$

Using the commutation relation $\left[\hat{b}_j,\hat{b}_k^\dagger\right]=\delta_{jk}$:

$$\left[\hat{b}_j^\dagger\hat{b}_j,\hat{b}_k\right] = \hat{b}_j^\dagger\left[\hat{b}_j,\hat{b}_k\right]+\left[\hat{b}_j^\dagger,\hat{b}_k\right]\hat{b}_j = -\delta_{jk}\hat{b}_j \tag{20}$$

Therefore,

$$\left[\hat{H}_{\text{bath}},\hat{b}_k\right] = -\hbar\Delta_k\hat{b}_k \tag{21}$$

Also, apply to Eq. (5) we have:

$$\begin{aligned}[\hat{H}_{\text{int}}, \hat{b}_k] &= [\hbar C \sum_j \ (\hat{a}^\dagger \hat{b}_j + \hat{b}_j^\dagger \hat{a}), \hat{b}_k] \\ &= \hbar C \sum_j \ (\hat{a}^\dagger [\hat{b}_j, \hat{b}_k] + [\hat{b}_j^\dagger, \hat{b}_k]\hat{a}) = -\hbar C \hat{a} \delta_{jk}\end{aligned} \tag{22}$$

Then

$$[\hat{H}_{\text{int}}, \hat{b}_k] = -\hbar C \hat{a} \tag{23}$$

Then combining Eq. (21) and Eq. (23), we have a differential equation:

$$\dot{\hat{b}}_k(t) = \frac{i}{\hbar}\left(-\hbar \Delta_k \hat{b}_k - \hbar C \hat{a}\right) = -i\Delta_k \hat{b}_k(t) - iC\hat{a}(t) \tag{24}$$

To solve this equation the homogeneous term, we have

$$\hat{b}_k(t) = \hat{b}_k(0) e^{-i\Delta_k t} - iC \int_0^t e^{-i\Delta_k (t-t')} \hat{a}(t') dt' \tag{25}$$

Now, by substitution Eq. (24) into Eq. (17), we get:

$$\dot{\hat{a}}(t) = -iC \sum_k \left(\hat{b}_k(0) e^{-i\Delta_k t} - iC \int_0^t e^{-i\Delta_k (t-t')} \hat{a}(t') dt' \right) - i\left[\hat{a}, V\left(\hat{a}, \hat{a}^\dagger\right)\right] \sum_n \delta(t - nT) \tag{26}$$

$$\dot{\hat{a}}(t) = -iC \sum_k \hat{b}_k(0) e^{-i\Delta_k t} + C^2 \sum_k \int_0^t e^{-i\Delta_k (t-t')} \hat{a}(t') dt' - i\left[\hat{a}, V\left(\hat{a}, \hat{a}^\dagger\right)\right] \sum_n \delta(t - nT) \tag{27}$$

By introducing a quasi-continuum model with $\Delta_k = k\Delta$, $k = 0, \pm 1, \pm 2, \ldots$, such that $2\pi C^2/\Delta \to 2\Gamma$ as $\Delta, C \to 0$, the second term on the right-hand side of (9) becomes $-\Gamma \hat{a}(t)$ and we are left with

$$\dot{\hat{a}}(t) = -iC \sum_k \ \hat{b}_k(0) \exp\left(-i\Delta_k t\right) - \Gamma \hat{a}(t) + f\left(\hat{a}, \hat{a}^\dagger\right) \sum_n \ \delta(t - nT) \tag{28}$$

where

$$f\left(\hat{a}, \hat{a}^\dagger\right) = -i\left[\hat{a}, V\left(\hat{a}, \hat{a}^\dagger\right)\right] = -i\left[\hat{a}, a\left(2\left(\hat{a} + \hat{a}^\dagger\right)\left(1 - \left(\hat{a} + \hat{a}^\dagger\right)\right) + 2e^{-b\left(\hat{a} + \hat{a}^\dagger\right)^2}\right)\right] \tag{29}$$

The quasi-continuum model provides a coherent explanation of dissipation. Specifically, the quantum Langevin noise term, represented by the first term on the right-hand side of equation (28), aligns with the dissipative nature of the second term. This alignment is essentially an illustration of the general fluctuation-dissipation theorem.

The quantum map describes the evolution of an operator $\hat{a}$ over discrete time intervals, incorporating both dissipation and non-linear dynamics. The approach used here involves integrating the differential equations governing $\hat{a}(t)$ over discrete steps from $t = nT - \epsilon$ to $t = (n+1)T - \epsilon$, a typical method for dealing with systems that include periodic or driven terms. Where the operator equation is

$$\hat{a}_{n+1} = \hat{a}_n e^{-\beta} + \hat{G}_n + f\left(\hat{a}_n, \hat{a}_n^\dagger\right) e^{-\beta} \tag{30}$$

Where the noise term $\left(\hat{G}_n\right)$ is

$$\hat{G}_n = -iC \sum_k \ \hat{b}_k(0) e^{-i\Delta_k (n+1)T} \left[\frac{1 - e^{i\Delta_k T - \beta}}{\Gamma - i\Delta_k}\right] \tag{31}$$

where $e^{-\beta}$ is a dissipation factor and $\beta = \Gamma T$ is represents the exponential decay over one period due to the dissipative interaction with the environment, quantified by Γ. The noise term $(\hat{G}_n)$ includes contributions from the bath oscillators, accounting for their state at the beginning and their evolution, modulated by the decay and the inherent frequencies of the oscillators (Δ_k).

now we will take the expectation value of Eq. (30), assuming $\langle \hat{b}_k(0) \rangle = 0$ for all k, resulting in

$$\langle \hat{a}_{n+1} \rangle = \left[\langle \hat{a}_n \rangle + \langle f(\hat{a}_n, \hat{a}_n^\dagger) \rangle \right] e^{-\beta} \tag{32}$$

Because we want to compare our quantum results to Eq. (1), we choose the "force".

$$f(\hat{a}_n, \hat{a}_n^\dagger) = -i \left[\hat{a}, a \left(2(\hat{a} + \hat{a}^\dagger) \left(1 - (\hat{a} + \hat{a}^\dagger) \right) + 2e^{-b(\hat{a}+\hat{a}^\dagger)^2} \right) \right] \tag{33}$$

Then Eq. (32) becomes:

$$\langle \hat{a}_{n+1} \rangle = \left[\langle \hat{a}_n \rangle + \langle a \left[2\hat{a}_n(1 - \hat{a}_n) + 2e^{-b\hat{a}_n \hat{t}_n} \right] \rangle \right] e^{-\beta} \tag{34}$$

The quantum operator $\hat{a}$ is decomposed into its expectation value and a fluctuation term:

$$\hat{a} = \langle \hat{a} \rangle + \delta\hat{a} \tag{35}$$

This decomposition helps in analyzing the dynamics by separating the mean behavior from quantum fluctuations.

now substitute and expand into our model we have

$$\hat{a}_{n+1} \approx [\langle \hat{a}_n \rangle + \delta\hat{a}_n] + a \left[2(\langle \hat{a}_n \rangle + \delta\hat{a}_n)\left(1 - (\langle \hat{a}_n \rangle + \delta\hat{a}_n)\right) + 2e^{-b\left(\left\langle \hat{a}_n^\dagger \right\rangle \langle \hat{a}_n \rangle + \left\langle \delta\hat{a}_n^\dagger \delta\hat{a}_n \right\rangle\right)} \right] e^{-\beta} \tag{36}$$

The expectation value then simplifies to be

$$\langle \hat{a}_{n+1} \rangle \approx \left[\langle \hat{a}_n \rangle + a \left(2\langle \hat{a}_n \rangle (1 - \langle \hat{a}_n \rangle) + 2e^{-b\left\langle \hat{a}_n^\dagger \hat{a}_n \right\rangle} \right) - a \left\langle \delta\hat{a}_n^\dagger \delta\hat{a}_n \right\rangle \right] e^{-\beta} \tag{37}$$

where $\langle \delta\hat{a}_n^\dagger \delta\hat{a}_n \rangle$ represent the effects of quantum fluctuations on the dynamics.

We can derive an equation for $\langle \delta\hat{a}_n^\dagger \delta\hat{a}_n \rangle$ from the Heisenberg equation of motion for $\delta\hat{a}$. This gives us an equation in which third-order quantum corrections appear. First definitions of variables $x_n = \langle \hat{a}_n \rangle$ represents the mean-field or expectation value of the annihilation operator, $y_n = \langle \delta\hat{a}_n^\dagger \delta\hat{a}_n \rangle$ represents the quantum variance or the second moment of the fluctuations, quantifying the intensity of quantum noise, and z_n could represent correlations like $\langle \delta\hat{a}_n \delta\hat{a}_n \rangle$, capturing the symmetric fluctuations or additional higher-order terms.

Then we have (x_n) :

$$x_{n+1} = \left[x_n + a\left(2x_n(1 - x_n) + 2e^{-b(x_n^* x_n + y_n)}\right) \right] e^{-\beta} \tag{38}$$

Fluctuation dynamics (y_n):

$$y_{n+1} = \left(1 - 2a(2x_n - 1)e^{-\beta} - ae^{-\beta} 2by_n\right) y_n e^{-2\beta} \tag{39}$$

Higher-Order Correlations (z_n)

$$z_{n+1} = e^{-2\beta}\left(z_n - r(2(1-x_n)z_n - 2x_n y_n)\right) \tag{40}$$

Then from Eq. (11), we have the final state of our quantum chaotic system is:

$$\begin{aligned} x_{n+1} &= \left[x_n + a\left(\sin\left(2(x_n + x_n^*)\left(1 - (x_n + x_n^*)\right)\right) + 2e^{-b(x_n^* x_n + y_n)}\right)\right] e^{-\beta} \\ y_{n+1} &= \left(1 - 2a(2x_n - 1)e^{-\beta} - ae^{-\beta} 2by_n\right) y_n e^{-2\beta} \\ z_{n+1} &= e^{-2\beta}\left(z_n - r(2(1-x_n)z_n - 2x_n y_n)\right) \end{aligned} \tag{41}$$

where r could be related to additional non-linear parameters influencing higher-order terms.

2.1.3. Dynamic quantum chaotic system analysis

Plotting spectrum bifurcation diagrams allows for the examination of the chaotic feature. The association between chaotic phases and the relevant control parameters is depicted in these graphs. The parameter that is most important in determining if the chaotic map is beneficial in encryption is the Lyapunov exponent. Once beginning conditions and control parameters, or any other seed parameter, are slightly altered, this exponent exhibits remarkable sensitivity. We can ascertain from the correlation coefficient whether the system performs completely chaotically or if there is any correlation at all with the original parameters. The system is totally predictable when the correlation coefficient is near unity. Perfect chaos is guaranteed once the correlation coefficient is around 0 [42].

- Phase Attractor

An efficient chaotic system is indicated by a complex attractor in phase space. The sensitivity of the chaotic system to beginning conditions and parameter changes is demonstrated by these visualizations, which also depict the interplay and feedback mechanisms among the variables. Through the analysis of the figures, we can see how every pair of variables functions within the broader system, providing insights into the erratic and aperiodic patterns that define the evolution of the system. The thorough examination of these phase space plots advances our knowledge of the dynamic mechanisms governing the chaotic behavior and yields priceless data for both theoretical and real-world applications in a variety of domains [43].

Figure 2 shows the attractor of system equations (41), where the initial state (x, y, z)=$(0.4, 0.1, 0.1)$ and parameters are $a = 2.3, b = 1.4, \beta = 1.001$ and $r = 0.4$;

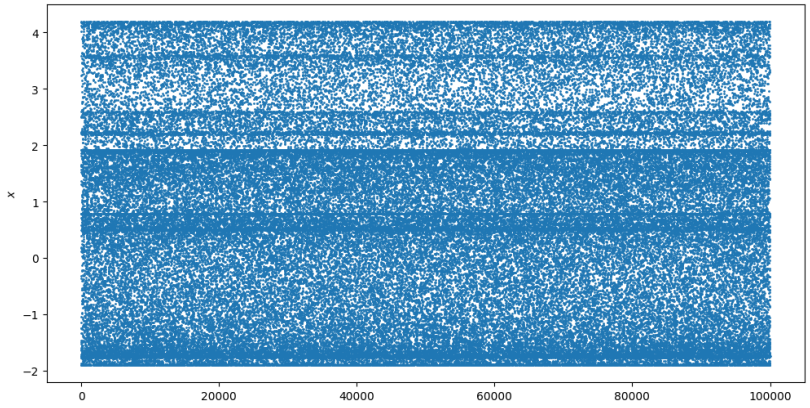


Figure 2. Phase attractor of the quantum system in (41).

- **Lyapunov Exponent (LE)**

An essential metric for illustrating the chaotic behavior of a nonlinear dynamical system is the Lyapunov Exponent (LE). It is a technique used to demonstrate how the routes created by two slightly different initial values diverge exponentially with increasing time when they are added to the same chaotic system. The Lyapunov exponent refers to the separation pace of infinitesimally close trajectories [43]. Mathematically, it is defined as

$$LE_i = \lim_{n\to\infty} \log_2 \frac{Pi(t)}{Pi(0)}$$

where $Pi(t)$ denotes the respective ellipsoidal length principal axis.

An n-D system has n number of LE. The existence of a positive exponent shows the presence of chaotic behavior on the map.

Figure 3 shows the LE of the system (41), where the initial state is (x, y, z)=$(0.4, 0.1, 0.1)$ and parameters are $a = 2.3, b = 1.4$, $\beta = 1.001$ and r control parameter change value between $[0.1 - 4]$.

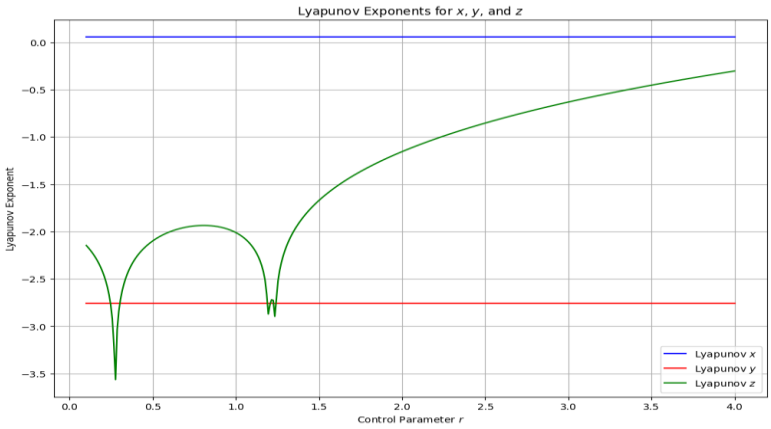


Figure 3. LE of the system (41) varies with the control parameter r.

Figure 4 shows the LE of the system (41), where the initial state is (x, y, z)=(0.4, 0.1,0.1) and parameters are $b = 1.4$, $r = 0.4$ and $\beta = 0.6$ and a is a control parameter $[0.1 - 4]$.

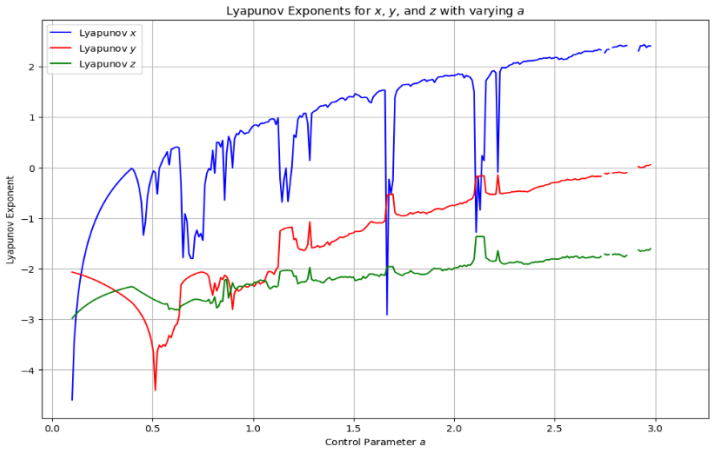


Figure 4. LE of the system (41) varies with the control parameter a

- **Bifurcation diagram**

The bifurcation diagram can be used to show how the characteristics of the chaotic system and the control settings are related. It illustrates how the performance of the system varies with different parameters and displays a sudden shift in performance when critical parameters are reached. For evaluation of dynamic systems in many disciplines, such as physics, engineering, biology, and economics, bifurcations are crucial [43].

Figure 5 shows the Bifurcation diagram of the system (41) where the initial state is (x, y, z)=(0.4, 0.1,0.1) and parameters are $b = 1.4$, $\beta = 1.001$, $r = 0.4$; and a is a control parameter $[0.1 - 4]$.

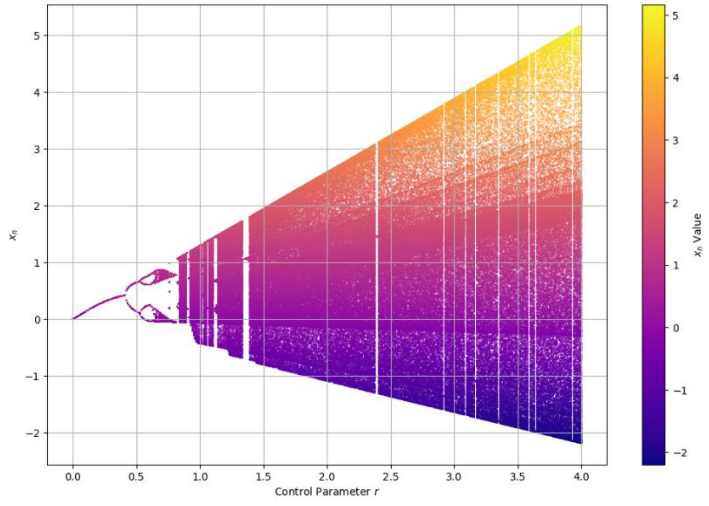


Figure 5. Bifurcation diagram of the system (41).

Relationships between $x\ vs\ y$, $x\ vs\ y$ and $y\ vs\ z$ are shown in Figure 6.

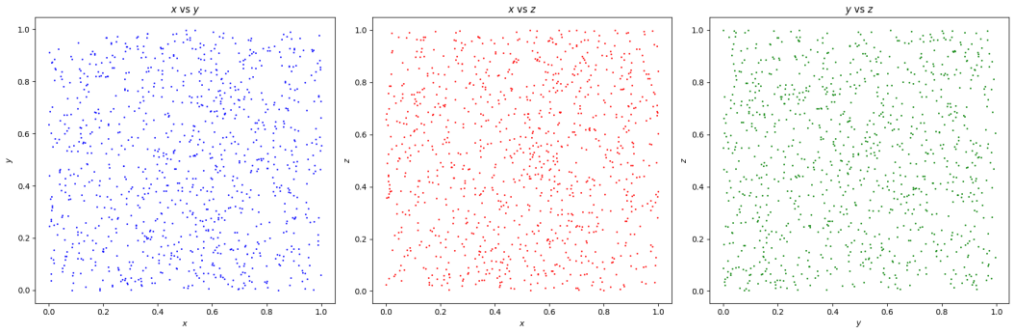


Figure 6. Relationship between x vs y, x vs y and y vs z.

Phase Space Plots for $x, y,$ and z of the system (41) are shown in Figure 7.

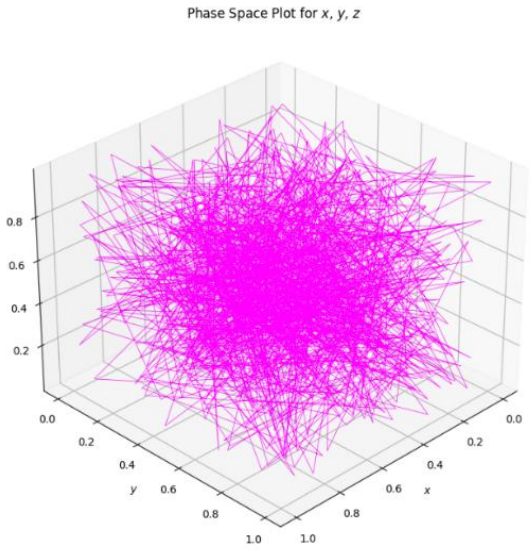


Figure. 7 Phase Space Plots for $x, y,$ and z of system (40).

Phase space between $x\ vs\ y$, $x\ vs\ y$ and $y\ vs\ z$ of system (41) is shown in Figure8.

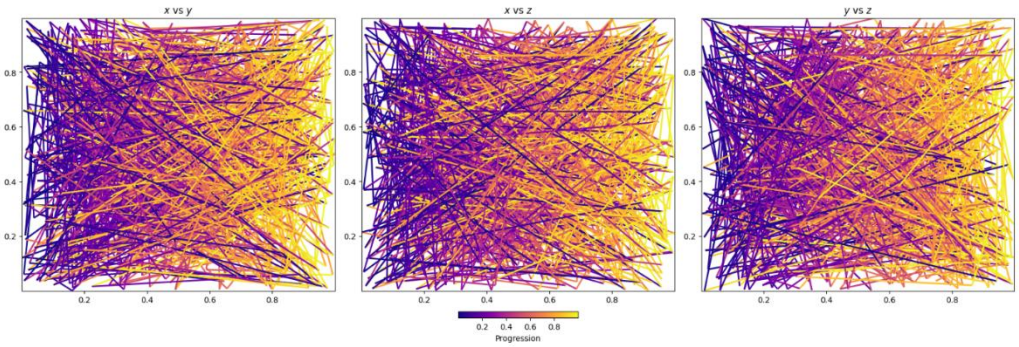


Figure 8. Phase space between $x\ vs\ y$, $x\ vs\ y$ and $y\ vs\ z$ of system (40).

Autocorrelation of x is shown in Figure 9.

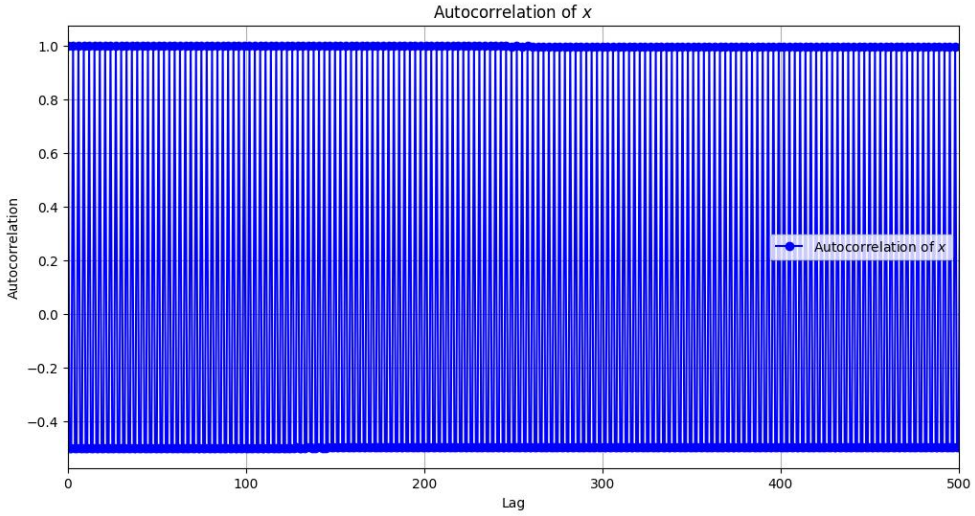


Figure 9. Autocorrelation of x.

2.2. Digital Signatures

There is a wide range of digital signature algorithms available. Some notable algorithms, such as Elgamal and Schnorr, have proven to be highly effective and suitable for specific applications like smart contracts. These algorithms offer robust security measures and yield favorable outcomes [44].

2.2.1. Schnorr digital signature algorithm

Claus Schnorr articulated this concept using his own language. This digital signature method is considered one of the oldest and is known for its simplicity. The security of this method relies on the complexity of specific discrete logarithm problems. It offers concise and efficient signatures. [45].

1. Choosing parameters:

It is widely believed that the discrete logarithm problem is difficult within the group of generators, G, of prime order, q, where each participant in the signature scheme agrees on a generator, g. Typically, Schnorr signatures are assigned to this group. All parties agree to use the encoded hash function $H:\{0,1\}^* \to \mathbb{Z}_q$, where $\mathbb{Z}_q$represents the set of integers ranging from 0 to $q-1$.

2. generation of Key:

From $\mathbb{Z}_q$, a secret signing key, u, is chosen. The public key for verification is defined as $t = g^u \, mod \, q$.

3. Signing:

To display a sign with a message, M:

From the appropriate range, a random integer l is chosen.

Declare a parameter w such that it:

$$w = g^l \tag{42}$$

- Afterwards, find an element z such that:

$$z = H(w||M) \tag{43}$$

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

- Suppose

$$s = l - uz \tag{44}$$

where s represents the value of the signature.

- Two different signatures combined are (s, z).
- Keep in mind that $s, z \in \mathbb{Z}_q$; if $q < 2^{160}$, then 40 bytes are sufficient to store the signature representation.

1. Verification

- Consider a parameter w_v such that:

$$w_v = g^s t^z \tag{45}$$

- Then suppose.

$$z_v = H(w_v||M) \tag{46}$$

- The signature will be considered as authenticated if z_v is equal to z.

2.2.2. Elgamal digital signature algorithm

The Elgamal signature scheme is based on the challenge of discrete logarithm computation. It was introduced by Taher Elgamal in 1985 [46].

1. Key generation

The process of generating keys involves two steps. The first step is selecting components that can be shared with other users of the system, while the second step is computing a unique key pair for a particular user.

2. Parameter generation

- A key length N is selected.
- A prime number q of length N - bits is chosen.
- A cryptographic hash function H is selected with an output length of L bits. Only the hash output's leftmost bits are processed if $L > N$.

- A generator $g < q$of the multiplicative group of integers z_q^*modulo q is also chosen as part of the scheme's components.
- These elements may be shared among system members.

3. Per-user keys

Are then generated using a set of elements. To calculate the key pair for each user:

An integer u is randomly selected from $\{1, \ldots., q-2\}$.

Calculate

$$t = g^u mod q \tag{47}$$

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

4. Signing

- To generate a message sign,
- We select a random integer, l, from a set of numbers, $\{2, \ldots., q-2\}$, which are relatively prime to $q-1$.
- We then estimate a parameter w using the equation:

$$w = g^l mod q \tag{48}$$

- Next, we estimate the signature value s using the equation:

$$s = (H(m) - uw)l^{-1} mod(q-1) \tag{49}$$

- In the rare case that s is not relatively prime to l, we need to start over with a new random l.
- The resulting value (w, s) is the signature.
- Verification
- To determine the validity of a message's signature, follow these three procedures. First, test if $0 < w < q$ and $0 < s < q-1$.
- The signature is considered authentic only if this condition is met.

$$g^{H(m)} \equiv t^w w^s \bmod q \tag{50}$$

2.3. Method

The proposal aims to enhance the secret signing key generation process by leveraging the randomness of a chaotic map to create a lengthy private key sequence. The secret signing key, denoted as u, is produced as a key sequence through the use of a chaotic map, specifically the enhanced logistic map. The verification public key is computed as $t = g^u \bmod q$. The signing and verification phases will follow the procedures outlined in sections 2.2.1 and 2.2.2. The flow chart illustrating the proposed algorithm can be found in Figure 10 and the steps of the proposed algorithm are described below.

Steps of the proposed algorithm
Input: q , g and l. **Output**: The private key, u, and a signature, s, for each private key. a. Specify the parameters and initial conditions for the map. b. Create a sequence of random iterations by applying the equation of the new map. c. Transform every random iteration into a 256-bit integer. d. Produce a signature,s, for each private key, u. e. Validate the authenticity of each signature.

3. Results

The utilization of traditional Schnorr and Elgamal algorithms has been widespread across various applications, including smart contracts and healthcare. While these algorithms have demonstrated satisfactory outcomes, their private key size (2^{160}) and randomness have not been sufficient to meet the required security standards. To address this issue, the proposed algorithms incorporate chaotic maps to generate a larger-sized (2^{256}).) and more random private key sequences. This optimization has significantly improved the time required for signature creation and verification. Careful consideration has been given to the selection of conditions, parameters, and iterations in order to eliminate any possibility of result repetition. The values applied in the proposed algorithms are presented in Table 1.

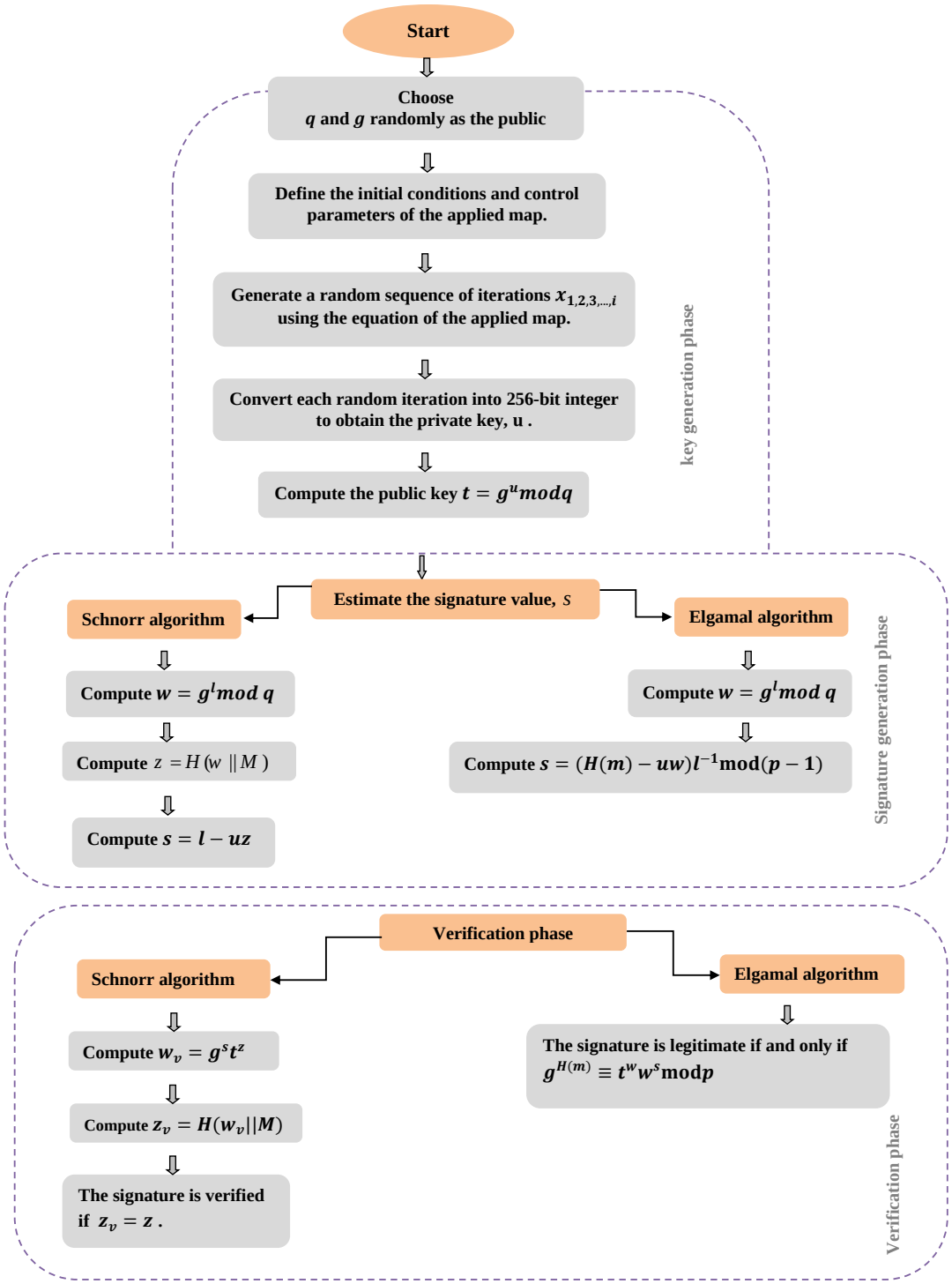


Figure 10. Flow chart of the new algorithm.

Table 1. Initialization values for the proposed algorithm.

Digital Signature Algorithm	Number Of Iterations	Output size	Initial Conditions	The range of q
Schnorr	10000	256- bit	0.4	$[10^{20}, 10^{50}]$
Elgamal	10000	256 -bit	0.4	$[10^{20}, 10^{50}]$

Table 2 shows the results of the proposed algorithm.

Table 2. Results of the proposed algorithm.

Digital Signature Algorithm	Part of the output Sign With "Hello World" Input Message
Schnorr	The Sign is 233424023953892737350307542927043465298781032704 47
	The Sign is 106703010638214195723266589943864914411799937331 17
	The Sign is 185850602017347618013488269844956641974730614146 61
Elgamal	The Sign is 106719540278645007781451803095821886421183311649 7
	The Sign is 199752572639424012896280598569522430492191092882 6
	The Sign is 539598027872528310325520354221350360256610406736 9

Furthermore, Table 3 provides a comprehensive comparison between the results of the proposed algorithms and those of the traditional approach.

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^{256}
Schnorr based on the new chaotic system	0.0000799212	0.0000100223	2^{256}
Traditional Elgamal	0.00034725805187	0.0006738269302593	2^{256}
Elgamal based on the new chaotic system	0.000029932	0.0000399298	2^{256}

Additionally, Table 4 presents a comparison between the results of the proposed algorithms and another set of tests involving 100,000 messages, conclusively demonstrating that our new algorithm achieves the shortest signing and verification time.

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

Algorithm	Signature time(ms)	Verification time(ms)	Total time(ms)
The proposed algorithm for Schnorr	0.11914	0.2036	0.32274
The proposed algorithm for Elgamal	0.1272	0.2378	0.365
Schnorr Scheme	0.1310	1.4503	1.5813
Elgamal Scheme	0.4946	0.2075	0.7021
Ref [52] structure 1	1.3081	1.4480	2.7561
Ref [52] structure 2	1.3456	1.4634	2.809
Ref [52] structure 3	0.3924	0.2609	0.6533
Ref [52] structure 4	0.5075	0.2538	0.7613
Ref [53]	3,5000	5,2200	40,200
Ref [54]	-	-	4465.38
Ref [55]	-	-	8508.74
Ref [56]	-	-	2344.23
Ref [57]	-	-	1515.03
Ref [58]	-	-	10.31
Ref [59]	-	-	912.19
Ref [60]	-	-	7.29
Ref [61]	-	-	29.570

Tables 5 and 6 exhibit Schnorr and Elgamal digital signatures based on the new chaotic system for 100,000 messages. These tables serve as evidence that our new algorithms do not necessitate a high level of computing complexity and are suitable for hardware implementation.

Table 5. Schnorr Digital signature based on the new chaotic system for 100000 messages.

	Length of characters	Signing time (ms)	Verification time (ms)
1	208	0.3295126	0.4322214
2	416	0.313355	0.323265
3	624	0.330325	0.4266658
4	832	0.387758	0.38859
5	1040	0.386322	0.409987
6	1248	0.338975	0.300011
7	1456	0.33998	0.469877
8	1660	0.310003	0.338977
9	1868	0.399998	0.42224
10	2076	0.390032	0.310025

Table 6. Elgamal Digital signature based on Improved logistic for 100000 messages.

	Length of characters	Signing time (ms)	Verification time (ms)
1	208	0.336525	0.43685
2	416	0.3200325	0.325726
3	624	0.30152	0.4000325
4	832	0.332547	0.3578995
5	1040	0.31236	0.430142
6	1248	0.39333	0.388879
7	1456	0.352756	0.413030
8	1660	0.33132	0.369865
9	1868	0.380123	0.434223
10	2076	0.33012223	0.318975

4. Conclusions

This proposal outlined an enhancement to the Schnorr and Elgamal digital signature schemes, focusing on the generation of the private key through the implementation of a new chaotic system. This new system is proposed by first generating a new 1D chaotic map based on sin and logistic maps. Then, a new system with quantum corrections is produced by coupling a

kicked quantum system with a harmonic oscillator bath. This system generates a random sequence of iterations that are then converted into 256-bit integers for use as the private key. Testing was conducted on various parameters and message sizes, with the results of the experiments demonstrating that the proposed digital signature algorithm offers high security and quality of service. The key space was expanded to 2^{256} from the traditional 2^{160} in other algorithms, and the signing and verification times were found to be faster compared to alternative algorithms. Furthermore, our proposed algorithms require fewer keys for signing and verification compared to previous studies. The results also indicated that the new algorithm does not necessitate a high level of computing complexity. Overall, our development enhances the security of the digital signature algorithm against brute force attacks without introducing time or hardware constraints.

Acknowledgements: In this section, you can acknowledge any support given that is not covered by the author's contribution or funding sections. This may include administrative and technical support, or donations in kind (e.g., materials used for experiments).

Conflicts of Interest: The authors declare that there are no conflicts of interest regarding the publication of this paper.

References:

[1] J. Vora, P. DevMurari, S. Tanwar, S. Tyagi, N. Kumar, M.S. Obaidat, Blind Signatures Based Secured E-Healthcare System, in: 2018 International Conference on Computer, Information and Telecommunication Systems (CITS), IEEE, Alsace, Colmar, France, 2018: pp. 1–5. https://doi.org/10.1109/CITS.2018.8440186.

[2] H.A.M.A. Basha, A.S.S. Mohra, T.O.M. Diab, W.I.E. Sobky, Efficient Image Encryption Based on New Substitution Box Using DNA Coding and Bent Function, IEEE Access 10 (2022), 66409–66429. https://doi.org/10.1109/ACCESS.2022.3183990.

[3] W. Alsobky, H. Saeed, A.N. Elwakeil, Different Types of Attacks on Block Ciphers, Int. J. Recent Technol. Eng. 9 (2020), 28-31.

[4] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, G. Wang, Digital Signature Scheme for Information Non-Repudiation in Blockchain: A State of the Art Review, EURASIP J. Wirel. Commun. Netw. 2020 (2020), 56. https://doi.org/10.1186/s13638-020-01665-w.

[5] A.K. Aboul-Seoud, A.K. Mahmoud, A. Hafez, et al. Minimum Variance Variable Constrain DOA Algorithm, in: PIERS Proceedings, Guangzhou, China, 2014.

[6] L.W. Cong, Z. He, Blockchain Disruption and Smart Contracts, Rev. Financial Stud. 32 (2019), 1754–1797. https://doi.org/10.1093/rfs/hhz007.

[7] L. Ante, Smart Contracts on the Blockchain – A Bibliometric Analysis and Review, Telemat. Inform. 57 (2021), 101519. https://doi.org/10.1016/j.tele.2020.101519.

[8] N.A. Alwan, S.J. Obaiys, N.F.B.M. Noor, N.M.G. Al-Saidi, Y. Karaca, Color Image Encryption Through Multi-S-Box Generated by Hyperchaotic System and Mixture of Pixel Bits, Fractals (2024), 2440039. https://doi.org/10.1142/S0218348X24400395.

[9] H. Natiq, N.M.G. Al-Saidi, S.J. Obaiys, M.N. Mahdi, A.K. Farhan, Image Encryption Based on Local Fractional Derivative Complex Logistic Map, Symmetry 14 (2022), 1874. https://doi.org/10.3390/sym14091874.

[10] D.S. Ali, N.A. Alwan, N.M.G. Al-Saidi, Image Encryption Based on Highly Sensitive Chaotic System, AIP Conf. Proc. 2183 (2019), 080007. https://doi.org/10.1063/1.5136200.

[11] Z. Shao, Digital Signature Schemes Based on Factoring and Discrete Logarithms, Electron. Lett. 38 (2002), 1518–1519. https://doi.org/10.1049/el:20021093.

[12] W.H. He, Digital Signature Scheme Based on Factoring Anddiscrete Logarithms, Electron. Lett. 37 (2001), 220–222. https://doi.org/10.1049/el:20010149.

[13] E. R, G. Anjaneyulu, A Modified Wei-Hua-He Digital Signature Scheme Based on Factoring and Discrete Logarithm, Symmetry 14 (2022), 2443. https://doi.org/10.3390/sym14112443.

[14] H. Qian, Z. Cao, H. Bao, Cryptanalysis of Li–Tzeng–Hwang's Improved Signature Schemes Based on Factoring and Discrete Logarithms, Appl. Math. Comput. 166 (2005), 501–505. https://doi.org/10.1016/j.amc.2004.06.054.

[15] C.T. Wang, C.H. Lin, C.C. Chang, Signature Schemes Based on Two Hard Problems Simultaneously, in: 17th International Conference on Advanced Information Networking and Applications, 2003. AINA 2003., IEEE Comput. Soc, Xi'an, China, 2003: pp. 557–560. https://doi.org/10.1109/AINA.2003.1192943.

[16] E.S. Ismail, N.M.F. That, R.R. Ahmad, A New Digital Signature Scheme Based on Factoring and Discrete Logarithms, J. Math. Stat. 4 (2008), 222-225.

[17] K. Chain, W.-C. Kuo, A New Digital Signature Scheme Based on Chaotic Maps, Nonlinear Dyn. 74 (2013), 1003–1012. https://doi.org/10.1007/s11071-013-1018-1.

[18] S. Chiou, Novel Digital Signature Schemes Based on Factoring and Discrete Logarithms, Int. J. Secur. Appl. 10 (2016), 295- 310.

[19] E.S. Ismail, N.M.F. Tahat, A New Signature Scheme Based on Multiple Hard Number Theoretic Problems, ISRN Commun. Netw. 2011 (2011), 231649. https://doi.org/10.5402/2011/231649.

[20] H. Cui, R.H. Deng, J.K. Liu, X. Yi, Y. Li, Server-Aided Attribute-Based Signature With Revocation for Resource-Constrained Industrial-Internet-of-Things Devices, IEEE Trans. Ind. Inform. 14 (2018), 3724–3732. https://doi.org/10.1109/TII.2018.2813304.

[21] C. Esposito, A. Castiglione, F. Palmieri, A.D. Santis, Integrity for an Event Notification Within the Industrial Internet of Things by Using Group Signatures, IEEE Trans. Ind. Inform. 14 (2018), 3669–3678. https://doi.org/10.1109/TII.2018.2791956.

[22] L. Shen, J. Ma, X. Liu, F. Wei, M. Miao, A Secure and Efficient ID-Based Aggregate Signature Scheme for Wireless Sensor Networks, IEEE Internet Things J. 4 (2017), 546–554. https://doi.org/10.1109/JIOT.2016.2557487.

[23] M.A. Mughal, X. Luo, A. Ullah, S. Ullah, Z. Mahmood, A Lightweight Digital Signature Based Security Scheme for Human-Centered Internet of Things, IEEE Access 6 (2018), 31630–31643. https://doi.org/10.1109/ACCESS.2018.2844406.

[24] D. Xiao, X. Liao, S. Deng, A Novel Key Agreement Protocol Based on Chaotic Maps, Inf. Sci. 177 (2007), 1136–1142. https://doi.org/10.1016/j.ins.2006.07.026.

[25] Y. Niu, X. Wang, An Anonymous Key Agreement Protocol Based on Chaotic Maps, Commun. Nonlinear Sci. Numer. Simul. 16 (2011), 1986–1992. https://doi.org/10.1016/j.cnsns.2010.08.015.

[26] X. Wang, J. Zhao, An Improved Key Agreement Protocol Based on Chaos, Commun. Nonlinear Sci. Numer. Simul. 15 (2010), 4052–4057. https://doi.org/10.1016/j.cnsns.2010.02.014.

[27] D. Veeman, H. Natiq, N.M.G. Al-Saidi, K. Rajagopal, S. Jafari, I. Hussain, A New Megastable Chaotic Oscillator with Blinking Oscillation Terms, Complexity 2021 (2021), 5518633. https://doi.org/10.1155/2021/5518633.

[28] E.J. Yoon, I.-S. Jeon, An Efficient and Secure Diffie–Hellman Key Agreement Protocol Based on Chebyshev Chaotic Map, Commun. Nonlinear Sci. Numer. Simul. 16 (2011), 2383–2389. https://doi.org/10.1016/j.cnsns.2010.09.021.

[29] M.S. Hwang, C.C. Yang, S.-F. Tzeng, Improved Digital Signature Scheme Based on Factoring and Discrete Logarithms, J. Discrete Math. Sci. Cryptogr. 5 (2002), 151–155. https://doi.org/10.1080/09720529.2002.10697946.

[30] S.F. Pon, E.-H. Lu, A.B. Jeng, Meta-He Digital Signatures Based on Factoring and Discrete Logarithms, Appl. Math. Comput. 165 (2005), 171–176. https://doi.org/10.1016/j.amc.2004.04.082.

[31] S.F. Tzeng, C.Y. Yang, M.-S. Hwang, A New Digital Signature Scheme Based on Factoring and Discrete Logarithms, Int. J. Comput. Math. 81 (2004), 9–14. https://doi.org/10.1080/00207160310001614954.

[32] L. Harn, Public-Key Cryptosystem Design Based on Factoring and Discrete Logarithms, IEE Proc. Comput. Digit. Tech. 141 (1994), 193-195. https://doi.org/10.1049/ip-cdt:19941040.

[33] N.-Y. Lee, T. Hwang, Modified Harn Signature Scheme Based on Factorising and Discrete Logarithms, IEE Proc. Comput. Digit. Tech. 143 (1996), 196. https://doi.org/10.1049/ip-cdt:19960335.

[34] N.M.G. Al-Saidi, S.J. Obaiys, N.A. Alwan, A.J. Mohammed, A.K. Farhan, Y. Karaca, Secure Image Encryption Using Single-Mode Fiber and Dense Wavelength Division Multiplexing in Chaotic Systems, in: O. Gervasi, B. Murgante, C. Garau, D. Taniar, A.M.A. C. Rocha, M.N. Faginas Lago (Eds.), Computational Science and Its Applications – ICCSA 2024 Workshops, Springer, Cham, 2024: pp. 72–90. https://doi.org/10.1007/978-3-031-65154-0_5.

[35] R.B. Naik, U. Singh, A Review on Applications of Chaotic Maps in Pseudo-Random Number Generators and Encryption, Ann. Data Sci. 11 (2024), 25–50. https://doi.org/10.1007/s40745-021-00364-7.

[36] N.A. Alwan, S.J. Obaiys, N.M.G. Al-Saidi, N.F.B.M. Noor, Y. Karaca, A Pseudo Random Number Generator Based on 4D Hyperchaotic Systems, Riddled Basins of Attraction and Advanced Microfluidic Technology, in: O. Gervasi, B. Murgante, C. Garau, D. Taniar, A.M.A. C. Rocha, M.N. Faginas Lago (Eds.), Computational Science and Its Applications – ICCSA 2024 Workshops, Springer, Cham, 2024: pp. 91–109. https://doi.org/10.1007/978-3-031-65154-0_6.

[37] Z.A. Abduljabbar, I.Q. Abduljaleel, J. Ma, et al. Provably Secure and Fast Color Image Encryption Algorithm Based on S-Boxes and Hyperchaotic Map, IEEE Access 10 (2022), 26257–26270. https://doi.org/10.1109/ACCESS.2022.3151174.

[38] H. Saeed, H.E. Ahmed, T.O. Diab, et al. Evaluation of the Most Suitable Hyperchaotic Map in S-Box Design Used in Image Encryption, Int. J. Multidiscip. Res. Publ. 5 (2022), 176-182.

[39] M.T. Wazi, D.S. Ali, N.M.G. Al-Saidi, N.A. Alawn, A Secure Image Cryptosystem via Multiple Chaotic Maps, Discrete Math. Algorithms Appl. 14 (2022), 2150141. https://doi.org/10.1142/S179383092150141X.

[40] M.E. Goggin, B. Sundaram, P.W. Milonni, Quantum Logistic Map, Phys. Rev. A 41 (1990), 5705–5708. https://doi.org/10.1103/PhysRevA.41.5705.

[41] E. Al Solami, M. Ahmad, C. Volos, M.N. Doja, M.M.S. Beg, A New Hyperchaotic System-Based Design for Efficient Bijective Substitution-Boxes, Entropy 20 (2018), 525. https://doi.org/10.3390/e20070525.

[42] A.A. Alzaidi, M. Ahmad, M.N. Doja, E.A. Solami, M.M.S. Beg, A New 1D Chaotic Map and β-Hill Climbing for Generating Substitution-Boxes, IEEE Access 6 (2018), 55405–55418. https://doi.org/10.1109/ACCESS.2018.2871557.

[43] H. Saeed, M.A. Elsisi, T.O. Diab, W.I. El Sobky, M.S. Abdel-Wahed, A.K. Mahmoud, Famous Digital Signatures Used in Smart Contracts, in: 2023 International Telecommunications Conference, IEEE, Alexandria, Egypt, 2023: pp. 649–656. https://doi.org/10.1109/ITC-Egypt58155.2023.10206283.

[44] J. Na, H.Y. Kim, N. Park, B. Seo, Comparative Analysis of Schnorr Digital Signature and ECDSA for Efficiency Using Private Ethereum Network, IEIE Trans. Smart Process. Comput. 11 (2022), 231-239.

[45] Y. Qin, B. Zhang, Privacy-Preserving Biometrics Image Encryption and Digital Signature Technique Using Arnold and ElGamal, Appl. Sci. 13 (2023), 8117. https://doi.org/10.3390/app13148117.