E-ISSN: 1115 – 8492 P-ISSN: 3027 – 0693
MPRI-JNSAR
INTERNATIONAL JOURNAL OF NATURE AND SCIENCE ADVANCE RES.
VOL. 10 NO. 9 OCTOBER-2025

RAJ CHAOTIC MAP (RCM): A HYBRID LOGISTIC–QUADRATIC MAP FOR SECURE TEXT ENCRYPTION USING PUBLIC KEY CRYPTOGRAPHY

RAJI FUNSHO ISAIAH; OKEYINKA ADEREMI ELISHA; ADAMU ABUBAKAR ISAH; & MAIPAN-UKU JAMILU YAHAYA

Department of Computer Science, Faculty of Applied Sciences and Technology, Ibrahim Badamasi Babangida University, Lapai, Niger State, Nigeria

Corresponding Author:
raygatecomputersolution@gmail.com

DOI: https://doi.org/10.70382/mejnsar.v10i9.065

Keywords: Public Key Chaotic Cryptosystem (PKCC), Chaotic Maps, Elliptic Curve Cryptosystem (ECC), Raj Chaotic Map (RCM), Lyapunov Exponent, Bifurcation, Lightweight, JoanS-MuraliP (JSPM)

Abstract

A new chaotic map tagged Raj Chaotic Map (RCM) derived from the combination of the logistic and quadratic maps, designed specifically to enhance security in public key cryptography is proposed in this study. The logistic map, while simple and widely used, suffers from periodic windows and limited chaotic range, making it vulnerable to predictability in certain parameter intervals. The quadratic map, on the other hand, exhibits sensitive dependence on initial conditions but lacks sufficient complexity and flexibility for robust cryptographic applications on its own. Hence, a chaos-based public key cryptosystem where a one-dimensional chaotic map is developed using the logistic map and a simple quadratic map. The new RCM inherits and amplifies the core chaotic properties of its constituent maps by leveraging the individual chaotic characteristics of the logistic map, such as its sensitivity to initial conditions and the quadratic map's broad range of bifurcation behaviors. The cryptosystem employs the use of elliptic curve cryptographic technique,

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

hash function, and Elliptic Curve Diffie-Helman (ECDH) key exchange protocol in its development. Shared Secret Key (SSK) was generated using ECDH key exchange protocol to solve the problem of key exchange among the communicators. The hash function was used to generate a hash value from the concatenation of the plaintext and SSK. Elliptic curve scalar multiplication operation was performed between the generated hash value and SSK to obtain a point on the elliptic curve. The obtained point was then used to determine the initial value and control parameter for the chaotic map, while the developed chaotic map was applied for the generation of chaotic sequence. Exclusive-or (XOR) operation is then performed between the obtained chaotic sequence and the plaintext to obtain ciphertext. The proposed RCM demonstrates an expanded parameter space with improved unpredictability and higher entropy verified through Bifurcation diagrams, Lyapunov exponents and Sequence diagrams, making it well-suited for cryptographic applications. This map is applied within a public key cryptographic framework. The enhanced key sensitivity, large key space, and efficient computation make the RCM a strong candidate for modern lightweight and in resource-constrained real-time environments.

Introduction

In recent decades, the growing reliance on digital communication and cloud-based infrastructure has heightened the demand for robust cryptographic schemes. Traditional encryption algorithms such as RSA and ECC rely heavily on the mathematical complexity of integer factorization and elliptic curve problems, respectively. However, these systems face increasing threats from quantum computing and algorithmic advances, thereby motivating the exploration of alternative frameworks such as chaos-based cryptography (Alvarez & Li, 2006).

Chaotic maps, known for their deterministic yet unpredictable behavior, have gained traction in the design of secure cryptosystems due to properties such as ergodicity, sensitivity to initial conditions, and topological mixing (Kocarev, 2001). Among the well-studied chaotic systems, the Logistic Map and the Quadratic Map stand out for their simplicity and low computational overhead. The Logistic Map, defined as $x_{i+1} = rx_i(1 - x_i)$, generates complex dynamics within a narrow range of control parameters, while the Quadratic Map, $x_{i+1} = r\left(x_i^2 - 1\right)$, offers a more abrupt transition between periodic and chaotic states (Strogatz, 2018). Despite their merits, both maps individually suffer from limitations such as low entropy under certain parameter conditions and limited chaotic ranges (Kanso & Smaoui, 2009).

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

To overcome these drawbacks, researchers have proposed hybrid chaotic maps that combine the strengths of two or more one-dimensional maps. Hybridization introduces higher complexity, wider chaotic intervals, and richer dynamical behavior, which are advantageous in constructing cryptographic primitives (Jangir et al., 2021). Specifically, combining the Logistic and Quadratic maps can harness the stable chaotic behavior of the Logistic map with the sharper transitions and increased nonlinearity of the Quadratic map. This synergy enhances unpredictability and keyspace diversity, making it a promising approach for secure text encryption.

A new map tagged Raj Chaotic Map (RCM) for Text Encryption Algorithm using a Public Key Cryptosystem by hybridizing Logistic and Quadratic Maps is proposed in this study. The hybrid map is carefully constructed to ensure chaotic behavior across a wider range of parameters, enabling stronger resistance to statistical and brute-force attacks. By incorporating this hybrid map into a public key framework, the proposed scheme offers a lightweight, yet secure alternative to traditional cryptographic methods, especially for IoT and low-power devices. These maps exhibit bifurcations, positive Lyapunov exponents, entropies and time series analytical behavior across specific parameter ranges, making them ideal candidates for secure encryption applications.

Motivation

The increasing reliance on digital communication across networks has intensified the demand for secure and efficient cryptographic systems. Traditional public key cryptographic algorithms such as RSA and ECC rely on the computational hardness of problems like integer factorization and elliptic curve discrete logarithms. While these methods have been foundational in modern security systems, the emergence of quantum computing threatens their long-term viability. In parallel, chaotic systems have shown promise for cryptographic applications due to their deterministic yet unpredictable behavior, high sensitivity to initial conditions, and excellent pseudo-random characteristics. These attributes make chaotic maps suitable for enhancing cryptographic processes, especially in data scrambling and key stream generation.

The logistic map and the quadratic map are two well-known one-dimensional chaotic systems that have been individually applied in cryptographic schemes. Each possesses unique advantages: the logistic map exhibits rich bifurcation behavior and good statistical properties under specific parameter settings, while the quadratic map demonstrates strong nonlinearity and high unpredictability. However, both maps suffer from weaknesses when used independently, including limited key space, periodicity under finite precision, and reduced randomness in certain parameter regions. These

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

shortcomings reduce their effectiveness in real-world encryption scenarios where robustness against statistical, differential, and brute-force attacks is essential.

To overcome these limitations, this study proposes the hybridization of logistic and quadratic maps tagged RCM to construct a more complex and secure chaotic generator for use in a public key cryptosystem. The combination is designed to harness the complementary strengths of both maps, producing a more uniformly distributed and statistically robust sequence. This hybrid chaotic system is integrated into a text encryption algorithm that leverages the asymmetry of public key cryptography for secure key exchange while employing chaotic dynamics for confusion and diffusion of plaintext. The resulting architecture not only enhances encryption strength but also offers resistance to cryptanalytic and quantum threats, making it a viable candidate for future-proof secure communication systems.

Related Works

Public-Key Cryptography (PKC) is another major direction in cryptography, which are usually based on mathematical hard problems. The main distinction between symmetric and asymmetric-key is that the latter uses distinct keys for encryption and decryption; a public key and private key. Depending on how the keys are used, asymmetric-key ciphers can not only provide confidentiality but also authentication and non-repudiation. Among PKCs, the best well-known and most widely used PKCs are RSA (Rivest et al., 2019) and Elliptic Curve Cryptograph (ECC)(Bos et al., 2014; Koblitz, 1987). However, ECC is rated as more resource efficient than RSA because ECC operates with higher performance, lower power consumption, and smaller area of hardware. Nevertheless, the performance is much slower than private-key cryptography such as AES(Sakiyama et al., 2006). The best algorithm known for solving the underlying mathematical problem of ECC, referred to as the elliptic curve discrete logarithm problem (ECDLP), takes full exponential time. On the contrary, sub-exponential time algorithms are known for tackling the integer factorization and the discrete logarithm problems that Rivest, Shamir, and Addleman (RSA) and Digital Signature Algorithm (DSA) are relied on (Crowie et al., 1996; Gordon, 1993). This implies that the algorithms for solving the ECDLP become infeasible much more rapidly as the problem size increases than those algorithms for tackling the integer factorization and the discrete logarithm problems. For this reason, ECC offers a security level equivalent to RSA and DSA while using a far smaller key size (Lucca et al., 2021). Generally, public key ciphers are considered more secure than their symmetric-key counterparts due to their underlying mathematical hard problems. However, public-key ciphers are computationally inefficient, especially when used with longer messages. Thus,

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

asymmetric encryption is usually used for key distribution or to exchange secret parameters in most security protocols. The trade-off between security and computational efficiency is a well-documented, open problem for chaos-based encryption algorithms, whereby efficiency is usually sacrificed to achieve optimal security. Chaotic maps have attracted significant attention in cryptography due to their sensitivity to initial conditions, ergodicity, and deterministic randomness.

The logistic map, defined by the recursive relation $x_{i+1} = rx_i(1 - x_i)$, has been widely adopted as a simple yet powerful nonlinear chaotic system. It has found use in numerous encryption algorithms for text, image, and voice data. For instance, (Luo et al., 2019) utilized a logistic map to generate dynamic keystreams in a symmetric encryption algorithm, showing improvements in entropy and correlation analysis. However, their work also highlighted vulnerabilities under finite precision arithmetic, especially for control parameters near the edge of chaos.

The quadratic map, expressed as $x_{i+1} = r\left(x_i^2 - 1\right)$, is another notable one-dimensional chaotic system. While it demonstrates similar chaotic behavior to the logistic map, it possesses a broader chaotic range and higher degree of nonlinearity. (Ramadan et al., 2016) proposed an image encryption method using the quadratic map for pixel scrambling and permutation, achieving better statistical resistance than logistic-based schemes. Nonetheless, the quadratic map also suffers from structural weaknesses when implemented with low-bit precision or fixed parameter values, making it predictable under certain attack models.

The Logistic-Quadratic Map is a hybrid of two classical nonlinear chaotic functions: The Logistic map (known for its sensitivity and simple structure). The Quadratic map (noted for its strong nonlinearity and bifurcation behaviour).

Recent works have explored hybrid chaotic systems to compensate for the limitations of individual maps. (Jangir et al., 2021) introduced a hybrid chaotic map formed by combining multiple 1D maps, including logistic and quadratic components, to improve complexity and resistance against known attacks. Their design was applied in a secure communication system, where the hybrid map enhanced key sensitivity and confusion-diffusion properties. Similarly, (Abd El-Latif et al., 2020) demonstrated that chaotic hybridization enhances encryption performance by increasing randomness and reducing periodicity, making it suitable for lightweight cryptographic applications. These studies collectively underscore the growing interest in map hybridization as a path toward designing more secure, efficient, and quantum-resilient cryptographic schemes.

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Strengths of the Logistic-Quadratic Map

Based on theoretical properties and recent hybrid map trends, the hybrid map offer:

- Extended Chaotic Range: The quadratic component reduces periodic windows commonly found in the Logistic map.
- Improved Lyapunov Exponents: Nonlinear interactions between logistic and quadratic terms boost the LE values, indicating stronger chaos.
- Better Diffusion and Confusion: The combined map produces more diverse output states, which is valuable for encryption.
- Enhanced Randomness and Entropy: Hybridization smoothens the distribution, leading to better randomness quality.
- Low Computational Cost: Unlike multi-map cascaded systems, both Logistic and Quadratic maps are lightweight, making the hybrid suitable for mobile, IoT, and real-time cryptosystems.

Weaknesses and Limitations of Logistic-Quadratic Map

Although more robust than single-map models, the Logistic-Quadratic hybrid may still face:

- Finite Precision Vulnerabilities: Digital implementations may introduce rounding errors that reduce chaotic quality.
- Parameter Sensitivity: Chaotic regions depend heavily on the chosen control parameters.
- One-Dimensional Limitations: Compared with 2D/3D maps, the Logistic–Quadratic remains more predictable in phase-space reconstruction attacks unless properly masked in encryption.

Observation From Review of Related Works

1. Hybrid maps require careful parameter tuning; otherwise, they may lose chaotic behavior and exhibit periodic or unstable dynamics(Wang et al., 2021).
2. The increased complexity from combining two or more maps leads to higher computational demands and longer processing time (Zhang & Chen, 2020).
3. Some hybrid maps can experience transitions from chaos to regular behavior under certain parameter settings, making long-term prediction difficult (Li et al., 2022)
4. Due to the novelty of many hybrid models, they often lack standardized analytical frameworks for evaluating bifurcation, Lyapunov exponents, or entropy metrics (Kumar & Singh, 2019).

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Methodology

Public Key Chaotic Cryptosystem (PKCC)

The proposed public key chaotic cryptosystem uses Elliptic Curve Cryptography (ECC) technique and Elliptic Curve Diffie-Helman (ECDH) key exchange protocol for the purpose of secure key generation. A new chaotic map (RCM) which applies logistic and quadratic maps is developed. The initial value and control parameter of the newly developed chaotic map are obtained from the shared secrete key (SSK) obtained from ECDH protocol. In this section the key generation process, chaotic map development, encryption and decryption algorithm of PKCC are discussed.

ECC Key Generation and Diffie-Helman Key Exchange Protocol

The PKCC uses elliptic curve Diffie-Helman key exchange protocol to generate shared secret key SSK. The communicating parties must agree on the elliptic curve to be used for the purpose of communication before each party can forge ahead to generate the private and public keys. Both sender and recipient use the same procedure to generate the keys. The sender does not know the secret key of the recipient neither does the recipient knows the secret key of the sender. However, the pubic keys of both are revealed to the public. The procedure used by both sender and recipient to generate private and public keys independently is represented by the flowchart in Figure 1.

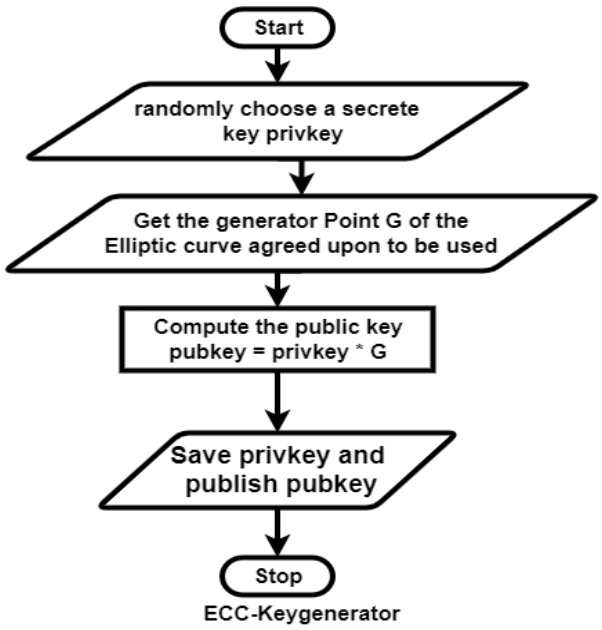

Figure 1: ECC Key generation

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

The generated ECC keys are used to generate SSK. SSK can be generated using Equation 1 where sprivkey, spubkey, rprivkey, and rpubkey are sender's private key, sender's public key, recipient's private key and recipient's public key respectively. The system of equations in Equation 1 is a description of ECDH key exchange protocol.

$$\begin{cases} SSK = spubkey * rprivkey \\ SSK = rpubkey * sprivkey \end{cases} \quad (1)$$

In order to make the cryptosystem sensitive to any changes in key or plaintext. Hash function HASH is used to generate hash value H and elliptic curve scalar multiplication between SSK and H is performed to obtain a point hkey on the elliptic curve as shown by the Equation 2.

$$hkey = H * SSK \quad (2)$$

Design of a New Map Tagged Raj Chaotic Map (RCM)

Logistic map is a simple chaotic map whose mathematical expression is presented in Equation 3

$$x_{i+1} = rx_i(1 - x_i) \quad (3)$$

Where $x \in [0,1]$ and $r \in [0,4]$are called logistic parameters. Logistic map is in chaotic state when $x \in [0,1]$. This means that the sequence generated by the initial condition x_0 under the action of the logistic map is non-periodic and does not converge. The generated sequence outside this range must converge to a certain value. The value r satisfies the condition $3.5699456 < r \leq 4$. In particular, the iteratively generated values are in a pseudo-randomly distributed state if the above mentioned condition is approximately 4.

The drawbacks of the sequence obtained from the above logistic chaotic sequence have been established in the literatures. One of the drawbacks is the fact that the pseudo-random number generated by using this 1D logistic chaotic system is not very secure. Hence various security attacks have been proposed to break the security of the system that applied its usage. The key space of the logistic map is also very small as only two parameters r and initial condition x_0 are used as the key for logistic chaotic sequence. Hence, it may be vulnerable to brute-force attack.

Also, sequences generated from existing logistic map have the disadvantages of uneven distribution, low security, and small parameter space. Therefore, logistic map $x_{i+1} = rx_i(1 - x_i)$ and quadratic map $x_{i+1} = r\left(x_i^2 - 7\right)$ are combined to develop a new chaotic map tagged Raj Chaotic Map (RCM) which is more secure and performs better than the existing maps. The novelty of RCM lies in the exhibition of a large chaotic band of 0.2 ≤ r ≤ 5000, which contributes to a large key space. The proposed map is denoted by Equation 4, where r is the control parameter and x_0 (n =0) is the initial value. $x_n \in [0,1]$ and $r \in [0.2,5000]$.

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

$$x_{n+1} = MOD\left(r^2(x^2 - 7)\left(1 - r({x_n}^2 - 7)\right), 1\right) \quad (4)$$

As part of improving the security of the public key chaos cryptosystem. The initial value x_0 and control parameter r is generated using Equation 2. The flowchart in Figure 2 shows the procedure of how the initial value x_0 and control parameter r are generated from hkey. hkey is a point on elliptic curve and it has x and y coordinates. The hash value of the x-coordinate of hkey modulus 0.99999 gives initial value x_0 while y-coordinate of hkey modulus 10.10111 computes the control parameter r. However, any value between 1 and 5000 could be used as the modulus. As x_0 and r depends on hkey any alteration on plaintext, sender's private or public key, or recipient's private or public key will alter hkey and by implication x_0 and r will equally be altered.

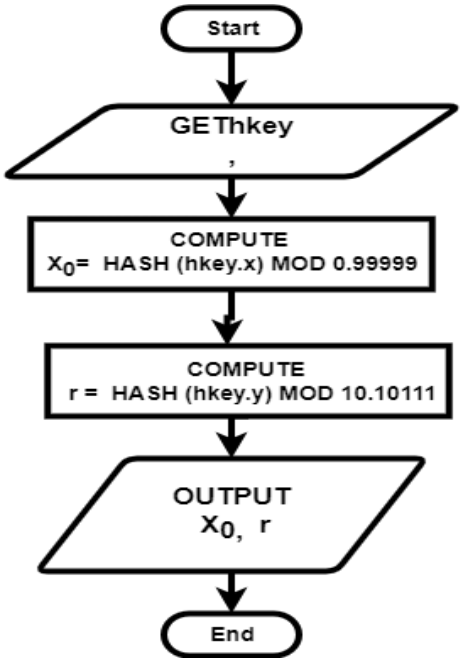

Figure 2: Generation of sequence initial conditions and control parameters

Using this procedure eliminates the need for sender and receiver to be looking for a secure way of exchanging these initial values and control parameters. Both the sender and recipient can independently generate these values and use them during encryption and decryption of the data being exchanged. Hence the security of the proposed cryptosystem will be very high. In addition, the security of the proposed cryptosystem is not solely depending on the initial values but also on difficulty involved in solving Elliptic Curve Discrete Logarithms Problem (ECDLP). The computation of the initial values and control parameter will always give initial value and control parameter that can only

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

generate non-periodic and non-convergent sequence as control parameter r will always be in the range $0.2 < r \leq 5000$ and x_0 will always be in the range $0 < x_0 \leq 1$.

Encryption and Decryption Algorithms of PKCC

Both encryption and decryption algorithms involves the generation of keys (public, private, and SSK), generation of a point hkey on the elliptic curve, generation of (x_0, r) and (x_{01}, r_1) from hkey and SSK respectively to serve as the pairs of initial values and control parameters for two different sequence of random numbers to be used for encryption and decryption operations, generation of sequence of random numbers using the generated initial values and control parameters and the use of XOR operation to form ciphertext from plaintext or to extract plaintext from the ciphertext. The flowchart in Figure 3 and Figure 4 give the description of the procedures involved in encryption and decryption operations respectively.

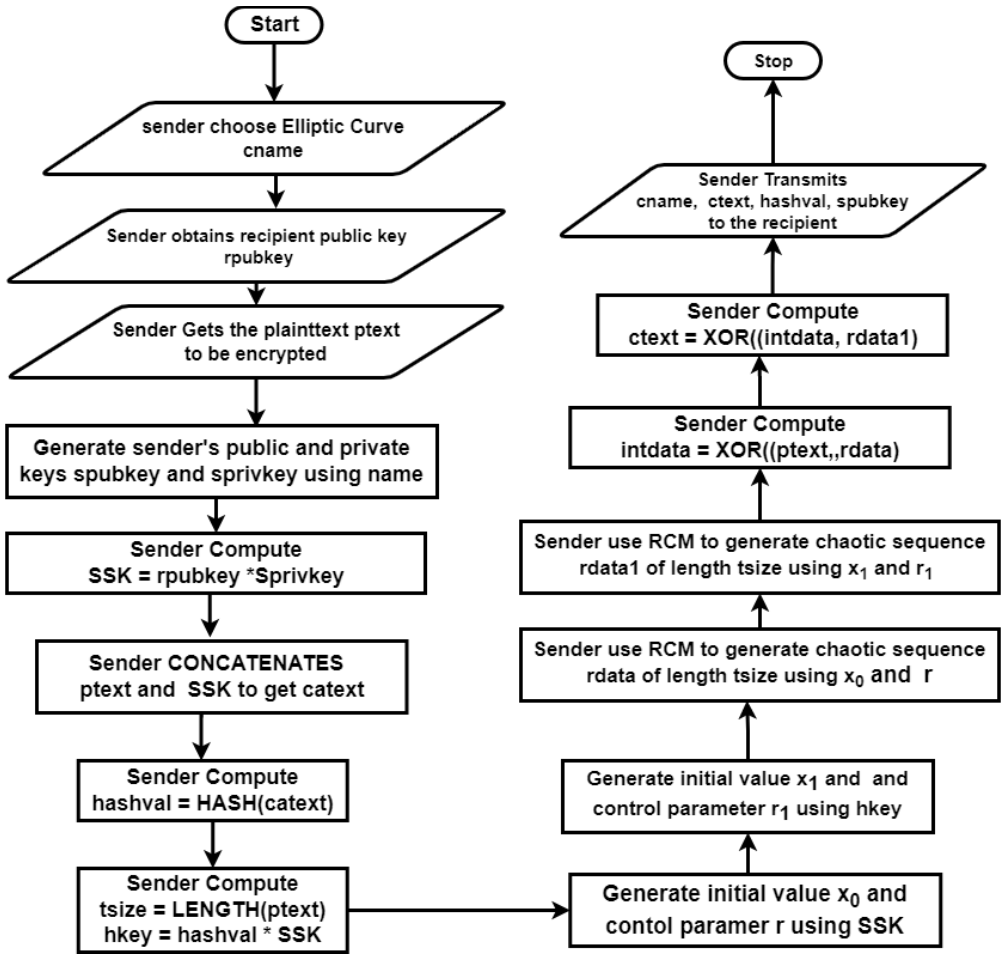

Figure 3: Flowchart showing the encryption algorithm in the proposed PKCC

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

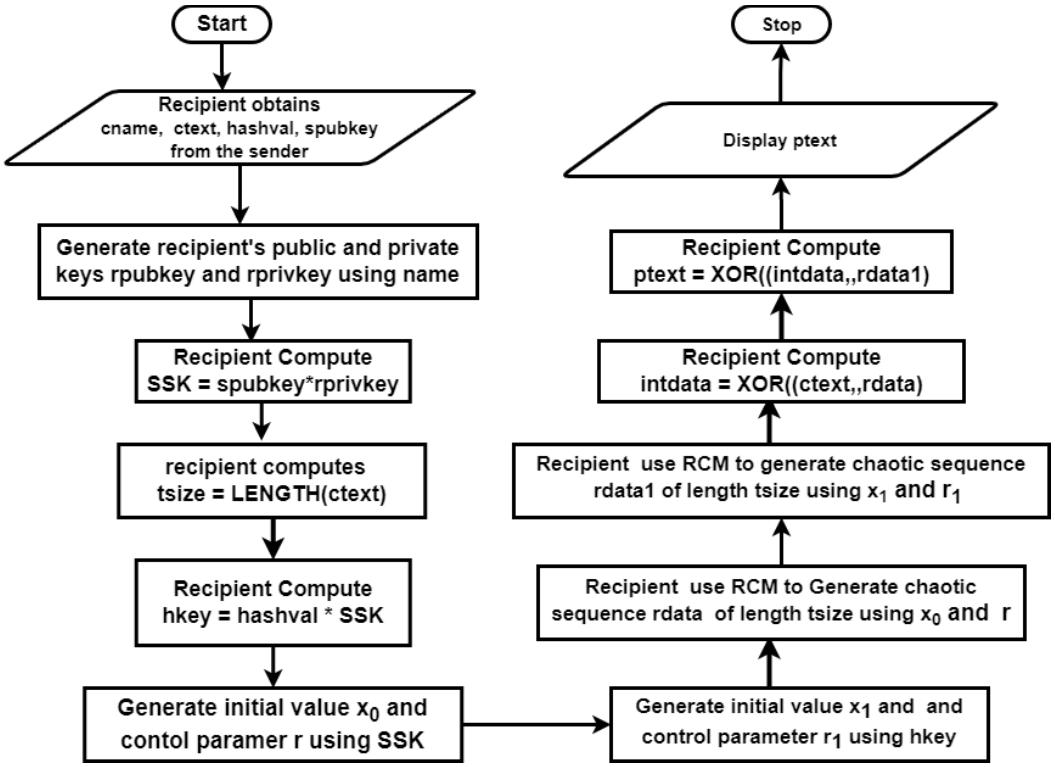

Figure 4: Flowchart showing the decryption algorithm in the proposed PKCC

In the encryption and decryption algorithms presented by the flowcharts in Figures 3 and 4, the initial values x_0, x_1 and control parameters r and r_1 are respectively generated from the x and y coordinates of the SSK and hkey as shown in Equations 5, 6, 7, and 8

$$r = MOD(SSK.x, 10.11111) \quad (5)$$

$$x_0 = MOD(SSK.y, 0.99999) \quad (6)$$

$$r_1 = MOD(hkey.x, 10.11111) \quad (7)$$

$$x_1 = MOD(hkey.y, 0.99999) \quad (8)$$

The chaotic sequences rdata and rdata1 are sequence of floating point numbers. However, Equation 9 is used to convert the sequence of the floating point number to sequence of American Standard Code for Information Interchange (ASCII) values.

$$rdata = [MOD(FLOOR(X[i] \times 10^{16}), 256)] \quad (9)$$

In Equation 9, sequence X is the sequence generated from floating point numbers using RCM where i = 1,2…, tsize and tsize is the number of elements in X.

In order to ensure confusion and diffusion in PKCC, two chaotic sequences rdata and rdata1 are generated. Intermediate random data is generated by computing exclusive-or operation (XOR) between the plaintext and rdata, and final ciphertext is computed by computing XOR operation between intermediate random data and rdata1.

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Computational Complexity Analysis

(a) *Time Complexity*

The time complexity evaluates the efficiency of encryption and decryption algorithms. The proposed system's encryption algorithm based on chaotic maps and substitution-permutation structure operates in O(n) time, where n is the data block length. This linear complexity is suitable for real-time applications with large user populations and frequent data transactions.

(b) *Space Complexity*

The space complexity quantifies the memory usage required during encryption. The proposed system maintains a low O(n) space complexity since chaotic key generation does not require extensive key storage or lookup tables. This ensures compatibility with resource-constrained devices (e.g., mobile learners' smartphones and tablets) which make it lightweight enough for real time applications.

Implementation Environment

The implementation was carried out using *Python 3.11* with NumPy for numerical computation and Matplotlib for visualization. The system was tested over a range of initial conditions and parameter values to assess its chaotic behavior through entropy, Lyapunov exponent, time series, and bifurcation analysis.

Verification and Analysis of RCM

Bifurcation Diagram

In the simulation experiments, the performance of RCM mapping was first compared and analyzed. The bifurcation diagrams of three chaotic maps are shown in Figure 5. From Figure 5, it can be seen that traditional logistic map has a small chaotic parameter range and contains many windows of periodicity, indicated by unshaded regions in its bifurcation diagram. When used for cryptographic applications, these periodic regions must be avoided. Thus, when the control parameter value is used as part of the secret key, the overall keyspace is greatly reduced. Therefore, increasing the chaotic parameter range helps to overcome brute force attacks due to the increased keyspace. To study chaotic parameter range, bifurcation diagrams can be used to represent the relationship between chaotic points and control parameters. It can also be seen in Figure 5.1 that RCM and JoanS-MuraliP (JSMP) maps no longer have windows of periodicity and the state variable, x is evenly distributed between 0 and 1 regardless of r. This implies that RCM and JSMP models have not only eliminated the periodic windows of the logistic map but also have larger control parameter range. Hence, RCM and JSMP mappings break through the

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

limitations of the parameters and exhibits good chaotic characteristics within the range of (0, 4]. This is because when scrambling and diffusion processing are carried out simultaneously, this experiment uses the modular operations to increase the range of parameter r. Hence, the ergodicity and uniformity of parameters are improved.

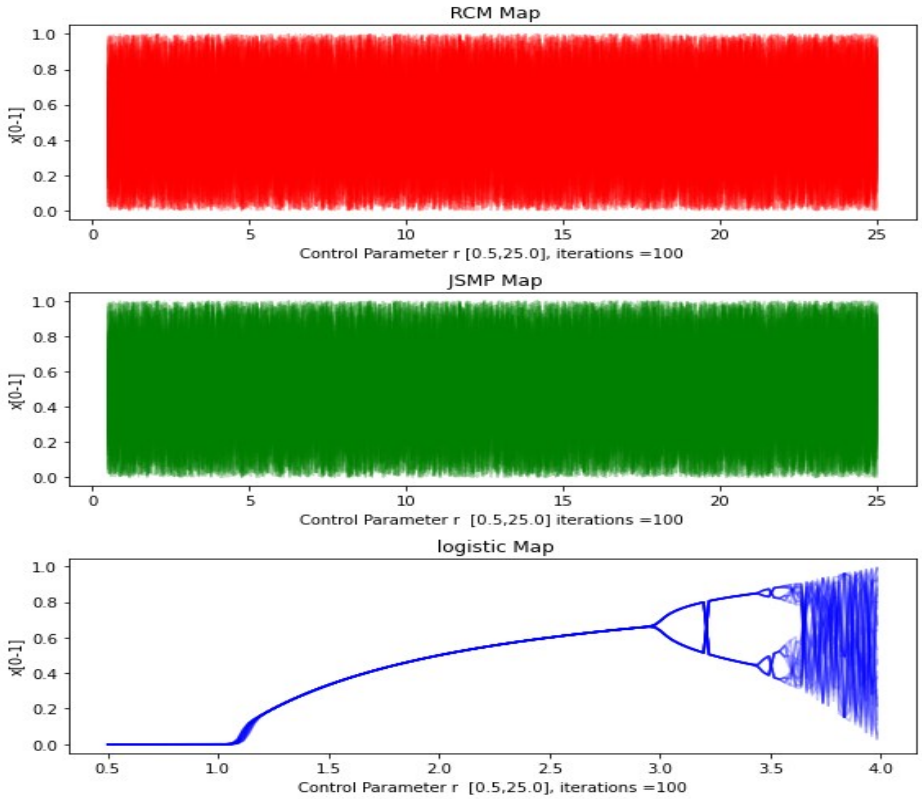

Figure 5: Bifurcation Diagrams of RCM, JSMP and Logistic maps.

Lyapunov Exponent

Sensitivity to small changes to initial conditions and control parameters play a significant role in chaos-based cryptographic systems. Lyapunov exponent (LE) is a mathematical indicator that can be calculated under different initial conditions and parameter settings. A chaotic map with large and positive LE values have chaotic points that diverge after a shorter period of time (fewer iterations) as compared to chaotic maps with smaller or negative LE values. This means that larger LE values suggest increased unpredictability and sensitivity. An experiment was conducted on three different chaotic maps for the analysis of their LE under varied values of control parameter r. The same initial value 0.00001 and number of iterations (100) were used while the values of control parameter r were varied between 0.5 and 4 during the experiment. Figure 6 shows the graphs of the

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Lyapunov exponent versus control parameter r for the three chaotic maps under consideration. As can be seen from the graph, LE of the traditional logistic map have negative values for values of r in the range (0.5-3.6) while its LE is greater than zero for r is above 3.6. The LE's of JSMP and RCM maps are greater than zero for values of r in the range (0.5-4). However, RCM map has higher values of LE than that of JSMP map for all values of r. JSMP has some negative values when the value of control parameter is low.

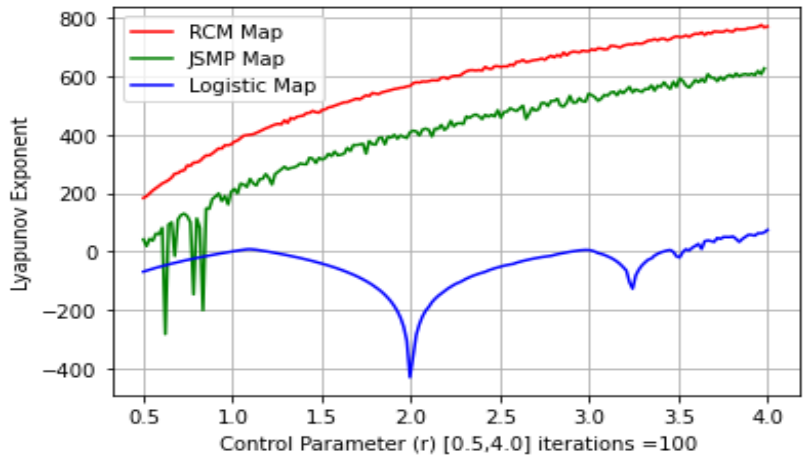

Figure 6: Lyapunov Exponent of RCM, JSMP and Logistic map

In order to verify what happens if the value of r exceeds 4. The range of r is increased to 25 for the three maps and the LE's were determined in each case. The graphs in Figure 7 shows the results of this experiment. As can be seen from Figure 7, the LE's of RCM and JSMP maps kept increasing while RCM still maintains highest LE's for all values of r.

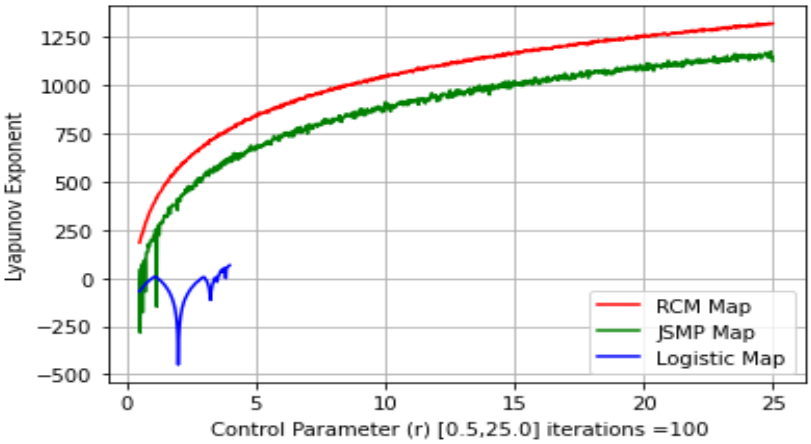

Figure 7: Lyapunov Exponent of RCM, JSMP and Logistic map when r is 25

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

In order to verify the effect of increasing number of iterations when the value of r is constant, an experiment where the number of iterations are varied while a constant value of control parameter r is used was conducted. In this experiment r = 3.7 was used as control parameter and the number of iterations were varied from from 1 to 100. The results of the experiment is shown in Figure 8. From the graphs in Figure 8, it can be seen that the higher the number of iterations the higher the values of LE. In all cases of iteration values, RCM have the highest value of LE.

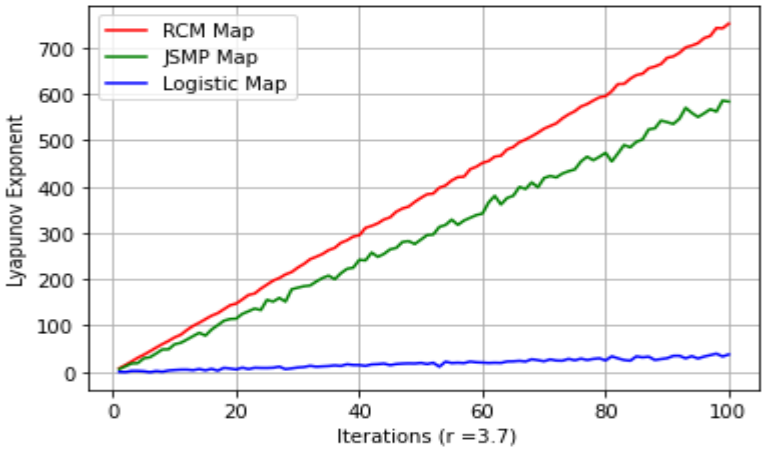

Figure 8: Lyapunov Exponent of RCM, JSMP and Logistic map when r is 3.7

These results show that RCM mapping has higher unpredictability and sensitivity than those of JSMP and traditional logistic maps. Hence, RCM has higher chaos performance.

Sequence Diagram

Sequence diagram was used to examine the sensitivity of RCM, JSMP, and traditional logistic map to the initial value. For each of the chaotic map, two sequence diagrams with different initial values 0.2 and 0.20000000000001 were compared. Figure 9 illustrates how minor changes in initial values affect the dynamic behavior of RCM and JSMP while there are no significant changes in the sequence diagram of the traditional logistic map. The chaotic properties of both RCM and JSMP are sensitive to insignificant changes, which implies that RCM and JSMP maps are highly dependent on the initial value.

The results of the evaluation of RCM revealed that range of control parameter that can be used is far more than that of the existing logistic map, the Lyapunov exponent of RCM is better than those of JSMP and logistic maps, and the sequence diagram showed that RCM is sensitive to small changes in initial value. These results show that the developed

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

RCM is capable of producing computationally secured pseudorandom sequence which can be very useful in cryptography.

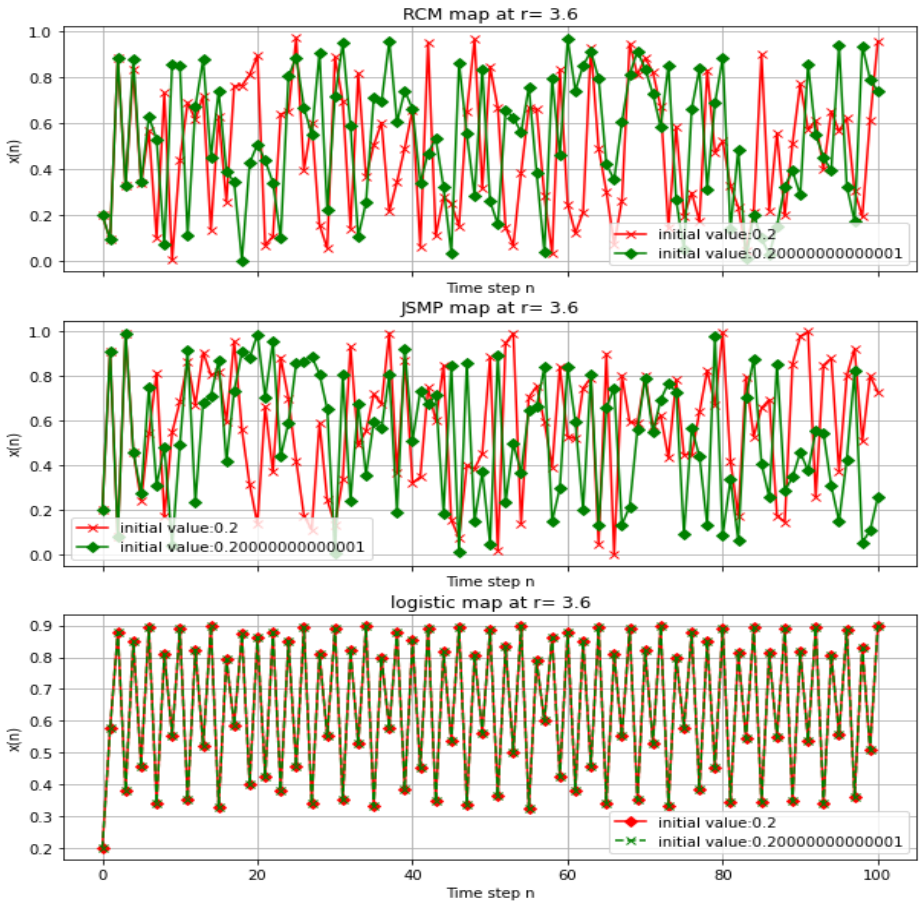

Figure 9: Sequence Diagram of RCM, JSMP and Logistic Map.

Conclusion, Summary and Future Work

This study has demonstrated the effectiveness of the proposed RCM as a foundation for developing a robust text-based public key cryptosystem. By leveraging the complementary nonlinear characteristics of both logistic and quadratic maps, the proposed scheme enhances randomness, unpredictability, and sensitivity to initial conditions, which are essential properties for cryptographic security. The utilization of bifurcation diagrams provided valuable insights into the system's dynamical behavior, illustrating a wider range of chaotic regimes when compared to the individual maps. This ensured a broader key space and minimized vulnerability to structural weaknesses associated with single chaotic functions.

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Furthermore, the Lyapunov exponent analysis confirmed the RCM's strong chaotic nature, as indicated by positive exponents across diverse parameter ranges. This result emphasizes the system's sensitivity to initial conditions and supports its resistance against differential and brute-force attacks. Similarly, the examination of sequence diagrams highlighted the pseudo-random nature of the generated keystreams, demonstrating uniform distribution and low correlation, which are critical for achieving high-quality encryption sequences.

In summary, the proposed RCM addresses the limitations of each individual map by combining their strengths into a more secure and versatile cryptographic framework. The inclusion of dynamical system analyses via bifurcation, Lyapunov, and sequence metrics provides strong theoretical and empirical validation of its security potential. Future research may focus on optimizing the algorithm for computational efficiency, testing its resilience against advanced cryptanalytic techniques, and extending its application to multimedia encryption and other domains requiring lightweight yet secure public key cryptographic solutions.

References

Abd El-Latif, A. A., Abd-El-Atty, B., Amin, M., & Iliyasu, A. M. (2020). Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications. *Scientific Reports*, *10*(1), 1930. https://doi.org/10.1038/s41598-020-58636-w

Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos*, *16*(08), 2129–2151. https://doi.org/10.1142/S0218127406015970

Bos, J. W., Halderman, J. A., Heninger, N., Moore, J., Naehrig, M., & Wustrow, E. (2014). Elliptic curve cryptography in practice. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8437*, 157–175. https://doi.org/10.1007/978-3-662-45472-5_11

Crowie, J., Dodson, B., Elkenbracht-Huizing, R., Lenstras, A., Montgomery, P., & Zayer, J. (1996). A world wide number field sieve factoring record: On to 512 bits. *IAdvances in Cryptology ASIACRYPT '96*, 382–394.

Gordon, D. (1993). Discrete logarithms in GF(p) using the number field sieve. *SIAM J. Discr. Math.*, *6*, 124–138.

Jangir, R., Yadav, R., & Jangir, R. (2021). Design of new hybrid chaotic map and its application in secure communication. *Journal of Information Security and Applications*, *80*(8), 11819–11838. https://doi.org/10.1007/s11042-020-09965-2

Kanso, A., & Smaoui, N. (2009). Logistic chaotic maps for binary numbers generations. *Chaos, Solitons & Fractals*, *40*(5), 2557–2568. https://doi.org/10.1016/j.chaos.2007.10.040

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, *48*(177), 201–209.

Kocarev, L. (2001). Chaos-based cryptography: A brief overview. *IEEE Circuits and Systems Magazine*, *1*(3), 6–21. https://doi.org/10.1109/7384.963463

Kumar, R., & Singh, A. (2019). A survey on hybrid chaotic maps and their cryptographic applications. *International Journal of Computer Applications*, *178*(21), 25–30. https://doi.org/https://doi.org/10.5120/ijca2019918620

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Li, Y., Xu, X., & Zhao, Y. (2022). Dynamical analysis of hybrid chaotic systems and their application in secure communication. *Chaos, Solitons & Fractals*, *154*, 111634. https://doi.org/https://doi.org/10.1016/j.chaos.2021.111634

Lucca, A. V., Augusto, G., Sborz, M., Reis, V., Leithardt, Q., Beko, M., Zeferino, C. A., & Parreira, W. D. (2021). *A Review of Techniques for Implementing Elliptic Curve Point Multiplication on Hardware*.

Luo, Y., Yu, J., Lai, W., & Liu, L. (2019). A novel chaotic image encryption algorithm based on improved baker map and logistic map. *Multimed Tools Appl*, *78*, 22023–22043. https://doi.org/10.1007/s11042-019-7453-3

Ramadan, N., Eldin, H., Ahmed, H., Elkhamy, S. E., & Abd El-Samie, F. E. (2016). Chaos-Based Image Encryption Using an Improved Quadratic Chaotic Map. *American Journal of Signal Processing*, *6*(1), 1–13. https://doi.org/10.5923/j.ajsp.20160601.01

Rivest, R. L., Shamir, A., & Adleman, L. M. (2019). A method for obtaining digital signatures and public key cryptosystems. In *Secure Communications and Asymmetric Cryptosystems* (pp. 217–239). https://doi.org/10.7551/mitpress/12274.003.0047

Sakiyama, K., Mulder, E. De, Preneel, B., & Verbauwhede, I. (2006). A PARALLEL PROCESSING HARDWARE ARCHITECTURE FOR ELLIPTIC CURVE CRYPTOSYSTEMS. *ICASSP 2006*, 904–907.

Strogatz, S. H. (2018). *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering* (Https://www.taylorfrancis.com/books/mono/10.1201/9780429492563/nonlinear-dynamics-chaos-steven-strogatz (ed.); 2nd Edition). CRC Press. https://doi.org/https://doi.org/10.1201/9780429492563

Wang, P., Bao, H., & Liu, J. (2021). On the stability and chaos of hybrid discrete-time systems. *Nonlinear Dynamics*, 1231–1247. https://doi.org/https://doi.org/10.1016/j.chaos.2021.111634

Zhang, Q., & Chen, G. (2020). Computational cost and dynamical features of chaotic map hybridization in digital cryptosystems. *IEEE Access*, *8*, 66432–66444. https://doi.org/https://doi.org/10.1109/ACCESS.2020.2985601

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]