I. J. Mathematical Sciences and Computing, **2026, 1, 17-28**
Published Online on February 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijmsc.2026.01.02

A Novel RSA Cryptosystem Variant Using Chaotic Exponent Selection and Ciphertext Blinding

Arshi Fatima
Department of Mathematics, School of Basic Sciences, CSJM University Kanpur, India
E-mail: arshianees29@gmail.com
ORCID iD: https://orcid.org/0009-0005-3403-342X

Namita Tiwari*
Department of Mathematics, School of Basic Sciences, CSJM University Kanpur, India
E-mail: namitatiwari@csjmu.ac.in
ORCID iD: https://orcid.org/0000-0002-9039-5696
*Corresponding Author

Received: 14 May, 2025; Revised: 22 September, 2025; Accepted: 20 January, 2026; Published: 08 February, 2026

Abstract: This paper presents an enhanced variant of the RSA cryptosystem that integrates chaotic exponent selection and ciphertext blinding to address security limitations inherent in classical RSA. Traditional RSA relies on a fixed public exponent, which generates predictable encryption patterns and increases exposure to exponent-based attacks. In the proposed scheme, the encryption exponent is dynamically derived from a logistic-map–based chaotic sequence, introducing high sensitivity to initial conditions and producing session-dependent exponent values. This chaotic exponentiation increases unpredictability without modifying the established RSA framework. Additionally, a ciphertext blinding factor is incorporated to prevent deterministic outputs and strengthen resistance against chosen-ciphertext and side-channel attacks. The paper outlines the mathematical background of the logistic map, details the complete encryption and decryption procedures, and demonstrates the correctness of the method through a numerical example using small primes. A theoretical security analysis shows that the combined effects of chaotic exponent selection and blinding significantly improve resistance to key-related attacks while maintaining compatibility with the original RSA structure. These enhancements offer a lightweight and practical improvement to RSA for environments requiring increased confidentiality and unpredictability in exponent selection.

Index Terms: RSA Cryptosystem, Chaotic Maps, Logistic Map, Dynamic Exponentiation, Ciphertext Blinding, Public-Key Cryptography, Cryptographic Security

1. Introduction

The RSA cryptosystem remains one of the most widely used public-key schemes for secure communication, relying on the computational hardness of integer factorization. However, classical RSA exhibits structural limitations, particularly due to its use of a fixed public exponent, which results in deterministic ciphertexts and increases susceptibility to pattern-based attacks, small-exponent attacks, and certain side-channel techniques. As modern cryptographic environments demand greater randomness and non-determinism, several researchers have sought lightweight modifications to enhance RSA without altering its core mathematical foundation.

Chaos theory offers one such direction. Chaotic maps exhibit sensitivity to initial conditions, non-linearity, and ergodicity, producing high-entropy sequences suitable for cryptographic use. Motivated by these characteristics, this work introduces a dynamic exponent selection mechanism based on the logistic map, enabling the encryption exponent to vary across sessions rather than remain constant.

In addition, RSA's deterministic nature makes it vulnerable to chosen-ciphertext and replay attacks. To address this issue, the proposed scheme incorporates a simple multiplicative blinding factor, ensuring that identical messages no longer produce identical ciphertexts. Together, chaotic exponent selection and ciphertext blinding provide enhanced unpredictability while maintaining full compatibility with traditional RSA operations.

This paper presents the mathematical background of the logistic map, formulates the complete algorithm for exponent generation and ciphertext blinding, demonstrates decryption correctness, and provides a detailed theoretical security analysis. The proposed method aims to strengthen unpredictability and limit structural attack surfaces, offering a lightweight enhancement to classical RSA.

1.1. Motivation

The development of our proposed scheme was guided by a detailed evaluation of existing RSA variants and the need to enhance its security without sacrificing efficiency. Several earlier works have demonstrated that RSA can be strengthened by optimizing arithmetic operations or introducing new structural components.

Liu et al. [1] showed that splitting plaintext and applying multi-key encryption with GPU parallelization can significantly reduce execution time. This revealed the advantages of modular computation, which inspired the session-based handling approach in our design.

Further contributions by Wu et al. and Verma [2,3] demonstrated that the use of high-radix Montgomery multipliers and multi prime RSA considerably improves decryption efficiency. These results reinforced our goal of maintaining computational practicality while integrating new security layers.

Rawat et al. [4] and Paixao Filho [5] presented scalable RSA architectures and hybrid implementations that retain classical RSA compatibility. Their findings suggested that security-enhancing modifications should not disrupt RSA's original structure—a principle we adopted.

In addition, Sehgal et al. [6] explored efficient hardware implementations of RSA, indicating that the algorithm can be engineered flexibly without reducing its deployability.

The most crucial inspiration came from chaos theory. Çavuşoğlu et al. [7] demonstrated the usefulness of chaos based random number generators for increasing key unpredictability in RSA. This motivated our adoption of chaotic logic for exponent generation. Similarly, Wang and Zhang [8] successfully integrated chaotic maps with RSA for secure applications such as image encryption, supporting the feasibility of combining chaos with the established RSA framework.

Collectively, these studies shaped the foundation of our proposed algorithm, motivating us to combine logistic map–based chaotic exponent selection with ciphertext blinding to enhance entropy, strengthen resistance to analysis-based attacks, and preserve classical RSA compatibility.

1.2. Objectives

The primary objective of the proposed scheme is to enhance the security of the classical RSA cryptosystem by introducing controlled randomness and non-determinism into its core operations, while ensuring that the fundamental mathematical structure of RSA remains intact. The chaotic exponent selection mechanism is designed to generate a dynamic, session-wise public exponent rather than relying on a fixed or commonly used value. This improves resistance against pattern-based attacks, small-exponent attacks, and adversaries attempting to exploit repeated exponent usage.

Another key objective is to integrate a ciphertext blinding factor into the encryption process. This provides an additional security layer by ensuring that identical plaintexts never produce identical ciphertexts, thereby mitigating chosen plaintext, adaptive chosen-plaintext, and replay-based attacks. Blinding also contributes to making decryption traces more resistant to side-channel leakage.

Moreover, the proposed system aims to increase output entropy and expand the attack surface complexity without introducing significant computational overhead. Although chaotic iteration and blinding add extra steps, these operations are lightweight and compatible with standard RSA arithmetic. The design therefore focuses on strengthening security while maintaining practical feasibility for real-world implementation.

Finally, the overall objective is to provide a theoretically sound variant of RSA that offers improved unpredictability, non-determinism, and robustness against several known cryptanalytic techniques. The scheme preserves compatibility with traditional RSA frameworks, ensuring that it can be adopted without major structural or infrastructural modifications.

2. Mathematical Background

This section provides the mathematical foundations required to understand the proposed chaotic–blinded RSA variant. The scheme is based on classical RSA arithmetic while incorporating two additional components: a chaotic map for dynamic exponent generation and a multiplicative blinding factor for ciphertext randomization.

2.1. Classical RSA Framework

The classical RSA scheme was introduced in 1978 by Rivest, Shamir, and Adleman [9]. For foundational mathematical and implementation details, see also [10].

RSA relies on the hardness of factoring a composite modulus. Two large primes p and q are chosen and used to compute

$$n = pq, \qquad \varphi(n) = (p-1)(q-1) \tag{1}$$

A public exponent e is selected such that gcd(e,$\varphi(n)$) = 1, and the private exponent d is computed from

$$ed \equiv 1 \ (mod \ \varphi(n)). \tag{2}$$

Encryption and decryption follow the standard operations:

$$C \equiv m^e \ (\text{mod } n), \qquad m \equiv C^d \ (\text{mod } n), \tag{3}$$

where m denotes the plaintext and C the ciphertext.

The security of RSA depends on the computational difficulty of recovering d from (n, e) without factoring n; however, the use of fixed, small, or predictable public exponents introduces attack surfaces exploited in several classical attacks. This motivates the development of a dynamic exponent generation mechanism.

2.2. Chaotic Map for Exponent Generation [11]

Chaos theory and the logistic map exhibit sensitivity to initial conditions, topological mixing, and ergodicity [11]. Chaotic maps have been widely studied for cryptographic entropy generation [12].

To introduce unpredictability, the proposed method uses the logistic map, a classical nonlinear system defined by

$$y_{t+1} = r y_t (1 - y_t), \tag{4}$$

with control parameter r chosen in the chaotic region $3.9 \leq r \leq 4.0$. For initial value $y_0 \in (0,1)$, the sequence $\{y_t\}$ exhibits:

- Sensitivity to Initial Conditions: small changes in y_0 cause exponential divergence of the trajectory.
- Ergodicity: the values cover the interval (0,1) densely.
- Non-periodicity: the sequence does not repeat or fall into short cycles.

A session-specific exponent e_t is generated by mapping the final (or averaged) chaotic value using a linear transformation:

$$e_t = (\text{offset} + \text{scale} \cdot y_t) \bmod \varphi(n), \tag{5}$$

followed by adjusting e_t until

$$\text{gcd}(e_t, \varphi(n)) = 1. \tag{6}$$

This ensures that the exponent is valid for RSA while being highly unpredictable and non-repeating across sessions.

2.3. Ciphertext Blinding

To eliminate RSA's deterministic behaviour, a multiplicative blinding factor is incorporated. A random value $B \epsilon \ \mathbb{Z}_n^*$ is selected such that $\text{gcd}(B, n) = 1$, and its modular inverse is computed:

$$B^{-1} \ (\text{mod } n). \tag{7}$$

During encryption, the blinded ciphertext is obtained as:

$$C' \equiv (m^{e_t} \cdot B) \ (\text{mod } n). \tag{8}$$

During decryption, the blinding is removed by multiplying with B^{-1}:

$$m'' \equiv (C' \cdot B^{-1}) \ (\text{mod } n), \tag{9}$$

after which the standard RSA decryption yields the original message:

$$m \equiv (m'')^d \ (\text{mod } n). \tag{10}$$

Blinding ensures semantic security by guaranteeing that identical plaintexts never lead to identical ciphertexts, thereby mitigating chosen-ciphertext and pattern-based attacks.

3. Proposed Algorithm

This section presents the complete workflow of the proposed chaotic–blinded RSA scheme. The algorithm retains the structural foundation of classical RSA while incorporating (i) a chaotic map for dynamic exponent generation and (ii) a ciphertext blinding mechanism for non-deterministic encryption.

3.1. Key Generation

1. Prime Selection: Choose two large primes p and q, and compute

$$n = pq, \qquad \varphi(n) = (p-1)(q-1). \tag{11}$$

2. Chaotic Exponent Generation: Select an initial seed $y_0 \in (0,1)$ and chaotic parameter $r \in [3.9,4.0]$. Iterate the logistic map

$$y_{t+1} = r y_t (1 - y_t) \tag{12}$$

for a fixed number of iterations to obtain the value x_t.
Map the chaotic output to an exponent:

$$e_t = (\text{offset} + \text{scale} \cdot y_t) \bmod \varphi(n). \tag{13}$$

If $\gcd(et, \varphi(n)) = 1$, repeat the mapping until a valid exponent is obtained.

3. Private Key Computation: Compute the private exponent d as the modular inverse of e_t:

$$e_t d \equiv 1 \pmod{\varphi(n)}. \tag{14}$$

Blinding Factor: Choose a random $B \epsilon \mathbb{Z}_n^*$ with $\gcd(B, n) = 1$. Compute its inverse:

$$B^{-1} \equiv B^{-1} \pmod{n}. \tag{15}$$

3.2. Encryption

For a plaintext message $m \in Z_n$:

1. Compute the chaotic RSA ciphertext component:

$$m' \equiv m^{e_t} \pmod{n}. \tag{16}$$

2. Apply ciphertext blinding:

$$C \equiv (m' \cdot B) \pmod{n}. \tag{17}$$

3.3. Decryption

1. Remove the blinding factor:

$$m'' \equiv (C \cdot B^{-1}) \pmod{n}. \tag{18}$$

2. Recover the original plaintext:

$$m \equiv (m'')^d \pmod{n}. \tag{19}$$

3.4. Algorithm Demonstration

A small numerical example is provided to demonstrate correctness.

Step 1: Key Generation

- Choosing $p = 7, q = 13$ we have $n = 91, \varphi(n) = 72$.
- Chaotic Exponent Generation: Use the logistic map with

$$r = 3.9, \qquad x_0 = 0.5.$$

Iterate for five steps:

$$x_1 = 3.9 \cdot 0.5 \cdot (1 - 0.5) = 0.975,$$
$$x_2 = 3.9 \cdot 0.975(1 - 0.975) = 0.09506,$$
$$x_3 = 3.9 \cdot 0.09506(1 - 0.09506) \approx 0.33541,$$
$$x_4 = 3.9 \cdot 0.33541(1 - 0.33541) \approx 0.86973,$$
$$x_5 = 3.9 \cdot 0.86973(1 - 0.86973) \approx 0.44223.$$

Map the final chaotic output:

$$e_t = (7 + 1000 \cdot 0.44223) \bmod 72 = 17.$$

Since gcd(17,72) = 1, et is valid.

- Private exponent:

$$17d \equiv 1 \pmod{72} \quad \Rightarrow \quad d = 17.$$

- Blinding factor: Choose B = 4 with $B^{-1} \equiv 23\ (mod\ 91)$.

Step 2: Encryption

$$m = 45$$

Chaotic RSA component:

$$m' = 4517\ mod\ 91 = 89.$$

Apply blinding:

$$C = 89 \cdot 4\ mod\ 91 = 83.$$

Step 3: Decryption

Remove blinding:

$$m'' = 83 \cdot 23\ mod\ 91 = 89.$$

Final plaintext:

$$m = 89^{17} \bmod 91 = 45.$$

The example verifies the correctness of the proposed method.

3.5. Correctness of the Proposed Algorithm

The correctness of the decryption process follows directly from the blinding structure and the classical RSA identity. Starting from the blinded ciphertext:

$$C \equiv m' \cdot B \pmod{n}, \qquad m' \equiv m^{e_t} \pmod{n}. \tag{20}$$

During decryption, the blinding factor is removed:

$$m'' \equiv C \cdot B^{-1} \pmod{n} \equiv (m' \cdot B) \cdot B^{-1} \pmod{n} \equiv m' \pmod{n}. \tag{21}$$

The final decryption step computes:

$$m \equiv (m'')^d \pmod{n} \equiv (m^{e_t})^d \pmod{n}. \tag{22}$$

Since the exponents satisfy the RSA condition

$$e_t d \equiv 1 \pmod{\varphi(n)}, \tag{23}$$

there exists an integer k such that:

$$e_t d = 1 + k\varphi(n). \tag{24}$$

Thus,

$$m^{e_t d} \equiv m^{1+k\varphi(n)} \pmod{n} \equiv m \cdot (m^{\varphi(n)})^k \pmod{n}. \tag{25}$$

By Euler's theorem $m^{\varphi(n)} \equiv 1 \pmod{n}$ for all $m \in \mathbb{Z}_n^*$ we obtain:

$$m^{e_t d} \equiv m \cdot 1^k \equiv m \pmod{n}. \tag{26}$$

Therefore,

$$\boxed{m \equiv (m'')^d \pmod{n}} \tag{27}$$

4. Security and Proofs

4.1. Exponent Unpredictability and Entropy

Chaotic systems with $r \approx 4.0$ are known to have a positive Lyapunov exponent, indicating exponential divergence [11]. This property directly supports the unpredictability of e_t.

Theorem 1. Let the sequence $\{y_t\}$ be generated by the logistic map

$$y_{t+1} = r y_t (1 - y_t), \quad r \in [3.9, 4.0], \tag{28}$$

and let the RSA exponent be generated as

$$e_t = \lfloor \alpha + \beta y_t \rfloor \bmod \varphi(n). \tag{29}$$

Then predicting e_t without knowledge of (y_0, r) is computationally infeasible.

Proof. The logistic map in the chaotic regime has Lyapunov exponent

$$\lambda = \ln|r(1 - 2y)| > 0, \tag{30}$$

so an initial perturbation Δy_0 grows as

$$|\Delta y_t| \approx e^{\lambda t} |\Delta y_0|. \tag{31}$$

Because double-precision gives $|\Delta y_0| < 2^{-53}$, after $t \geq 5$ iterations,

$$|\Delta y_t| > 2^{-10}. \tag{32}$$

Therefore, the values of e_t differ significantly, even for microscopic differences in the seed. Hence e_t is unpredictable and exhibits high entropy.

4.2. Resistance to Fixed-Exponent and Continued-Fraction Attacks

Theorem 2. Let e_t be derived chaotically as above. Then the probability that the corresponding private exponent satisfies $d < n^{0.25}$ is negligible, and continued-fraction attacks do not apply [13].

Proof. Since

$$d \equiv e_t^{-1} \pmod{\varphi(n)}, \tag{33}$$

and e_t spans a wide, well-distributed range of $\mathbb{Z}_{\varphi(n)}^*$, the induced distribution of d is uniform over the multiplicative group. Thus,

$$\Pr[d < n^{0.25}] = \frac{n^{0.25}}{\varphi(n)} \to 0 \tag{34}$$

as $n \to \infty$. Therefore Wiener-style and related attacks fail [14].

4.3. Non-Deterministic Encryption via Multiplicative Blinding

Deterministic RSA leakage is well-understood in cryptanalytic literature [15] .

Theorem 3. Let $m \in \mathbb{Z}_n^*$. For two independent encryptions,

$$C_1 = m^{e_t} B_1 \pmod{n}, \qquad C_2 = m^{e_t} B_2 \pmod{n}, \tag{35}$$

where $B_1, B_2 \leftarrow \mathbb{Z}_n^*$. Then

$$\Pr[C_1 = C_2] = \frac{1}{|\mathbb{Z}_n^*|} \approx 0. \tag{36}$$

Proof.

$$C_1 = C_2 \Leftrightarrow B_1 \equiv B_2 \pmod{n}. \tag{37}$$

Since B_1, B_2 are uniform over the multiplicative group, the equality holds with negligible probability. Hence encryptions of identical messages are distinct.

4.4. Preservation of RSA Hardness

Theorem 4. The proposed scheme does not reduce the hardness of RSA: recovering m from

$$C' = m^{e_t} B \pmod{n} \tag{38}$$

is computationally equivalent to breaking classical RSA.
Proof. Multiplying C' by B^{-1} yields

$$C' B^{-1} \equiv m^{e_t}. \tag{39}$$

Recovering m requires computing

$$m = (m^{e_t})^d \pmod{n}, \tag{40}$$

where $e_t d \equiv 1 \pmod{\varphi(n)}$. Thus all security reduces to the classical RSA inversion problem and, ultimately, to factoring n.

4.5. Necessity and Effectiveness of Ciphertext Blinding

The use of ciphertext blinding is essential because classical RSA is fully deterministic:

$$C = m^e \pmod{n}, \tag{41}$$

so identical plaintexts always produce identical ciphertexts. This determinism leaks structural information and enables several practical attacks, including:

- Chosen-plaintext attacks (CPA): An attacker can test whether a guessed message matches a ciphertext by simply encrypting the guess and comparing outputs.
- Adaptive chosen-plaintext attacks: Repeated encryption queries allow reconstruction of patterns or partial information about the plaintext.
- Side-channel leakage: Deterministic ciphertexts make timing and power patterns easier to correlate across multiple encryptions of the same message.

To eliminate this vulnerability, a random blinding factor $B \in \mathbb{Z}_n^*$ is introduced:

$$C' \equiv m^{e_t} \cdot B \pmod{n}. \tag{42}$$

Because B is freshly chosen each session, the probability that two encryptions of the same message yield the same ciphertext is negligible:

$$\Pr[C_1' = C_2'] \approx \frac{1}{|\mathbb{Z}_n^*|}. \tag{43}$$

This ensures that encryption becomes non-deterministic, message patterns cannot be inferred, replay, CPA, and adaptive CPA attacks are neutralized and deblinding is efficient using $B^{-1} \pmod{n}$. Its security benefit is significant and complements chaotic exponent selection by removing all deterministic leakage from the ciphertext.

5. Efficiency Analysis

5.1. Asymptotic Computational Complexity

Classical RSA encryption with exponent *e* requires

$$O(\log e) \cdot M(k) \tag{44}$$

where $M(k)$ is the cost of multiplication on k −bit integers. The proposed scheme adds:

- logistic-map iteration: $T = O(1)$
- one modular multiplication: $O(k^2)$

Therefore,

$$T_{\text{proposed}} = T_{\text{RSA}} + O(k^2), \tag{45}$$

and since exponentiation dominates at $O(k^3)$,

$$\frac{O(k^2)}{O(k^3)} = O\left(\frac{1}{k}\right), \tag{46}$$

the overhead becomes negligible for large key sizes. The asymptotic complexity results follow standard RSA analyses [10].

5.2. Chaotic Exponent Generation Cost

The logistic map requires *T* iterations with constant-time arithmetic:

$$T_{\text{chaos}} = O(1). \tag{47}$$

Mapping to $e_t = \lfloor \alpha + \beta x_t \rfloor$ requires integer operations:

$$T_{e_t} = O(k^2). \tag{48}$$

5.3. Cost of Multiplicative Blinding

Blinding modifies the ciphertext as

$$C' = m^{e_t} B \pmod{n}, \tag{49}$$

which is a single modular multiplication:

$$O(k^2). \tag{50}$$

De-blinding during decryption adds another multiplication of the same complexity.

5.4. Scalability with Respect to Key Size

Because chaos iteration is constant-time and blinding involves only one multiplication, the additional work grows as

$$O(k^2),$$

while RSA exponentiation grows as $O(k^3)$. Therefore,

$$\lim_{k \to \infty} \frac{T_{\text{proposed}} - T_{\text{RSA}}}{T_{\text{RSA}}} = 0, \tag{51}$$

demonstrating excellent scalability for large key sizes.

5.5. Efficiency Comparison

To provide a clearer and more realistic performance perspective, the proposed chaotic–exponent RSA scheme is compared against both classical RSA and RSA–OAEP, which is a widely deployed randomized variant used in practical applications. RSA–OAEP introduces padding overhead but significantly improves semantic security. Our proposed scheme achieves non-determinism and enhanced security without the computational cost of padding-based constructions.

Table 1. Efficiency comparison among Classical RSA, RSA–OAEP, and Proposed Scheme

Component	Classical RSA [9]	RSA–OAEP [16]	Proposed Scheme
Key Generation	$O(k^3)$	$O(k^3)$	$O(k^3)$
Encryption Cost	$O(k^3)$	$O(k^3) + O(k)$ (padding)	$O(k^3) + O(k^2)$ (chaos +blinding)
Decryption Cost	$O(k^3)$	$O(k^3)$	$O(k^3) + O(k^2)$
Randomization	None	Yes (OAEP padding)	Yes (chaotic exponent +blinding)
Security Strength	Deterministic	High semantic security	High unpredictability and randomness
Overhead	0	Hashing/padding	One multiplication + chaos iteration

Table 2. Comparison with other RSA enhancements

Method	Goal	Extra Cost	Features Added
Multiprime RSA [17]	Faster decryption	Key generation complexity	Performance improvement
Rebalanced RSA [18]	Faster decryption	Weaker public exponent	Decryption optimization
RSA–OAEP [16]	CCA-security	Hashing operations	Padding based non- determinism
Proposed Scheme	Security + randomness	1 multiplication + chaos	Dynamic exponent +blinding

6. Conclusion and Future Work

This work introduced a strengthened variant of the RSA cryptosystem that integrates two lightweight but effective enhancements: chaotic exponent selection and ciphertext blinding. The proposed design preserves full compatibility with classical RSA while mitigating key structural limitations associated with fixed-exponent usage and deterministic encryption. By generating session-wise exponents through a logistic-map–based chaotic process and incorporating a multiplicative blinding factor, the scheme significantly increases exponent unpredictability, ciphertext entropy, and resistance to pattern-based cryptanalysis.

The theoretical analysis demonstrates that the chaotic exponent exhibits high sensitivity to initial conditions, ensuring non-repeatability and reducing the feasibility of structural attacks linked to exponent reuse. Likewise, ciphertext blinding eliminates RSA's determinism and introduces built-in randomness without compromising correctness. The efficiency study confirms that the additional computational overhead remains lightweight—bounded by a single modular multiplication. Overall, the proposed chaotic–blinded RSA framework offers a practical, efficient, and deployable enhancement to classical RSA, delivering stronger unpredictability and improved resilience against several conventional attack vectors while retaining the simplicity and established security foundations of RSA.

Future Work

Several research directions arise from this study:

- Alternative chaotic systems: Exploring higher-dimensional or coupled chaotic maps (such as Henon, Ikeda, or piecewise-linear systems) may further enhance exponent entropy and dynamic behaviour.
- Hardware-level evaluation: Implementing the scheme on embedded and IoT platforms would provide practical insights into timing behaviour, energy efficiency, and real-world side-channel resistance.
- Formal security characterization: Developing reduction-based proofs and simulation-based models would strengthen the theoretical security foundations of the scheme under contemporary cryptographic frameworks.
- Hybrid cryptographic constructions: Integrating the chaotic RSA approach with modern lattice-based or post-quantum primitives may yield complementary hybrid systems that retain RSA compatibility while improving robustness against emerging computational threats.
- Extended performance profiling: Large-scale testing using 4096-bit and 8192-bit moduli, as well as GPU-accelerated implementations, would help characterize long-term scalability and deployment feasibility.

These directions collectively aim to expand the analytical depth, implementation scope, and future readiness of the proposed chaos-enhanced RSA framework.

Appendix: Extended Numerical Demonstration (32-bit scale)

This appendix provides a full worked demonstration of the proposed chaotic-exponent RSA variant using two 32 bit- scale primes. All numeric outputs below were produced by the attached reproducible Python script; these values can be verified by running the same script locally or in any standard Python 3 environment.

Parameters

- $p = 1789368727.$
- $q = 1282648399.$
- $n = p \times q = 2295130932907218073.$
- $\varphi(n) = (p-1)(q-1) = 2295130929835200948.$

.

Chaotic exponent generation (logistic map)

We used logistic-map parameters:

- seed $x_0 = 0.6180339887,$
- control parameter $r = 3.99,$
- iterations $T = 7.$

The iterates produced (rounded to 10 decimal digits) were:

$$x_1 = 0.9419112303$$
$$x_2 = 0.2183107136$$
$$x_3 = 0.6808980722$$
$$x_4 = 0.8669307910$$
$$x_5 = 0.4602935606$$
$$x_6 = 0.9912093607$$
$$x_7 = 0.0347663222$$

The final logistic value x_T (used for mapping) is 0.46270862231801596.
We mapped the chaotic output to an exponent using:

$$e_T = (\text{offset} + \lfloor \text{scale} \cdot x_T \rfloor) \bmod \varphi(n) \tag{52}$$

Using offset $= 3$ and scale = 1000000000 the derived exponent is:

- $e = 462708625.$

Key computation

Compute modular inverse d such that $ed \equiv 1 \pmod{\varphi(n)}$:

- $d = 900864009787456001.$

Encryption and blinding

Let plaintext message m = 123456789. The chaotic encryption yields:

- $m' = m^e \bmod n = 1385732106490630125.$
- choose blinding factor B = 998283070589756339 (with $\gcd(B, n) = 1$).
- blinded ciphertext $C = m' \cdot B \bmod n = 2123840253022621798.$

Deblinding and decryption

- $B^{-1} \bmod n = 357070359741707395.$
- remove blinding: $m'' = C \cdot B^{-1} \bmod n = 1385732106490630125$
- recover plaintext: $m_{\text{recovered}} = (m'')^d \bmod n = 123456789$

The recovered plaintext matches the original message, verifying correctness.

References

[1] Jun-Jie Liu, Kang-Too Tsang, and Yu-Hui Deng. A variant rsa acceleration with parallelisation. *International Journal of Parallel, Emergent and Distributed Systems*, 37(3):318–332, 2022.

[2] Tao Wu, ShuGuo Li, and LiTian Liu. Fast rsa decryption through high-radix scalable montgomery modular multipliers. *Science China. Information Sciences*, 58(6):1–16, 2015.

[3] Seema Verma. Rsa variant with improved computational performance and memory usage. *International Journal of Sensors Wireless Communications and Control*, 7(3):211–225, 2017.

[4] Abhishek Rawat, Kartik Sehgal, Amartya Tiwari, Abhishek Sharma, and Ashish Joshi. A novel accelerated implementation of rsa using parallel processing. *Journal of Discrete Mathematical Sciences and Cryptography*, 22(2):309–322, 2019.

[5] CAM Paixao Filho. Dlg: An efficient variant of the rsa cryptosystem. *Eprint Archive*, 2003.

[6] Kamal Sehgal, Anurag Tiwari, and R K Bajaj. Fast and area efficient implementation of rsa algorithm. *Procedia Computer Science*, 152:198–205, 2019.

[7] Ü. Çavuşoğlu, A. Akgül, A. Zengin, and İ. Pehlivan, "The design and implementation of hybrid RSA algorithm using a novel chaos based RNG, "Chaos, Solitons & Fractals, vol. 104, pp. 655–667, 2017, doi: 10.1016/j.chaos.2017.09.025.

[8] Y. Wang, X. Leng, C. Zhang, and B. Du, "Adaptive fast image encryption algorithm based on three-dimensional chaotic system," Entropy, vol. 25, no. 10, Art. no. 1399, 2023, doi: 10.3390/e25101399.

[9] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[10] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[11] Robert M. May. Simple mathematical models with very complicated dynamics. *Nature*, 261(5560):459–467, 1976.

[12] Ljupco Kocarev. Chaos-based cryptography: A brief overview. *IEEE Circuits and Systems Magazine*, 1(3):6–21, 2001.

[13] Dan Boneh and Glenn Durfee. Cryptanalysis of rsa with private key d less than n0.292. 1592:1–11, 1999.

[14] M. Wiener. Cryptanalysis of short rsa secret exponents. In *Proceedings of CRYPTO '90*, pages 372–389, 1990.

[15] J. Kelsey, B. Schneier, and D. Wagner. Cryptanalytic attacks on pseudorandom number generators. In *Fast Software Encryption*, 1998.

[16] Mihir Bellare and Phillip Rogaway. Optimal asymmetric encryption: How to encrypt with rsa. pages 92–111, 1995.

[17] Dan Boneh and Hovav Shacham. Fast variants of rsa. *CryptoBytes*, 5(1), 2002.

[18] Michael Wiener. Rebalanced rsa. *Proceedings of the USENIX Security Symposium*, 1990.

Authors' Profiles

Arshi Fatima was born in Kanpur, India. She received her B.Sc. degree in Mathematics from Brahmanand College, Kanpur (affiliated to CSJM University Kanpur), India, in 2023, and her M.Sc. degree in Mathematics from CSJM University Kanpur, India, in 2025. Her major field of study is cryptography, with a focus on public key security and mathematical foundations of encryption.

She is currently engaged in research in Cryptography, where she is working on enhancing the RSA cryptosystem through chaotic exponent selection and ciphertext blinding techniques. Her research has resulted in the development of a lightweight chaos-based RSA variant suitable for secure communication environments, and her work has been submitted to peer-reviewed journals. Her research interests include number theory, cryptographic algorithms, chaotic maps, and mathematical security analysis.

Ms. Fatima aims to pursue doctoral studies in Cryptography and Mathematical Sciences. She is an active academic researcher and has participated in university-level research initiatives.

Namita Tiwari is associate professor and serving as join faculty in the Department of Mathematics, School of Basic Sciences and Department of Computer Application, University Institute of Technology, CSJMU Kanpur. She received her B.Sc. from CSJMU Kanpur in 2006, M.Sc. in Pure Mathematics from IIT Kanpur in 2008, and Ph.D. in Cryptography from MNNIT Allahabad in 2013. She also qualified CSIR-NET (AIR-81) and GATE (Mathematics). Her professional experience spans more than fifteen years, during which she has served in various academic positions at engineering institutions and universities. Her research interests include cryptography, elliptic-curve based digital signatures, proxy signatures, network security, and applications of machine learning in secure communication. She has authored several SCI/Scopus-indexed research papers, book chapters, and patents, and has presented her work at numerous international conferences.

Dr. Tiwari has delivered several invited lectures in cryptography, quantum computing, and mathematical modeling. She is a life member of the Cryptology Research Society of India (CRSI) and the Indian Society for Technical Education (ISTE). She has also contributed to organising national and international workshops, seminars, and conferences, and currently serves in multiple administrative roles at CSJMU Kanpur.

How to cite this paper: Arshi Fatima, Namita Tiwari, "A Novel RSA Cryptosystem Variant Using Chaotic Exponent Selection and Ciphertext Blinding", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.12, No.1, pp. 17-28, 2026. DOI: 10.5815/ijmsc.2026.01.02