Dual-Layer RSA–Paillier Encryption: Design and Evaluation Against Wiener Attacks

Dian Rachmawati
Department of Computer Science, Universitas Sumatera Utara, Medan, North Sumatra, Indonesia
dian.rachmawati@usu.ac.id (corresponding author)

Maya Silvi Lydia
Department of Computer Science, Universitas Sumatera Utara, Medan, North Sumatra, Indonesia
maya.silvi@usu.ac.id

Mohammad Andri Budiman
Department of Computer Science, Universitas Sumatera Utara, Medan, North Sumatra, Indonesia
mandrib@usu.ac.id

Romi Fadillah Rahmat
Department of Information Technology, Universitas Sumatera Utara, Medan, North Sumatra, Indonesia
romi.fadillah@usu.ac.id

Received: 11 March 2026 | Revised: 3 April 2026, 24 April 2026, and 4 May 2026 | Accepted: 8 May 2026

 DOI: https://doi.org/10.48084/etasr.18671

ABSTRACT

Standard RSA encryption is vulnerable to Wiener's continued fraction attack when the private exponent is small, and its deterministic nature limits semantic security. This paper proposes a dual-layer encryption framework that combines RSA with the Paillier probabilistic cryptosystem to address these limitations. The scheme independently encrypts each plaintext under both RSA and Paillier using separate key pairs, transmits the ciphertext pair, and accepts the message only when both decrypted values agree. Because RSA relies on the Integer Factorization Problem (IFP) whereas Paillier relies on the Decisional Composite Residuosity Assumption (DCRA), the two layers provide orthogonal security guarantees: breaking the dual-layer scheme requires compromising both the IFP-based RSA layer and the DCRA-based Paillier layer. A formal adversarial model with a reduction-based security analysis demonstrates that the scheme achieves Indistinguishability under Chosen-Plaintext Attack (IND-CPA) semantic security by inheritance from Paillier, but not Indistinguishability under Adaptive Chosen-Ciphertext Attack (IND-CCA2). It also provides improved resilience against Wiener's attack, chosen-ciphertext exploits, and side-channel leakage compared with standalone RSA. Experimental evaluation using a Python implementation with key sizes of 1,024–4,096 bits shows that dual-layer encryption with a 2,048-bit modulus completes in approximately 98.19 ms, decryption in 125.04 ms, and the ciphertext expansion factor is 3× relative to RSA alone. Comparative analysis against RSA-only, RSA–Optimal Asymmetric Encryption Padding (RSA–OAEP), Paillier-only, and recent hybrid frameworks demonstrates that the proposed scheme provides a practical security--performance trade-off suitable for high-assurance applications where resilience against key-recovery attacks is a primary requirement.

Keywords-RSA cryptosystem; Paillier cryptosystem; dual-layer encryption; hybrid cryptosystem; Wiener attack; continued fractions; homomorphic encryption; semantic security

I. INTRODUCTION

Public-key cryptography plays a crucial role in securing modern digital communication. The concept of asymmetric encryption was first introduced by authors in [1], leading to practical schemes such as RSA [2], which is widely used in applications including TLS/SSL, PGP, and digital certificates. However, the security of RSA depends heavily on proper parameter selection. Authors in [3] showed that RSA becomes vulnerable when the private exponent is too small, enabling key recovery through continued fraction analysis. This attack was further refined by authors in [4] and extended by authors in [5], whereas authors in [6] demonstrated that lattice-based techniques can compromise RSA even beyond the original bound established in [3].

In addition to these mathematical attacks, practical vulnerabilities have also been identified. Authors in [7]

revealed that deterministic RSA is susceptible to Chosen-Ciphertext Attacks (CCAs), and authors in [8] showed that side-channel attacks can leak secret key information. These findings highlight the need for more robust encryption approaches that can address both theoretical and implementation-level weaknesses.

The Paillier cryptosystem [9] provides probabilistic encryption and semantic security based on the Decisional Composite Residuosity Assumption (DCRA). Its additive homomorphic property makes it suitable for privacy-preserving computation. Unlike RSA, Paillier generates different ciphertexts for the same plaintext, reducing information leakage and mitigating risks from chosen-ciphertext and side-channel attacks. It has been widely recognized as a prominent partially homomorphic encryption scheme [10], and comparative studies have highlighted differences between RSA and other public-key systems such as ElGamal [11] in terms of performance and security [12, 13].

The integration of multiple cryptographic primitives has been widely explored to enhance security. Hybrid and multi-layer approaches combining symmetric and asymmetric schemes have been proposed across various domains, including secure file transmission [14], Internet of Things (IoT) systems [15], cloud storage [16], and healthcare applications [17-21]. These studies generally demonstrate improved security and performance trade-offs by leveraging complementary cryptographic mechanisms. Additionally, recent work has discussed the long-term vulnerability of classical schemes such as RSA and Paillier in the presence of quantum computing [22].

Table I summarizes the characteristics of recent hybrid and multi-layer encryption frameworks. Despite these developments, existing approaches typically combine public-key and symmetric cryptography or introduce additional layers that increase system complexity. Furthermore, a systematic review of hybrid cryptography models [23] highlights that most cascaded schemes suffer from single points of failure if the primary asymmetric key is compromised. Critically, the reviewed works predominantly focus on performance and functional integration without addressing the combination of mathematical hardness assumptions: when the primary cryptographic assumption is violated (e.g., through Wiener's attack on a weak RSA key), the security of the entire system collapses. RSA–Optimal Asymmetric Encryption Padding (RSA–OAEP) [24], although providing provable Indistinguishability under Adaptive Chosen-Ciphertext Attack (IND-CCA2) security under the Integer Factorization Problem (IFP) in the random oracle model, still relies entirely on a single hardness assumption; if the RSA private key is recovered, all OAEP-padded ciphertexts are immediately exposed. To the best of our knowledge, none of the reviewed works employ a dual-layer design that directly combines RSA and Paillier to address Wiener's continued fraction attack while preserving both multiplicative and additive homomorphic properties. This gap motivates the present study.

Unlike conventional hybrid encryption approaches that use RSA merely for key encapsulation (Key Encapsulation Mechanism (KEM)) alongside a symmetric data cipher, the proposed framework combines two independent public-key cryptosystems to form a dual-layer structure. This design goes beyond simple redundancy: it provides orthogonal security guarantees where the compromise of one mathematical assumption (e.g., Integer Factorization) does not directly invalidate the other (e.g., Decisional Composite Residuosity). The scheme achieves Indistinguishability under Chosen-Plaintext Attack (IND-CPA) semantic security by inheriting Paillier's probabilistic encryption; however, it is explicitly acknowledged that the scheme does not achieve full IND-CCA2 security. This dual-assumption design ensures improved resilience against vulnerabilities associated with single cryptosystems, particularly those related to weak RSA parameter configurations such as small private exponents susceptible to Wiener's attack. The novelty of this work lies in: (i) the specific dual-layer composition with cross-verification, (ii) the formal reduction argument bounding security to the IFP and DCRA, and (iii) the explicit mathematical analysis of Wiener-attack resilience in a dual-layer context, rather than proposing fundamentally new cryptographic primitives.

TABLE I. COMPARISON OF RECENT HYBRID AND MULTI-LAYER ENCRYPTION FRAMEWORKS

Ref.	Algorithms	Security basis	Semantic sec.	Wiener resist.
[14]	AES+RSA+HMAC	IFP+Sym.	No	Conditional
[15]	RSA+AES-128	IFP+Sym.	No	Conditional
[16]	Multi-algo per layer	Mixed	Partial	No
[17]	AES+RSA+Paillier	Sym.+IFP+DCRA	Yes	Conditional
[18]	ISSO+Paillier	DCRA	Yes	N/A
[19]	Paillier+Blowfish	DCRA+Sym.	Yes	N/A
[20]	KAC+Double Enc.	ID-based	Partial	No
[25]	Dict+AES+RSA	Sym.+IFP	No	Conditional
Proposed	RSA+Paillier	IFP+DCRA	Yes	Yes

IFP: Integer Factorization Problem; DCRA: Decisional Composite Residuosity Assumption; Sym.: Symmetric-key assumption; N/A: Not Applicable.

This study proposes a dual-layer RSA–Paillier encryption framework that integrates the strengths of both cryptosystems to address the known limitations of standalone RSA, particularly its vulnerability to Wiener's attack. The framework independently encrypts each plaintext under both RSA and Paillier using separate key pairs and accepts the message only when both decrypted values agree. Because RSA and Paillier rely on orthogonal hardness assumptions (IFP and DCRA), an adversary must break both to recover the plaintext. The main contributions of this paper are as follows:

- A dual-layer encryption framework combining RSA and Paillier with cross-verification of decrypted outputs.
- A formal adversarial model and security analysis covering Wiener's attack, CCAs, and side-channel threats.
- Experimental evaluation using a Python implementation with realistic key sizes (1,024–4,096 bits), including encryption and decryption benchmarks, and ciphertext size analysis.

- Comparative analysis against RSA-only, Paillier-only, and recent hybrid encryption frameworks.

II. PROPOSED DUAL-LAYER RSA–PAILLIER ENCRYPTION FRAMEWORK

A. RSA Algorithm

The RSA cryptosystem [2], proposed by Rivest, Shamir, and Adleman, is based on the computational intractability of factoring the product of two large primes. Key generation proceeds as follows:

- Select two distinct large primes p and q.
- Compute the modulus $n = pq$ and Euler's totient $\varphi(n) = (p-1)(q-1)$.
- Choose a public exponent e with $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$.
- Compute the private exponent $d \equiv e^{-1} \pmod{\varphi(n)}$.
- Public key: (n, e); Private key: (n, d).

For plaintext $M \in \mathbb{Z}_n$, encryption and decryption are:

$$C_R = M^e \bmod n \quad (1)$$

$$M = C_R^d \bmod n \quad (2)$$

Correctness follows from Euler's theorem: $M^{ed} = M^{1+k\varphi(n)} \equiv M \pmod{n}$ for any integer k. A notable structural property of RSA is its multiplicative homomorphism: for ciphertexts $C_1 = M_1^e \bmod n$ and $C_2 = M_2^e \bmod n$,

$$C_1 \cdot C_2 \equiv (M_1 M_2)^e \pmod{n}, \quad (3)$$

so, multiplication of ciphertexts corresponds to multiplication of plaintexts. While useful in certain protocols, this homomorphic property also exposes RSA to CCAs [7] when not appropriately padded.

B. Paillier Cryptosystem

The Paillier cryptosystem [9] rests on the DCRA: distinguishing n-th power residues from non-residues in $\mathbb{Z}_{n^2}^*$ is computationally infeasible. Key generation is as follows:

- Select two distinct large primes p and q.
- Compute $n = pq$, n^2, generator $g = n + 1$, and $\lambda = \text{lcm}(p-1, q-1)$.
- Public key: (n, g); Private key: λ.

For plaintext $M \in \mathbb{Z}_n$ and randomly chosen $r \in \mathbb{Z}_n^*$ with $\gcd(r, n) = 1$, encryption is:

$$C_P = g^M \cdot r^n \bmod n^2 \quad (4)$$

Using the binomial identity $(1+n)^M \equiv 1 + Mn \pmod{n^2}$, the generator $g = n + 1$ simplifies ciphertext computation:

$$g^M \bmod n^2 = 1 + Mn \quad (5)$$

Decryption applies the L-function $L(x) = (x-1)/n$ with normalization constant $\mu = [L(g^\lambda \bmod n^2)]^{-1} \bmod n$. For $g = n + 1$, since $L(g^\lambda \bmod n^2) = \lambda$, we have $\mu = \lambda^{-1} \bmod n$, and decryption is:

$$M = L(C_P^\lambda \bmod n^2) \cdot \mu \bmod n \quad (6)$$

The additive homomorphic property of Paillier is central to its utility: for plaintexts M_1 and M_2 with respective encryptions $E(M_1)$ and $E(M_2)$:

$$E(M_1) \cdot E(M_2) \equiv E(M_1 + M_2 \bmod n) \pmod{n^2} \quad (7)$$

allowing the addition of encrypted values without decryption. Table II summarizes the key properties distinguishing RSA and Paillier.

TABLE II. COMPARISON OF RSA AND PAILLIER CRYPTOSYSTEMS

Property	RSA [2]	Paillier [9]
Security assumption	IFP	DCRA
Encryption type	Deterministic	Probabilistic
Homomorphism	Multiplicative	Additive
Semantic security	No (plain)	Yes (IND-CPA)
Ciphertext space	$\mathbb{Z}_n$	$\mathbb{Z}_{n^2}$
Wiener attack risk	Yes (small d)	Not applicable

IFP: Integer Factorization Problem; DCRA: Decisional Composite Residuosity Assumption.

C. Dual-Layer RSA–Paillier Framework

The proposed dual-layer encryption framework independently encrypts the same plaintext under both RSA and Paillier, transmitting a ciphertext pair. The dual-layer design introduces an additional protection layer by combining two independent cryptographic mechanisms based on different hardness assumptions:

- Dual-layer encryption: For message M and Paillier random nonce $r \in \mathbb{Z}_{n_2}^*$:

$$C_R = M^e \bmod n_1 \text{ (RSA layer)} \quad (8)$$

$$C_P = (1 + Mn_2) \cdot r^{n_2} \bmod n_2^2 \text{ (Paillier layer)} \quad (9)$$

The transmitted ciphertext is the pair (C_R, C_P).

- Dual-layer decryption: Using RSA private key d and Paillier private key λ:

$$M_R = C_R^d \bmod n_1 \quad (10)$$

$$M_P = L(C_P^\lambda \bmod n_2^2) \cdot \mu_2 \bmod n_2 \quad (11)$$

Accept and output M if and only if $M_R = M_P$.

Algorithm 1 and Algorithm 2 present the pseudocode for dual-layer encryption and decryption, respectively.

```
Algorithm 1: Dual-Layer RSA-Paillier Encryption
Input: Plaintext M; RSA public key (n1, e); Paillier public key (n2, g)
Output: Ciphertext pair (C_R, C_P)
1. // RSA Layer
   C_R ← M^e mod n1
2. // Paillier Layer
   Choose random r ← Z*_n2 with gcd(r, n2) = 1
```

$C_P \leftarrow g^M \cdot r^{n_2} \bmod n_2^2$
3. return (C_R, C_P)

Algorithm 2: Dual-Layer RSA–Paillier Decryption
Input: Ciphertext pair (C_R, C_P); RSA private key (n_1, d); Paillier private key (λ, μ_2, n_2)
Output: Plaintext M or $\perp$ (rejection)
1. // RSA Decryption
$M_R \leftarrow C_R^d \bmod n_1$
2. // Paillier Decryption
$u \leftarrow C_P^\lambda \bmod n_2^2$
$M_P \leftarrow L(u) \cdot \mu_2 \bmod n_2$ // where $L(x) = (x-1)/n_2$
3. // Cross-verification
if $M_R = M_P$ then
return $M \leftarrow M_R$
else
return $\perp$ // Reject: possible tampering

1) Distinction from Existing Approaches

The proposed framework differs from standard hybrid encryption [14], which typically pairs a public-key algorithm with a symmetric cipher using a KEM–Data Encryption Mechanism (KEM–DEM) architecture. It also differs from multi-layer encryption schemes [16, 25], which cascade multiple algorithms sequentially. In the dual-layer design, both RSA and Paillier encrypt the same plaintext independently, and the cross-verification step $M_R = M_P$ provides an integrity check absent from redundant or parallel encryption. Furthermore, the two layers rely on fundamentally different hardness assumptions, the IFP for RSA and the DCRA for Paillier, so compromising one layer does not weaken the other. Existing RSA–Paillier combinations such as [17] include a third symmetric layer (AES), introducing additional key management complexity, whereas the proposed scheme achieves dual-assumption security using only two public-key primitives. Unlike threshold schemes [18], the dual-layer framework does not require distributed key shares, keeping deployment simple.

Table III summarizes the framework parameters for the illustrative example developed in Section IV, and Figure 1 illustrates the architecture of the proposed dual-layer RSA–Paillier encryption framework.

TABLE III. DUAL-LAYER RSA–PAILLIER FRAMEWORK: TOY PARAMETERS

Parameter	RSA layer	Paillier layer
Prime p	11	17
Prime q	13	19
Modulus n	143	323
Public parameter	$e = 7$	$g = 324$
Private key	$d = 103$	$\lambda = 144$
Ciphertext	$C_R = 29$	$C_P = 20{,}340$

The toy example uses a message $M = 68$ (ASCII character "D") and Paillier nonce $r = 2$.

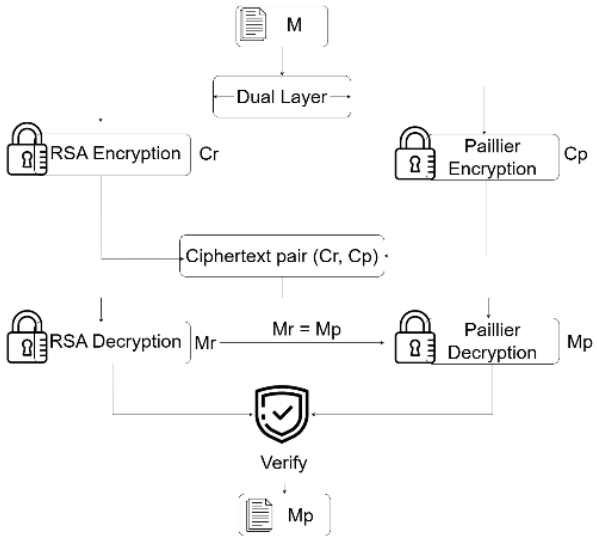

Fig. 1. Architecture of the proposed dual-layer RSA–Paillier encryption framework.

2) Security Rationale

The dual-layer scheme inherits IND-CPA security from Paillier, removing the deterministic leakage of plain RSA. Wiener's attack affects only the RSA component when $d < (1/3)n_1^{1/4}$, whereas the Paillier ciphertext remains protected under the DCRA. Conversely, compromising the Paillier layer does not reveal the RSA plaintext without factoring n_1, and inconsistent decryptions are rejected by cross-verification. The independence of IFP and DCRA constitutes a defense-in-depth architecture: compromising one assumption does not automatically expose the plaintext, although an adversary capable of breaking both assumptions simultaneously would recover the message. This represents a meaningful improvement over single-assumption schemes where violating the sole underlying problem results in total compromise. It is explicitly noted that the scheme achieves IND-CPA security, not formal IND-CCA2 security.

III. WIENER ATTACK MODEL AND SECURITY ANALYSIS

A. Mathematical Background

Wiener's attack is based on the relationship between the RSA public and private exponents. From the key equation $ed \equiv 1 \pmod{\varphi(n)}$, there exists an integer k such that $ed - k\varphi(n) = 1$. By approximating $\varphi(n) \approx n$, the fraction e/n can be closely approximated by k/d.

When the private exponent is sufficiently small, specifically $d < (1/3)n^{1/4}$, authors in [3] showed that k/d appears among the convergents of the continued fraction expansion of e/n. This vulnerability allows the private key d to be efficiently recovered.

In practice, this implies that RSA remains secure against Wiener's attack as long as the private exponent is not chosen too small. In the proposed dual-layer framework, the attack applies only to the RSA component, whereas the Paillier layer

remains unaffected due to its different structure and security assumption.

B. Attack Procedure

The Wiener attack algorithm executes in $O(\log n)$ steps [3]:

- Compute the continued fraction expansion of e/n to obtain convergents k_i/d_i for $i = [0,1, \dots]$.
- For each convergent k_i/d_i with $k_i > 0$: (a) compute $\hat{\varphi} = (e \cdot d_i - 1)/k_i$; if not a positive integer, skip; (b) solve $x^2 - (n - \hat{\varphi} + 1)x + n = 0$; (c) if x has positive integer roots p, q with $pq = n$, output $d = d_i$ and halt.
- If no convergent produces valid prime factors, the attack fails.

The Wiener attack applies exclusively to the RSA component of the dual-layer scheme; the Paillier component is structurally immune since it does not employ an RSA-style private exponent relation. Even a successful Wiener attack on the RSA layer does not compromise the Paillier ciphertext C_P: verifying or decrypting C_P requires the private parameter λ, whose recovery from (n_2, g, C_P) is governed by the DCRA. Thus, the dual-layer framework provides a security backstop absent from RSA used in isolation.

C. Adversarial Model

The security analysis considers a computationally bounded adversary $\mathcal{A}$ operating in the following threat model:

- Public knowledge: $\mathcal{A}$ knows both public keys (n_1, e) and (n_2, g) and the dual-layer ciphertext pair (C_R, C_P).
- Oracle access: In the CCA setting, $\mathcal{A}$ may query a decryption oracle on ciphertext pairs of its choice, except the challenge pair.
- Goal: $\mathcal{A}$ aims to recover the plaintext M or distinguish encryptions of two chosen messages with non-negligible advantage.

The dual-layer scheme achieves IND-CPA confidentiality under the conjunction of the two independent hardness assumptions. Let $\mathrm{Adv}_{\mathrm{DL}}^{\mathrm{IND-CPA}}(\mathcal{A})$ denote the advantage of a Probabilistic Polynomial-Time (PPT) adversary $\mathcal{A}$ in the standard IND-CPA game against the dual-layer scheme. Since the RSA and Paillier key pairs are generated independently from distinct primes, the two ciphertext components (C_R, C_P) carry no shared cryptographic dependency. The security is formalized through the following reductions based on standard definitions [26]:

- Reduction $\mathcal{B}_P$ to Paillier. Suppose $\mathcal{A}$ achieves non-negligible advantage ϵ in the dual-layer IND-CPA game. Construct an adversary $\mathcal{B}_P$ against the Paillier IND-CPA game: $\mathcal{B}_P$ receives a Paillier challenge ciphertext C_P^* for one of two messages M_0, M_1, independently samples an RSA key pair, encrypts the same two messages under RSA to obtain $C_{R,0}, C_{R,1}$, and sends the pairs $(C_{R,b}, C_P^*)$ to $\mathcal{A}$ for $b \in \{0,1\}$. $\mathcal{A}$'s guess of b directly translates to a guess in the Paillier game, yielding $\mathrm{Adv}_{\mathrm{Paillier}}^{\mathrm{IND-CPA}}(\mathcal{B}_P) \geq \epsilon$. A contradiction to the DCRA follows.
- Reduction $\mathcal{B}_R$ to RSA (IFP): Symmetrically, $\mathcal{B}_R$ embeds an RSA challenge ciphertext C_R^* (under textbook RSA; the adversary simulates the Paillier layer using a freshly generated Paillier key pair) and forwards (C_R^*, C_P) to $\mathcal{A}$. This reduction is presented for structural completeness: the practical security of the dual-layer scheme against ciphertext-only attacks on the RSA layer is bounded by standard factorization, whereas the IND-CPA guarantee is carried exclusively by Paillier.

Therefore, assuming the hardness of both the IFP and the DCRA, the dual-layer scheme satisfies IND-CPA security. The advantage of any PPT adversary against the dual-layer scheme satisfies:

$$\mathrm{Adv}_{\mathrm{DL}}^{\mathrm{IND-CPA}}(\mathcal{A}) \leq \min \left(\mathrm{Adv}_{\mathrm{RSA}}^{\mathrm{IND-CPA}}(\mathcal{B}_R),\ \mathrm{Adv}_{\mathrm{Paillier}}^{\mathrm{IND-CPA}}(\mathcal{B}_P)\right) \quad (12)$$

It is explicitly noted that the bound in (12) characterizes IND-CPA security only; it does not extend to the IND-CCA2 setting where an adversary with decryption oracle access could potentially exploit structural properties of the dual-layer composition. Formal IND-CCA2 security for this construction remains an open problem [26].

D. Indistinguishability under Chosen-Plaintext Attack Security

The Paillier cryptosystem is provably IND-CPA secure under the DCRA [9]. For any two messages M_0, M_1 , a computationally bounded adversary cannot distinguish $E(M_0)$ from $E(M_1)$ without solving the DCRA. Since the dual-layer ciphertext includes the Paillier component C_P, the dual-layer scheme inherits IND-CPA security: even if the adversary can distinguish RSA ciphertexts (which is trivial for deterministic RSA), the Paillier component prevents the adversary from distinguishing dual-layer ciphertexts of different messages. Thus, the dual-layer scheme achieves semantic security that plain RSA alone does not provide.

E. Resistance to Chosen-Ciphertext Attacks

Standard (textbook) RSA is vulnerable to CCAs due to its multiplicative homomorphism: an adversary can construct $C' = C_R \cdot s^e \bmod n_1$ for any s and learn information about M from the decryption of C' [7]. In the dual-layer scheme, an adversary who modifies C_R must also produce a matching C_P that decrypts to the same altered message, requiring an independent break of the Paillier scheme. The cross-verification step ($M_R = M_P$) rejects any inconsistent ciphertext pair, closing the malleability channel exploited by Bleichenbacher-style attacks on RSA alone.

It must be explicitly noted that the proposed dual-layer scheme does not achieve formal IND-CCA2 security. Full IND-CCA2 requires either a plaintext-aware construction or a padding transform proven secure under adaptive chosen-ciphertext queries, such as RSA–OAEP [24] as standardized in PKCS #1 v2.2 [27]. The dual-layer cross-verification provides practical CCA resistance against attacks targeting a single layer, but a sophisticated adversary with oracle access to both decryption components could in principle mount attacks not

covered by this construction. Closing this gap to achieve formal IND-CCA2 remains an open direction for future work.

In exchange, the dual-layer scheme offers a qualitatively different guarantee unavailable from RSA–OAEP: even if the RSA private key d is fully recovered (e.g., through Wiener's continued fraction attack on a weak exponent), the Paillier ciphertext C_P remains computationally protected under the independent DCRA, preserving confidentiality in a scenario where RSA–OAEP would be entirely compromised.

F. Side-Channel Considerations

Side-channel attacks such as differential power analysis [8] can leak secret key information through timing or power consumption measurements during modular exponentiation. In the dual-layer scheme, the Paillier layer offers a natural countermeasure: its encryption involves a fresh random nonce r in every operation, which randomizes the computation and masks power-consumption patterns. Even if an attacker extracts the RSA private key d through side-channel analysis, the Paillier private key λ remains protected and the Paillier ciphertext cannot be decrypted. The independence of the two key pairs ensures that a side-channel compromise of one layer does not propagate to the other, providing defense-in-depth against implementation-level attacks.

G. Key Leakage and Attack Propagation

A central advantage of the dual-layer design is the independence of its security assumptions. If the RSA private key d is leaked or recovered through any means—Wiener's attack, factorization, or side-channel leakage—the adversary obtains M_R from C_R but still cannot decrypt C_P without λ. Conversely, if the Paillier private key λ is compromised, the adversary obtains M_P but cannot verify or recover M from C_R without factoring n_1. Attack propagation between layers is prevented because the RSA key pair (n_1, e, d) and the Paillier key tuple (n_2, g, λ, μ_2) are generated from independent primes. No mathematical or computational relationship links one key set to the other.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

A. Experimental Setup

All experiments were performed on a Linux 6.8 (x86_64) server with an Intel Core processor (Haswell) and 19.4 GB RAM. The implementation uses Python 3.12.3 with the PyCryptodome 3.23 library for RSA and gmpy2 2.3 for arbitrary-precision Paillier arithmetic. RSA key generation relies on PyCryptodome's RSA.generate(), whereas the Paillier implementation follows the original construction of [9] with $g = n + 1$. Each timing measurement is the mean of 30 independent runs; standard deviations are reported. Key sizes of 1,024, 2,048, 3,072, and 4,096 bits are evaluated. A random 128-bit plaintext $M < \min(n_1, n_2)$ is used in each trial.

B. Correctness Verification with Toy Parameters

To illustrate the correctness of the proposed dual-layer scheme, a simple example with toy parameters is used. The RSA and Paillier components are initialized independently, and the same plaintext is encrypted under both schemes.

After decryption, both components recover identical plaintext values, i.e., $M_R = M_P$, confirming that the encryption and decryption processes operate correctly. This also validates the cross-verification mechanism of the dual-layer design.

Detailed intermediate calculations are omitted for brevity, as the focus is on demonstrating the correctness of the overall framework rather than step-by-step computation.

C. Wiener Attack Analysis

1) Toy Parameter Analysis

The Wiener attack requires $d < (1/3)n_1^{1/4}$. For $n_1 = 143$:

$$(1/3)\, n_1^{1/4} = (1/3)(143)^{0.25} \approx 1.154 \qquad (13)$$

Since $d = 103 \gg 1.154$, the Wiener condition is not met. The continued fraction expansion $e/n_1 = 7/143 = [0; 20, 2, 3]$ yields the convergents in Table IV; none recover d.

TABLE IV. CONTINUED FRACTION CONVERGENTS OF 7/143

i	a_i	k_i	d_i	Attack outcome
0	0	0	1	$k_0 = 0$; skip
1	20	1	20	$\hat{\varphi} = 139; \Delta = -547 < 0$
2	2	2	41	$\hat{\varphi} = 143; \Delta = -571 < 0$
3	3	7	143	$\hat{\varphi} = 142.86$; non-integer; skip

All computed discriminants are negative or $\hat{\varphi}$ is non-integer, indicating that the attack fails.

2) Simulation with Realistic Keys

The Wiener attack was implemented in Python using the continued fraction algorithm described in Section III-B. On a deliberately weak 512-bit RSA key with $d = 601$ (satisfying $d < (1/3)n^{1/4}$), the attack successfully recovered d in under 1 ms. On a properly generated 2,048-bit RSA key (d of 2,047 bits), the attack failed and returned no candidate. These results confirm that the Wiener attack succeeds only when the private exponent is inappropriately small, and that standard key generation prevents this vulnerability.

3) Dual-Layer Protection

Even under a hypothetical RSA compromise, the Paillier ciphertext C_P cannot be decrypted without λ, whose recovery is governed by the DCRA. The dual-layer scheme therefore retains confidentiality through the Paillier layer in this scenario.

D. Performance Benchmarks

Table V presents the measured encryption and decryption times for RSA, Paillier, and the dual-layer scheme across key sizes from 1,024 to 4,096 bits. Each entry reports the mean and standard deviation over 30 runs.

RSA encryption is the fastest operation (sub-millisecond for all key sizes) because the public exponent $e = 65{,}537$ is small. Paillier encryption is slower due to two modular exponentiations in $\mathbb{Z}_{n^2}$. The dual-layer encryption time is dominated by the Paillier component and is approximately equal to the Paillier encryption time alone (≈ 98.11 ms at 2,048 bits), since the RSA encryption adds only ≈ 0.13 ms.

TABLE V. ENCRYPTION AND DECRYPTION TIME (MS), MEAN ± STD. DEV., 30 RUNS

Key	RSA	RSA–OAEP [24]	Paillier	Dual-layer
	Enc / Dec	Enc / Dec	Enc / Dec	Enc / Dec
1,024	0.05 ± 0.01 / 4.05 ± 0.19	0.30 ± 0.07 / 0.47 ± 0.05	13.91 ± 1.12 / 13.66 ± 1.12	13.55 ± 0.12 / 17.28 ± 0.16
2,048	0.13 ± 0.01 / 26.52 ± 1.14	0.54 ± 0.05 / 1.31 ± 0.04	98.11 ± 3.79 / 98.05 ± 2.86	98.19 ± 2.67 / 125.04 ± 4.32
3,072	0.27 ± 0.02 / 83.21 ± 1.12	0.81 ± 0.04 / 3.40 ± 0.19	298.92 ± 4.44 / 298.13 ± 4.16	298.69 ± 4.72 / 382.89 ± 6.96
4,096	0.44 ± 0.02 / 191.01 ± 1.48	1.16 ± 0.05 / 6.92 ± 0.20	694.64 ± 22.38 / 695.30 ± 9.43	688.69 ± 10.81 / 880.53 ± 12.58

From a security perspective, the proposed scheme mitigates vulnerabilities such as Wiener's attack on weak exponents by combining two orthogonal public-key layers. Unlike the triple-layer approach of [17], which relies on AES key management, the dual-layer design achieves comparable security guarantees through a simpler architecture without introducing a third symmetric cipher.

E. Performance Properties Summary

Table VI presents a summary of the structural performance properties of the three encryption schemes.

TABLE VI. STRUCTURAL PERFORMANCE PROPERTIES OF THE THREE ENCRYPTION SCHEMES

Property	RSA	Paillier	Dual-layer
Encryption type	Deterministic	Probabilistic	Probabilistic
Homomorphism	Multiplicative	Additive	Both
Enc. mod. exp. count	1	2	3
Dec. mod. exp. count	1	1	2
Random nonces needed	0	1	1
Ciphertext size	$\log_2 n$	$2\log_2 n$	$3\log_2 n$
Security layers	1	1	2

At the recommended key size of 2,048 bits, dual-layer encryption completes in ≈ 98.19 ms and decryption in ≈ 125.04 ms.

F. Comparison with RSA–OAEP and Practical Trade-Offs

RSA–OAEP [24, 27] is the standard IND-CCA2-secure RSA variant, standardized in PKCS #1 v2.2. It applies an OAEP transform using cryptographic hash functions, achieving provable security against adaptive CCAs under the IFP in the random oracle model.

Table V includes RSA–OAEP benchmark results from the same experimental platform using PyCryptodome's PKCS1_OAEP with SHA-256. At 2,048 bits, RSA–OAEP achieves encryption in 0.54 ± 0.05 ms and decryption in 1.31 ± 0.04 ms—approximately $181\times$ faster at encryption and $95\times$ faster at decryption than the dual-layer scheme. The RSA–OAEP ciphertext equals the modulus size (2,048 bits) versus 6,144 bits for the dual-layer ($3\times$ expansion).

The key distinction lies in the threat model each scheme addresses:

- RSA–OAEP provides IND-CCA2 security under the IFP. If the RSA private key d is recovered via Wiener's attack on a weak exponent, all ciphertexts are immediately decryptable; the OAEP padding offers no defense against key recovery.
- Dual-layer RSA–Paillier provides IND-CPA security under the joint IFP and DCRA. Full compromise of the RSA key still leaves C_P protected under the DCRA. Both assumptions must be broken simultaneously to recover M.

1) Bandwidth Analysis

The $3\times$ ciphertext expansion adds 768 bytes per message at 2,048-bit security. In strictly bandwidth-constrained environments (e.g., LoRaWAN with 51–242-byte payloads), this overhead is significant and would require fragmentation. However, for high-bandwidth applications—such as cloud storage, financial systems, or hybrid encryption where only a short session key ($\leq$ 32 bytes) is protected—the per-session overhead is modest and the orthogonal security guarantee is highly valuable. Standard lossless compression applied prior to encryption can further reduce the effective overhead. Table VII summarizes the trade-off.

TABLE VII. RSA–OAEP VS. DUAL-LAYER SCHEME TRADE-OFFS (2,048-BIT)

Property	RSA–OAEP	Dual-layer
Security model	IND-CCA2	IND-CPA
Security assumption	IFP + ROM	IFP + DCRA
Wiener attack resilience	No	Yes
Key compromise isolation	No	Yes (orthogonal)
Enc. time (2,048-bit)	0.54 ± 0.05 ms	98.19 ± 2.67 ms
Dec. time (2,048-bit)	1.31 ± 0.04 ms	125.04 ± 4.32 ms
Ciphertext size	2,048 bits	6,144 bits ($3\times$)
Random oracle assumption	Yes	No
Homomorphic property	None	Additive (Paillier)

IFP: Integer Factorization Problem; DCRA: Decisional Composite Residuosity Assumption; ROM: Random Oracle Model.

For scenarios where IND-CCA2 security and minimal overhead are the primary requirements, RSA–OAEP is the superior choice. For scenarios where long-term confidentiality against key-recovery attacks is the primary concern and moderate computational overhead is acceptable, the dual-layer RSA-Paillier scheme provides qualitatively stronger security by eliminating any single point of cryptographic failure.

V. CONCLUSION

This paper presents a dual-layer RSA–Paillier encryption framework that combines two independent public-key cryptosystems under orthogonal hardness assumptions, namely the Integer Factorization Problem (IFP) and the Decisional Composite Residuosity Assumption (DCRA). Unlike conventional hybrid or redundant encryption approaches, the proposed design introduces a cross-verification mechanism that enforces consistency across layers and provides defense-in-depth: compromising one assumption does not automatically expose the plaintext, although an adversary capable of breaking both assumptions simultaneously would recover the message.

The framework achieves Indistinguishability under Chosen-Plaintext Attack (IND-CPA) semantic security under the joint assumptions, supported by a formal reduction argument bounding dual-layer security to the IFP and the DCRA. The Paillier component provides semantic security absent from plain RSA, whereas the cross-verification step offers practical resistance to attacks targeting a single layer, including Wiener-based key recovery and chosen-ciphertext manipulation of RSA. It is explicitly stated that formal Indistinguishability under Adaptive Chosen-Ciphertext Attack (IND-CCA2) security is not achieved by the present construction and remains future work.

Compared with RSA–Optimal Asymmetric Encryption Padding (RSA–OAEP), which provides efficient IND-CCA2 security under a single assumption (IFP), the proposed scheme addresses a different threat model by preserving confidentiality even under partial key compromise, at the cost of increased computation and a $3\times$ ciphertext expansion. For bandwidth-constrained environments such as LoRaWAN, standard lossless compression can mitigate the overhead; for cloud storage and financial transaction systems, the per-session overhead is modest relative to the orthogonal security guarantee.

Experimental results confirm the correctness and feasibility of the proposed framework for key sizes ranging from 1,024 to 4,096 bits, with the additional computational overhead representing a deliberate trade-off suitable for high-assurance applications where resilience against key-recovery attacks is a primary requirement. Future work includes achieving formal IND-CCA2 security, improving computational efficiency, and exploring post-quantum extensions using lattice-based analogs.

DECLARATION OF COMPETING INTERESTS

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

ACKNOWLEDGMENT

Not applicable to this work.

FUNDING SOURCES

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

AI USE AND DECLARATION OF GENERATIVE AI USE

The authors declare that no Generative AI tools were used in the preparation of this work.

REFERENCES

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976, https://doi.org/10.1109/TIT.1976.1055638.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978, https://doi.org/10.1145/359340.359342.

[3] M. J. Wiener, "Cryptanalysis of short RSA secret exponents," *IEEE Transactions on Information Theory*, vol. 36, no. 3, pp. 553–558, May 1990, https://doi.org/10.1109/18.54902.

[4] A. Dujella, "Continued fractions and RSA with small secret exponent," *Tatra Mountains Mathematical Publications,* vol. 29, no. 3, pp. 101–112, 2004.

[5] A. Nitaj, "Another Generalization of Wiener's Attack on RSA," in *First International Conference on Cryptology in Africa*, Casablanca, Morocco, 2008, pp. 174–190, https://doi.org/10.1007/978-3-540-68164-9_12.

[6] D. Boneh and G. Durfee, "Cryptanalysis of RSA with Private Key d Less than N0.292," in *International Conference on the Theory and Application of Cryptographic Techniques*, Prague, Czech Republic, 1999, pp. 1–11, https://doi.org/10.1007/3-540-48910-X_1.

[7] D. Bleichenbacher, "Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1," in *18th Annual International Cryptology Conference*, Santa Barbara, CA, USA, 1998, pp. 1–12, https://doi.org/10.1007/BFb0055716.

[8] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *19th Annual International Cryptology Conference*, Santa Barbara, CA, USA, 1999, pp. 388–397, https://doi.org/10.1007/3-540-48405-1_25.

[9] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," in *International Conference on the Theory and Application of Cryptographic Techniques*, Prague, Czech Republic, 1999, pp. 223–238, https://doi.org/10.1007/3-540-48910-X_16.

[10] C. Marcolla, V. Sucasas, M. Manzano, R. Bassoli, F. H. P. Fitzek, and N. Aaraj, "Survey on Fully Homomorphic Encryption, Theory, and Applications," *Proceedings of the IEEE*, vol. 110, no. 10, pp. 1572–1609, Oct. 2022, https://doi.org/10.1109/JPROC.2022.3205665.

[11] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, July 1985, https://doi.org/10.1109/TIT.1985.1057074.

[12] N. R. D. P. Astuti, D. P. Setiawan, and D. C. Hakika, "Comparative Study of ElGamal and LUC Algorithm in Cryptographic Key Generation," *Asean Engineering Journal*, vol. 13, no. 4, pp. 61–68, Dec. 2023, https://doi.org/10.11113/aej.v13.19184.

[13] A. P. U. Siahaan, E. Elviwani, and B. Oktaviana, "Comparative Analysis of RSA and ElGamal Cryptographic Public-key Algorithms," in *Joint Workshop KO2PI and The 1st International Conference on Advance & Scientific Innovation*, Medan, Indonesia, 2018, pp. 163–172.

[14] E. S. I. Harba, "Secure Data Encryption Through a Combination of AES, RSA and HMAC," *Engineering, Technology & Applied Science Research*, vol. 7, no. 4, pp. 1781–1785, Aug. 2017, https://doi.org/10.48084/etasr.1272.

[15] S. Bin-Faisal, D. Nandi, and M. Rahman, "Dual Layer Encryption for IoT based Vehicle Systems over 5G Communication," *International Journal of Information Technology and Computer Science*, vol. 14, no. 2, pp. 17–30, https://doi.org/10.5815/ijitcs.2022.02.02.

[16] A. Zabian, S. Mrayyen, A. M. Jonan, T. Al-Shaikh, and M. G. Al-Khaiyat, "Multi-layer encryption algorithm for data integrity in cloud computing," in *Neural Networks, Machine Learning, and Image Processing*, 1st. ed., M. Sahni, R. Sahni, and J. M. Merigo, Eds. Boca Raton, FL, USA: CRC Press, 2022, pp. 101–114, https://doi.org/10.1201/9781003303053-10.

[17] M. N. Jeyakumar and J. Samraj, "Secure medical sensor monitoring framework using novel hybrid encryption algorithm driven by internet of things," *Measurement: Sensors*, vol. 33, June 2024, Art. no. 101122, https://doi.org/10.1016/j.measen.2024.101122.

[18] R. S. Kanakasabapathi and J. E. Judith, "An intelligent hybrid encryption framework for cloud systems in cybernetics using ISSO and Paillier cryptosystem," *International Journal of Machine Learning and Cybernetics*, vol. 16, no. 12, pp. 10541–10567, Dec. 2025, https://doi.org/10.1007/s13042-025-02785-9.

[19] B. Seth *et al.*, "Secure Cloud Data Storage System Using Hybrid Paillier–Blowfish Algorithm," *Computers, Materials & Continua*, vol.

67, no. 1, pp. 779–798, Jan. 2021, https://doi.org/10.32604/cmc.2021.014466.

[20] K. K. Almuzaini, A. K. Sinhal, R. Ranjan, V. Goel, R. Shrivastava, and Awal Halifa, "Key Aggregation Cryptosystem and Double Encryption Method for Cloud-Based Intelligent Machine Learning Techniques-Based Health Monitoring Systems," *Computational Intelligence and Neuroscience*, vol. 2022, no. 1, Apr. 2022, Art. no. 3767912, https://doi.org/10.1155/2022/3767912.

[21] A. Mishra, T. S. Jabar, Y. I. Alzoubi, and K. N. Mishra, "Enhancing privacy-preserving mechanisms in Cloud storage: A novel conceptual framework," *Concurrency and Computation: Practice and Experience*, vol. 35, no. 26, Nov. 2023, Art. no. e7831, https://doi.org/10.1002/cpe.7831.

[22] D.-T. Dam, T.-H. Tran, V.-P. Hoang, C.-K. Pham, and T.-T. Hoang, "A Survey of Post-Quantum Cryptography: Start of a New Race," *Cryptography*, vol. 7, no. 3, p. 40, Aug. 2023, Art. no. 40, https://doi.org/10.3390/cryptography7030040.

[23] A. A.-R. El-Douh, S. F. Lu, A. Elkony, and A. S. Amein, "A Systematic Literature Review: The Taxonomy of Hybrid Cryptography Models," in *Proceedings of the 2022 Future of Information and Communication Conference*, San Francisco, CA, USA, 2022, pp. 714–721, https://doi.org/10.1007/978-3-030-98015-3_49.

[24] M. Bellare and P. Rogaway, "Optimal asymmetric encryption," in *Workshop on the Theory and Application of Cryptographic Techniques*, Perugia, Italy, 1994, pp. 92–111, https://doi.org/10.1007/BFb0053428.

[25] O. A. Qasim and S. Golshannavaz, "Enhancing data security using a multi-layer encryption system," *International Journal of Electrical and Computer Engineering*, vol. 15, no. 2, pp. 1961–1967, Apr. 2025, https://doi.org/10.11591/ijece.v15i2.pp1961-1967.

[26] D. Boneh and V. Shoup. "A Graduate Course in Applied Cryptography." Cryptobook. https://toc.cryptobook.us.

[27] K. Moriarty, B. Kaliski, J. Jonsson, and A. Rusch, "PKCS #1: RSA Cryptography Specifications Version 2.2," Internet Engineering Task Force, Request for Comments RFC 8017, Nov. 2016. https://doi.org/10.17487/RFC8017.