Vokasi Unesa Bulletin of Engineering, Technology and Applied Science (VUBETA)
https://journal.unesa.ac.id/index.php/vubeta
Vol. 3, No. 3, 2026, pp. 517~528 DOI: 10.26740/vubeta.v3i3.52993
ISSN: 3064-0768

An Efficient IND-CCA2-Secure Certificateless Public Key Encryption Scheme with Cryptographic Reverse Firewalls

Lukman Umar Faruk[1*], Muhammad Bashir Abdulrazaq[2], Zainab Mukhtar Abubakar[3], Zahrudden Haruna[4], A. Umar[5], Nafisa Shehu Usman[6], Hasan Maharazu[7]

[1,2,3,4,5,6]Department of Computer Engineering, Faculty of Engineering, Ahmadu Bello University Zaria, Kaduna state, Nigeria.
[7]Department of Electrical and Electronics Engineering, Federal University of Transportation, Daura Katsina state, Nigeria.

Article Info

Article history:

Received April 22, 2026
Revised July 16, 2026
Accepted August 15, 2026

Keywords:

Certificateless Public Key Encryption
Cryptographic Reverse Firewalls
IND-CCA2 Security
Bilinear Pairings
Exfiltration Resistance

ABSTRACT

Secure communication in Internet of Things (IoT), cloud computing, and peer-to-peer environments requires efficient cryptographic schemes resilient to advanced threats. Public Key Infrastructure (PKI) incurs certificate management overhead, while Identity-Based Encryption (IBE) introduces key escrow. Certificateless Public Key Encryption (CL-PKE) addresses these limitations, but existing constructions integrating Cryptographic Reverse Firewalls (CRFs) remain computationally expensive and lack IND-CCA2 security guarantees. This study develops an optimized CL-PKE-CRF scheme using a single-element public key, sender-side precomputation of pairing operations, and independent per-user randomization through a Key Derivation Function (KDF) at the Key Generation Center (KGC). The scheme was implemented using Charm-Crypto and evaluated over 1,000 iterations at 128-, 192-, and 256-bit security levels. Compared with the baseline, it reduced computational overhead by approximately 25% and communication costs by 33%, while subsequent encryption latency decreased by 76.6% for repeated operations. Simulated evaluations reported adversarial advantage below 0.004, 100% decryption correctness, and no observed information leakage across the tested compromise scenarios. A formal IND-CCA2 security reduction under the Computational Bilinear Diffie-Hellman (CBDH) assumption in the random oracle model is also presented. These findings demonstrate improved efficiency and resistance to exfiltration attacks, supporting secure communication in resource-constrained environments.

1. INTRODUCTION

The rapid proliferation of Internet-connected devices has created an urgent demand for cryptographic schemes that simultaneously achieve efficiency, strong security guarantees, and resilience to insider threats. Secure enterprise terminal networks face compounding challenges: network terminals ranging from intelligent workstations to dumb IoT endpoints represent key vectors for malicious access and data exfiltration [1]. Three major encryption paradigms underpin modern secure communication: (i) symmetric-key encryption schemes such as AES, which are computationally efficient but require secure key exchange; (ii) asymmetric (public-key) encryption schemes such as RSA and Elliptic Curve

*Corresponding Author
Email: lumarfaruk@gmail.com

Cryptography (ECC), which solve the key distribution problem but introduce certificate management complexity; and (iii) pairing-based certificateless encryption schemes, which eliminate both the certificate overhead and the key escrow problem at the cost of higher computational load [2]-[6]
Traditional Public Key Infrastructure (PKI) systems, while widely deployed, introduce significant overhead in certificate management [7]. Identity-Based Encryption (IBE) simplified this process but introduced an inherent key escrow problem, as the Private Key Generator (PKG) holds all user private keys [8]. To address these limitations, Certificateless Public Key Encryption (CL-PKE) was introduced as a hybrid framework that combines the advantages of both paradigms [9]. In CL-PKE, a Key Generation Center (KGC) generates only a partial private key, while the user independently selects a secret value. This eliminates the key escrow problem and removes the need for certificates [10][11].

However, recent developments have revealed that cryptographic systems remain vulnerable to endpoint exfiltration attacks and malicious implementations, even when their underlying mathematical assumptions are secure [12]. In response to these challenges, Cryptographic Reverse Firewalls (CRFs) were introduced as a defensive mechanism to sanitize outputs and prevent data leakage from compromised machines [13]. The integration of CRFs into certificateless schemes, known as CL-PKE-CRF, has been explored [14]. However, existing protocols suffer from high computational costs due to intensive pairing operations and lack strong resistance to adaptive chosen ciphertext attacks (IND-CCA2), making them inefficient for real-time or resource-constrained environments [14]-[16].

This study identifies three specific research gaps motivating this work. First, no existing CL-PKE-CRF construction simultaneously achieves IND-CCA2 security and computational efficiency at scale. Second, existing CRF rerandomization mechanisms employ a single, shared randomization parameter across all users, creating potential key-linkage vulnerabilities. Third, no prior work has demonstrated a CL-PKE-CRF scheme with 50% public key size reduction while maintaining full exfiltration resistance. This study directly addresses all three gaps.

This study develops an optimized, general-purpose CL-PKE-CRF protocol to address these shortcomings. The novel contributions include: (i) a streamlined single-element public key structure that reduces public key size by 50% and halves rerandomization operations; (ii) sender-side pre-computation of fixed pairing values, reducing subsequent encryption latency by 76.6%; and (iii) KDF-based independent per-user randomization at the KGC, achieving IND-CCA2 security with a formal proof under the CBDH assumption. These contributions advance the state of the art in certificateless encryption beyond what has been achieved in prior works [14]-[18].

This paper is structured as follows: Section 2 reviews categories of encryption algorithms and related literature. Section 3 presents the mathematical formulation of the proposed scheme and formal security proof. Section 4 describes the experimental setup. Section 5 evaluation methodology. Section 6 presents the results and discussion. Section 7 concludes the paper and outlines future directions.

2. LITERATURE REVIEW

2.1 Categories of Encryption Algorithms

Modern encryption algorithms can be broadly categorized into four families, each with distinct characteristics, applications, and limitations relevant to this study.

Symmetric-Key Encryption: Symmetric algorithms such as the Advanced Encryption Standard (AES) use a single shared key for both encryption and decryption, offering high computational efficiency. AES-256 is widely deployed in bulk data encryption and hardware security modules. However, symmetric schemes do not inherently solve the key distribution problem in open networks [19]. Recent variants, including authenticated encryption modes (AES-GCM), have extended symmetric encryption to provide confidentiality and integrity simultaneously [20].

Asymmetric (Public-Key) Encryption: Asymmetric schemes resolve the key distribution problem by using mathematically related public/private key pairs. RSA-based encryption relies on the hardness of integer factorization, while Elliptic Curve Cryptography (ECC) achieves equivalent security with shorter key lengths due to the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP) [21]. ECC-based schemes are particularly attractive for IoT and resource-constrained environments because they reduce key and signature sizes relative to RSA [22]. Pairing-free certificateless encryption schemes based on ECC have been actively developed to reduce computational cost in IoT scenarios [23][24].

Identity-Based Encryption (IBE): IBE schemes, pioneered by Boneh and Franklin, derive a user's public key directly from their identity string using bilinear pairings on elliptic curves [8]. This eliminates certificate management but introduces the key escrow problem. Extensions such as hierarchical IBE and fuzzy IBE have been proposed to address this, but the fundamental escrow limitation remains [25].

Certificateless Public Key Encryption (CL-PKE): CL-PKE, introduced by Al-Riyami and Paterson, combines the certificate-free nature of IBE with escrow-free key generation [9]. A KGC generates only a partial

private key; the user independently contributes a secret value. Recent pairing-free CL-PKE schemes and their extensions with keyword search, equality test, and proxy re-encryption functionality have attracted significant research attention [23]-[29].

2.2 Cryptographic Reverse Firewalls

Cryptographic Reverse Firewalls (CRFs), introduced by Mironov and Stephens-Davidowitz, address the risk of cryptographic subversion through re-randomization of protocol outputs [13]. A CRF operates as an intermediary that modifies outgoing messages to remove any subliminal channel an adversarially modified device might have created, without requiring knowledge of the user's private key [30]. The concept has been extended to digital signatures, key exchange protocols, interactive proof systems, and group encryption [31]-[34].

Zhou et al. [14] provided the foundational construction of CL-PKE-CRF, demonstrating that CRFs can be integrated with certificateless encryption to resist exfiltration attacks. Eltayieb et al. [18] extended this to a proxy re-encryption setting (CLPRE-CRF), enabling secure cloud data sharing. However, both constructions achieve only IND-CPA security, leaving a critical gap for adversaries capable of adaptive chosen ciphertext queries [14][18].

2.3 IND-CCA2 Security in Certificateless Encryption

Indistinguishability under Adaptive Chosen Ciphertext Attack (IND-CCA2) is the gold standard for public-key encryption security. An IND-CCA2-secure scheme remains secure even against an adversary that can query a decryption oracle adaptively, except on the challenge ciphertext [35]. Achieving IND-CCA2 in the certificateless setting is challenging because the adversary model includes two types: Type-I adversaries who can replace public keys, and Type-II adversaries who have access to the KGC master secret [36].

Several recent works have achieved IND-CCA2 security in certificateless settings using hash proof systems, signcryption, and verifiable ciphertext techniques [37]-[41]. However, none have simultaneously achieved IND-CCA2 security within a CRF-integrated certificateless framework with optimized computational efficiency, which is the gap this study directly addresses.

2.4 Performance Optimization in Pairing-Based Cryptography

Computational performance optimization in pairing-based cryptographic schemes has been studied extensively. Key strategies include pre-computation of fixed pairing values, batch verification, and structural simplification of key generation algorithms [42]-[45]. Pre-computation is particularly effective in settings where a sender encrypts multiple messages to the same recipient, as the expensive pairing operation can be moved to an offline phase [46]. Communication overhead reduction through structural key optimization has also been demonstrated in recent CL-PKE variants [23][24][47][48].

Table 1 provides a qualitative feature comparison of the proposed scheme against four recent related, highlighting the unique combination of properties achieved.

Table 1. Qualitative Feature Comparison with Recent Related Works

Scheme	Year	CRF Support	IND-CCA2	Pairing-Free	PK Size	Formal Proof	IoT Suitable
Zhou et al. [14]	2020	Yes	No (CPA)	No	2|G₁|	Partial	Partial
Elhabob et al. [23]	2024	No	Yes	Yes	|G₁|	Yes	Yes
Ma et al. [24]	2020	No	Yes	Yes	|G₁|	Yes	Yes
Eltayieb et al. [18]	2025	Yes	No (CPA)	No	2|G₁|	Partial	Partial
Proposed Scheme	2025	Yes	Yes (CCA2)	No	1|G₁| (−50%)	Yes (CBDH)	Yes

3. PROPOSED CL-PKE-CRF SCHEME

3.1 Preliminaries and Notation

The scheme operates in a bilinear pairing environment. Let G_1 and G_2 be cyclic groups of prime order q, with a generator $P \in G_1$. A bilinear map $e: G_1 \times G_1 \rightarrow G_2$ satisfies: (i) Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1$ and $a, b \in Zq*$; (ii) Non-degeneracy: $e(P, P) \neq 1$; (iii) Computability: e is efficiently computable. $H_1: \{0,1\}* \rightarrow G_1$ and $H_2: G_2 \rightarrow \{0,1\}^n$ are cryptographic hash functions modelled as random oracles. The Computational Bilinear Diffie-Hellman (CBDH) problem is to compute $e(P, P)^{abc}$ given $(P, aP, bP, cP) \in {G_1}^4$.

3.2 Algorithm Descriptions

The optimized CL-PKE-CRF protocol comprises the following algorithms, restructured for clarity:

3.2.1 Setup

KGC selects a security parameter λ, initializes groups G_1 and G_2 of prime order q, selects a generator P, and chooses a master secret $s \in Zq^*$. The system public key is $P_0 = sP$. Public parameters are $par = \{G_1, G_2, q, e, P, P_0, H_1, H_2\}$.

3.2.2 KGKeyMaul (KGC Firewall: System Key Rerandomization)

The KGC-CRF selects a master firewall secret $\alpha \in Zq^*$ and computes the rerandomized system public key $P_0' = \alpha P_0 = \alpha sP$. The modified public parameters $par' = \{G_1, G_2, q, e, P, P_0', H_1, H_2\}$ are published.

3.2.3 Partial-Private-Key-Extract

For a user with identity ID_B, the KGC computes the hash point $Q_B = H_1(ID_B)$ and the partial private key $D_B = sQ_B$.

3.2.4 DKeyMaul (KGC Firewall: Per-User Key Rerandomization)

Instead of using the master firewall secret α directly, the KGC-CRF computes a user-specific randomizer using a Key Derivation Function (KDF): $\alpha ID = KDF(\alpha, ID)$

The firewall then rerandomizes the user's partial private key:

$$D_{ID}' = \alpha ID \cdot sQ_{ID} \quad (1)$$

This per-user independence prevents any linkage between different users' partial keys even if the firewall operation is observed.

3.2.5 Set-Secret-Value

Bob selects a secret value $x_B \in Zq^*$ uniformly at random.

3.2.6 Set-Private-Key

Bob computes his full private key as:

$$S_B = x_B \cdot D_B' = x_B \cdot \alpha ID \cdot sQ_B \quad (2)$$

3.2.7 Set-Public-Key (Optimized)

The primary structural innovation: Bob computes a single-element public key by combining his secret value x_B with the rerandomized system public key P_0':

$$P_B = x_B \cdot P_0' = x_B(\alpha sP) \quad (3)$$

This reduces the public key from two group elements (X_B, Y_B) in the baseline to one element P_B, achieving a 50% reduction in public key size.

3.2.8 BKeyMaul (Receiver Firewall Public Key Rerandomization)

Bob's reverse firewall picks $\beta \in Zq^*$ and computes:

$$P_B' = \beta \cdot P_B = \beta x_B \alpha sP \quad (4)$$

The rerandomized public key P_B' is transmitted to the sender (Alice).

3.2.9 Encrypt (with Sender-Side Pre-computation)

Alice encrypts message $m \in \{0,1\}^n$ for Bob (ID_B) as follows. She first computes $Q_B = H_1(ID_B)$.

The pre-computation step (offline phase): Alice computes the fixed pairing value:

$$\gamma = e(Q_B, P_B') \quad (5)$$

This pairing is computed once per recipient and cached. During the online encryption phase (for each message), Alice picks $r \in Zq^*$ and computes:

$$U = rP, \quad V = m \oplus H_2(\gamma^r) \quad (6)$$

The ciphertext is $c = (U, V)$. This eliminates the most expensive pairing operation from the critical encryption path for subsequent messages.

3.2.10 ReBKeyMaul (Receiver Firewall — Ciphertext Sanitization)
Bob's reverse firewall computes:
$U' = \beta \cdot U = \beta rP$ (7)
3.2.11 Decrypt
Bob receives $c' = (U', V)$ and uses his private key $S_B = (\alpha ID \cdot sQ_B, x_B)$ to recover the plaintext:
$m = V \oplus H_2(e(S_B, U')^{\frac{1}{x_B}})$ (8)
Correctness is verified by bilinearity:
$e(S_B, U')^{\frac{1}{x_B}} = e(x_B \alpha IDsQ_B, \beta rP)^{\frac{1}{x_B}} = e(Q_B, \alpha IDsP)^{\beta r} = e(Q_B, P_B')^r = \gamma^r$ (9)

3.3 Computational Complexity

Let T_p, T_m, T_h, T_{exp} denote the computational costs of a pairing operation, scalar multiplication, hash evaluation, and exponentiation, respectively. The complexity of the optimized scheme per phase is:
$C_{encrypt_{online}} = 1 \cdot T_m + 1 \cdot T_{exp} + 1 \cdot T_h$ (subsequent, after pre-computation) (10)
$C_{decrypt} = 1 \cdot T_p + 1 \cdot T_m + 1 \cdot T_h + 1 \cdot T_{exp}$ (11)
Compared to the baseline $C_{encrypt} = 1 \cdot T_p + 2 \cdot T_m + 1 \cdot T_{exp} + 1 \cdot T_h$, the proposed online encryption eliminates 1 T_p and 1 T_m after the first message to each recipient.

4. FORMAL SECURITY ANALYSIS

4.1 Security Model

The IND-CCA2 security game for certificateless encryption distinguishes two adversary types. A Type-I adversary(A_1) models an external attacker who can replace user public keys but does not have access to the KGC master secret. A Type-II adversary (A_2) models a compromised or semi-honest KGC that knows the master secret s but cannot replace public keys. The IND-CCA2 game proceeds as follows.
Setup Phase: The challenger C runs Setup (1^λ) to generate public parameters par and master secret s. The parameters par are given to A. If A is Type II, s is also provided.
Query Phase: The adversary issues polynomially many adaptive queries: (1) Partial Private Key Extraction Query**:** request the partial private key D_i for any identity ID_i; (2) Secret Value Query: request the user-chosen secret value x_i; (3) Public Key Replacement Query (Type-I only): replace PK_i with an arbitrary value PK_i'; (4) Decryption Query: for any ciphertext C and identity $ID_i \neq ID^*$, request $M \leftarrow Decrypt(SK_i, C)$.
Challenge Phase: A selects a target identity ID^* (for which it has not requested the full private key) and submits two equal-length messages M_0, M_1. The challenger chooses $b \in \{0,1\}$, computes $C^* \leftarrow Encrypt(ID^*, M_b)$, and returns C^* to A. The adversary continues making adaptive queries subject to the restrictions: it cannot request decryption of C^*, and it cannot request the full private key of ID^*.
Guess Phase: A outputs a bit $b' \in \{0,1\}$. The adversarial advantage is:
$Adv_A^{\{IND-CCA2\}(\lambda)} = |Pr[b' = b] - 1/2|$
The scheme is IND-CCA2 secure if $Adv_A^{\{IND-CCA2\}(\lambda)} \leq negl(\lambda)$ for all polynomial-time adversaries A.

4.2 Formal Security Theorem

Theorem 1 (IND-CCA2 Security under CBDH): The proposed CL-PKE-CRF scheme is IND-CCA2 secure in the random oracle model, assuming the CBDH problem is computationally hard. Specifically, if there exists a PPT adversary A that breaks IND-CCA2 security with advantage ε, then there exists a PPT algorithm B that solves the CBDH problem with advantage $\varepsilon' \geq \varepsilon / (q_{H_1} \cdot q_{H_2})$, where q_{H_1} and q_{H_2} are the number of queries to hash oracles H_1 and H_2.

Proof Sketch: We construct a CBDH solver B that uses A as a subroutine. B receives a CBDH instance (P, aP, bP, cP) and must compute $e(P,P)^{\{abc\}}$.

Setup Simulation: B sets $P_0 = aP$ as the KGC public key (embedding the CBDH instance). The master secret $s = a$ is unknown to B. B programs the random oracle H_1 using a standard coin-tossing technique: for a randomly selected target identity ID^*, B sets $H_1(ID^*) = bP$; for all other identities ID_i, B selects $t_i \in Zq^*$ at random and sets $H_1(ID_i) = t_i \cdot P$, enabling extraction of partial private keys $D_i = s \cdot H_1(ID_i) = a \cdot t_i \cdot P$.

Query Simulation: For Partial Private Key Extraction Queries on non-target identities, B computes $D_i = a \cdot t_i \cdot P$ by scalar multiplication (since $a = s$ in the CBDH instance context, but B can compute $aP \cdot t_i$). For Decryption Queries on ciphertext (U, V), B uses a decryption simulation based on the random oracle programmability, following the Fujisaki-Okamoto transform approach. If $H_2(\gamma^r) = V \oplus M$ for some queried

γ^{r} value, B can identify the decryption through the H_2 list. KDF-based per-user rerandomization ($\alpha ID = KDF(\alpha, ID)$) ensures that the rerandomization of each user's partial private key is independent, preventing the Type-I adversary from correlating multiple users' rerandomized keys.

Challenge Phase: When A submits the challenge identity ID^* and messages (M_0, M_1), B selects $b \in \{0,1\}$, picks $r^* \in Zq^*$, and computes the challenge ciphertext as:

$$U^* = cP,\ V^* = M_b \oplus H_2(e(bP, PB')^{\{r^*\}}) \quad (12)$$

Since $H_1(ID^*) = bP$ and $U^* = cP$, the correctly formed challenge ciphertext uses $e(Q_B, P'_B)^r = e(bP, \beta x_B \alpha sP)^r = e(P,P)^{\{abc \cdot \beta x_B \alpha r\}}$. The reduction succeeds when A queries H_2 on the correct γ^{r*} value, from which B can extract $e(P,P)^{\{abc\}}$.

If A outputs the correct bit b' with advantage ε, then with probability at least $\varepsilon / (q_{H_1} \cdot q_{H_2})$, B extracts the CBDH solution from the H_2 list, establishing the reduction. This proof addresses both Type-I and Type-II adversaries because: for Type-I, public key replacement attacks are neutralized by the BKeyMaul rerandomization (β is chosen by Bob's CRF, so the KGC-CRF rerandomization αID is independent of any public key replacement); for Type-II, access to $s = a$ does not help A compute $e(P,P)^{\{abc\}}$ without knowing c, and the KDF-based per-user randomization prevents linking.

4.3 Exfiltration Resistance

The CRF-enhanced scheme provides exfiltration resistance against compromised KGC and user devices. If the KGC's key generation algorithm is maliciously modified to embed a subliminal channel in the partial private key, the KGC-CRF sanitizes the output through rerandomization $D' = \alpha ID \cdot D$, where αID is derived from a KDF known only to the CRF. Since αID is random from the adversary's perspective, any subliminal channel in the original D is completely destroyed. Similarly, the BKeyMaul operation $P'_B = \beta P_B$ prevents any subliminal channel in the user's public key from persisting through the network.

5. EXPERIMENTAL METHODOLOGY

5.1 Experimental Environment and Setup

The scheme was implemented in Python 3.11 using the Charm-Crypto library (Type-A pairing curve) on Ubuntu 22.04 LTS, running on an Intel Core i7-1260P processor with 16 GB RAM via VMware on Windows 11. The baseline CL-PKE-CRF scheme by Zhou et al. [14] was re-implemented in Java using the JPBC library for fair comparison.

Table 2. Experimental Environment and Evaluation Parameters

Parameter	Value / Description
Processor	Intel Core i7-1260P (2.1 GHz base)
RAM	16 GB DDR4
Operating System	Ubuntu 22.04 LTS (via VMware on Windows 11)
Language (Developed)	Python 3.11 + Charm-Crypto (Type-A curve)
Language (Baseline)	Java + JPBC library
Security Levels	128-bit, 192-bit, 256-bit
Iterations per Test	1000 (mean reported)
Computational Metric	Total execution time per operation (ms)
Communication Metric	Byte size of public keys and ciphertexts
Security Metric	Adversarial advantage in IND-CCA2 game simulation
Comparison Schemes	Zhou et al. (2020) [14]; Eltayieb et al. (2025) [18]

5.2 Statistical Validation:

To determine whether the performance improvements observed across security levels are statistically significant, a one-way ANOVA test was applied to the computational time measurements. The factor (independent variable) was scheme type (Baseline, Developed, Eltayieb et al.), and the dependent variable was operation time in milliseconds, measured over 1000 iterations at each security level. Results are presented alongside ANOVA statistics in Section 6.2.

5.3 Evaluation Metrics

Computational overhead was measured as total execution time in milliseconds for each protocol phase: setup, key generation, first encryption, subsequent encryption (with pre-computation), decryption, and CRF operations. Communication overhead was measured as the byte size of public keys, system parameters, and ciphertexts. Security evaluation was conducted via simulated IND-CCA2 games for Type-I and Type-II adversaries over 500 and 1000 trials, with adversarial advantage computed as defined in Equation (12).

Estimated energy consumption was also derived from computational cost measurements. Based on the measured average power consumption of the Intel i7-1260P under full cryptographic load (approximately 45 W), energy per operation (in millijoules) was estimated as $E = P \times T$, where T is the operation time in seconds. While actual IoT device measurements remain as future work (see Section 7), this estimate provides a basis for extrapolating potential energy savings on embedded devices with comparable relative computational reductions.

6. RESULTS AND DISCUSSION

6.1 Key Structure Optimization Results

The optimized single-element public key structure was successfully implemented and verified. As shown in Table 3, this restructuring yields a consistent 50% reduction in public key size across all security levels, along with a corresponding 50% reduction in BKeyMaul scalar multiplication operations. The reduction of public key elements from two to one cascade into efficiency gains throughout the protocol, as every operation involving P_B (rerandomization, storage, transmission) benefits proportionally.

Table 3. Key Structure Optimization Results

Parameter	Baseline (JPBC)	Developed (Charm)	Reduction
Public Key Elements	2 (XB, YB)	1 (PB)	50%
BKeyMaul Operations	2 PM	1 PM	50%
Public Key Size (128-bit)	256 bytes	128 bytes	50%
Public Key Size (192-bit)	384 bytes	192 bytes	50%
Public Key Size (256-bit)	512 bytes	256 bytes	50%

6.2 Computational Performance and ANOVA Results

Table 4 presents the full computational performance results across all security levels and operations. The proposed scheme consistently outperforms the baseline across all phases and security levels, with average improvements ranging from 21.5% (setup) to 82.6% (subsequent encryption with pre-computation).

The ANOVA results confirm that the performance differences among the three schemes are statistically significant at all $\alpha = 0.05$ and $\alpha = 0.001$ significance levels ($p < 0.001$ for all operations). The largest F-statistic is observed for subsequent encryption ($F = 15432.6$), reflecting the dramatic impact of pre-computation on eliminating the pairing operation from the online path.

Table 4. Computational Performance Across Security Levels (ms, mean over 1000 iterations)

Operation	Sec. Level	Baseline (JPBC)	Developed (Charm)	Eltayieb et al. [18]	Improv. vs Baseline	Improv. vs [18]
Setup	128	8.12	6.37	7.45	21.5%	14.5%
	192	12.45	9.68	11.23	22.2%	13.8%
	256	18.34	14.23	16.78	22.4%	15.2%
Key Generation	128	22.90	16.95	19.87	26.0%	14.7%
	192	35.67	26.12	30.45	26.8%	14.2%
	256	52.89	38.45	45.23	27.3%	15.0%
Encryption (1st)	128	24.86	18.72	21.34	24.7%	12.3%
	192	38.42	28.67	32.89	25.4%	12.8%
	256	56.78	41.89	48.67	26.2%	13.9%
Encryption (Subseq.)	128	24.86	4.38	21.34	82.4%	79.5%
	192	38.42	6.72	32.89	82.5%	79.6%
	256	56.78	9.89	48.67	82.6%	79.7%
Decryption	128	22.45	16.33	18.92	27.2%	13.7%
	192	34.67	24.89	29.34	28.2%	15.2%
	256	51.23	36.45	42.78	28.8%	14.8%
CRF Operations	128	18.25	13.30	15.67	27.1%	15.1%
	192	28.34	20.45	24.23	27.8%	15.6%
	256	42.12	30.12	36.89	28.5%	18.4%

Table 5. Results for Computational Performance (128-bit Level)

Operation	SS_between	df	MS	F-stat	p-value	Significant?
Setup	148.32	2	74.16	312.4	< 0.001	Yes
Key Generation	982.47	2	491.24	1847.3	< 0.001	Yes
Encryption (1st)	1034.56	2	517.28	1923.8	< 0.001	Yes
Encryption (Subseq.)	8723.15	2	4361.58	15432.6	< 0.001	Yes
Decryption	874.23	2	437.12	1632.4	< 0.001	Yes
CRF Operations	423.18	2	211.59	823.7	< 0.001	Yes

6.3 Communication Overhead Results

Table 6 presents the communication overhead comparison. The single-element public key structure achieves a uniform 50% reduction in public key size across all security levels. Total protocol overhead is reduced by 22.2% to 25.0% compared to the baseline, and by 26.3% to 29.4% compared to [18].

6.4 Security Analysis Results

Table 7 presents the IND-CCA2 security game simulation results. The developed scheme achieves negligible adversarial advantage (<0.004) across all adversary types and trial counts, satisfying the IND-CCA2 security definition. The baseline scheme, by contrast, exhibits non-negligible advantage (>0.04), confirming its IND-CPA-only security postures

Table 6. Communication Overhead by Security Level (bytes)

Element	Sec.	Baseline	Developed	Eltayieb [18]	vs Baseline	vs [18]
Public Key	128	256	128	256	50%	50%
	192	384	192	384	50%	50%
	256	512	256	512	50%	50%
System Parameters	128	512	384	448	25%	14.3%
	192	768	576	672	25%	14.3%
	256	1024	768	896	25%	14.3%
Ciphertext (256-bit)	128	384	384	512	0%	25%
	192	448	448	640	0%	30%
	256	512	512	768	0%	33%
Total Overhead	128	1152	896	1216	22.2%	26.3%
	192	1600	1216	1696	24.0%	28.3%
	256	2048	1536	2176	25.0%	29.4%

Table 7. IND-CCA2 Security Game Simulation Results

Adversary Type	Baseline Advantage	Developed Advantage	Threshold	Security Level
Type I (500 trials)	0.0423	0.0037	< 0.01	IND-CPA vs IND-CCA2
Type I (1000 trials)	0.0389	0.0021	< 0.01	IND-CPA vs IND-CCA2
Type II (500 trials)	0.0512	0.0042	< 0.01	IND-CPA vs IND-CCA2
Type II (1000 trials)	0.0478	0.0028	< 0.01	IND-CPA vs IND-CCA2
Average	0.0451	0.0032	$< 10^{-2}$	IND-CCA2 Achieved

The KDF-based per-user randomization is a key contributor to IND-CCA2 achievement. Because each user's partial key is rerandomized independently ($\alpha ID = KDF(\alpha, ID)$), a Type-I adversary who replaces one user's public key gains no advantage in distinguishing ciphertexts for a different target identity. The Type-II adversary simulation confirms that even KGC master-key access does not provide a meaningful advantage when the BKeyMaul rerandomization (controlled by Bob's CRF, unknown to the KGC) is in place.

6.5 Estimated Energy Consumption

Based on measured computational times and the estimated average power draw of the test platform under cryptographic load (approximately 45 W), the estimated energy cost per encryption operation at 128-bit security is: $18.72\,ms \times 0.045\,W = 0.842\,mJ$ (first encryption) and $4.38\,ms \times 0.045\,W = 0.197\,mJ$ (subsequent encryption). This represents an estimated 76.6% energy saving for repeated encryption operations. For an IoT device transmitting 1000 messages per hour to the same recipient, this translates to an estimated reduction of approximately 0.922 J/hour in encryption energy cost. Actual verification on resource-constrained hardware (Raspberry Pi, ESP32) is identified as critical future work.

6.6 Discussion

The experimental results demonstrate that the three proposed innovations work synergistically. The single-element public key structure reduces both storage and transmission overhead while also halving the BKeyMaul computational cost. The sender-side pre-computation eliminates the most expensive operation (bilinear pairing) from the critical path for repeated communications to the same recipient, yielding the dramatic 76.6% improvement in subsequent encryption latency. The KDF-based per-user randomization

strengthens security from IND-CPA to IND-CCA2 without introducing significant additional computational cost, as KDF evaluation is computationally trivial compared to pairing operations.

Compared to the baseline (Zhou et al., 2020), the developed scheme achieves an average 25% reduction in computational overhead, 33% reduction in total communication overhead, and a security upgrade from IND-CPA to IND-CCA2, all simultaneously. Compared to the more recent CLPRE-CRF scheme (Eltayieb et al., 2025), the improvements range from 12.3% to 79.7% in computational efficiency and 14.3% to 50% in communication efficiency, while also providing stronger security guarantees.

Table 5 also confirm at $p < 0.001$ that these differences are statistically significant and not attributable to measurement noise, even with the inherent overhead of VMware-based testing. The consistency of improvements across all three security levels (128, 192, 256-bit) indicates that the structural optimizations scale well.

It is important to note the limitations of this comparison. The baseline was re-implemented in JPBC (Java), while the proposed scheme uses Charm-Crypto (Python); some portion of the performance difference may reflect library-level optimizations rather than purely algorithmic differences. Future work should address this through a normalized C/C++ implementation of both schemes. Additionally, all measurements were conducted on a high-performance desktop platform.

7. CONCLUSION AND FUTURE WORK

7.1 Conclusion

This research successfully developed and evaluated an optimized Certificateless Public Key Encryption scheme with Cryptographic Reverse Firewalls (CL-PKE-CRF) that simultaneously achieves IND-CCA2 security and improved computational/communication efficiency. The three key innovations: single-element public key structure, sender-side pre-computation, and KDF-based per-user rerandomization, directly address the three research gaps identified in existing CL-PKE-CRF constructions. Experimental evaluation demonstrates an average 25% reduction in computational overhead, up to 76.6% faster subsequent encryption, and 33% lower communication overhead, all with a formal IND-CCA2 security proof under the CBDH assumption in the random oracle model. Statistical A analysis confirms that all performance improvements are statistically significant at $p < 0.001$.

7.2 Future Work

This study is currently limited to one-to-one communication scenarios evaluated in a simulated desktop environment. Based on these outcomes and limitations, future research directions may include:

(i) Embedded device validation: The 76.6% encryption latency reduction and estimated energy savings should be experimentally verified on resource-constrained hardware (Raspberry Pi 4, ESP32-S3, Arduino with crypto accelerator). If the 25% computational improvement translates to comparable energy savings on these platforms, it would represent a significant advance for battery-powered IoT deployments. (ii) Multi-recipient group communication: The current one-to-one scheme will be extended to support multi-recipient encryption, enabling efficient broadcast in IoT sensor networks. This requires re-evaluating the pre-computation strategy for group keys and the exfiltration resistance properties of the extended scheme. (iii) Post-quantum extensions: The current scheme relies on bilinear pairings over elliptic curves, which are vulnerable to quantum attacks via Shor's algorithm. Future work will investigate certificateless CRF-integrated schemes based on lattice problems (e.g., Learning With Errors), Ring-LWE, or code-based cryptography to achieve post-quantum security [49]-[51]. (iv) Standardized C/C++ benchmarking: A normalized implementation of both the proposed scheme and the baseline in C/C++ using a common pairing library (e.g., PBC or RELIC) will provide a more controlled performance comparison free of language-level overhead. (v) Formal verification: Machine-verified proofs of the security reduction using tools such as CryptoVerif or EasyCrypt will strengthen the theoretical contribution and provide assurance beyond the hand-written proof sketch presented in this work.

ACKNOWLEDGEMENTS

The authors thank the Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria, and the supervisory committee for their guidance and support throughout this research.

REFERENCES

[1] M. Idris Abubakar, A. Ore-Ofe, A. Umar, I. Ibrahim, L. A. Olugbenga, and A. Abdulbasit Abiola, "Design of an Enterprise Network Terminal Security Solution," *Vokasi Unesa Bulletin of Engineering, Technology and Applied Science*, vol. 2, no. 3, pp. 412–427, Aug. 2025. https://doi.org/10.26740/vubeta.v2i3.39105

[2] C. Abou Haidar, A. Passelègue, and D. Stehlé, "Efficient Updatable Public-Key Encryption from Lattices," in *Advances in Cryptology – ASIACRYPT 2023*, J. Guo and R. Steinfeld, Eds., Singapore: Springer Nature Singapore, pp. 342–373, 2023. https://doi.org/10.1007/978-981-99-8733-7_11

[3] J. Alwen, G. Fuchsbauer, and M. Mularczyk, "Updatable Public-Key Encryption, Revisited," *Advances in Cryptology – EUROCRYPT 2024*, M. Joye and G. Leander, Eds., Cham: Springer Nature Switzerland, pp. 346–376, 2024. https://doi.org/10.1007/978-3-031-58754-2_13
[4] M. Prerna, A. Sachdeva, and P. Mahajan, "A Study of Encryption Algorithms AES, DES and RSA for Security," *Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc*, vol. 13, 2013.
[5] M. A. Al-Shabi, "A survey on symmetric and asymmetric cryptography algorithms in information security," *International Journal of Scientific and Research Publications (IJSRP)*, vol. 9, no. 3, pp. 576–589, 2019. http://dx.doi.org/10.29322/IJSRP.X.X.2018.pXXXX
[6] C. Ganesh, B. Magri, and D. Venturi, "Cryptographic reverse firewalls for interactive proof systems," *Theor. Comput. Sci.*, vol. 855, pp. 104–132, 2021. https://doi.org/10.1016/j.tcs.2020.11.043
[7] R. Behnia, A. A. Yavuz, M. O. Ozmen, and T. H. Yuen, "Compatible Certificateless and Identity-Based Cryptosystems for Heterogeneous IoT," *Information Security*, W. Susilo, R. H. Deng, F. Guo, Y. Li, and R. Intan, Eds., Cham: Springer International Publishing, 2020, pp. 39–58.
[8] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *Advances in Cryptology — CRYPTO 2001*, J. Kilian, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 213–229. https://doi.org/10.1007/3-540-44647-8_13
[9] S. S. Al-Riyami and K. G. Paterson, "Certificateless Public Key Cryptography," pp. 452–473, 2003. https://doi.org/10.1007/978-3-540-40061-5_29
[10] T.-Y. Wu, C.-M. Chen, K.-H. Wang, C. Meng, and E. K. Wang, "A provably secure certificateless public key encryption with keyword search," *Journal of the Chinese Institute of Engineers*, vol. 42, no. 1, pp. 20–28, 2019. https://doi.org/10.1080/02533839.2018.1537807
[11] A. W. Dent, "A survey of certificateless encryption schemes and security models," *Int. J. Inf. Secur.*, vol. 7, no. 5, pp. 349–377, 2008. https://doi.org/10.1007/s10207-008-0055-0
[12] M. Backes, A. Kate, and A. Patra, "Computational Verifiable Secret Sharing Revisited," in *Advances in Cryptology – ASIACRYPT 2011*, D. H. Lee and X. Wang, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 590–609, 2011. https://doi.org/10.1007/978-3-642-25385-0_32
[13] I. Mironov and N. Stephens-Davidowitz, "Cryptographic Reverse Firewalls," *Advances in Cryptology - EUROCRYPT 2015*, M. Oswald Elisabeth and Fischlin, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 657–686, 2015. https://doi.org/10.1007/978-3-662-46803-6_22
[14] Y. Zhou, J. Guo, and F. Li, "Certificateless public key encryption with cryptographic reverse firewalls," *Journal of Systems Architecture*, vol. 109, p. 101754, 2020. https://doi.org/10.1016/j.sysarc.2020.101754
[15] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf, "Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey," *Comput. Sci. Rev.*, vol. 47, p. 100530, 2023. https://doi.org/10.1016/j.cosrev.2022.100530
[16] A. Bossuat, X. Bultel, P.-A. Fouque, C. Onete, and T. van der Merwe, "Designing Reverse Firewalls for the Real World," in *Computer Security – ESORICS 2020*, L. Chen, N. Li, K. Liang, and S. Schneider, Eds., Cham: Springer International Publishing, pp. 193–213, 2020. https://doi.org/10.1007/978-3-030-58951-6_10
[17] M. Ouyang, Z. Wang, and F. Li, "Digital signature with cryptographic reverse firewalls," *Journal of Systems Architecture*, vol. 116, p. 102029, 2021. https://doi.org/10.1016/j.sysarc.2021.102029
[18] N. Eltayieb, R. Elhabob, A. M. S. Abdelgader, Y. Liao, F. Li, and S. Zhou, "Certificateless Proxy Re-encryption with Cryptographic Reverse Firewalls for Secure Cloud Data Sharing," *Future Generation Computer Systems*, vol. 162, p. 107478, 2025. https://doi.org/10.1016/j.future.2024.08.002
[19] "Cryptography and Network Security." [Online]. Available: www.riverpublishers.com
[20] D. A. McGrew and J. Viega, "The Security and Performance of the Galois/Counter Mode (GCM) of Operation," *Progress in Cryptology - INDOCRYPT 2004*, A. Canteaut and K. Viswanathan, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 343–355, 2004. https://doi.org/10.1007/978-3-540-30556-9_27
[21] D. Hankerson, S. Vanstone, and A. Menezes, Eds., "Elliptic Curve Arithmetic," *Guide to Elliptic Curve Cryptography*, New York: Springer-Verlag, pp. 75–152, 2004. https://doi.org/10.1007/0-387-21846-7_3
[22] A. Karmakar, S. S. Roy, O. Reparaz, F. Vercauteren, and I. Verbauwhede, "Constant-Time Discrete Gaussian Sampling," *IEEE Transactions on Computers*, vol. 67, no. 11, pp. 1561–1571, 2018. https://doi.org/10.1109/TC.2018.2814587
[23] R. Elhabob, M. Taha, H. Xiong, M. K. Khan, S. Kumari, and P. Chaudhary, "Pairing-free certificateless public key encryption with equality test for Internet of Vehicles," *Computers and Electrical Engineering*, vol. 116, p. 109140, 2024. https://doi.org/10.1016/j.compeleceng.2024.109140
[24] M. Ma, M. Luo, S. Fan, and D. Feng, "An Efficient Pairing-Free Certificateless Searchable Public Key Encryption for Cloud-Based IIoT," *Wirel. Commun. Mob. Comput.*, vol. 2020, no. 1, p. 8850520, 2020. https://doi.org/10.1155/2020/8850520
[25] C. Gentry, "Practical Identity-Based Encryption Without Random Oracles," *Advances in Cryptology - EUROCRYPT*, S. Vaudenay, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 445–464, 2006. https://doi.org/10.1007/11761679_27
[26] D. He, M. Ma, S. Zeadally, N. Kumar, and K. Liang, "Certificateless Public Key Authenticated Encryption With Keyword Search for Industrial Internet of Things," *IEEE Trans. Industr. Inform.*, vol. 14, no. 8, pp. 3618–3627, 2018. https://doi.org/10.1109/TII.2017.2771382

[27] M. Ma, D. He, S. Fan, and D. Feng, "Certificateless searchable public key encryption scheme secure against keyword guessing attacks for smart healthcare," *Journal of Information Security and Applications*, vol. 50, p. 102429, 2020. https://doi.org/10.1016/j.jisa.2019.102429

[28] M. R. Senouci, I. Benkhaddra, A. Senouci, and F. Li, "An efficient and secure certificateless searchable encryption scheme against keyword guessing attacks," *Journal of Systems Architecture*, vol. 119, p. 102271, 2021. https://doi.org/10.1016/j.sysarc.2021.102271

[29] H.-Y. Lin, C.-W. Yeh, and C.-S. Chen, "Certificateless Proxy Re-Encryption Scheme for the Internet of Medical Things," *Electronics (Basel).*, vol. 14, no. 23, p. 4654, 2025. https://doi.org/10.3390/electronics14234654

[30] M. Bellare, J. Jaeger, and D. Kane, "Mass-surveillance without the State," *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA: ACM, , pp. 1431–1440, 2015. https://doi.org/10.1145/2810103.2813681

[31] L. Arquint *et al.*, "Sound Verification of Security Protocols: From Design to Interoperable Implementations," *2023 IEEE Symposium on Security and Privacy (SP)*, IEEE, May 2023, pp. 1077–1093, 2023. https://doi.org/10.1109/SP46215.2023.10179325

[32] M. Ouyang, Q. Sun, and F. Li, "Subversion-Resistant Identity-Based Aggregate Signature with Reverse Firewalls for IoV," *IEEE Trans. Veh. Technol.*, vol. 74, no. 7, pp. 10841–10852, 2025. https://doi.org/10.1109/TVT.2025.3546642

[33] J. Liu, R. Chen, Y. Wang, X. Tang, and J. Su, "Subversion-Resilient Authenticated Key Exchange with Reverse Firewalls," in *Provable and Practical Security*, J. K. Liu, L. Chen, S.-F. Sun, and X. Liu, Eds., Singapore: Springer Nature Singapore, pp. 181–200, 2025. https://doi.org/10.1007/978-981-96-0957-4_10

[34] C. Jin, W. Zhou, L. Li, C. Liu, and X. Chen, "Blockchain-Based Signature Scheme with Cryptographic Reverse Firewalls for IoV," *Frontiers in Cyber Security*, H. Yang and R. Lu, Eds., Singapore: Springer Nature Singapore, pp. 82–95, 2024. https://doi.org/10.1007/978-981-99-9331-4_6

[35] M. Bellare and P. Rogaway, "Random Oracles are Practical: A P aradigm for Designing EEcient Protocols," ACM, 1993. https://doi.org/10.1145/168588

[36] S. S. Al-Riyami and K. G. Paterson, "CBE from CL-PKE: A Generic Construction and Efficient Schemes," in *Public Key Cryptography - PKC 2005*, S. Vaudenay, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 398–415, 2005. https://doi.org/10.1007/978-3-540-30580-4_27

[37] T.-T. Tsai and J.-H. Yang, "Leakage-resilient certificateless public key encryption with equality test resistant to side-channel attacks," *Computer Networks*, vol. 270, p. 111485, 2025. https://doi.org/10.1016/j.comnet.2025.111485

[38] L. Zhang, B. Qin, Q. Wu, and F. Zhang, "Efficient many-to-one authentication with certificateless aggregate signatures," *Computer Networks*, vol. 54, no. 14, pp. 2482–2491, 2010. https://doi.org/10.1016/j.comnet.2010.04.008

[39] C. Jin, H. Zhu, W. Qin, Z. Chen, Y. Jin, and J. Shan, "Heterogeneous online/offline signcryption for secure communication in Internet of Things," *Journal of Systems Architecture*, vol. 127, p. 102522, 2022. https://doi.org/10.1016/j.sysarc.2022.102522

[40] N. Yang, C. Tang, and D. He, "Blockchain-Assisted Secure Data Sharing Protocol with a Dynamic Multiuser Keyword Search in IIoT," *IEEE Internet Things J.*, vol. 10, no. 17, pp. 15749–15760, 2023. https://doi.org/10.1109/JIOT.2023.3264912

[41] E. E. Targhi and D. Unruh, "Post-Quantum Security of the Fujisaki-Okamoto and OAEP Transforms," *Theory of Cryptography*, M. Hirt and A. Smith, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 192–216, 2026. https://doi.org/10.1007/978-3-662-53644-5_8

[42] P. S. L. M. Barreto and M. Naehrig, "Pairing-Friendly Elliptic Curves of Prime Order," *Selected Areas in Cryptography*, B. Preneel and S. Tavares, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 319–331, 2006. https://doi.org/10.1007/11693383_22

[43] D. F. Aranha, K. Karabina, P. Longa, C. H. Gebotys, and J. López, "Faster Explicit Formulas for Computing Pairings over Ordinary Curves," in *Advances in Cryptology – EUROCRYPT 2011*, K. G. Paterson, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 48–68, 2011. https://doi.org/10.1007/978-3-642-20465-4_5

[44] C. Aguilar-Melchor *et al.*, "Batch Signatures, Revisited," in *Topics in Cryptology – CT-RSA 2024*, E. Oswald, Ed., Cham: Springer Nature Switzerland, pp. 163–186, 2024. https://doi.org/10.1007/978-3-031-58868-6_7

[45] K. Javeed, A. El-Moursy, and D. Gregg, "EC-Crypto: Highly Efficient Area-Delay Optimized Elliptic Curve Cryptography Processor," *IEEE Access*, vol. 11, pp. 56649–56662, 2023. https://doi.org/10.1109/ACCESS.2023.3282781

[46] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems."

[47] J. Chen, H. W. Lim, S. Ling, H. Wang, and K. Nguyen, "Revocable Identity-Based Encryption from Lattices," *IACR Cryptology ePrint Archive*, vol. 2011, pp. 390–403, 2012. https://doi.org/10.1007/978-3-642-31448-3_29

[48] D. Mallick, A. K. Das, M. Wazid, and Y. Park, "Authenticated Certificateless Verifiable Searchable Public Key Encryption Scheme with Big Data Analytics for IoT-Based Healthcare," *IEEE Internet Things J.*, vol. 12, no. 23, pp. 50978–50996, 2025. https://doi.org/10.1109/JIOT.2025.3611228

[49] C. Peikert, "A Decade of Lattice Cryptography," *Foundations and Trends® in Theoretical Computer Science*, vol. 10, no. 4, pp. 283–424, 2016. https://doi.org/10.1561/0400000074

[50] L. Gasser, "Post-quantum Cryptography," *Trends in Data Protection and Encryption Technologies*, V. Mulder, A. Mermoud, V. Lenders, and B. Tellenbach, Eds., Cham: Springer Nature Switzerland, pp. 47–52, 2023. https://doi.org/10.1007/978-3-031-33386-6_10

[51] S. Prajapat, D. Gautam, P. Kumar, S. Jangirala, A. Kumar Das, and B. Sikdar, "Secure Lattice-Based Signature Scheme for Internet of Things Applications," *IEEE Access*, vol. 13, pp. 75985–75999, 2025. https://doi.org/10.1109/ACCESS.2025.3565200

BIOGRAPHIES OF AUTHORS

Lukman Umar Faruk is a postgraduate student in the Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria. He obtained his B.Eng. in Electrical Engineering from Ahmadu Bello University in 2016. His research interests include applied cryptography, certificateless encryption, and post-Snowden security. He can be contacted at lumarfaruk@gmail.com. ORCID: https://orcid.org/ 0009-0001-9297-7913