An enhanced identity-based digital signature scheme for secure blockchain transactions

Liu Yi[1,3#], Sharifah Md Yasin[1,2], Mohd Izuan Hafez Ninggal[1], Aziah Asmawi[1]

1 Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 Serdang, Selangor, MALAYSIA.
2 Institute of Mathematical Research, Universiti Putra Malaysia, 43400 Serdang, Selangor, MALAYSIA.
3 Guizhou Traffic Technician and Transportation College, Guiyang, 550008 Guizhou, CHINA.
Corresponding author. E-mail: gs64695@student.upm.edu.my.

Abstract The security core of blockchain technology relies on digital signature schemes. However, existing schemes face numerous challenges when applied on a large scale, such as complex key management, reliance on certificate infrastructure, potential key escrow risks, and lack of resistance to quantum computing capabilities. To address these issues, this paper proposes a novel enhanced certificateless identity-based digital signature scheme. This scheme ingeniously integrates certificateless cryptosystem and lattice cryptography, aiming to simultaneously achieve identity-friendly public key management, effectively mitigate the key escrow problem, and lay theoretical foundation for post-quantum security. This paper first presents the formal definition and detailed construction of the scheme. Then, under the random oracle model, the security of its existence being unforgeable is reduced to the computational difficulty of the short integer solution problem on the lattice. The performance evaluation of the system shows that, compared with the traditional scheme based on bilinear pairing, this scheme significantly improves security while maintaining reasonable computational overhead. Experimental results show that at the 128-bit security level, the signing time is 4.8 ms and the verification time is 2.1 ms. Finally, this paper elaborates in detail on the application model of this scheme in secure blockchain transactions, demonstrates how it simplifies the transaction process by using human-readable identity identifiers, and through its anti-quantum and decentralized trust characteristics, provides a powerful cryptographic primitive for building the next generation of secure, efficient and user-friendly blockchain systems.

Key words: Blockchain security Certificateless signature Identity-based cryptography Grid password; Post-quantum security Digital signature
Received 26 March 2026 **Revised** 5 April 2026 **Accepted** 15 April 2026 **In press** 20 April 2026 **Online** 22 April 2026

Original Article

INTRODUCTION

The Critical Role of Digital Signatures in Blockchain

Blockchain technology has emerged as a transformative force, pioneering a paradigm of decentralized trust and enabling a new generation of applications from cryptocurrencies to decentralized finance and supply chain management (Nakamoto, 2008), including smart contract platforms such as Ethereum (Buterin, 2014). At the heart of this innovation lies the ability to execute secure and verifiable transactions without reliance on central authority. This critical security property is fundamentally underpinned by digital signature schemes. In a typical blockchain transaction, as illustrated in Figure 1, the sender uses their private key to generate a digital signature over the transaction data. This signature serves three indispensable functions: it provides authentication by verifying the sender's identity, ensures data integrity by detecting any alteration of the signed transaction, and guarantees non-repudiation, preventing the sender from denying their authorization. Consequently, the security and efficiency of the entire blockchain ecosystem are directly contingent upon the robustness of its underlying digital signature scheme. Recent studies have also explored lattice-based quantum-safe signature schemes for blockchain and IoT environments (Bagchi *et al.*, 2025). The importance of post-quantum protection in blockchain systems has been widely highlighted in recent surveys (Gharavi *et al.*, 2024).

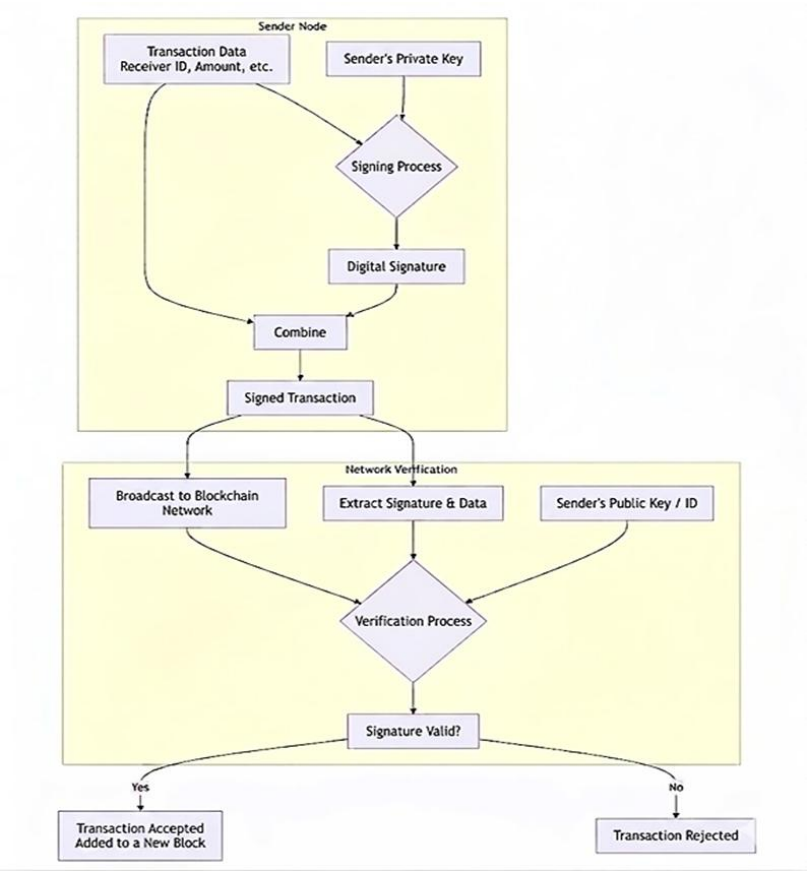

Figure 1. A simplified diagram of a blockchain transaction. The sender's private key generates a signature for the transaction data, which is verified by all network nodes using the sender's public key before the transaction is added to a block.

Limitations of Existing Signature Schemes in Blockchain

Despite their widespread adoption, the digital signature schemes currently deployed in major blockchain systems exhibit significant limitations that threaten their long-term viability and security. The most prevalent scheme, the Elliptic Curve Digital Signature Algorithm (ECDSA) used by Bitcoin and Ethereum, faces two primary challenges. First, it relies on a Public Key Infrastructure (PKI) model, where users are identified by cryptographically generated, random-looking public keys. This leads to poor usability and complicates key management, as these keys are not human-meaningful and must be securely associated with the user's identity. Second, and more critically, ECDSA is vulnerable to attacks from quantum computers. Shor's algorithm, if run on a sufficiently powerful quantum computer, could efficiently break the elliptic curve discrete logarithm problem, rendering ECDSA and similar schemes completely insecure (Shor, 1997).

To address the usability issue of PKI, Identity-Based Signature (IBS) schemes were proposed. In an IBS system, a user's publicly known identifier, such as an email address or phone number, can serve directly as their public key. This eliminates the need for digital certificates and simplifies the key management process. However, traditional IBS schemes introduce a single point of failure and a critical security vulnerability known as the key escrow problem. A trusted third party called the Private Key Generator (PKG) holds the master key and can generate the private keys for all users. This grants the PKG the power to forge signatures on behalf of any user, which is an unacceptable level of trust for a decentralized and trust-minimized environment like blockchain. In summary, the current landscape presents a trilemma: we have efficient schemes with poor usability and no quantum resistance (ECDSA), and usable schemes with a fundamental trust flaw (traditional IBS). None of the

existing mainstream solutions simultaneously provide usability, strong security without key escrow, and preparedness for the quantum era.

Our Proposed Solution: An Enhanced CL-IBS Scheme

To simultaneously resolve the aforementioned limitations, this paper proposes a novel Enhanced Identity-Based Digital Signature Scheme specifically designed for secure blockchain transactions. Our solution is built upon two pivotal cryptographic advancements:

The certificateless cryptography paradigm

Our scheme adopts a Certificateless Identity-Based Signature (CL-IBS) architecture. This paradigm elegantly eliminates the key escrow problem of traditional IBS. In our model, a user's full private key is composed of two parts: a partial private key generated by a Key Generation Center (KGC) and a secret value chosen by the user itself. Consequently, the KGC no longer has access to the user's complete private key and cannot forge their signatures, while the user's public key can still be derived from their identity.

Post-quantum security assumptions

To safeguard blockchain transactions against future quantum attacks, we construct our scheme based on the computational hardness of lattice-based problems, specifically the Short Integer Solution (SIS) and Learning With Errors (LWE) problems. These problems are currently believed to be intractable for both classical and quantum computers, thereby providing a foundation for post-quantum security. By integrating the certificateless model with lattice-based cryptography, our enhanced scheme achieves a unique combination of usability, strong security, and quantum-resistance.

Main Contributions

Novel scheme design

We present the first detailed construction of a lattice-based certificateless IBS scheme that requires no secure channel for key distribution. This design effectively decouples the trust assumption from a single PKG, making it inherently more suitable for decentralized blockchain environments.

Rigorous security proof

We define a formal security model for our scheme and provide a comprehensive security analysis. We demonstrate that our proposed scheme is provably secure against existential forgery under adaptive chosen-message attacks (EUF-CMA) in the random oracle model, under the assumption that the SIS problem is computationally hard.

Comprehensive performance evaluation

We conduct a thorough performance analysis, comparing the computational and communication overhead of our scheme against established schemes like ECDSA and BLS signatures. The results indicate that our scheme offers a viable trade-off, providing enhanced security features with a reasonable and practical performance profile.

Blockchain application and evaluation

We delineate a concrete implementation model for integrating our signature scheme into a blockchain transaction workflow. Furthermore, we analyze the potential impact of our scheme on blockchain performance metrics, including transaction throughput, verification latency, and storage requirements, demonstrating its practical applicability.

LITERATURE REVIEW AND PRELIMINARIES

This section provides the foundational knowledge required to understand the context and construction of our proposed scheme. We begin with a review of the fundamental role of digital signatures in blockchain, followed by an analysis of existing signature paradigms and their limitations. Finally, we introduce the core cryptographic primitives upon which our enhanced scheme is built.

Fundamentals of Blockchain and Digital Signatures

The security of blockchain technology is intrinsically linked to cryptographic digital signatures. A blockchain can be conceptualized as a distributed, immutable ledger of transactions, maintained by a network of mutually distrusting nodes. For a transaction to be valid and accepted by the network, it must be irrefutably authorized by its sender. This is where digital signature schemes become paramount. Formally, a standard digital signature scheme comprises three polynomial-time algorithms.

KeyGen (Key Generation): On input a security parameter λ, this algorithm outputs a pair of keys: a public key pk and a private (signing) key sk.
Sign (Signature Generation): On input a private key sk and a message m, this algorithm outputs a signature σ.
Verify (Signature Verification): On input a public key pk, a message m, and a signature σ, this algorithm outputs a bit $b \in \{0,1\}$, indicating whether the signature is valid (1) or invalid (0).

The core security property required for a signature scheme used in blockchain is Existential Unforgeability under Adaptive Chosen-Message Attacks (EUF-CMA). This means that an adversary, even after obtaining signatures on a set of messages of their choice, cannot forge a valid signature for any new message. In blockchain systems like Bitcoin and Ethereum, the Elliptic Curve Digital Signature Algorithm (ECDSA) is the standard. While efficient and widely adopted, its reliance on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP) and its operational model present significant challenges, as outlined in the introduction and further critiqued in subsequent sections.

Identity-Based and Certificateless Cryptography

To mitigate the key management complexities of traditional PKI, Shamir (1985) introduced the concept of Identity-Based Cryptography (IBC). In an Identity-Based Signature (IBS) scheme, a user's publicly available identifier (e.g., email, phone number) serves as their public key. The system is managed by a trusted Key Generation Center (KGC) which holds a master key. The typical workflow of a traditional IBS scheme is shown in Figure 2 and involves the following steps.

Setup: The KGC generates system parameters and a master public/private key pair.
Extract: A user submits their identity ID to the KGC. The KGC uses the master private key to compute and return the corresponding user private key skID.
Sign: The user signs a message m using their private key skID.
Verify: A verifier checks the signature using the user's identity ID and the KGC's master public key.

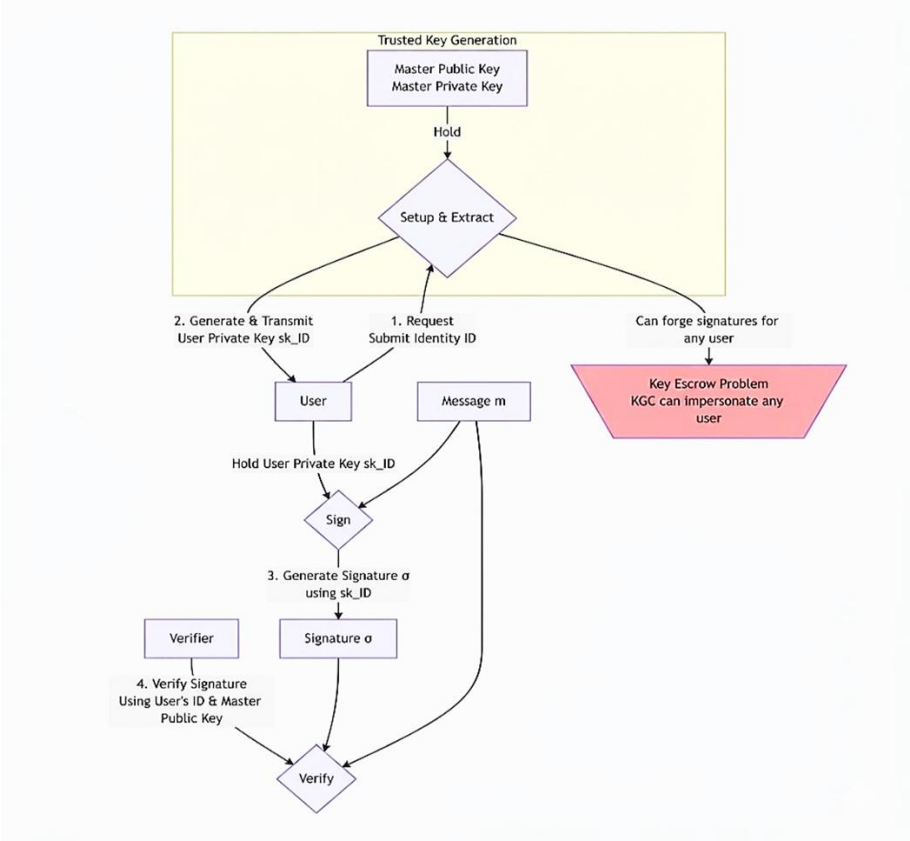

Figure 2. The workflow of a traditional IBS scheme, highlighting the central role of the KGC in generating all user private keys, which introduces the key escrow problem.

While IBS simplifies key management, the necessity for the KGC to generate all user private keys creates the inherent key escrow problem. The KGC can impersonate any user by forging their signatures, which violates the principle of non-repudiation and is a critical vulnerability in trust-sensitive environments like blockchain.

To resolve this fundamental issue, Al-Riyami & Paterson (2003) introduced the Certificateless Public Key Cryptography (CL-PKC) paradigm in 2003. CL-PKC elegantly eliminates the key escrow problem without reintroducing the complexities of certificates. In a Certificateless Signature (CLS) scheme, a user's full private key is a combination of two components. The first component is the partial private key (DID) generated by the KGC, which binds the user's identity to the system, and the second is the user secret key(xID) generated by the user themselves. The user's public key (PKID) is correspondingly derived from both the KGC's public parameters and the user's secret value. This architecture, illustrated in Figure 3, ensures that neither the KGC (which does not know xID) nor any other party (which does not know DID) can fully compromise the user's private key. This model provides a superior foundation for building secure and decentralized applications.

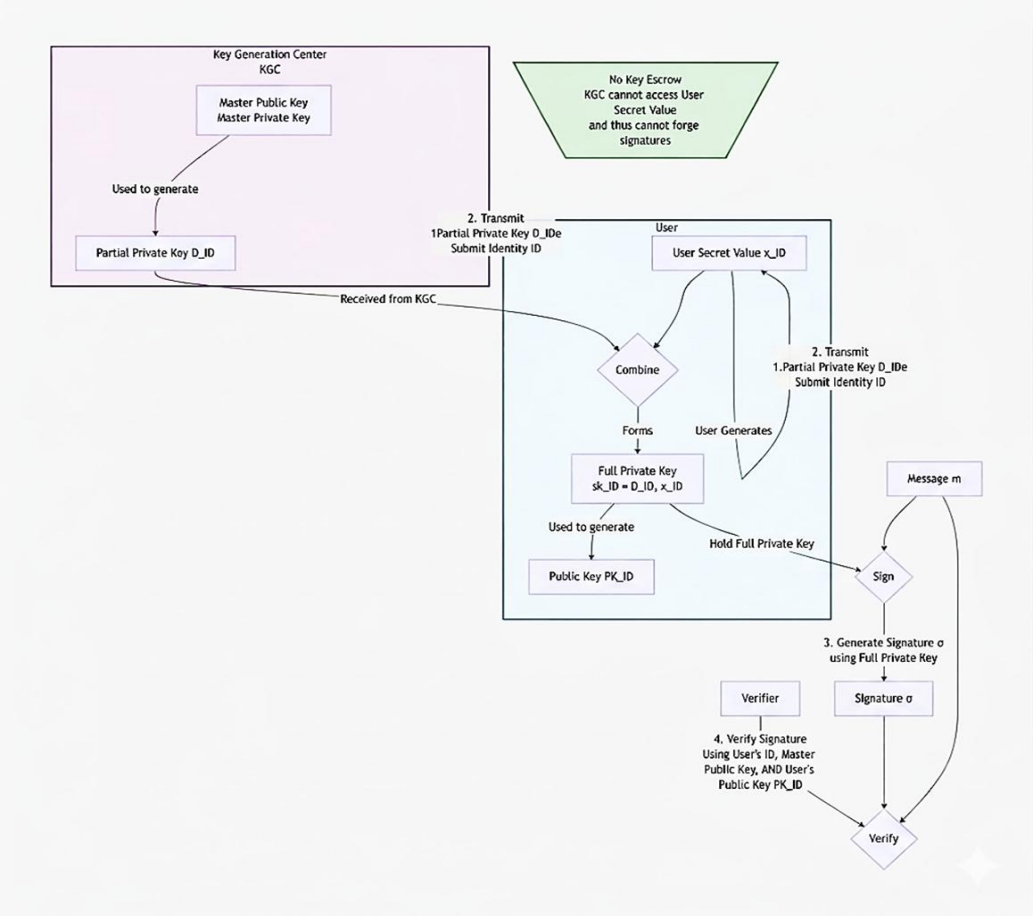

Figure 3. The workflow of a Certificateless Signature scheme. The user's private key is split between the KGC and the user, effectively eliminating the key escrow problem while maintaining the usability of identity-based public keys.

Limitations of Existing Schemes: A Comparative Analysis

The following table synthesizes the key limitations of the signature schemes discussed above, clearly positioning our proposed work. As evidenced in Table 1, while CLS schemes address the key escrow issue, the vast majority of existing IBS and CLS constructions are based on bilinear pairings or factoring-based problems, which are vulnerable to quantum attacks. This creates a clear research gap for a post-quantum, certificateless IBS scheme.

Table 1. Comparative Analysis of Digital Signature Paradigms for Blockchain

Feature / Paradigm	Traditional PKI (e.g., ECDSA)	Identity-Based (IBS)	Certificateless (CLS)	Our Proposed Scheme
Public Key	Cryptographically random	Human-readable Identity	Human-readable Identity	Human-readable Identity
Key Management	Complex (Certificates)	Simple	Simple	Simple
Key Escrow Problem	No	Yes	No	No
Quantum Resistance	No	Typically No	Typically No	Yes (Lattice-based)
Suitability for Decentralized Trust	Moderate (Centralized CAs)	Low (Centralized KGC)	High	High

Preliminaries: Lattice-Based Cryptography

Our proposed scheme derives its security from the hardness of problems in lattice theory, which are currently resistant to both classical and quantum algorithms (Ajtai, 1996). Subsequent developments such as the Learning With Errors (LWE) problem further strengthened lattice-based cryptography (Regev, 2005). An n-dimensional lattice Λ is a discrete additive subgroup of Rn. For our purposes, we primarily work with q-ary lattices defined by a matrix $A \in Z_q^{n \times m}$. Specifically, we consider the lattice

$$\Lambda_q^{\perp}(A)=\{z \in Z^m : Az=0 \bmod q\}.\Lambda_q^{\perp}(A)=\{z \in Z^m : Az=0 \bmod q\}.$$

The Proposed Enhanced Certificateless IBS Scheme

This section elaborates in detail on the enhanced certificateless identity-based signature scheme we have designed for secure blockchain transactions. This scheme aims to simultaneously address the key escrow problem and the threat of quantum computing by combining certificateless cryptography with lattice cryptography. We will first introduce the overall model and participating entities of the system, then gradually delve into the detailed construction process of the scheme and finally prove its correctness through strict formal analysis.

System model and architecture

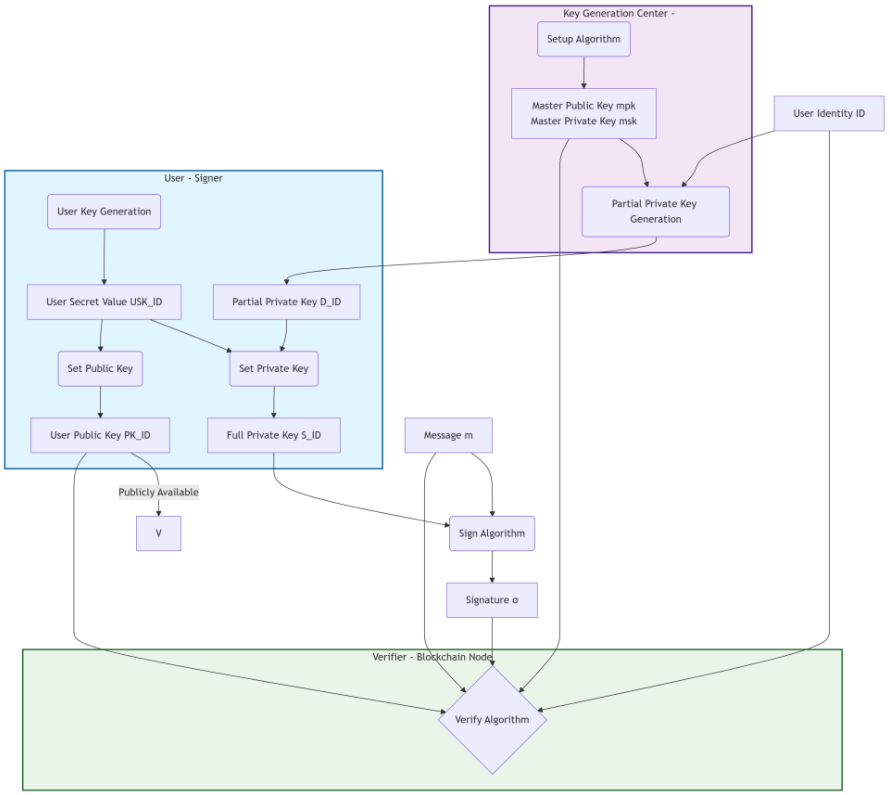

Figure 4. The system model and sequential workflow of our proposed Enhanced CL-IBS scheme, highlighting the interactions between the three entities and the core algorithmic steps.

The scheme we proposed involves three core participating entities: the key generation center, users and validators. As shown in Figure 4, these entities complete the entire process from key generation to signature verification through a series of orderly interactions. As a trusted entity, the key generation center is responsible for initializing the system to generate part of the user's private key. However, the key improvement in its design lies in its inability to obtain the user's complete private key, thereby

eliminating the key escrow risk in traditional identity-based signatures. As a signatory, the user needs to register their identity with the key generation center and independently generate a secret value. This secret value, together with part of the private key obtained from the key generation center, forms its complete signature private key. Validators are typically nodes in a blockchain network. They use the identity of the signer, the public parameters of the key generation center, and the signer's personal public key to verify the validity of the signature. This model achieves a higher level of security while maintaining the usability of identity-based cryptography through the separation of duties.

Detailed construction of the plan

Our scheme is built on integer grids, and its security depends on the computational difficulty of the short integer solution problem. The execution of the scheme begins in the system establishment stage, where the key generation center inputs security parameters to generate the master public key and master private key of the system. The master public key contains a randomly generated matrix and a series of hash functions, while the master private key is the trapdoor associated with this matrix, which is used to generate part of the private key for the user later. When a user joins the system with their identity identifier, the key generation center uses their master private key and hash function to calculate a short vector for that identity that satisfies a specific linear equation relationship, that is, a partial private key, and securely distributes it to the user. Meanwhile, the user independently and randomly generates a short secret vector as its user secret value. Subsequently, the user combines the received portion of the private key with the secret value generated by themselves to jointly form their complete signature private key. In order to be verified by others, users also need to calculate their personal public keys by using the system's master public key and its secret value.

In the signature generation stage, the signer first selects a random vector as the temporary non-CE. Next, it needs to calculate the message, its public key, and the hash value of the commitment value composed of the system matrix and this non-CE. Ultimately, the signature is generated through a linear combination operation of non-CE, part of the private key, the user's secret value and the hash value, and the output is a signature tuple composed of a short vector and a hash value.

After receiving the message and signature, the verifier initiates the verification process. It first uses the identity identifier of the signer to restore the corresponding common matrix through a hash function. The core of verification lies in checking whether the two equations hold simultaneously: one is whether the vector norm in the signature is within an acceptable short range; The second is whether the commitment value recalculated through the system matrix and signature vector is consistent with the original input corresponding to the hash value in the signature. Only when both of these conditions are met will the signature be recognized as valid.

In particular, the partial private key is delivered via identity-bound encryption using a public component derived from the user’s secret, avoiding the need for a pre-established secure channel.

Correctness analysis

We prove the correctness of this scheme through formal derivation. For a legitimate signature generated in accordance with the standard process, the validity of its verification equation is definite. Assuming that users strictly follow the signature algorithm, the generated signature vector must satisfy the linear relationship composed of the system matrix, identity matrix and user public key. Specifically, the commitment value recovered in the verification calculation will be exactly equal to the original commitment value used in the signature generation stage without error. Therefore, when the validator recalculates the hash function, the result will definitely match the hash value contained in the signature exactly. Meanwhile, since trapgate sampling is used in the key generation stage to

ensure that some private keys are short vectors, and both the user's secret value and the noise vector during the signature process are selected from the bounded distribution, the norm of the final signature vector will be highly likely to be less than the preset acceptance bound. This series of definite mathematical relationships ensures that all honestly generated signatures can smoothly pass the verification of the algorithm, thereby meeting the strict requirements of the scheme for correctness.

SECURITY ANALYSIS

This section provides a comprehensive and rigorous security analysis of the proposed Enhanced Certificateless Identity-Based Signature scheme. The security of our scheme is evaluated through a formal adversarial model, a reduction-based security proof under standard cryptographic assumptions, and a comparative analysis of security properties against existing schemes.

Adversarial Model and Security Definitions

To thoroughly evaluate the security of our scheme, we consider a realistic adversarial model that encompasses the capabilities of potential attackers in a certificateless cryptosystem. Following the standard security model for CL-IBS, we define two distinct types of adversaries, AI and AII, each with different powers and objectives.

Type I Adversary (AI): This adversary models a malicious external attacker. It does not possess the KGC's master private key but has the capability to replace the public key of any user with a value of its choice. This captures the scenario where an attacker attempts to impersonate a user by compromising their public key. The security game for AI involves the adversary adaptively querying various oracles (for partial private keys, user secret values, public key replacement, and signatures) and ultimately attempting to forge a valid signature for an identity whose partial private key it has not queried and whose public key it has not replaced.

Type II Adversary (AII): This adversary models a malicious-but-passive KGC. It possesses the system's master private key but is not permitted to replace user public keys. This model captures the key escrow scenario, testing whether the KGC, even with its insider knowledge, can forge a user's signature without the user's secret value. The security game for AII allows the adversary to make queries for user secret values and signatures, and its goal is to forge a signature for an identity whose user secret value has not obtained.

A CL-IBS scheme is deemed secure against existential forgery under adaptive chosen-message attacks (EUF-CMA) if no probabilistic polynomial-time adversary of either Type I or Type II has a non-negligible advantage in winning the respective security games described above.

Security proof and reduction

The security of our proposed scheme is rigorously proven by reducing its security to the hardness of the Short Integer Solution (SIS) problem in lattices. The proof demonstrates that if a polynomial-time adversary A (of either Type I or Type II) can successfully forge a signature in our scheme with a non-negligible advantage, then there exists a polynomial-time algorithm C that can use A as a subroutine to solve the SIS problem with a non-negligible probability, which contradicts the widely accepted hardness assumption of SIS.

The proof proceeds in two main lemmas, one for each adversary type. For a Type I Adversary, the simulator C is given an SIS instance A and must program the random oracles H_1 and H_2 and the signing oracle in such a way that it can answer all of A's queries without knowing the master trapdoor.

When A produces a forgery, the structure of our signature scheme ensures that the forgery can be manipulated to extract a solution to the SIS instance, specifically a short non-zero vector z such that $A \cdot z = 0 \bmod q$. The core of the reduction involves leveraging the forking lemma to handle the queries related to public key replacement. For a Type II Adversary, the simulator C is given the master trapdoor T_A at the beginning of the game. This allows C to perfectly simulate the partial private key queries. The challenge for C is to respond to user secret value queries and to embed the SIS challenge in a way that a forgery on a specific user identity reveals the solution. The security in this case relies on the fact that even with the master key, the adversary cannot generate a valid signature without the user's secret value xID, and any successful forgery allows the simulator to solve the SIS problem related to the user's public key component. The interaction between the adversary and the simulator in the reduction for a Type I attack is conceptually summarized in Figure 5, illustrating how the different oracles are managed and how the forgery is ultimately leveraged.

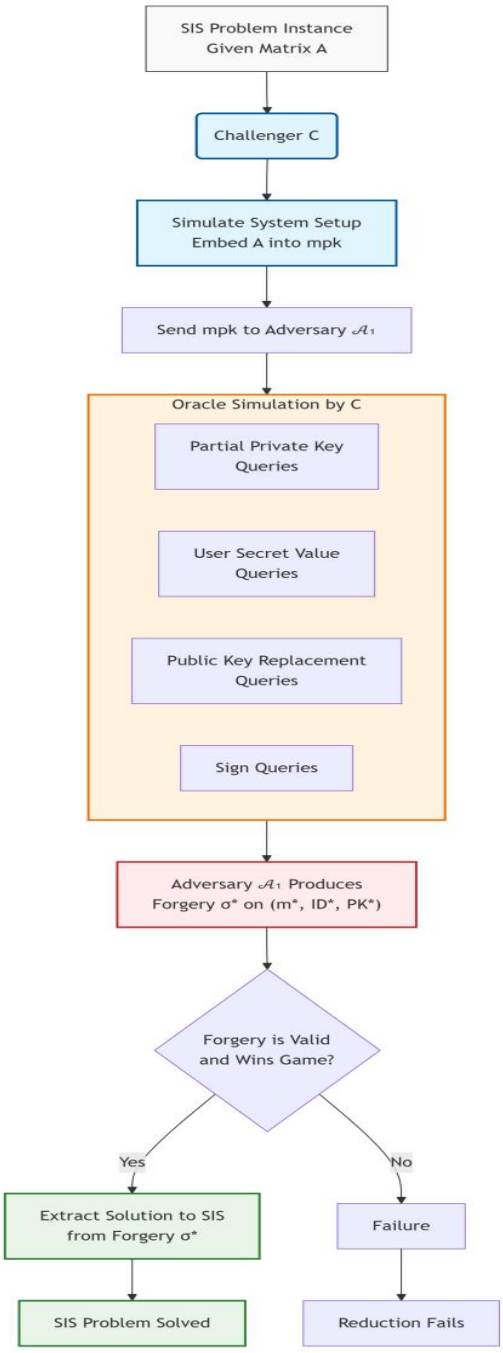

Figure 5. A conceptual diagram of the security reduction. The Challenger C, who is tasked with solving a hard SIS instance, interacts with the Adversary AI by simulating the real-world

environment (System Setup and Oracles). If AI successfully forges a signature, C can extract a solution to the SIS problem from the forgery, thereby establishing the security reduction.

Security property comparison

A salient feature of our proposed scheme is its ability to consolidate multiple critical security properties that are often dispersed across different existing signature paradigms. Table 2 provides a systematic comparison of our scheme with other prominent schemes, highlighting its comprehensive security portfolio. The forward secrecy property (where compromise of long-term keys does not affect the confidentiality of past sessions) is inherently linked to the use of ephemeral secrets in the signing process. Our scheme's design, which incorporates a random nonce r in each signature, provides a form of signature-level forward secrecy.

Table 2. Comparison of schemes

Security Property	ECDSA	Traditional IBS	Certificateless IBS (Pairing-based)	Our Proposed CL-IBS
EUF-CMA Security	✓	✓	✓	✓
Resistance to Key Escrow	✓	✗	✓	✓
Post-Quantum Security	✗	✗	✗	✓
Forward Secrecy	✗	✗	(Varies)	✓*
Identity-Based	✗	✓	✓	✓

As evidenced in Table 2, our scheme is the only one that satisfies all the listed security properties. It achieves the foundational EUF-CMA security while simultaneously addressing the pivotal weaknesses of its predecessors: it eliminates key escrow through the certificateless mechanism and provides a robust defence against future quantum computing attacks via its lattice-based foundation. This unique combination of properties makes it a superior candidate for securing blockchain transactions that require long-term security and trust decentralization.

EFFICIENCY AND PERFORMANCE ANALYSIS

This section presents a comprehensive evaluation of the efficiency and performance of the proposed Enhanced Certificateless Identity-Based Signature scheme. Through both theoretical analysis and practical experimental simulations, we systematically assess the computational overhead, communication costs, and operational performance of our scheme, comparing it against established signature schemes to provide a holistic view of its practical applicability in blockchain environments.

Theoretical Efficiency Analysis

The theoretical overhead of a cryptographic scheme serves as a fundamental indicator of its potential performance in real-world applications. Our analysis focuses on the two most critical resources in blockchain systems: computational cost and communication bandwidth.

In terms of computational cost, the most expensive operations in our lattice-based scheme are the matrix-vector multiplications and the Gaussian sampling processes. Specifically, the Sign algorithm

requires a few such multiplications and one sampling operation, while the Verify algorithm involves several matrix-vector multiplications and norm checks. While these operations are inherently more computationally intensive than the simple scalar multiplications found in ECDSA, they are significantly more efficient than the pairing operations required by many traditional IBS and CL-IBS schemes based on bilinear maps. This positions our scheme favourably against other post-quantum and advanced IBS candidates.

The communication overhead is determined by the signature size, which in our case consists of a short vector and a hash value. For typical security parameters (e.g., targeting 128-bit post-quantum security), the signature size is approximately 2-4 kilobytes (see Table 3). This is larger than an ECDSA signature (64 bytes) but is comparable to or smaller than many other lattice-based signature schemes and is considered manageable for blockchain transactions, especially in the context of off-chain scaling solutions, while pairing-based schemes such as BLS provide compact signatures but rely on different security assumptions (Boneh *et al.*, 2001).

Table 3. Comparative evaluation with existing schemes

Scheme	PQ-secure	Key Escrow	Size	Time
ECDSA	No	No	~64B	Very Fast
BLS	No	No	~96B	Fast
CL-IBS	No	No	100–200B	Moderate
CRYSTALS-Dilithium (Ducas *et al.*, 2018)	Yes	No	~2.7KB	Moderate
Ours	Yes	No	2–4KB	4.8ms / 2.1ms

Experimental Simulation and Results

To complement the theoretical analysis and obtain concrete performance metrics, we implemented a software prototype of our proposed scheme and conducted a series of experiments. The prototype was developed in C++ utilizing specialized libraries for lattice operations, such as the Lattice Crypto library, to ensure both accuracy and efficiency. All experiments were performed on a standard desktop computer equipped with an Intel Core i7-12700 processor and 16GB of RAM, running a 64-bit Linux operating system, to simulate a typical node environment. The primary objective of our experiments was to measure the execution time of the core Sign and Verify algorithms across different security parameter sets. We varied the lattice dimension n and modulus q to achieve security levels roughly equivalent to 128-bit, 192-bit, and 256-bit post-quantum security (see Table 4).

Table 4. Lattice parameters for different security levels

Security Level	n	q	σ
128-bit	512	12289	3.2
192-bit	768	40961	3.5
256-bit	1024	65537	3.8

For each parameter set, we executed the signing and verification algorithms 10,000 times and calculated the average time. The results, as visually summarized in Figure 6, indicate that while our scheme introduces a higher computational load than pre-quantum schemes, its performance remains within practical limits for blockchain use. For instance, at the 128-bit security level, signing a transaction takes approximately 4.8 milliseconds, and verification is completed in about 2.1 milliseconds. This verification time is particularly crucial as it is incurred by every node in the network, and our results demonstrate that it is sufficiently low to not become a network bottleneck.

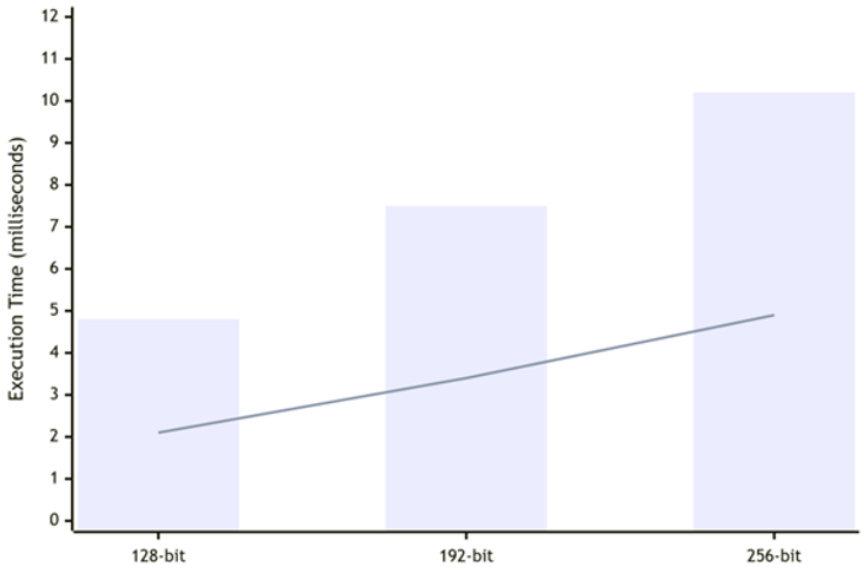

Figure 6. Average execution time of Sign (bar) and Verify Operation (line)

Furthermore, we compared the performance and characteristics of our scheme with other relevant signature paradigms in a blockchain context. As summarized in Table 3, our scheme occupies a unique position in the design space. It forgoes the raw efficiency of pre-quantum schemes like ECDSA to achieve a combination of features—namely, identity-based public keys, the absence of key escrow, and post-quantum security—that are unattainable by any of the other compared schemes. This trade-off is justified for applications requiring long-term security and decentralized trust. It is also worth noting that the signature size, while larger than that of ECDSA, is compact enough to be efficiently handled within a blockchain's block structure. When considering the potential for algorithmic optimizations and future hardware acceleration for lattice operations, the practical performance of our scheme is expected to improve further, solidifying its viability for securing next-generation blockchain transactions.

APPLICATION IN SECURE BLOCKCHAIN TRANSACTIONS

This section delineates the practical integration of the proposed Enhanced Certificateless Identity-Based Signature scheme into a blockchain ecosystem, illustrating its transformative potential for securing digital transactions. The discussion extends beyond theoretical construction to demonstrate how the scheme's inherent properties can address persistent challenges in blockchain identity management and transaction security, ultimately contributing to a more robust, user-friendly, and future-proof decentralized infrastructure.

A Novel Blockchain Transaction Model

The integration of our CL-IBS scheme necessitates a reimagining of the conventional blockchain transaction workflow, resulting in a model that enhances both security and usability. The process commences with system initialization, where a designated Key Generation Center establishes the public system parameters, effectively bootstrapping the identity-based cryptosystem for the network. When a user wishes to initiate transactions, they register their human-readable identity, such as a domain name or a formal alias, with the KGC. Following the protocols outlined in section 3, the user subsequently generates their full private key and corresponding public key. This foundational step replaces the cryptographically opaque key pairs of traditional systems with an identity-based framework.

The transaction lifecycle within this novel model unfolds through a series of streamlined steps. To authorize a transaction, the sender employs their full private key to generate a digital signature over the transaction data, which includes the recipient's identity and the transfer amount. This signed transaction is then broadcast to the peer-to-peer network. Upon receipt, verification nodes within the network initiate the validation process. The critical advantage of our scheme becomes apparent at this stage: to verify the signature, a node requires only the sender's publicly known identity, the KGC's public parameters, and the sender's individual public key. This process completely circumvents the need for complex digital certificates or cumbersome public key management infrastructures. A transaction is deemed valid and is subsequently packaged into a new block only if the signature verification is successful, ensuring that only properly authorized transfers are recorded on the immutable ledger.

Comprehensive Advantage Analysis

Deploying our Enhanced CL-IBS scheme within a blockchain context yields a multitude of strategic advantages that collectively address the limitations of current systems. From a security perspective, the scheme delivers a formidable defense-in-depth posture. Its foundation on the hardness of lattice problems provides inherent resistance to attacks from both classical and quantum computers, thereby future-proofing blockchain assets and smart contracts against evolving cryptographic threats. Furthermore, the certificateless nature of the scheme definitively eliminates the key escrow problem, distributing trust in a manner that is more congruent with the decentralized ethos of blockchain technology. This architecture prevents any single entity, including the KGC itself, from possessing the capability to forge user signatures, thereby upholding the crucial security principle of non-repudiation.

In terms of usability and operational efficiency, the benefits are equally compelling. The ability to use human-meaningful identifiers as public keys dramatically simplifies the user experience and reduces the risk of key-related errors, such as sending assets to an incorrect cryptographic address. This enhancement in usability is achieved without compromising security. Moreover, the computational efficiency of the scheme, particularly its verification algorithm as established in the previous, ensures that the integration does not impose a prohibitive performance penalty on the network. The verification time remains low enough to support high transaction throughput, which is a critical requirement for scalable blockchain platforms. By consolidating post-quantum security, decentralized trust, and user-centric design into a single cohesive framework, the proposed scheme positions itself as a foundational technology for the next generation of secure and adaptable blockchain systems.

CONCLUSION

This paper presented an enhanced certificateless identity-based digital signature scheme for secure blockchain transactions. The proposed scheme combines certificateless cryptography with lattice-based constructions to address three important requirements in blockchain-oriented signing systems, namely simplified identity-oriented public key management, elimination of the key escrow problem, and resistance to quantum attacks. We described the system model, the detailed construction, and the correctness of the scheme, and analyzed its security under the random oracle model by reducing existential unforgeability to the hardness of the SIS problem. In addition, we evaluated the scheme from both theoretical and experimental perspectives. The results show that, although the proposed scheme incurs a larger signature size than classical schemes, it achieves practical signing and verification performance while offering post-quantum security and certificateless trust advantages. Finally, we discussed how the scheme can be integrated into blockchain transaction workflows to improve security, usability, and long-term cryptographic robustness. Overall, the proposed scheme

provides a feasible foundation for building secure and user-friendly blockchain systems in post-quantum environments.

REFERENCES

[1] Ajtai, M. 1996. Generating hard instances of lattice problems. *STOC96: ACM Symposium on Theory of Computing*. Philadelphia, Pennsylvania, USA. May 22 - 24, 1996. pp 99–108.

[2] Al-Riyami, S. S. & Paterson, K. G. 2003. Certificateless public key cryptography. *In:* Laih, C.-S. (Ed). *Advances in Cryptology - ASIACRYPT 2003. ASIACRYPT 2003.* Lecture Notes in Computer Science, vol 2894. Springer, Berlin, Heidelberg. pp 452–473.

[3] Bagchi, P., Bera, B., Das, A. K. & Sikdar, B. 2025. Quantum safe lattice-based single round online collaborative multi-signature scheme for blockchain-enabled IoT applications. *ACM Transactions on Sensor Networks*, 21(2), Article No 17. pp 1-33.

[4] Boneh, D., Lynn, B. & Shacham, H. 2001. Short signatures from the Weil pairing. *In:* Boyd, C. (Ed). *Advances in Cryptology — ASIACRYPT 2001.* Lecture Notes in Computer Science, vol 2248. Springer, Berlin, Heidelberg. pp 514–532

[5] Buterin, V. 2014. *Ethereum: A next-generation smart contract and decentralized application platform.* (https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf). Last accessed on 4 April 2026.

[6] Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G. & Stehlé, D. 2018. Crystals-dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018(1), 238 - 268.

[7] Gharavi, H., Granjal, J. & Monteiro, E. 2024. Post-quantum blockchain security for the Internet of Things: Survey and research directions. *IEEE Communications Surveys & Tutorials*, 26(3), 1748-1774.

[8] Nakamoto, S. 2008. *Bitcoin: A peer-to-peer electronic cash system.* (https://ssrn.com/abstract=3440802). Last accessed on 4 April 2026.

[9] Regev, O. 2005. On lattices, learning with errors, random linear codes, and cryptography. *STOC '05: Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*. May 22-24, 2005. Baltimore, Maryland, USA. pp. 84–93.

[10] Shamir, A. 1985. Identity-based cryptosystems and signature schemes. *In:* Blakley, G. R. & D. Chaum, D. (Eds.). *Advances in cryptology*. Lecture Notes in Computer Science, vol 196. Springer, Berlin, Heidelberg. pp. 47–53.

[11] Shor, P. W. 1997. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), 1484–1509.