

sensors



Article

A Decentralized Signcryption Scheme Based on CFL

Leyi Shi and Mengting Liu



<https://doi.org/10.3390/s25061773>

Article

A Decentralized Signcryption Scheme Based on CFL

Leyi Shi ^{1,2,*}  and Mengting Liu ¹ 

¹ College of Computer Science and Technology, China University of Petroleum, Qingdao 266580, China; by1907010303@s.upc.edu.cn

² Qingdao Guochuang Intelligent Appliance Research Institute Co., Ltd., National Innovation Institute of High-End Smart Appliances, Qingdao 266101, China

* Correspondence: shileyi@upc.edu.cn

Abstract: The rapid advancement of quantum computing technology poses a significant threat to conventional public key cryptographic infrastructure. The SM2 (state key cryptography algorithm no. 2) elliptic curve public key cryptographic algorithm, which adopts elliptic curve cryptography, has demonstrated strong resistance to quantum attacks. However, existing signcryption schemes remain vulnerable due to their reliance on a single certification authority (CA) managing all keys. The cryptography fundamental logics (CFL) authentication process eliminates the need for third-party involvement, achieving decentralized authentication and reducing the burden on certificate generation centers. Therefore, a decentralized signcryption scheme based on CFL was proposed using the SM2 national cryptographic algorithm. Unlike traditional signcryption schemes, this approach does not depend on the certification authority's private key during the public–private key generation process. This innovation helps avoid risks associated with certification authority private key leakage and ensures decentralized characteristics. The proposed scheme was rigorously verified under the random oracle model (ROM) and based on the complexity assumption of the elliptic curve Diffie–Hellman (ECDH) problem. The theoretical analysis and experimental results demonstrate that compared to traditional methods, the proposed scheme exhibits higher efficiency in communication and computation. Specifically, the proposed scheme reduces computational overheads by approximately 30% and communication overheads by approximately 20% in practical working environments. These quantitative improvements highlight the scheme's promising application prospects and practical value.

Keywords: signcryption; CFL; provable security; random oracle model; SM2



Received: 2 February 2025

Revised: 8 March 2025

Accepted: 10 March 2025

Published: 12 March 2025

Citation: Shi, L.; Liu, M. A

Decentralized Signcryption Scheme Based on CFL. *Sensors* **2025**, *25*, 1773. <https://doi.org/10.3390/s25061773>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Confidentiality and authentication are two crucial indicators in cryptography, and the newly developed signcryption technology has adhered to these principles in its evolution. Early cryptographic research explored and applied these two indicators separately, such as confidentiality in public-key cryptosystems and authentication in digital signatures. However, with societal advancement, the demands of electronic operations (such as email and electronic payments) require signcryption technology to simultaneously satisfy both key indicators while keeping pace with the times. Addressing this need, researchers initially proposed the “sign-then-encrypt” implementation path, but this approach was not widely adopted due to high computational and communication costs. Subsequently, in 1997, Zheng et al. [1] proposed integrating both functions into one unified approach, efficiently satisfying both key indicators simultaneously. This method became known as public-key signcryption.

Signcryption technology offers the advantages of cost-effectiveness, high operational efficiency, enhanced security, and simplified design implementation. In recent years, with increasing security awareness, signcryption technology has become a focal point of research among scholars and engineers due to its dual capability of ensuring both confidentiality and authentication. Based on the maturity of existing research theories and scheme designs, it has gradually achieved mass production and widespread application (such as in electronic payments, mobile agent security, and firewalls), yielding favorable practical results. Through these practical applications, signcryption technology has gradually crossed over from cryptography to network security and other fields, becoming a crucial topic in related domains.

Simultaneously, with the rapid development of quantum computing technology, traditional public-key cryptosystems face unprecedented security challenges [2]. The SM2 algorithm [3], independently developed in China, based on elliptic curve cryptography principles, demonstrates significant advantages in resisting quantum computing attacks. The SM2 algorithm utilizes the discrete logarithm problem in elliptic curve point groups and provides higher security strength than the RSA algorithm. Furthermore, the SM2 algorithm employs shorter key lengths, typically 256 bits, whereas RSA typically requires 2048 bits or more. These shorter key lengths enable reduced storage and transmission data volume while maintaining equivalent security levels, thereby improving efficiency. The SM2 algorithm's computational complexity is lower than that of RSA, offering advantages in processing speed, particularly in scenarios requiring rapid encryption and decryption. Most importantly, due to its elliptic curve-based characteristics, the SM2 algorithm is considered to possess some degree of resistance against quantum computing attacks.

Traditional public key infrastructure (PKI) relies heavily on centralized certificate authorities (CAs) to manage and validate digital certificates, which bind public keys to identities. This centralized model, while widely adopted, introduces several inherent weaknesses. Firstly, it creates a single point of failure and a potential target for attacks. Compromise of a CA's private key can have catastrophic consequences, potentially invalidating the entire trust framework and enabling widespread impersonation and data breaches. Secondly, the CA model can be cumbersome and inefficient, particularly in dynamic and large-scale distributed systems. Certificate generation, distribution, and revocation processes can introduce latency and complexity, hindering the agility and scalability of applications. Furthermore, the reliance on a central authority can be antithetical to the principles of decentralization and autonomy, which are increasingly valued in modern distributed systems, such as blockchain technologies, Internet-of-Things (IoT) networks, and vehicular ad hoc networks (VANETs). The need for decentralized authentication and authorization mechanisms that minimize or eliminate reliance on centralized authorities is becoming increasingly apparent. This drive toward decentralization is not merely a matter of architectural preference but a fundamental requirement for building robust, resilient, and scalable secure communication systems in the face of evolving threats and increasingly distributed environments. The exploration of novel cryptographic approaches that address both quantum resistance and decentralization is therefore a critical area of research in modern cryptography.

The initial signcryption schemes were primarily based on traditional public key infrastructure (PKI), inheriting the reliance on certificate authorities for key management and identity verification. However, the inherent limitations of PKI, particularly its centralized nature and certificate management overheads, motivated the development of more advanced signcryption paradigms. Identity-based signcryption (IBSC), introduced by Shamir in 1984 and later adapted to signcryption, has emerged as a promising alternative. IBSC eliminates the need for digital certificates by using a user's identity (e.g., email address or

username) as their public key. This simplifies key management significantly, as users do not need to obtain and manage certificates. Instead, a trusted private key generator (PKG) generates private keys for users based on their identities. While IBSC offers advantages in terms of key management simplicity, it introduces the key escrow problem, where the PKG has access to all users' private keys. This key escrow issue is a significant concern in many applications, as it implies a centralized point of trust and potential for abuse. Tanksale [4] highlights vulnerabilities in identity-based signcryption schemes, demonstrating attacks against specific constructions, including Zhang et al.'s assertion signcryption scheme designed for decentralized autonomous environments. This underscores the importance of rigorous security analysis and the potential pitfalls of even seemingly decentralized identity-based approaches if not carefully designed. Furthermore, Tanksale [4] points out weaknesses in Yu et al.'s identity-based signcryption scheme in the standard model, showing its failure to achieve indistinguishability against chosen plaintext attacks. These findings emphasize the need for robust security proofs and careful consideration of attack vectors when designing and deploying identity-based signcryption schemes.

Certificateless signcryption (CLSC), proposed by Al-Riyami and Paterson in 2003, was developed to address the key escrow problem of IBSC while retaining the certificate-free nature of identity-based cryptography. CLSC eliminates the PKG's ability to access users' private keys by allowing users to generate partial private keys themselves, combined with a partial private key provided by a key generation center (KGC). This distributed key generation process mitigates the key escrow issue and enhances user autonomy. Xie et al. [5] propose a certificateless aggregate signcryption scheme for edge computing-based Internet of Vehicles (IoV), highlighting the relevance of CLSC in decentralized and resource-constrained environments. Their scheme aims to address the limitations of VANETs, such as network congestion and privacy leakage, by leveraging edge computing and certificateless cryptography. The scheme incorporates online/offline encryption and aggregate signcryption techniques to further enhance efficiency and security. Yang et al. [6] also focus on certificateless signcryption for VANETs, proposing a pairing-free online/offline scheme with batch verification for edge computing. They identify vulnerabilities in existing CLSC schemes, specifically in Xie et al.'s scheme, demonstrating its susceptibility to public key replacement attacks. Their proposed scheme aims to address these security concerns while also improving efficiency through online/offline signature and batch verification techniques. Rastegari et al. [7] revisit Luo and Wan's certificateless signcryption scheme, pointing out errors in their construction and proposing a corrected and improved CLSC scheme that is provably secure in the standard model. This work emphasizes the importance of rigorous security analysis and the ongoing refinement of CLSC schemes to ensure their robustness and practicality.

The security of signcryption schemes is typically analyzed using formal security models and provable security techniques. Provable security aims to demonstrate that a cryptographic scheme is secure under well-defined assumptions and against specific attack models. The random oracle model (ROM) is a widely used tool in provable security, where hash functions are modeled as ideal random oracles. While the ROM provides a useful framework for security analysis, it has been criticized for not accurately reflecting the behavior of real-world hash functions. Therefore, achieving provable security in the standard model without relying on random oracles is a desirable goal. Several of the reviewed papers, including Scheme [5], Scheme [6], Scheme [7], and Scheme [8], mention security proofs in the random oracle model (ROM). Scheme [4] and Scheme [7] emphasize provable security in the standard model, highlighting the stronger security guarantees offered by standard model proofs. Security proofs typically rely on computational hardness assumptions, such as the elliptic curve Diffie–Hellman (ECDH) problem or the computa-

tional Diffie–Hellman problem (CDHP). These assumptions are based on the presumed difficulty of solving certain mathematical problems, which underpins the security of the cryptographic schemes. Security analysis usually considers security properties such as confidentiality (indistinguishability against chosen ciphertext attacks, IND-CCA), unforgeability (existential unforgeability against adaptive chosen message attacks, EUF-CMA), and, sometimes, other properties, like anonymity or privacy preservation. Rigorous security analysis and provable security results are crucial for establishing confidence in the robustness and reliability of signcryption schemes.

The CFL certification system [9], proposed by researcher Chen Huaping and Professor Lü Shuwang, is an identity-based authentication mechanism. This system not only integrates the advantages of certificate-based and identity-based authentication but also effectively complements and enhances their respective limitations. The SM2 algorithm, independently designed in China as a commercial cryptographic algorithm, demonstrates advantages in resisting quantum computing attacks. Against this background, based on the limitations of existing signcryption schemes and drawing inspiration from the CFL authentication system, this research innovatively designs a decentralized signcryption scheme [10] implemented using the SM2 algorithm within the CFL framework. The security of this scheme has been rigorously proven using the random oracle model [11]. Finally, experiments demonstrate the scheme's exceptional performance and effectiveness.

This paper makes significant contributions to the field of cryptography by addressing the limitations of existing signcryption schemes and proposing a novel decentralized signcryption scheme based on cryptography fundamental logics (CFL) and the SM2 algorithm. The key contributions of this paper are as follows:

Proposed decentralized signcryption scheme: The paper introduces a decentralized signcryption scheme that eliminates the need for a single certification authority (CA) to manage all keys. This scheme leverages the CFL authentication process, which achieves decentralized authentication and reduces the burden on certificate generation centers.

Security analysis: The security of the proposed scheme is rigorously analyzed under the random oracle model (ROM) and based on the complexity assumption of the elliptic curve Diffie–Hellman (ECDH) problem. This analysis ensures that the scheme provides strong resistance against quantum attacks and maintains confidentiality, unforgeability, public verifiability, non-repudiation, and forward secrecy.

Efficiency improvement: The theoretical analysis and experimental results demonstrate that the proposed scheme significantly improves computational and communication efficiency compared to traditional signcryption schemes. Specifically, the scheme reduces computational overheads by approximately 30% and communication overheads by approximately 20% in practical working environments.

The structure of this paper is organized as follows: Section 2 introduces preliminary knowledge; Section 3 presents the definition and specific details of the CFL-based decentralized signcryption scheme; Section 4 provides security proofs for the proposed scheme; and Section 5 analyzes the scheme's efficiency through theoretical analysis and experimental evaluation. The paper concludes with final remarks.

2. Preliminary Knowledge

2.1. CFL: Cryptography Fundamental Logics

In response to current challenges in binding users with public keys in the identity authentication domain, the CFL (cryptography fundamental logics) system [12] has emerged as an innovative solution, ingeniously integrating the technical essence of both certificate-based and identity-based authentication to address existing problems.

In conventional certificate authentication systems, the relationship between public key (PK) and private key (SK) is typically formalized as $PK = F(SK)$, where the public key, PK, is not directly associated with the user's identity, ID. To establish the connection between PK and ID, a trusted third party (such as a certificate authority, CA) must be introduced to verify this relationship through certificate issuance. In current certificate authentication systems, trusted third parties play a central role, managing certificate application, issuance, verification, and revocation processes. As identity authentication application scenarios expand, the increasing burden on these third parties has become a constraint on overall system performance improvement.

In identity authentication mechanisms, the public key and user ID essentially form an inseparable entity, where the relationship between public and private keys can be further abstracted as $SK = F(ID, MSK)$, with ID and PK considered equivalent elements. The key generation center (KGC) generates private keys for each user based on their ID and the system's master secret key (MSK), implying that users do not have exclusive control over their private keys. As the identity authentication field increasingly emphasizes personal privacy protection, this approach, where KGC computes private keys for users, poses potential threats to system security, to some extent, challenging the overall security protection framework.

Researchers developed the certificate-free algorithm with CFL by combining the advantages of certificate- and identity-based authentication mechanisms. The framework involves generating two pairs of public-private keys: one identity-related and one randomly generated. The identity private key is used by the certificate authority (CA) for signing, while users maintain the random private key to sign their ID and request certificates, which are then stored securely in a UKey. Verifiers can derive both the identity public key and random public key from the user's ID through specific algorithms, enabling decentralized verification without third-party intervention. This reduces the operational burden on certificate authorities while enhancing system efficiency and security. The CFL framework maintains identity authentication principles where identity public keys naturally link to user IDs, and the binding between user IDs and random public keys is secured through identity private key signatures and verification. By generating unique identity private keys for each user based on their ID, rather than using CA's traditional single-key approach, the CFL system significantly improves security, enhances signature uniqueness, and strengthens the overall robustness of the authentication process.

2.2. Related Hard Problems

The signcryption scheme in this paper relies on the following hard problems.

Definition 1. Given an elliptic curve $E(F_q)$ with elements $a, b \in F_q$, compute common parameters $params = \{p, q, E, G, n\}$, where $G = (x_G, y_G)$ is the base point of the elliptic curve with order n . Given an elliptic curve E with base point G of order n , compute the common parameters abG . The elliptic curve Diffie–Hellman (ECDH) problem on this curve is defined as follows: Given $aG, bG \in \langle G \rangle$, compute abG .

Definition 2. Given an elliptic curve $E(F_q)$ with elements $a, b \in F_q$, compute common parameters $params = \{p, q, E, G, n\}$, where $G = (x_G, y_G)$ is the base point of the elliptic curve with order n . The discrete logarithm problem (DLP) on this curve is defined [13] as follows: Given $aG \in \langle G \rangle$, find aG .

3. CFL-Based Signcryption Scheme

This section delves into the core proposal of our research: the decentralized signcryption scheme built upon cryptography fundamental logics (CFL). The scheme represents a novel approach to signcryption by leveraging the unique advantages of CFL to address limitations in existing methods. It eliminates reliance on a central certification authority's private key during public-private key generation, thereby enhancing security and decentralization.

3.1. Formal Definition

The scheme is abstracted into the following four algorithms:

Setup: A system initialization algorithm where users generate unique identifiers. The key generation center (KGC) receives a security parameter k as input and produces two crucial outputs: the master secret key (MSK) and system parameters (params). During this process, the MSK must be kept strictly confidential to ensure security, while the system parameters (params) are publicly available for widespread access and use.

The signcryption key pair is generated based on the user's ID and public-private key fundamentals. A random public-private key pair (P_k, S_k) is generated, and the user's ID along with the public key P_k are submitted to the key generation center (KGC). The KGC verifies the authenticity and uniqueness of the submitted ID, then generates the identity public key $ID_{PK} = f(P_k)$ and identity private key $ID_{SK} = f(S_k)$.

Signcrypt: The signcrypt algorithm takes as the input the system parameters params, plaintext m , the recipient's identity ID_B , and the sender's private key SK_A , generating a ciphertext σ as the output. This algorithm can be represented as $\sigma = \text{Signcrypt}(m, ID_{SKA}, ID_{PKB})$.

Unsigncrypt: The unsigncrypt algorithm takes as the input the ciphertext σ , the sender's identity ID_A , and the recipient's private key SK_B , outputting either the plaintext message m or an error symbol " \perp " (indicating invalid or illegal ciphertext). This algorithm can be represented as $m = \text{Unsigncrypt}(\sigma, ID_{PKA}, ID_{SKB})$.

These algorithms must satisfy the consistency principle of the signcryption scheme: if $\sigma = \text{Signcrypt}(m, \text{ID}_{\text{SKA}}, \text{ID}_{\text{PKB}})$, then $m = \text{Unsigncrypt}(\sigma, \text{ID}_{\text{PKA}}, \text{ID}_{\text{SKB}})$. As shown in Figure 1 below.

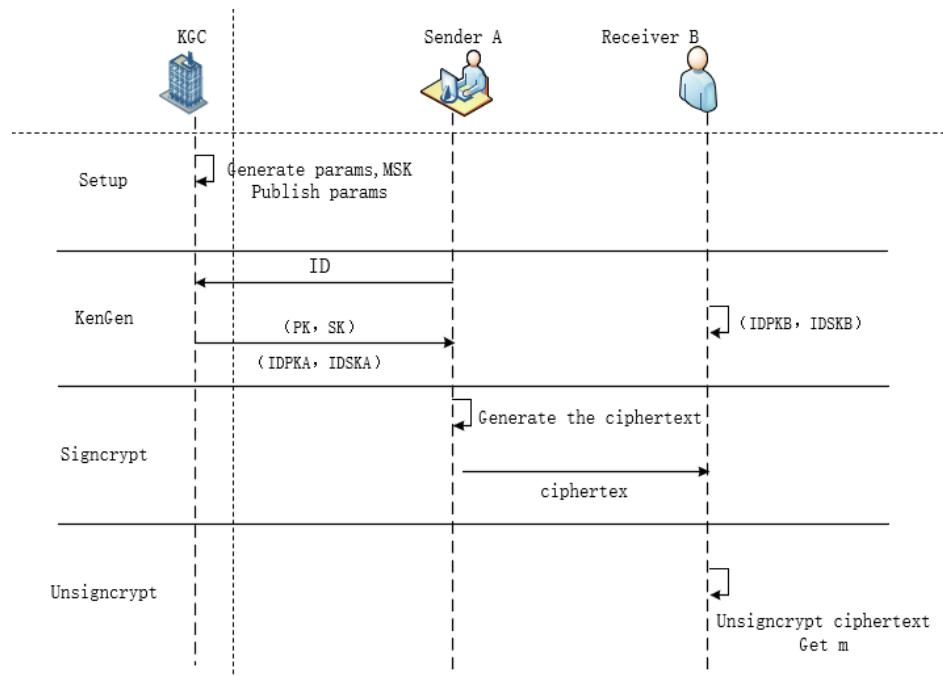


Figure 1. CFL-based signcryption algorithm.

3.2. Scheme Design

Setup: Define two elements $a, b \in F_q$ for the elliptic curve $E(F_q)$, compute common parameters $\text{params} = \{p, q, E, G, n\}$, where p is a large prime number, E represents the elliptic curve defined over finite field F_q , and $G = (x_G, y_G)$ is the base point of order n on curve $E(F_q)$.

KeyGen: Given a user's ID, randomly generate a user's public-private key pair (P_k, S_k) . The KMC generates the identity private key IDSK using the ID and private key PASK and generates the verification identity public key IDPK using RAPK and the corresponding ID, where a relationship exists between the identity public key and the identity private key such that $\text{IDSK} = \text{IDPK} \cdot G$.

Signcrypt: For user A (with identity ID_A , public key PAPK_A , identity private key IDSK_A) sending message m (length $m\text{len}$) to user B:

1. Randomly select $k \in Z_n$;
2. Compute $C_1 = kG = (x_1, y_1)$, and convert C_1 to bit string;
3. Compute $e = \text{Hash}(Z||m)$, and convert e to an integer, where Z is the hash value of the system parameters;
4. Compute $r = (e + x_1) \bmod n$; if $r = 0$ or $r + k = n$, return to step (1) and repeat by randomly selecting a new k and recalculating r until the conditions are satisfied;
5. Compute $s = (1 + \text{IDSK}_A)^{-1}(k - r\text{IDSK}_A) \bmod n$; if $s = 0$, return to step (1), select a new random number k , and recalculate the value of s until the conditions are satisfied;
6. Convert r, s to byte strings with lengths $r\text{len}, s\text{len}$;
7. Compute $k \cdot \text{IDPK}_B = (x_2, y_2)$;
8. Compute $k\text{len} = m\text{len} + r\text{len} + s\text{len} = \text{KDF}(x_2||y_2, k\text{len})$; if t is an all-0 bit string, return to step (1), iteratively select a new random number k , and recalculate t until the condition is met;
9. Compute $C_2 = t \oplus (m||r||s)$.
10. Generate ciphertext $\sigma = C_1||C_2$, and send σ to user B.

Unsigncrypt: User B receives ciphertext σ and performs the following operations:

1. Extract the bit string C_1 from ciphertext σ , and convert it to a point on the elliptic curve. Then, verify if point C_1 satisfies the elliptic curve equation. If not satisfied, terminate the operation;
2. Calculate $C_1 \cdot \text{IDSK}_B = (x'_2, y'_2)$;
3. Calculate $k\text{len} = m\text{len} + r\text{len} + s\text{len}$, $t' = \text{KDF}(x'_2||y'_2, k\text{len})$; if t' is an all-zero bit string, report error, and exit;
4. Calculate $m' || r' || s' = t' \oplus C_2$;
5. Extract bit strings r', s' , and convert them to integers. Verify if $r' \in Z_n, s' \in Z_n$. If not valid, report decryption failure, and exit;
6. Calculate $e' = \text{Hash}(Z||m')$, convert e' to an integer;
7. Calculate $u' = (r' + s') \bmod n$; if $u' = 0$, report decryption verification failure and exit;
8. Calculate the point $(x'_1, y'_1) = s'G + u' \cdot \text{IDPK}_A$ on the elliptic curve;
9. Calculate $R = (e' + x'_1) \bmod n$, and verify if $R = r'$. If true, output plaintext m , and user B receives the message. Otherwise, report decryption verification failure, and exit;

4. Security Proof

This section rigorously examines the security properties of the proposed CFL-based signcryption scheme. The analysis is conducted under the random oracle model and

is based on the hardness assumption of the elliptic curve Diffie–Hellman (ECDH) problem. The security of the scheme is evaluated against various attack vectors to ensure its robustness in real-world applications.

4.1. Security Definitions

The signcryption scheme must satisfy the following properties:

Confidentiality: Ensures that no information from the document can be obtained by an attacker through the ciphertext. The core concept is the computational infeasibility of decryption.

Unforgeability: Ensures that valid user signatures cannot be obtained by attackers. The core concept is the infeasibility of signature forgery.

Public verifiability: Ensures that signature verification has relative independence. This operation can be executed without requiring the recipient's private key for verification. The core concept is the universal applicability of verification.

Non-repudiation: Ensures that once a sender chooses to send a command, they cannot deny their signcrypted message. The core concept is the undeniability of signatures.

Forward secrecy: Ensures the uniqueness of user private keys, meaning no method can recover the content of any previously signcrypted messages. The core concept is the non-recoverability of signatures.

Definition 3. *The CFL-based signcryption scheme demonstrates IND-IBSC-CCA2 indistinguishability against adaptive chosen-ciphertext attacks if no polynomial-time adversary can win the game with significant advantage [14]. Here, IND-IBSC-CCA2 denotes the indistinguishability property of the signcryption scheme under adaptive chosen-ciphertext attacks (CCA2). Specifically, an adversary cannot distinguish between real and forged messages in their choices of ciphertext and plaintext. In this definition, indistinguishability means that even when an adversary can select ciphertexts and make queries across multiple stages (adaptive chosen-ciphertext attack), they cannot effectively distinguish between the original messages represented by any two ciphertexts. In other words, this definition ensures that even if an adversary can perform multiple operations on the ciphertexts, they still cannot obtain any useful information about the messages, thereby guaranteeing the message confidentiality of the system.*

1. Upon receiving security parameter k , challenger C executes the setup algorithm and transmits the resulting system parameters, params , to attacker A for subsequent use. During the query phase, adversary A performs the following operations:
 2. Signcrypt query: Challenger C executes the key generation algorithm to generate the sender's and receiver's public/private key pairs, computes $\sigma = \text{Signcrypt}(m, ID_{PKA}, ID_{PKB})$, and sends σ to adversary A .
 3. Unsignedcrypt query: A submits a ciphertext σ and a sender's public key ID_{PKA} to challenger C . If the ciphertext is valid, C computes $\text{Unsignedcrypt}(\sigma, ID_{PKA}, ID_{PKB})$ and returns message m to A ; otherwise, the rejection symbol “ \perp ” is returned.
 4. A generates two equal-length plaintexts, m_0 and m_1 . C randomly selects $u \in \{0, 1\}$, computes $\sigma = \text{Signcrypt}(m, ID_{PKA}, ID_{PKB})$, and sends the result σ to A .
 5. During the guessing phase, similar to the search phase, A can make a polynomial-bounded number of queries.
 6. At the end of the game, attacker A submits a predicted value b' for b . If b' matches b , then A is determined to have won the game.

A 's advantage is defined as $\text{Adv}(A) = |2\Pr[b' = b] - 1|$.

Definition 4. A CFL-based signcryption scheme is considered existentially unforgeable against adaptive chosen-message attacks (EUF-IBSC-CMA secure) if no polynomial-time adversary can win the game with significant advantage.

1. Initialization phase: Challenger C accepts a security parameter k as input and executes the setup algorithm to generate the system parameter set params . Subsequently, C transmits the generated system parameters params to adversary A, enabling the adversary to utilize these parameters in subsequent operations.
2. As described in Definition 3, adversary A can make a polynomial-bounded number of queries to obtain the required information. These queries are constrained by polynomial bounds to ensure fairness and reasonability in the game.
3. Finally, adversary A outputs a new triple $(\sigma', \text{IDPK}_A, \text{IDSK}_B^*)$. A wins the game if this triple was not produced by the Signcrypt oracle and $\text{Unsigncrypt}(\sigma', \text{IDPK}_A, \text{IDSK}_B^*)$ does not return the symbol “ \perp ”.

A's advantage is defined as their probability of winning.

4.2. Security Analysis

(1) Confidentiality: The confidentiality of this scheme is proven through Theorem 1.

Theorem 1. Under the random oracle model, if there exists an adversary A who complies with the IND-BCSC-CCA2 security model and can achieve a significant advantage ϵ within a specified time period t , meeting the success criteria described in Definition 3 (during which adversary A can perform at most q_k key derivation function (KDF) queries, q_h hash function queries, q_s signcryption requests, and q_u unsigncryption requests), then there exists a challenger C who can solve the ECDH problem with advantage $\epsilon' > \epsilon \frac{2\epsilon}{q_k + q_s}$ within time $t' \leq t + q_k t_k + q_h t_h + q_s t_s + q_u t_u$, where t_k is the time for one KDF execution, t_h is the time for one hash execution, t_s is the time for one Signcrypt execution, and t_u is the time for one Unsigncrypt execution.

Proof. Distinguisher C receives a randomly generated instance of the elliptic curve Diffie–Hellman (ECDH) problem as the input for analysis. Given $(G, P_1, P_2) = (\langle G \rangle, aG, bG)$, the goal is to compute abG ; C runs A as a subroutine and plays the role of challenger in the IND-BCSC-CCA2 game. At the start of the game, C sets $\text{IDPK}_B = bG$, randomly selects $a' \in Z_n^*$, and computes $\text{IDPK}_A = a'G$. C then sends the system parameters $(G, n, \text{IDPK}_B, \text{IDPK}_A)$ to challenger A. C maintains four initially empty lists: L_{KDF} , L_H , L_s , L_u , where L_s simulates the signcryption oracle and L_u simulates the unsigncryption oracle.

KDF query: Upon receiving input $q_{\text{KDF}} = (x||y)$, C first checks if q_{KDF} exists in list L_{KDF} . If it exists, return t_i ; if not, randomly select $t_i \in \{0, 1\}^{\text{klen}}$, add (q_{KDF}, t_i) to list L_{KDF} , and return t_i .

H query: Upon receiving a query, check if (m, e_i) exists in list L_H . If found, return e_i ; if not found, randomly select Z_n^* , add (m, e_i) to L_H , and return e_i .

Signcrypt query:

Randomly select k from Z_n^* , compute $C_1 = kG = (x_1, y_1)$;

Compute $e_i = H(Z||m)(H(Z||m))$ (obtained from a hash query);

Compute $r = e_i + x_1$;

Compute $s = (1 + a')^{-1}(k - ra')$;

Compute $q_{\text{KDF}} = k \cdot \text{IDPK}_B$;

Compute $C_2 = t_i \oplus (m||r||s)$;

Return $\sigma = C_1||C_2$.

Unsigncrypt query:

Parse ciphertext σ into C_1 and C_2 components;

Compute $(x_1, y_1) = C_1$; if $C_1 \in L_{KDF}$, $t' = t_i$, compute $m||r||s = t \oplus C_2$, $u = r + s$, $(x'_1, y'_1) = s'G + u' \cdot IDPK_A$;

If the equation $r = e + x'_1$ holds, then return message m ; otherwise, return an error symbol.

After a polynomial-bounded number of aforementioned queries, the adversary outputs two plaintext messages, m_0 and m_1 , of equal length. The challenger then computes $C'_1 = aG$, randomly selects $C'_2 \{0, 1\}^{klen}$, constructs $\sigma = C'_1 || C'_2$, and sends the challenge ciphertext σ to adversary A.

After the second round of queries, A's inquiries remain identical to those in the first round. Upon successful completion of this simulation process, A submits a prediction value p' as an estimate or inference of the original value p . If $p' = p$, then C has solved the ECDH problem; otherwise, C has not solved the ECDH problem.

Assuming challenger C has previously input abG for a KDF query (meaning abG is stored in table) and C wins the above game with non-negligible advantage ϵ , then according to reference [4], the probability of the above event occurring is $\Pr \geq 2\epsilon$. The probability of randomly selecting from L_{KDF} and obtaining exactly abG is at least $2\epsilon / |L_{KDF}|$. Since $|L_{KDF}| \leq q_k + q_s$, the probability of C solving the ECDH problem is at least $\frac{2\epsilon}{q_k + q_s}$. The computational time t' is the sum of all operational time costs incurred by challenger C and adversary A. Therefore, $t' \leq t + q_k t_k + q_h t_h + q_s t_s + q_u t_u$.

The proof is complete. \square

(2) Unforgeability: The unforgeability of the proposed scheme is established by the following Theorem 2.

Theorem 2. *Under the assumption that the elliptic curve discrete logarithm problem (ECDLP) is computationally infeasible to solve and within the random oracle model, this scheme demonstrates strong resistance against forgery under adaptive chosen-message attacks.*

Proof. Assume the signer receives a random instance of the elliptic curve discrete logarithm problem ($< G, IDPK_A >$), where the objective is to find $a \in Z_n$ satisfying $IDPK_A = a \cdot G$.

Signature: The signer randomly selects $k \in Z_n$ and computes $C_1 = kG = (x_1, y_1)$, $e \in Z_n$, $r = e + x_1$, $s = (1 + IDSK_A)^{-1}(k - rIDSK_A)$. The signature for message m is $\sigma = (r, s)$.

Verification: According to reference [15], assume there exists an adversary A who can break the proposed signature scheme with parameters $(t, n_{sig}, n_h, \epsilon)$, meaning that with access to at most n_{sig} valid signatures and n_h hash queries, A can successfully forge a valid signature within time t with a probability of no less than ϵ . Then, the adversary can obtain two signatures, (r_1, s_1) and (r_2, s_2) , corresponding to the same random value e' within time t^* with a probability of no less than ϵ^* and compute $\frac{s_2 - s_1}{s_1 - s_2 + r_1 - r_2}$ satisfying $\frac{s_2 - s_1}{s_1 - s_2 + r_1 - r_2} \cdot G = IDPK_A$.

Based on all the above analysis, under the assumption that the elliptic curve discrete logarithm problem (ECDLP) is computationally infeasible to solve and within the random oracle model, the signcryption scheme proposed in this paper maintains its unforgeability property even when subjected to adaptive chosen-message attacks. Thus, the security proof has been completed. \square

(3) Public verifiability: Assume the ciphertext $\sigma = C_1 || C_2$ is generated by user A with user B as the recipient. The verifier can publicly verify whether the equation $(x'_1, y'_1) = s'G + u' \cdot IDPK_A = sG + (r + s)G \cdot IDSK_A = kG = (x_1, y_1)$ holds. Thus, the scheme achieves public verifiability.

(4) Non-repudiation: Given the unforgeability property of the proposed scheme, if a sender has indeed signcrypted a message, they cannot deny the fact of having signcrypted that message. This ensures that the sender cannot repudiate their signed messages, thereby achieving non-repudiation.

(5) Forward security: In this scheme, the generation of public and private keys is independent of the certification authority's private key, thus avoiding dependence on the certification authority's private key during certificate generation and eliminating the risk of leakage or theft of the certification authority's private key. Even if user A's key is compromised or stolen, and even if private key information is inadvertently leaked, third parties cannot derive the session key from this information. Therefore, this scheme satisfies forward security.

4.3. Scyther: A Formal Tool for Security Protocol Analysis

Scyther is a formal tool for security protocol analysis. As an automated validation tool, it aims to identify vulnerabilities and attack paths in security protocols. It helps security researchers and protocol designers detect potential risks and improve protocol design. Scyther uses formal methods to analyze security protocols. It employs a formal modeling language for security protocols and performs automated analysis to uncover vulnerabilities and attack paths. Scyther uses model checking, symbolic execution, and simulation to analyze protocol security. It uses a modeling language based on security protocol description language (SPDL), which is a formal language specifically designed for security protocols. It describes messages, roles, and attack models in protocols. Scyther can detect common vulnerabilities in security protocols, such as authentication flaws, key distribution issues, and replay attack vulnerabilities. It can automatically analyze protocol models to detect design defects that may lead to security problems. Scyther can generate attack paths that attackers might exploit and attack sequences that may occur during protocol execution. This helps clarify potential security risks and vulnerabilities in protocols. Scyther offers a visual interface to display protocol models, vulnerability detection results, and attack paths. This allows users to intuitively understand analysis results and make further investigations and improvements. Scyther supports multiple security protocols, including TLS, SSH, IPSec, Kerberos, etc. In summary, Scyther is a powerful security protocol analysis tool that uses formal methods and automation to detect vulnerabilities and attack paths in security protocols. By using Scyther v1.1.3, security researchers and protocol designers can more comprehensively evaluate and improve the design of security protocols to enhance their security.

To analyze the security of a decentralized signcryption scheme based on CFL using the Scyther tool, first, the protocol process and message format of the scheme is converted into an SPDL model. Protocol roles, such as sender, receiver, and attacker, as well as message formats and processes, including the signcryption and unsigncryption stages and attacker interactions, are defined. Then, the SPDL model is input into the Scyther tool, analysis parameters like attacker capabilities are set, and the tool is run to generate protocol execution paths and detect potential attack paths. Finally, the analysis shows that the decentralized signcryption scheme based on CFL performs well in relation to security, effectively preventing issues like confidentiality breaches and signature forgeries. It also supports public key verification and non-repudiation and has forward security. Potential vulnerabilities, such as replay attacks, man-in-the-middle attacks, and public key replacement attacks, can be mitigated by adding timestamps, enhancing key exchange security, and strictly managing public keys. This scheme holds promise for high-security applications like V2X and IoT.

5. Performance Analysis

This section provides a comprehensive evaluation of the newly proposed signcryption scheme based on computational complexity and communication costs [16].

5.1. Computational Overhead

In the simulation process, the system adopts the C/C++ library of high-precision integer operation and rational arithmetic and integrates the encryption algorithm library based on pairing theory. In the simulation, the execution time of the bilinear pairing operation is expressed as $t_{bp} = 6.574$ ms, the execution time of scalar multiplication on bilinear pairs is expressed as $t_{bpm} = 2.123$ ms, the execution time of scalar multiplication on elliptic curves is expressed as $t_m = 0.576$ ms, the execution time of point addition on elliptic curves is expressed as $t_a = 0.02$ ms, the execution time of modular exponentiation is expressed as $t_{ex} = 0.249$ ms, and the execution time of hashing operations is expressed as $t_h = 0.002$ ms.

Table 1 compares the performance differences between our newly proposed scheme and several signcryption schemes. The proposed scheme shows competitive performance compared to the referenced schemes in Figure 2. It has a signcryption time of 1.738 ms, unsigncryption time of 3.566 ms, and a total overhead of 5.304 ms. Compared to other schemes, our scheme has a lower computational overhead and a shorter execution time. These performance metrics enhance its applicability in real-world scenarios, especially in environments with limited computational resources.

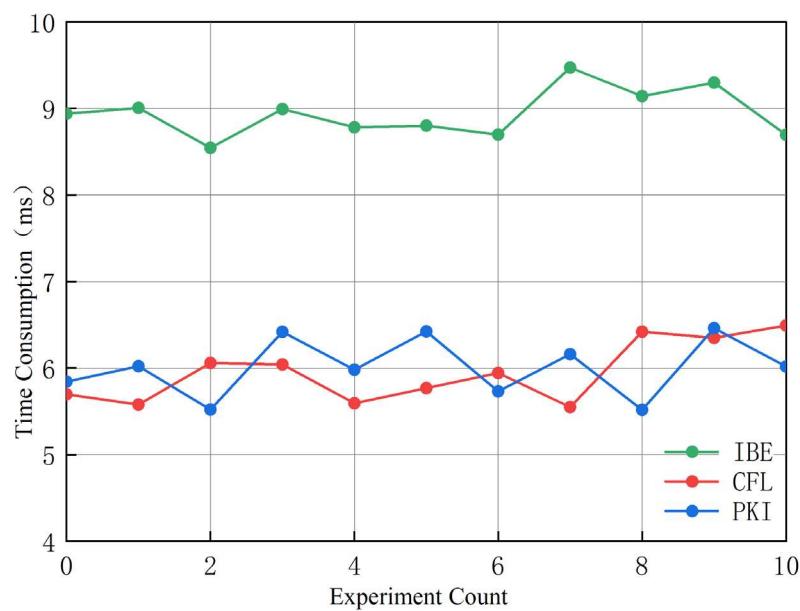


Figure 2. Time consumption comparison.

Table 1. Comparison between our scheme and other signcryption schemes.

Scheme	Signcryption (ms)	Unsigncryption (ms)	Total Overhead (ms)
Reference [17]	$3t_m + t_a + t_{ex} + 3t_h$	$3t_m + 3t_a + 3t_h + t_{bp}$	$6t_m + 4t_a + t_{ex} + 6t_h + t_{bp}$
Reference [18]	$6t_m + 4t_a + 5t_h$	$3t_m + 1t_a + 7t_h + 5t_{bp}$	$9t_m + 5t_a + 12t_h + 5t_{bp}$
Reference [19]	$4t_{ex}$	$2t_{ex} + 2t_{bp}$	$6t_{ex} + 2t_{bp}$
Reference [20]	$7t_m + t_h$	$2t_h$	$3t_h$
Reference [21]	$5t_m + t_{bp}$	$t_{ex} + t_{bp}$	$2t_{bp} + 5t_m + t_{ex}$
Proposed Scheme	$3t_m + 5t_h$	$6t_m + 5t_a + 5t_h$	$9t_m + 5t_a + 10t_h$

For experimental verification, the test program was built using the open-source cryptographic library Bouncy Castle and written in Java programming language. The experimental laptop configuration included the following: Intel(R) Core(TM) i7-8550U processor (Intel Corporation, Santa Clara, CA, USA), 8 GB RAM, running Windows 11 64-bit operating system. The average efficiency overhead of the CFL-based signcryption scheme was approximately 6.32 ms, the PKI-based signcryption scheme was about 5.79 ms, and the IBE-based signcryption scheme was around 9.63 ms. This demonstrates that the time complexity of CFL-based and PKI-based signcryption schemes is similar, while the IBE-based signcryption scheme has lower efficiency due to higher computational overheads, consistent with the theoretical analysis.

5.2. Communication Overhead

Since certificate registration and verification occur independently, this paper discusses the communication overhead for both phases separately, ignoring the communication gap between certificate authentication and registration. Conclusions are drawn by comparing our scheme with two other mainstream schemes.

The registration phase involves data users submitting identity information and registration requests to the certification authority and the certification authority generating and returning certificates. The certificate authentication phase involves data users sending certificates to the cloud data center and the cloud data center verifying and returning the authentication results. In the authentication system's communication interaction process, the core components include device-to-device communications and remote communications between devices and authentication authorities. Here, RV represents the cost of a single short-range communication between device nodes, while RC represents the cost of a single remote communication between devices and the certification center. Table 2 details the comparative analysis of the communication costs for three different schemes.

Table 2. Communication overhead comparison of different schemes.

Scheme	Registration Phase	Authentication Phase	Total Communication Overhead
PKI	2RC	2RC + 2RV	4RC + 2RV
CFL	2RC	2RV	2RC + 2RV
IBE	2RC	2RC + 2RV	4RC + 2RV

As shown in Table 2, during the registration phase, the PKI scheme, IBE scheme, and our proposed CFL scheme have identical communication overheads, each requiring two RC sessions. During the authentication phase, since our scheme's authentication process does not require third-party certification authority participation, it requires two fewer device-to-certification center sessions compared to the PKI and IBE schemes. The PKI and IBE schemes have identical communication overheads, both requiring two device-to-certification center sessions and two device-to-device sessions. The comparison demonstrates that our proposed scheme effectively reduces the communication phase overhead.

To verify the aforementioned theoretical analysis, the experimental setup was designed as follows: A Tencent Cloud server in Shanghai was deployed with the Ubuntu 20.04 system (Server C) as the remote node, equipped with Intel Xeon Platinum 8255C CPU and a Tencent VirtIO network card (Tencent Technology (Shenzhen) Company Limited, Shenzhen, China). In addition, two Windows 10 laptops (A and B) were configured in adjacent campus buildings as local devices, simulating the realistic network layout of the certification authority and communication entities. The Microsoft PsPing tool was then utilized to conduct continuous inter-device access tests, meticulously recording the number of transit nodes for each communication and average round-trip delay to thoroughly investigate network

performance. The average round-trip latency measured by the testing tool represents the transmission delay for data packets traveling from the source to the destination and back to the source in the network. This metric is primarily influenced by the number of routing hops and real-time network load conditions and can be considered as a communication cost independent of device performance.

In this experiment, laptops A and B simulated the sender and receiver, respectively, with access to remote server C simulating the certificate verification process. The average delay RC was used to record remote communication (C-end) latency, while interactions between A and B simulated short-distance communication, with the average delay recorded as RV. The experimental data packet size followed SSL/TLS protocol specifications, set at 500 bytes, with 100 inter-access attempts per group [22]. The final experimental results are shown in Figure 3.

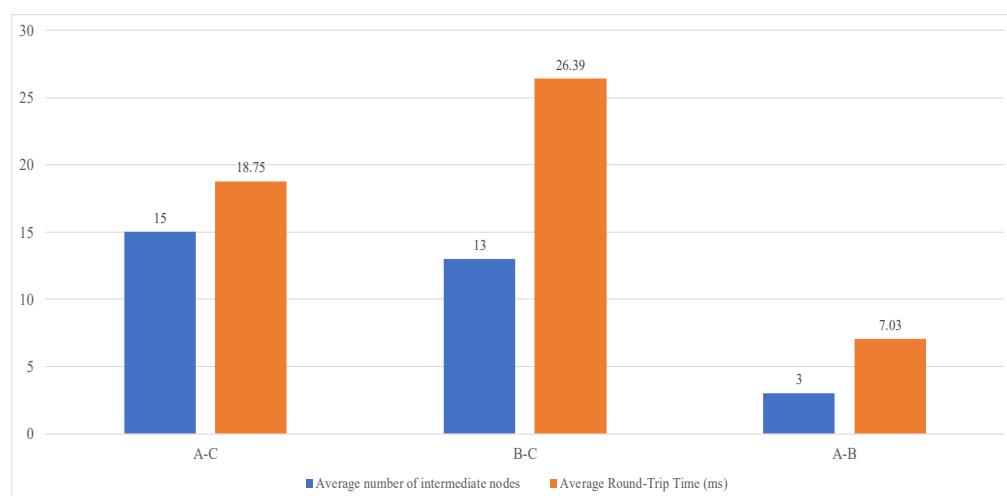


Figure 3. Remote access time consumption comparison.

Based on these experimental results, the short-range communication overhead can be estimated as $RV \approx 7.03/2 = 3.515$ ms and the remote communication overhead as $RC \approx (18.75 + 26.39)/4 = 11.285$ ms. Calculations show that the PKI and IBE schemes require approximately 52.17 ms of communication overheads during the authentication phase, while our proposed scheme requires only about 29.60 ms due to its center-free verification phase. This experimental design did not cover practical challenges such as packet loss, network congestion, connection establishment requests, and data caching. In real-world application scenarios, centralized authentication mechanisms like PKI or IBE might incur higher communication costs. In comparison, our proposed scheme demonstrates advantages in communication overheads, meeting millisecond-level security response requirements, highlighting its significant potential and value in practical applications.

6. Conclusions

In this study, a decentralized signcryption scheme based on the cryptography fundamental logics (CFL) framework was proposed. This scheme represents a significant departure from traditional signcryption schemes, as it does not rely on the certification authority's private key during the public-private key generation process. By eliminating this dependency, the proposed scheme effectively resolves the risk of private key leakage from the certification authority and achieves robust decentralized characteristics. This is a crucial advancement in cryptographic security, as it reduces the potential attack surface and enhances the overall security posture.

Security analysis of the proposed scheme was conducted under the random oracle model, a widely accepted framework for analyzing cryptographic protocols. The security of the scheme was rigorously proven under the hardness assumption of the elliptic curve Diffie–Hellman (ECDH) problem. This mathematical foundation provides a strong theoretical guarantee of the scheme’s security against various types of attacks.

Comparative analysis with existing traditional signcryption schemes revealed that the proposed scheme demonstrates significant advantages in both communication and computational efficiency [23]. These improvements are particularly noteworthy in practical applications where resources are limited and performance is critical. The experimental results further corroborate these findings, indicating that the proposed scheme not only offers enhanced security but also maintains superior efficiency, making it highly suitable for implementation in real-world scenarios.

Future research should focus on designing even more efficient CFL-based signcryption schemes and exploring their applications in diverse practical working environments [24]. This could include optimizing the cryptographic algorithms used, developing new protocols for specific application scenarios, and conducting extensive empirical studies to validate the scheme’s performance in different contexts. Additionally, further research could explore the integration of this scheme with other emerging technologies, such as blockchain, to create more secure and decentralized systems.

Author Contributions: Conceptualization, M.L.; methodology, M.L.; software, M.L.; validation, M.L.; formal analysis, M.L.; investigation, M.L.; resources, M.L.; data curation, M.L.; writing—original draft preparation, M.L.; writing—review and editing, L.S.; visualization, M.L.; supervision, M.L.; project administration, M.L.; funding acquisition, L.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (NNSF), grant number 62111530052, and the APC was funded by M.L.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data that support the findings of this study are not publicly available due to privacy concerns. Requests for access to the data should be directed to the corresponding author.

Acknowledgments: We would like to express our sincere gratitude to Shi for his valuable advice and guidance throughout the research process. This research was supported by the NNSF, grant number 62111530052.

Conflicts of Interest: Author Leyi Shi was employed by the company Qingdao Guochuang Intelligent Appliance Research Institute Co., Ltd. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Zheng, Y. Digital Signcryption or How to Achieve $\text{Cost}(\text{Signature} \& \text{Encryption}) \ll \text{Cost}(\text{Signature}) + \text{Cost}(\text{Encryption})$. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 1997.
2. Yu, H.F.; Qiao, Y.F.; Meng, R. Quantum-resistant attribute-based threshold ring signcryption scheme for blockchain finance. *Inf. Netw. Secur.* **2023**, *23*, 44–52.
3. Ke-Zhen, Z.; Jing-Qiang, L.; Wei, W.; Yong, L.; Guang-Zheng, L.; Zhen-Ya, L. Research on Two-Party SM2 Threshold Signature Schemes with a Blind Cooperative Server. *J. Cryptologic Res.* **2024**, *11*, 945–962. [[CrossRef](#)]
4. Wang, X.; Qian, H. Attacks against Two Identity-Based Signcryption Schemes. In Proceedings of the Second International Conference on Networks Security, Wireless Communications and Trusted Computing, Wuhan, China, 24–25 April 2010.

5. Xie, Z.; Chen, Y.; Ali, I.; Pan, C.; Li, F.; He, W. Efficient and Secure Certificateless Signcryption Without Pairing for Edge Computing-Based Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2023**, *72*, 5642–5653. [[CrossRef](#)]
6. Yang, W.; Cao, P.; Zhang, F. A Secure Pairing-Free Certificateless Online/Offline Signcryption Scheme with Batch Verification for Edge Computing-Based VANETs. *IEEE Trans. Veh. Technol.* **2025**, *74*, 1570–1583. [[CrossRef](#)]
7. Rastegari, P.; Susilo, W.; Dakhllalian, M. Efficient Certificateless Signcryption in the Standard Model: Revisiting Luo and Wan’s Scheme from Wireless Personal Communications (2018). *Comput. J.* **2019**, *62*, 1178–1193. [[CrossRef](#)]
8. Ullah, I.; Khan, M.A.; Kumar, N.; Abdullah, A.M.; AlSanad, A.A.; Noor, F. A Conditional Privacy Preserving Heterogeneous Signcryption Scheme for Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2023**, *72*, 3989–3998. [[CrossRef](#)]
9. Xie, Y.F.; Zhao, D.D.; Shi, L.Y. Signature Authentication Scheme for Decentralized Industrial Control System Based on CFL. *Comput. Syst. Appl.* **2024**, *33*, 84–93.
10. Zhang, Y.; Wang, Z.; Qin, T. An Efficient Signature and Encryption Scheme Based on SM2. *Inf. Secur. Res.* **2024**, *10*, 526–531. [[CrossRef](#)]
11. Brendel, J.; Cremers, C.J.F.; Jackson, D.; Zhao, M. The Provable Security of Ed25519: Theory and Practice. In Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 24–27 May 2021; pp. 1659–1676.
12. Chen, H.P.; Fan, X.B.; Lv, S.W. Certificate Authentication System CFL Based on Identity. CN102957536A, 6 March 2013.
13. Hu, R.L.; Li, W.J.; Jiang, H.; Zhang, X.R. Certificateless aggregate signcryption scheme based on discrete logarithm. *Inf. Netw. Secur.* **2019**, *19*, 42–49.
14. Qin, H.; Pan, Y.; Fan, X.; Wang, H. Provably Secure Analysis of CFL. *Inf. Secur. Res.* **2016**, *2*, 589–599.
15. Ohta, K.; Okamoto, T. On Concrete Security Treatment of Signatures Derived from Identification. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 23–27 August 1998.
16. Hussain, S.; Ullah, I.; Khattak, H.; Khan, M.A.; Chen, C.M.; Kumari, S. A lightweight and provable secure identity-based generalized proxy signcryption (IBGPS) scheme for Industrial Internet of Things (IIoT). *J. Inf. Secur. Appl.* **2021**, *58*, 102625. [[CrossRef](#)]
17. Yang, Y.; He, D.; Vijayakumar, P.; Gupta, B.B.; Xie, Q. An Efficient Identity-Based Aggregate Signcryption Scheme With Blockchain for IoT-Enabled Maritime Transportation System. *IEEE Trans. Green Commun. Netw.* **2022**, *6*, 1520–1531. [[CrossRef](#)]
18. Yang, Y.; Zhang, L.; Zhao, Y.; Choo, K.K.R.; Zhang, Y. Privacy-Preserving Aggregation-Authentication Scheme for Safety Warning System in Fog-Cloud Based VANET. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 317–331. [[CrossRef](#)]
19. Karati, A.; Islam, S.H.; Biswas, G.P.; Bhuiyan, M.Z.A.; Vijayakumar, P.; Karuppiah, M. Provably Secure Identity-Based Signcryption Scheme for Crowdsourced Industrial Internet of Things Environments. *IEEE Internet Things J.* **2018**, *5*, 2904–2914. [[CrossRef](#)]
20. Nkenyereye, L.; Liu, C.H.; Song, J.S. Towards secure and privacy preserving collision avoidance system in 5G fog based Internet of Vehicles. *Future Gener. Comput. Syst.* **2019**, *95*, 488–499. [[CrossRef](#)]
21. Deng, L. Anonymous certificateless multi-receiver encryption scheme for smart community management systems. *Soft Comput.* **2020**, *24*, 281–292. [[CrossRef](#)]
22. Lan, S.B.; Li, F.X.; Shi, L.Y. Authentication communication scheme for industrial control system based on CFL. *J. Comput. Appl.* **2023**, *43*, 1183–1190.
23. Ashok, K.; Gopikrishnan, S. A Hybrid Secure Signcryption Algorithm for data security in an internet of medical things environment. *J. Inf. Secur. Appl.* **2024**, *85*, 103836. [[CrossRef](#)]
24. Hussain, S.; Ullah, S.S.; Uddin, M.; Iqbal, J.; Chen, C.-L. A Comprehensive Survey on Signcryption Security Mechanisms in Wireless Body Area Networks. *Sensors* **2022**, *22*, 1072. [[CrossRef](#)] [[PubMed](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.