

Title	A multi-receiver certificateless signcryption (MCLS) scheme
Authors	Umrani, Alia;Vangujar, Apurva K.;Palmieri, Paolo
Publication date	2024-07-31
Original Citation	Umrani, A., Vangujar, A.K. and Palmieri, P. (2024) 'A multi-receiver certificateless signcryption (MCLS) scheme', 8th International Conference on Cryptography, Security and Privacy (CSP). Osaka, Japan: IEEE, pp. 46–52. https://doi.org/10.1109/CSP62567.2024.00015
Type of publication	Conference item
Link to publisher's version	https://ieeexplore.ieee.org/document/10600656 - 10.1109/CSP62567.2024.00015
Rights	© 2024, IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.
Download date	2026-10-13 22:38:29
Item downloaded from	https://hdl.handle.net/10468/17348

A Multi-receiver Certificateless Signcryption (MCLS) Scheme

Alia Umrani

School of Computer Science & IT
University College Cork
Cork, Ireland
a.umrani@cs.ucc.ie

Apurva K Vangujar

School of Computer Science & IT
University College Cork
Cork, Ireland
a.vangujar@cs.ucc.ie

Paolo Palmieri

School of Computer Science & IT
University College Cork
Cork, Ireland
p.palmieri@cs.ucc.ie

Abstract—In this paper, we substantially modify Hung *et al.* [1] Anonymous Multi-receiver Certificateless Encryption (AMCLE) scheme to a Multi-receiver Certificateless Signcryption (MCLS) scheme, which provides authentication and introduces public verifiability as an additional feature. We show that, as compared to existing signcryption, our scheme requires less computation for the signcryption and unsigncryption phases. Additionally, the signcryption cost is linear with the number of designated receivers, while the unsigncryption cost remains constant. We compare the results with existing single-receiver and multi-receiver signcryption schemes and show that our proposed MCLS scheme is more efficient for single and multi-receiver signcryption schemes while providing an exemption from the key escrow problem and working in certificateless public key settings.

Index Terms—Signcryption, Certificateless, Multi-receiver, Public Key Cryptography

I. INTRODUCTION

A message in digital communication must be secure in terms of authentication, confidentiality, and integrity. Encryption schemes are generally used for confidentiality, whereas Digital Signature (DS) schemes are used for authentication, integrity, and non-repudiation. However, in sign-then-encrypt schemes, signing and then encrypting a message has a high computational cost. Signcryption, on the other hand, not only signs the message as the traditional approach requires but also encrypts it in a single step. This ensures that the message is meaningless to anyone but the intended recipient, who can also verify the sender's Identity (ID) and the message's integrity. Signcryption is more attractive because it requires less computation time and message expansion rate [2], [3].

Zheng *et al.* [2] proposed the first signcryption scheme, which combines DS and Public Key Encryption (PKE) to provide authentication, confidentiality, and non-repudiation at a lower cost. Malone-Lee [4] proposed the first ID-based signcryption scheme to provide public verifiability and forward security. Following that, several ID-based signcryption schemes were proposed. Chen *et al.* [5] and Chow *et al.* [6] proposed ID-based signcryption schemes, respectively, to demonstrate public verifiability, forward security, unlinkability,

and anonymity. However, ID-based cryptography has an inherent key escrow problem in which a malicious Key Generation Center (KGC) compromises the entity's private key. To solve the key escrow problem, Al-Riyami *et al.* [7] proposed the concept of certificateless Public Key Cryptography (PKC). In certificateless PKC, the KGC generates the partial private key for the user, and the full private key pair is the combination of the user's secret value and the partial private key. The above signcryption schemes are based on a single receiver, which is insufficient for broadcast communication. For example, to send an identical message to multiple receivers, a sender must encrypt the message for each designated receiver, resulting in poor performance. Yu *et al.* [8] proposed the first multi-receiver signcryption scheme based on ID-based PKC in which the message is encrypted for n designated receivers and is secure under the Random Oracle Model (ROM) and Computational Diffie-Hellman (CDH). Later, Hung *et al.* [1] proposed an efficient Anonymous Multi-receiver Certificateless Encryption (AMCLE) scheme based on Bilinear Pairing (BP). The scheme proves Indistinguishability against Chosen Ciphertext Attack (IND-CCA) and Anonymous Indistinguishability against Chosen Ciphertext Attack (ANON-CCA). The encryption cost is linear with the number of designated receivers, while the decryption cost is constant. Moreover, several publicly verifiable signcryption schemes have also been introduced [9]–[11]. Public verifiability enables any third party to verify the authenticity and integrity of a signcrypted message without requiring knowledge of the private keys possessed by either the sender or the receiver. This capability significantly enhances the transparency and trustworthiness of the signcryption scheme [6].

In this paper, we modify the functionalities of Hung *et al.*'s AMCLE encryption-only scheme into a Multi-receiver Certificateless Signcryption (MCLS) scheme. The MCLS scheme demonstrates Existential Unforgeability against Chosen Message Attack (EUF-CMA) considered a potential attack in signcryption. In addition, we incorporate a public verifiability feature into our scheme, which is not provided in the AMCLE scheme. As our work and, more generally, most signcryption applications focus on authentication along with confidentiality, we omit from this paper the IND-CCA and ANON-CCA proofs. However, the proof provided by the

Alia Umrani and Apurva K Vangujar are supported by PhD scholarships funded by the Science Foundation Ireland Centre under Grant number 18/CRT/6222. This research has also been supported by Science Foundation Ireland under Grant number 13/RC/2077_P2.

AMCLE encryption-only scheme will remain in line with our extended scheme. Our signcryption scheme has a lower computational cost with respect to the number of operations, with the cost of signcryption being linear with the number of designated receivers and the cost of unsigncryption remaining constant for each designated receiver. Compared to the other existing signcryption techniques, the proposed MCLS scheme overcomes the key escrow problem and works in a multi-receiver certificateless public key setting. Specifically, the main contributions are as follows:

- 1) We design a Multi-receiver Certificateless Signcryption (MCLS) scheme that significantly enhances the functionalities of the existing AMCLE scheme by modifying it to a signcryption scheme, we enable secure authentication.
- 2) We provide security proof in a ROM under the CDH and Decisional Bilinear Diffie-Hellman Inversion (DBDHI) assumptions, which claim that the proposed scheme can achieve authentication by demonstrating EUF-CMA. We also show that, along with authentication, our scheme simultaneously achieves public verifiability.
- 3) We evaluate the performance of the proposed MCLS scheme and present a comparison with other existing signcryption schemes.

The remainder of this paper is organized as follows. Sec. II reviews the research related to the scheme. Sec. III introduces the security assumptions. Sec. IV describes the framework and security model in the MCLS scheme. Sec. V shows the construction of the MCLS scheme. In Sec. VI, we provide a security proof in ROM, and in Sec. VII, we compare it to existing schemes. Sec. VIII concludes this paper.

II. RELATED WORK

Barbosa and Farshim [12] proposed the first certificateless-based signcryption scheme based on BP that provides authentication and is secure against insider attacks in a ROM. For security, it employs Gap-BDH, Decisional-BDH, and BCDH assumptions and is shown to be IND-CPA and strong-UF-CMA secure. Selvi *et al.* [13] proposed an efficient and provably secure certificateless multi-receiver signcryption scheme. The scheme is based on the strong DH assumption, the Collusion Attack Algorithm with k -Traitors, Modified BDHI for k -Values, and the Gap-BDH assumptions. The scheme employs BP operations and compares the efficiency with ID-based schemes. The scheme proposed by Selvi *et al.* [13] is not secure against external adversaries and is improved as an enhanced certificateless multi-receiver signcryption scheme [14]. However, Miao *et al.* [15] proposed a cryptanalysis of [14], and the authors demonstrated that the scheme is insecure against an external adversary and presented an attack on [13]'s enhanced scheme. They demonstrate that the adversary can first replace the sender's public key and then generate ciphertext on the sender's behalf. Islam *et al.* [16] proposed an anonymous and provably secure certificateless multi-receiver encryption scheme that uses an elliptic curve-based technique under the CDH assumption. In this scheme, the encryption cost is quadratic with the number of receivers, whereas the

decryption cost is linear. However, its security proof failed to generate the challenge ciphertext successfully, and thus, the security did not hold, and the scheme has a key escrow problem. To overcome the key escrow problem and provide more efficiency, Hung *et al.* [1] proposed an AMCLE scheme that provides confidentiality and anonymity. This scheme uses BP under the BDDH, GBDH, and CDH assumptions. To prove confidentiality, the scheme defines the IND-CCA, and to achieve anonymity, the authors present the ANON-CCA. The proposed AMCLE scheme provides a constant decryption cost, which means that the required decryption cost of each receiver is independent of the number of receivers as compared to Islam *et al.*'s scheme. However, the security proof cannot cover all possible attacks due to some restrictions on attackers. Guo *et al.* [17] proposed an efficient certificateless ring signcryption scheme with conditional privacy preservation. The scheme employs a certificateless PKC and compares the results to ID-based signature schemes. Moreover, several heterogeneous signcryption schemes have been proposed that show interoperability between signcryption and sign-and-encrypt schemes, while we only focus on signcryption schemes.

Similarly, Chaudhry *et al.* [9] proposed an efficient signcryption scheme with authentication, forward security, and public verifiability based on a hyperelliptic curve. Karati *et al.* [10] introduced a provably secure and generalized signcryption scheme with public verifiability for secure data transmission between resource-constrained IoT devices. The scheme achieves authentication using strong DH and BDHI assumptions and is based on certificateless PKC. Similarly, Hu *et al.* [11] proposed a sanitizable signcryption scheme with public verifiability. The scheme utilizes the chameleon hash function as a trapdoor commitment for signcryption and proves security in the ROM. In this paper, we expand Hung *et al.*'s scheme and propose an efficient multi-receiver certificateless signcryption that provides authentication and public verifiability.

III. PRELIMINARIES

A. Bilinear Pairing

The BP definition is adopted from [18].

Definition 1. Let G be cyclic additive and multiplicative group, respectively, over a prime order q . A BP is a map: $e : G \times G \rightarrow G$ which satisfies the following properties:

- **Bilinearity:** For any $P \in G$, $e(aP, bP) = e(P, P)^{ab}$ where $a, b \in \mathbb{Z}_q^*$.
- **Computability:** For some $P \in G$, $e(P, P)$ can be efficiently computed.
- **Non-degenerate:** For some $P \in G$, $e(P, P) \neq 1$.

B. Assumptions

1) **Computational Diffie-Hellman (CDH) Assumption:** The definition of CDH assumption is taken from Joux *et al.* [19].

Definition 2. Let $P, aP, bP \in G$, the CDH assumption hold if no PPT algorithm with non-negligible ϵ can compute abP . The advantage (ϵ) of an adversary ($\mathcal{A}$) is defined as

$$\epsilon^{CDH} = \Pr [\mathcal{A}(P, aP, bP) = abP] \quad (1)$$

2) *Decisional Bilinear Diffie-Hellman Inversion (DBDHI) Assumption:* DBDHI assumption is adopted from Chen *et al.* [20].

Definition 3. Given input $P, aP, bP, cP \in G_1$ and $R \in G_2$ where $G_1 = G_2$, the DBDHI assumption holds if no PPT algorithm with non-negligible ϵ can decide whether $R = e(P, P)^{ab^{-1}c}$ or not. The ϵ of $\mathcal{A}$ is given as below:

$$\epsilon^{DBDHI} = \Pr [\mathcal{A}(P, aP, bP, cP, e(P, P)^{ab^{-1}c}) = 1] - \Pr [\mathcal{A}(P, aP, bP, cP, R) = 1] \quad (2)$$

IV. FRAMEWORK AND SECURITY MODEL

A. Framework

This paper adopts the certificateless signcryption scheme framework from the AMCLE scheme [1]. The scheme has two roles: KGC and n number of users (a sender and t receivers), where $t < n$. The AMCLE scheme allows a sender to generate a signcrypted ciphertext CT_i where $1 \leq i \leq t$ of a message m for t designated receivers. We assume that the KGC is fully trusted in the system while we prove the authenticity of users, including a sender and t receivers. The KGC generates and stores its master secret key (s) and master public key (P_{pub}), and computes and shares a partial private key (D) for users. Users generate, store, and manage their private and public keys (pk, sk). The sender encrypts a m with the receiver's public key pk_{r_i} , signs it with its private key sk_s , and sends a CT_i to receivers. The designated receiver decrypts the m with its private key sk_{r_i} and verifies the signature S_i with the sender's public key pk_s . Moreover, any third party can verify the authenticity of the m without having knowledge of the private keys of either the sender or receiver. The scheme consists of seven polynomial-time algorithms, as listed below:

- 1) **Setup:** On input security parameter 1^λ , the KGC generates s, P_{pub} , and public parameters PP . The PP is given as input to other algorithms.
- 2) **Partial Private Key:** Taking s and user $ID \in \{0, 1\}^*$ as input, the KGC generates D .
- 3) **Set Secret Value:** Taking user ID as input, this algorithm outputs a secret value x .
- 4) **Set Private Key:** Each user takes (D, x) as input and outputs a full private key sk .
- 5) **Set Public Key:** Taking secret value x as input, each user outputs a public key pk .
- 6) **Signcryption:** On input (m, sk_s, pk_{r_i}) , a sender generates a CT_i .
- 7) **Unsigncryption:** The receiver takes (CT_i, pk_s, sk_{r_i}) as input and retrieves m , or “rejects”.

B. Security Model

For unforgeability, we propose and demonstrate the EUF-CMA against two types of adversaries (i.e., Type-I ($\mathcal{A}_I$) and Type-II ($\mathcal{A}_{II}$)) in Def. 4. Each Type of $\mathcal{A}$ is defined as follows:

- 1) $\mathcal{A}_I$: $\mathcal{A}_I$ is a common user who cannot access the master secret key but can replace the user's public key with a value of his/her own choice. It is not allowed to ask a partial private key query for any of the target ID^* .
- 2) $\mathcal{A}_{II}$: $\mathcal{A}_{II}$ is considered an insider who cannot make public key replace query for the ID^* and is not allowed to make secret value extract queries. The secret value extract query will be denied for ID^* , if it has already been replaced.

Definition 4. The MCLS scheme is EUF-CMA secure if every PPT Adversary $\mathcal{A}$ has a negligible winning advantage ϵ .

Proof: The interaction between the challenger $\mathcal{B}$ and $\mathcal{A}$ as follows:

- 1) **Setup:** In this algorithm, $\mathcal{B}$ generates the s, P_{pub} , and PP . The $\mathcal{B}$ sends PP to $\mathcal{A}$.
- 2) **Phase-1:** The $\mathcal{A}$ outputs a target identity denoted by ID_s^* . The $\mathcal{A}$ asks $q_{H_j} \{j = 0, 1, \dots, 5\}$ hash queries, q_p public key retrieve query, q_r public key replace query, q_e partial private key query, q_s secret value extract query, q_{sc} signcryption query, and q_{usc} unsigncryption query. The $\mathcal{B}$ sets empty lists pk^{list} to record public and private key values. The response to each query is as follows:
 - q_p : $\mathcal{B}$ receives the query for ID and runs the **Set Secret Value** algorithm to generate a random x , and then **Set Public Key** algorithm to return the pk to $\mathcal{A}$.
 - q_r : Upon receiving such query, $\mathcal{B}$ replaces the pk of the user with pk^* and records the replacement.
 - q_e : Given ID , $\mathcal{B}$ checks if $ID = ID_s^*$. If it does, $\mathcal{B}$ aborts. Otherwise, it fetches the D from pk^{list} and returns. If it does not exist, $\mathcal{B}$ runs the **Partial Private Key** algorithm to return D .
 - q_s : Upon such query, $\mathcal{B}$ searches the pk^{list} for x and returns. If it does not exist, $\mathcal{B}$ runs the **Set Secret Value** algorithm to return x to $\mathcal{A}$.
 - q_{sc} : On input (m, sk_s, pk_{r_i}) , $\mathcal{B}$ checks if $ID = ID_s^*$. If not, $\mathcal{B}$ runs normal **Signcryption** by fetching values from pk^{list} . Otherwise, it performs the **Signcryption** to generate the CT_i and returns to $\mathcal{A}$.
 - q_{usc} : Upon receiving CT_i , $\mathcal{B}$ checks if $ID = ID_s^*$. If not, $\mathcal{B}$ either runs normal **Unsigncryption** operation, or it takes the values from the pk^{list} and runs the **Unsigncryption** and returns the answer. Then $\mathcal{B}$ checks the equation. If it holds, it returns m ; otherwise, it rejects. If $ID = ID_s^*$, $\mathcal{B}$ aborts.
- 3) **Forgery:** $\mathcal{A}$ outputs the forged signature under a target ID_s^* . $\mathcal{A}$ wins if unsigncryption does not return $\perp$. The ϵ of $\mathcal{A}$ is:

$$\epsilon_{\mathcal{A}}^{EUF-CMA} = \Pr [(\text{Unsigncryption}) \neq \perp] \quad (3)$$

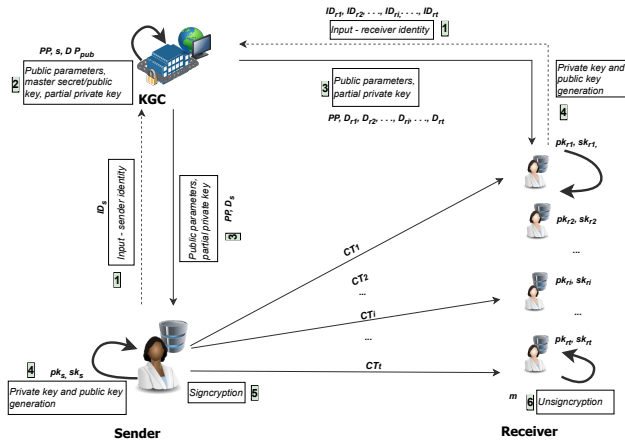


Fig. 1. The Multi-receiver Certificateless Signcryption (MCLS) Scheme

V. MULTI-RECEIVER CERTIFICATELESS SIGNCRYPTION SCHEME

In this section, we define the MCLS scheme according to the framework defined in Sec. IV-A. The main scheme is shown in Fig. 1.

- 1) **Setup:** Taking the security parameter 1^λ as input, KGC initializes the system. It generates a cyclic group G of a large prime order $q \geq 2^\lambda$, a BP $e : G \times G \rightarrow G$, and selects a generator P of G . KGC chooses six hash functions $H_0 : \{0, 1\}^* \rightarrow G$, $H_1 : G \times G \rightarrow \{0, 1\}^w$, $H_2, H_3, H_4 : \{0, 1\}^w \rightarrow \{0, 1\}^w$, $H_5 : \{0, 1\}^* \times G \rightarrow Z_q^*$ for a positive integer w . KGC then chooses $s \in Z_q^*$ randomly as the master secret key and calculates the master public key $P_{pub} = sP$. KGC publishes $PP = \{G, e, P, q, H_0, H_1, H_2, H_3, H_4, H_5\}$ and keeps s .
- 2) **Partial Private key:** Taking the user's ID as input, the KGC computes $Q = H_0(ID)$ and $D = sQ$. The KGC sends D to the user via a secure channel.
- 3) **Set Secret Value:** Each user with ID selects a random positive integer $x \in Z_q^*$ as a secret value.
- 4) **Set Public Key:** On input x , each user outputs $pk = xP$.
- 5) **Set Private Key:** Taking (D, x) as input, each user outputs a private key pair $sk = (D, x)$.
- 6) **Signcryption:** A sender takes (sk_s, pk_{r_i}, m) and generates a CT_i to transfer a message m to multiple receivers. The sender runs the following steps:
 - a) Chooses a value $r \in Z_q^*$ randomly and computes $U = rP$, $F_i = rpk_{r_i}$.
 - b) Computes $K_i = e(P_{pub}, Q_{r_i})^r$, $Q_{r_i} = H_0(ID_{r_i})$ and $T_i = H_1(K_i, F_i)$.
 - c) Picks an ephemeral value $\sigma \in \{0, 1\}^w$ randomly and computes $C_i = H_2(T_i) \parallel (H_3(T_i) \oplus \sigma)$. Use σ to compute $\alpha = H_4(\sigma)$ and generate $V_i = Enc_\alpha(m)$.
 - d) Computes $h_i = H_5(\{C_1, C_2, \dots, C_t\}, V_i, U, T_s)$. It signs the m as $S_i = (r + h_i)x_s$.

e) Set the $CT_i = (\{C_1, C_2, \dots, C_t\}, V_i, U, S_i, h_i)$.

7) **Unsigncryption:** Upon receiving CT_i , the designated receiver takes (sk_{r_i}, pk_s) as input and runs the following steps:

- a) Computes $K_i = e(U, D_{r_i})$, $F_i = x_{r_i}U$, $T_i = H_1(K_i, F_i)$ and $H_2(T_i)$.
- b) Uses $H_2(T_i)$ to find associated C_i by the relation $C_i = (H_2(T_i) \parallel W_i)$ where $W_i = (H_3(T_i) \oplus \sigma)$. Computes $\sigma' = W_i \oplus H_3(T_i)$. If $\sigma' = \sigma$, the receiver runs the following steps:
- c) Computes $\alpha' = H_4(\sigma')$ and computes $m' = Dec_{\alpha'}(V_i)$ and $h'_i = H_5(\{C_1, C_2, \dots, C_t\}, V_i, U)$. If $h'_i = h_i$, the receiver runs the following steps:
- d) Verifies the signature by checking if $S_iP = F_i + h_i pk_s$, hold or not. If it holds, the receiver gets the m , else returns 'reject'.

Correctness Proof

- 1) $K_i = e(P_{pub}, Q_{r_i})^r = e(sP, Q_{r_i})^r = e(rP, sQ_{r_i}) = e(U, D_{r_i})$.
- 2) $F_i = rpk_{r_i} = rx_{r_i}P = x_{r_i}U$.
- 3) $S_iP = ((r + h_i)x_s)P = rx_sP + h_ix_sP = rpk_s + h_i pk_s = F_i + h_i pk_s$.

VI. SECURITY PROOF

Here, we illustrate that the MCLS scheme fulfills both unforgeability and public verifiability. For unforgeability, Theorems 1 and 2 below demonstrate that the scheme is secure against EUF-CMA $\mathcal{A}_I$ and $\mathcal{A}_{II}$ according to the Def. 4.

A. Authentication

Theorem 1. The scheme is provably secure against EUF-CMA $\mathcal{A}_I$. Assume that an $\mathcal{A}_I$ with a non-negligible advantage ϵ can break the MCLS scheme with running time τ in ROM. Then, there exists $\mathcal{B}$ that can solve the DBDHI assumption with a non-negligible advantage ϵ' with running time τ' .

Assume that $\mathcal{B}$ is given a random instance (P, aP, bP, cP) , where $P, aP, bP, cP \in G$ with unknown $a, b, c \in Z_q^*$. Let $R = e(P, P)^{ab^{-1}c}$ be the solution of DBDHI assumption. The $\mathcal{B}$ would compute R by interacting with the $\mathcal{A}_I$ as follows:

- 1) **Setup:** $\mathcal{B}$ runs the initial algorithm and generates $PP = \{G, e, P, q, H_0, H_1, H_2, H_3, H_4, H_5\}$ with $P_{pub} = aP$. The $\mathcal{B}$ sends PP to $\mathcal{A}_I$.
- 2) **Phase-1:** The $\mathcal{A}_I$ first selects a target ID denoted by ID_s^* . The $\mathcal{A}_I$ makes a number of queries including $q_{H_j} \{j = 0, \dots, 5\}$ hash queries, $q_p, q_r, q_e, q_s, q_{sc}$, and q_{usc} (each query is defined briefly in Def. 4). The $\mathcal{B}$ sets empty lists pk^{list} to record public key values and maintains six empty lists $\{L_0, L_1, \dots, L_5\}$ to record the responses of q_{H_j} queries. The $\mathcal{B}$ responds to $\mathcal{A}_I$'s queries as follows:
 - H_0 -query: If there exists (ID_i, u, Q_i) in the L_0 , $\mathcal{B}$ returns Q_i to $\mathcal{A}_I$. Otherwise, $\mathcal{B}$ performs the following steps:
 - a) Picks a value $u \in Z_q^*$ at random.

- b) If $ID_i = ID_s^*$, sets $Q_i = ub^{-1}P$. Otherwise, sets $Q_i = uP$, stores (ID_i, u, Q_i) in L_0 and responds with Q_i to $\mathcal{A}_I$.
- H_1 -query: Upon receiving the query, $\mathcal{B}$ checks if (K_i, F_i, T_i) exists in the L_1 . If yes, $\mathcal{B}$ returns T_i to $\mathcal{A}_I$. Else, $\mathcal{B}$ picks a string $T_i \in \{0, 1\}^w$ at random, stores (K_i, F_i, T_i) in L_1 , and responds with T_i .
- H_2 and H_3 -query: On such query, $\mathcal{B}$ checks L_2 and L_3 for (T_i, x) and (T_i, y) respectively. If they exist, $\mathcal{B}$ returns x and y to $\mathcal{A}_I$. Otherwise, $\mathcal{B}$ picks a string $x \in \{0, 1\}^w$ and $y \in \{0, 1\}^w$ at random, stores (T_i, x) and (T_i, y) in L_2 and L_3 respectively, and responds with x and y .
- H_4 -query: If there exists (k, w) in L_4 , $\mathcal{B}$ returns w to $\mathcal{A}_I$. Else, $\mathcal{B}$ randomly picks a string $w \in \{0, 1\}^w$, stores (k, w) in L_4 , and returns w .
- H_5 -query: If $(\{C_1, C_2, \dots, C_t\}, V_i, U, h_i)$ exists in the L_5 , $\mathcal{B}$ returns h_i to $\mathcal{A}_I$. Else, $\mathcal{B}$ picks a random value $h_i \in Z_q^*$, stores the tuple $(\{C_1, C_2, \dots, C_t\}, V_i, U, h_i)$ in L_5 , and then returns h_i to $\mathcal{A}_I$.
- q_p : Upon such query, $\mathcal{B}$ checks pk_i^{list} for (ID_i, pk_i, x_i) , if it exists, $\mathcal{B}$ returns pk_i to $\mathcal{A}_I$. Else, randomly picks $x_i \in Z_q^*$, sets $pk_i = x_i P$ and stores in pk_i^{list} and provide pk_i to $\mathcal{A}_I$.
- q_r : $\mathcal{B}$ replaces the associated tuple (ID_i, pk_i, x_i) in pk_i^{list} with the new tuple $(ID_i, pk_i^*, \perp)$. Since, the x_i for pk_i^* is unknown, $\mathcal{B}$ will set $\perp$ as x_i .
- q_e : If $ID_i = ID_s^*$, $\mathcal{B}$ returns $\perp$ because, ID_s^* is a target ID and $\mathcal{A}_I$ is not allowed to ask for a q_e for the target ID. Otherwise, if (ID_i, u, Q_i) exists in L_0 , $\mathcal{B}$ computes and returns $D_i = uP_{pub}$ to $\mathcal{A}_I$. Otherwise, $\mathcal{B}$ randomly picks a value $u \in Z_q^*$, sets $Q_i = uP$, and $D_i = uP_{pub}$, and stores (ID_i, u, Q_i) in L_0 . $\mathcal{B}$ returns D_i to $\mathcal{A}_I$.
- q_s : If (ID_i, pk_i, x_i) exists in pk_i^{list} , $\mathcal{B}$ returns x_i to the $\mathcal{A}_I$. Else, randomly picks $x_i \in Z_q^*$, sets $pk_i = x_i P$, stores in pk_i^{list} and returns x_i to $\mathcal{A}_I$.
- q_{sc} : $\mathcal{B}$ checks if $ID_i = ID_s^*$. If $ID_i \neq ID_s^*$, the $\mathcal{B}$ runs the normal signcryption. Otherwise, $\mathcal{B}$ obtains the tuple (D_i, x_i, pk_i) via q_p , q_e , and q_s queries and generates a CT_i via following procedure:
 - a) Pick a value $r \in Z_q^*$ randomly and compute $U = rP$, and $F_i = rpk_{r_i}$
 - b) Picks an ephemeral value $\sigma \in \{0, 1\}^w$ at random and compute $C_i = H_2(T_i) \parallel (H_3(T_i) \oplus \sigma)$ and adds in L_2 and L_3 .
 - c) Use σ to compute $\alpha = H_4(\sigma)$ and generate $V_i = Enc_\alpha(m)$.
 - d) Set $h_i = H_5(\{C_1, C_2, \dots, C_t\}, V_i, U)$ and update L_5 . Compute $S_i = (r + h_i)x_s$, and sets $CT_i = (\{C_1, C_2, \dots, C_t\}, V_i, U, S_i, h_i)$.
- q_{usc} : If $ID_i \neq ID_s^*$, $\mathcal{B}$ aborts because $\mathcal{A}_I$ cannot ask for the q_{usc} for the target identity. Otherwise, $\mathcal{B}$ checks if $(\{C_1, C_2, \dots, C_t\}, V_i, U, h_i)$ in L_5 . If not, $\mathcal{B}$ terminates. Otherwise, $\mathcal{B}$ further obtains the

values from pk_i^{list} and computes the signature and generates m' . If it holds, the $\mathcal{B}$ responds with m' , otherwise it aborts.

- 3) **Forgery**: After the query phase completes, $\mathcal{A}_I$ outputs the challenge ID_s^* , a m , and a $CT_i^* = (\{C_1^*, C_2^*, \dots, C_t^*\}, V_i^*, U^*, S_i^*, h_i^*)$. However, it cannot ask for the q_{usc} for the CT_i^* with the private key of any target ID.

If the game does not abort, the $\mathcal{B}$ fetches the L_1 for (K_i, F_i) to obtain $R = e(P, P)^{ab^{-1}c}$ which is the solution to the DBDHI assumption. Since, $Q_i = ub^{-1}P$, $P_{pub} = aP$, and $U^* = cP$, $\mathcal{B}$ can obtain $R = e(P, P)^{ab^{-1}c}$ by evaluating $K_i^{ui^{-1}}$. Next, we evaluate the advantage of $\mathcal{B}$ winning by calculating the probability of occurrence of the following events:

- 1) The $\mathcal{B}$ will obtain the L_1 for the some (K_i, F_i) with the probability $1/q_{H_1}$.
- 2) In the unsigncryption query if $(\{C_1, C_2, \dots, C_t\}, V_i, U, h_i)$ cannot be found in L_5 , $\mathcal{B}$ return failure and terminates. The probability is $1/q_{H_5}$.
- 3) In the q_e , the game terminates if $ID \neq ID_s^*$. The probability is $1/q_e$.
- 4) In the q_{usc} , the game aborts due to invalid message $m' \neq m$. The probability is q_{usc}/q .

Hence, if $\mathcal{A}_I$ can break the MCLS scheme with a non-negligible advantage ϵ , the DBDHI assumption can be solved with a non-negligible advantage ϵ'

$$\epsilon' \geq \epsilon \left(\frac{1}{q_{H_5}} \right) \left(\frac{1}{q_{H_1}} \right) \left(1 - \frac{1}{q_e} \right) \left(1 - \frac{q_{usc}}{q} \right) \quad (4)$$

τ' is the required computation time while answering the queries in the aforementioned simulation game. It turns out that $\tau' = \tau + \mathcal{O}(q_0 + q_p + q_e)\tau_1 + \mathcal{O}(q_1 + q_2 + q_3 + q_4 + q_5 + q_r + q_s + q_{usc})$ where τ_1 is the time to perform a scalar multiplication in G and t is the number of target identities.

Theorem 2. *The scheme is provably secure against EUF-CMA $\mathcal{A}_{II}$. Assume that an $\mathcal{A}_{II}$ with a non-negligible advantage ϵ can break the MCLS scheme with running time τ in ROM. Then, there is $\mathcal{B}$ that can solve the CDH assumption with a non-negligible advantage ϵ' with running time τ' .*

Assume that $\mathcal{B}$ is given a random instance (P, aP, bP) , where $P, aP, bP \in G$, within unknown $a, b \in Z_q^*$. Let $R = abP$ be the solution of the CDH assumption. The $\mathcal{B}$ would compute J by interacting with the $\mathcal{A}_{II}$ as follows:

- 1) **Setup**: $\mathcal{B}$ runs the initialized algorithm and generates $PP = \{G, e, P, q, H_0, H_1, H_2, H_3, H_4, H_5\}$ with $P_{pub} = aP$. The $\mathcal{B}$ sends PP to $\mathcal{A}_{II}$.
- 2) **Phase-1**: The $\mathcal{A}_{II}$ first selects a target ID denoted by ID_s^* . The $\mathcal{A}_{II}$ makes number of queries including a H_0 -query, q_e , q_r , q_s , q_{usc} and q_{sc} . The $\mathcal{B}$ responds as follows:

- H_0 -query: If there exists (ID_i, u, Q_i) in L_0 , $\mathcal{B}$ returns Q_i to $\mathcal{A}_{II}$. Otherwise, $\mathcal{B}$ picks a value $u \in Z_q^*$ randomly and computes $Q_i = uP$. Then, $\mathcal{B}$ Stores in L_0 and responds with Q_i .

- q_p : If there exists (ID_i, pk_i, x_i) in the pk^{list} , $\mathcal{B}$ returns pk_i to $\mathcal{A}_{II}$. Otherwise, $\mathcal{B}$ performs the following steps:
 - a) Pick $x_i \in Z_q^*$ at random.
 - b) If $ID_i = ID_s^*$, set $pk_i = x_i aP$; otherwise, set $pk_i = x_i P$.
 - c) Store (ID_i, pk_i, x_i) in the pk^{list} and returns pk_i to $\mathcal{A}_{II}$.
- q_r : If $ID_i = ID_s^*$, $\mathcal{B}$ terminates and returns $\perp$ because $\mathcal{A}_{II}$ is not allowed to ask q_r for the target identity ID_s^* . Otherwise, $\mathcal{B}$ replaces the tuple (ID_i, pk_i, x_i) in the pk^{list} with $(ID_i, pk_i', \perp)$.
- q_s : If $ID_i = ID_s^*$, $\mathcal{B}$ returns $\perp$. If (ID_i, pk_i, x_i) exists in the pk^{list} , $\mathcal{B}$ returns x_i to the $\mathcal{A}_{II}$. Otherwise, $\mathcal{B}$ randomly picks $x_i \in Z_q^*$ sets $pk_i = x_i P$, stores (ID_i, pk_i, x_i) in pk^{list} , and returns x_i .
- q^{sc} : The q^{sc} remains the same as in Theorem 1.
- q_{usc} : q_{usc} remains the same as in previous Theorem 1.

3) **Forgery**: After the query phase completes, $\mathcal{A}_{II}$ outputs the $\mathcal{B}$ sender's ID_s^* , a m , and a $CT_i^* = (\{C_1^*, C_2^*, \dots, C_t^*\}, V_i^*, U^*, S_i^*, h_i^*)$. However, it cannot ask for the q_{usc} for the CT_i^* with the private key of any target ID.

If the game does not abort, the $\mathcal{B}$ fetches the L_1 for (K_i, F_i) such that $e(P, F_i) = e(U^*, pk_{r_i})$. The $\mathcal{B}$ can find such a F_i by verifying the equality $e(P, F_i) = e(U^*, pk_{r_i})$. Since, $U^* = bP$, $pk_{r_i} = x_i(aP)$, $\mathcal{B}$ can obtain $R = abP$ by evaluating $x_i^{-1}F_i$ which is the solution to the CDH assumption. Next, we assess the advantage of $\mathcal{B}$ winning from $\mathcal{A}_{II}$ by calculating the probability of the following events occurring:

- 1) In the q_{usc} , if $(\{C_1, \dots, C_t\}, V_i, U, h_i)$ cannot be found in L_5 , $\mathcal{B}$ returns failure and terminates. The probability is $1/q_{H_5}$.
- 2) In the q_r , the game terminates if $ID_i = ID_s^*$. The probability is $1/q_r$.
- 3) In the q_s , the game terminates if $ID_i = ID_s^*$. The probability is $1/q_s$.
- 4) In the q_{usc} , the game aborts due to invalid message $m' \neq m$. The probability is q_{usc}/q .

Hence, if the $\mathcal{A}_{II}$ can break the proposed MCLS scheme with a non-negligible advantage ϵ , the CDH assumption can be solved with a non-negligible advantage ϵ'

$$\epsilon' \geq \epsilon \left(\frac{1}{q_{H_5}} \right) \left(\frac{1}{q_{H_1}} \right) \left(1 - \frac{1}{q_r} \right) \left(1 - \frac{1}{q_s} \right) \left(1 - \frac{q_{usc}}{q} \right). \quad (5)$$

In the following, we assess the required computation time τ' while answering queries in the aforementioned simulation game. It turns out that $\tau' = \tau + \mathcal{O}(q_0 + q_p) \cdot \tau_1 + \mathcal{O}(q_{usc}) \cdot \tau_2 + \mathcal{O}(q_1 + q_2 + q_3 + q_4 + q_5 + q_r + q_s)$, where τ_1 is the time to perform a scalar multiplication in G , τ_2 is the time to perform a pairing operation and t is the number of target identities.

B. Public Verifiability

In the **Signcryption** step in section V, the sender computes $h_i = H_5(\{C_1, C_2, \dots, C_t\}, V_i, U)$ and then signs the message

$S_i = (r + h_i)x_s$. The h_i value is a hash of the message and other parameters, and the S_i value is a signature of the sender that can be verified using the sender's public key, pk_s . In the **Unsigncryption** step, the receiver takes CT_i as input and computes $h'_i = H_5(\{C_1, C_2, \dots, C_t\}, V_i, U)$ and checks if $h'_i = h_i$. If true, the receiver verifies if $S_iP = F_i + h_i pk_s$ holds. If true, then the receiver accepts the message as valid and authentic. Otherwise, the receiver rejects the message.

The public verifiability feature allows any third party to perform these steps as well, using only the ciphertext $CT_i = (\{C_1, C_2, \dots, C_t\}, V_i, U, S_i, h_i)$ and the public keys of the sender pk_s and receiver pk_r . Thus, anyone can verify that the signcrypted message is valid and authentic without knowing the private keys of either party. This was not provided in the original Hung *et al.* [1] scheme due to some of the parameters not being publicly available.

VII. PERFORMANCE COMPARISON AND DISCUSSION

We compare the proposed MCLS scheme with the existing single-receiver and multi-receiver encryption and signcryption schemes Table I, which are mainly based on BP [1], [21]–[25]. It demonstrates that the proposed scheme outperforms other signcryption schemes in terms of efficiency for both single receivers and multi-receivers.

TABLE I
COMPARISON BETWEEN MCLS SCHEME WITH THE EXISTING SINGLE AND MULTI-RECEIVER ENCRYPTION AND SIGNCRYPTION SCHEMES BASED ON BILINEAR PAIRINGS.

2 nd Scheme	Single receiver		Multi-receiver	
	Enc/Signcrypt	Dec/Unsigncrypt	Enc/Signcrypt	Dec/Unsigncrypt
[24]	$T_e + T_p + 4T_m$	$T_p + 5T_m$	-	-
[23]	$4T_e$	$2T_e + 2T_p + T_i$	-	-
[22]	-	-	$2nT_e + 2nT_p + (n+2)T_m$	$4T_p + T_m$
[21]	-	-	$(n+1)T_e + nT_m$	$2T_p + 2T_m$
[25]	-	-	$nT_e + 2nT_{pm} + 2nT_m$	$nT_p + nT_m + 3nT_{pm}$
[1]	-	-	$nT_e + nT_p + (n+1)T_m$	$T_p + T_m$
Our scheme	$T_e + T_p + 4T_m$	$T_p + 2T_m$	$nT_e + nT_p + (2n+1)T_m$	$T_p + 2T_m$

Legend: T_p shows the time of executing a bilinear pairing $e: G \times G \rightarrow G$; T_m is the time of executing a scalar multiplication in G ; T_e is the time of executing exponentiation in G_2 or exponentiation in Z_q^* ; T_i is the time of executing a modular inversion; T_{pm} shows the time of executing a point multiplication; and n is the number of receivers.

In contrast to the AMCLE scheme, our approach offers additional security measures, namely public verifiability and authentication. In Table II, we compare the public key settings, exemption of key escrow problem, and public verifiability security requirements with existing signcryption schemes. As compared to sign and encrypt schemes, our approach optimizes the combination of H_2 , H_3 , and V_i operations to achieve a

TABLE II
COMPARISON OF PUBLIC KEY SETTINGS, EXEMPTION OF KEY ESCROW AND PUBLIC VERIFIABILITY REQUIREMENT

Schemes	Public key settings	Exemption of key escrow	Public verifiability
[24]	IDPKC - CLPKC	✓	×
[23]	IDPKC	×	×
[22]	IDPKC - CLPKC	✓	×
[21]	IDPKC - PKC	×	×
[25]	IDPKC	×	×
[1]	CLPKC	✓	×
Our scheme	CLPKC	✓	✓

more efficient integration of sign and encrypt, resulting in enhanced signcryption. Li *et al.* [24] and Niu *et al.* [22] work in ID-Public Key Cryptography (IDPKC)-CLPKC, therefore, the sending entities do not exempt the key escrow and Hung *et al.* [1] work in CLPKC, therefore, it exempts the key escrow. Further, [21], [23], [25] work in an IDPKC environment and do not exempt the key escrow. However, none of these schemes provide public verifiability. Compared to the above schemes, the proposed MCLS scheme works in CLPKC, exempts the key escrow, and achieves public verifiability. Finally, while the proposed scheme significantly modifies Hung *et al.*'s AMCLE scheme into an efficient MLCS scheme, this comes at a relatively small cost and, therefore, can handle large volumes of data.

VIII. CONCLUSION

This paper presents a Multi-receiver Certificateless Signcryption (MCLS) scheme that fulfills authentication requirement, by modifying Hung *et al.*'s encryption [1] scheme. In the proposed scheme, we introduce signcryption, where the message is encrypted and signed with the sender's private key, ensuring the message's reliability and authenticity. The scheme is efficient, with the signcryption cost increasing linearly with the number of receivers, while the required unsigncryption cost of each receiver is constant and independent of the number of receivers. We formally demonstrate the semantic security of the scheme against the EUF-CMA (proposed) attacks in the ROM using the CDH and DBDHI assumptions. We also introduce public verifiability as an additional feature that is achieved simultaneously along with authentication. Finally, we compare the proposed MCLS scheme's performance and functionality to the existing single-receiver and multi-receiver signcryption approaches. In comparison to other existing single-receiver and multi-receiver signcryption techniques, the MCLS scheme is more efficient, while both avoiding the key escrow problem and working in multi-receiver certificateless public key setting.

REFERENCES

- [1] Y. Hung, S. Huang, Y. Tseng, and T. Tsai, "Efficient anonymous multireceiver certificateless encryption," *IEEE Systems J.*, vol. 11, no. 4, pp. 2602–2613, 2017.
- [2] Y. Zheng, "Signcryption or how to achieve cost (signature & encryption); cost (signature)+ cost (encryption)," in *Annu. Int. Cryptol. Conf.*, 1999.
- [3] P. Palmieri, "Hash-based signatures for the internet of things: position paper," in *Proceedings of the 15th ACM International Conference on Computing Frontiers, CF 2018*. ACM, 2018, pp. 332–335.
- [4] J. Malone-Lee, "Identity-based signcryption," *IACR Cryptology ePrint Arch.*, p. 98, 2002.
- [5] L. Chen and J. Malone-Lee, "Improved identity-based signcryption," in *Public Key Cryptography - PKC 2005, 8th International Workshop on Theory and Practice in Public Key Cryptography, Proceedings*, ser. LNCS, vol. 3386. Springer, 2005, pp. 362–379.
- [6] S. S. M. Chow, S. Yiu, L. C. K. Hui, and K. Chow, "Efficient forward and provably secure id-based signcryption scheme with public verifiability and public ciphertext authenticity," in *Information Security and Cryptology - ICISC, 6th International Conference, 2003, Revised Papers*, ser. LNCS, vol. 2971. Springer, pp. 352–369.

- [7] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology - ASIACRYPT 2003, 9th International Conference on the Theory and Application of Cryptology and Information Security, 2003, Proceedings*, ser. LNCS, vol. 2894. Springer, pp. 452–473.
- [8] Y. Yu, B. Yang, X. Huang, and M. Zhang, "Efficient identity-based signcryption scheme for multiple receivers," in *Autonomic and Trusted Computing, 4th International Conference, ATC 2007, Proceedings*, ser. LNCS, vol. 4610. Springer, pp. 13–21.
- [9] S. A. Chaudhry, Nizamuddin, M. Sher, A. Ghani, H. Naqvi, and A. Irshad, "An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography," *Multim. Tools Appl.*, vol. 74, no. 5, pp. 1711–1723, 2015.
- [10] A. Karati, C. Fan, and R. Hsu, "Provably secure and generalized signcryption with public verifiability for secure data transmission between resource-constrained iot devices," *IEEE Internet of Things J.*, vol. 6, no. 6, pp. 10431–10440, 2019.
- [11] S. Hu, R. Zhang, F. Wang, K. Chen, B. Lian, and G. Chen, "A sanitizable signcryption scheme with public verifiability via chameleon hash function," *J. Inf. Secur. Appl.*, vol. 71, p. 103371, 2022.
- [12] M. Barbosa and P. Farshim, "Certificateless signcryption," in *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security, ASIACCS 2008*, M. Abe and V. D. Gligor, Eds. ACM, 2008, pp. 369–372.
- [13] S. S. D. Selvi, S. S. Vivek, D. Shukla, and C. P. Rangan, "Efficient and provably secure certificateless multi-receiver signcryption," in *Provable Security, Second International Conference, ProvSec 2008, Proceedings*, ser. LNCS, vol. 5324. Springer, 2008, pp. 52–67.
- [14] S. S. D. Selvi, S. S. Vivek, and C. P. Rangan, "A note on the certificateless multi-receiver signcryption scheme," *IACR Cryptology ePrint Arch.*, p. 308, 2009.
- [15] S. Miao, F. Zhang, and L. Zhang, "Cryptanalysis of a certificateless multi-receiver signcryption scheme," in *2010 International Conference on Multimedia Information Networking and Security*. IEEE, 2010, pp. 593–597.
- [16] S. H. Islam, M. K. Khan, and A. M. Al-Khouri, "Anonymous and provably secure certificateless multireceiver encryption without bilinear pairing," *Secure Communication Networks*, vol. 8, no. 13, pp. 2214–2231, 2015.
- [17] R. Guo, L. Xu, X. Li, Y. Zhang, and X. Li, "An efficient certificateless ring signcryption scheme with conditional privacy-preserving in vanets," *J. of Systems Architecture*, vol. 129, p. 102633, 2022.
- [18] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology-CRYPTO 2001: 21st Annual International Cryptology Conference, 2001 Proceedings*. Springer, 2001, pp. 213–229.
- [19] A. Joux and K. Nguyen, "Separating decision diffie-hellman from computational diffie-hellman in cryptographic groups," *Journal of cryptography*, vol. 16, pp. 239–247, 2003.
- [20] Y. Chen and L. Chen, "The twin bilinear diffie-hellman inversion problem and applications," in *Information Security and Cryptology - ICISC 2010: 13th International Conference, Revised Selected Papers*. Springer, 2011, pp. 113–132.
- [21] C. Wang, C. Liu, Y. Li, H. Qiao, and L. Chen, "Multi-message and multi-receiver heterogeneous signcryption scheme for ad-hoc networks," *Inf. Secur. J. A Glob. Perspect.*, vol. 26, no. 3, pp. 136–152, 2017.
- [22] S. Niu, L. Niu, X. Yang, C. Wang, and X. Jia, "Heterogeneous hybrid signcryption for multi-message and multi-receiver," *PloS one*, vol. 12, no. 9, p. e0184407, 2017.
- [23] A. Karati, S. H. Islam, G. P. Biswas, M. Z. A. Bhuiyan, P. Vijayakumar, and M. Karuppiah, "Provably secure identity-based signcryption scheme for crowdsourced industrial internet of things environments," *IEEE Internet of Things J.*, vol. 5, no. 4, pp. 2904–2914, 2018.
- [24] S. Li, F. Tao, and T. Shi, "Security analysis and improvement of hybrid signcryption scheme based on heterogeneous system," in *14th International Conference on Computer Science & Education, ICCSE 2019*. IEEE, 2019, pp. 840–845.
- [25] Y. Yang, D. He, P. Vijayakumar, B. B. Gupta, and Q. Xie, "An efficient identity-based aggregate signcryption scheme with blockchain for iot-enabled maritime transportation system," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 3, pp. 1520–1531, 2022.