A Multireceiver Certificateless Signcryption (MCLS) Scheme

Alia Umrani* and Paolo Palmieri

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

Abstract. User authentication and message confidentiality are the basic security requirements of high-end applications such as multicast communication and distributed systems. Several efficient signature-then-encrypt cryptographic schemes have been proposed to offer these security requirements with lower computational cost and communication overhead. However, signature-then-encryption techniques take more computation time than signcryption techniques. *Signcryption* accomplishes both digital signature and public key encryption functions in a single logical step and at a much lower cost than "signature followed by encryption." Several signcryption schemes based on bilinear pairing operations have been proposed. Similarly, anonymous multi-receiver encryption has recently risen in prominence in multicast communication and distributed settings, where the same messages are sent to several receivers but the identity of each receiver should remain private. Anonymous multi-receiver encryption allows a receiver to obtain the plaintext by decrypting the ciphertext using their own private key, while their identity is kept secret to anyone, including other receivers. Among the Certificateless Multi-receiver Encryption (CLMRE) schemes that have been introduced, Hung et al. proposed an efficient Anonymous Multireceiver Certificateless Encryption (AMCLE) scheme ensuring confidentiality and anonymity based on bilinear pairings and is secure against IND-CCA and ANON-CCA.
In this paper, we substantially extend Hung et al.'s multireceiver certificateless encryption scheme to a Multireceiver Certificateless Signcryption (MCLS) scheme that provides confidentiality along with authentication. We show that, as compared to Hung et al.'s encryption scheme, our signcryption scheme requires only three additional multiplication operations for signcryption and unsigncryption phases. Whereas, the signcryption cost is linear with the number of designated receivers while the unsigncryption cost remains constant for each designated receiver. We compare the results with other existing single receiver and multireceiver signcryption schemes in terms of number of operations, exemption of key escrow problem, and public key settings. The scheme proposed in this paper is more efficient for single and multireceiver signcryption schemes while providing exemption from the key escrow problem, and working in certificateless public key settings.

* This publication has emanated from research supported in part by a Grant from Science Foundation Ireland under Grant number 18/CRT/6222

Keywords: Authentication · Confidentiality · Certificateless · Public Key Cryptography · Multireceiver · Signcryption

1 Introduction

A message in digital communication must be secure in terms of confidentiality, authentication, and integrity. Encryption-based schemes are generally used for confidentiality, whereas digital signature-based schemes are used for authentication, integrity, and non-repudiation. As a result, digital signatures and public-key encryption are fundamental requirements for achieving security. However, 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 and the message's integrity. Signcryption is more attractive than the sign-then-encrypt procedure because it requires less computation time and has a lower message expansion rate. For typical security parameters in high level security applications, signcryption costs 50% less in computation time and 85% less in message expansion than signature followed by encryption [19]. Furthermore, Authenticated Encryption (AE) provides security against both Chosen Ciphertext Attack (CCA) and Chosen Plaintext Attack (CPA), and signcryption provides AE and thus CCA and CPA security.

Zheng et al. [18] proposed the first signcryption scheme, which combines digital signature and public key encryption to provide authentication, non-repudiation, and confidentiality at a lower cost than signing and encrypting operations separately. Malone-Lee [10] proposed the first identity-based signature scheme to provide public verifiability and forward security. Following that, several Identity (ID) - based encryption schemes were proposed. Chen et al. [3] and Chow et al. [4] proposed ID-based signcryption schemes respectively, to demonstrate public verifiability, forward security, ciphertext 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. proposed the concept of certificateless Public Key Cryptography (PKC) [1]. 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. [17] proposed the first multireceiver signcryption scheme based on ID-based PKC in which the message is encrypted for n number of designated receivers. The security is demonstrated through the Random Oracle Model (ROM) and the Computational Diffie-Hellman (CDH) assumption. Later, Hung et al. [6] proposed an efficient anonymous multireceiver certificateless encryption scheme based on bilinear pairing. The scheme proves Indistinguishability

against Chosen Ciphertext Attack (IND-CCA) and Anonymity against Chosen Ciphertext Attack (ANON-CCA). The encryption cost in this scheme is linear with the number of designated receivers, while the decryption cost is constant for each designated receiver.
In this paper, we extend the functionalities of Hung et al.'s encryption scheme into a Multireceiver Certificateless Signcryption (MCLS) scheme. Hung et al.'s encryption scheme demonstrate security against IND-CCA and ANON-CCA to prove confidentiality and anonymity whereas, we demonstrate security against IND-MCLS-CCA and EUF-MCLS-CMA for t designated receivers that proves confidentiality and authentication. Furthermore, as signcryption focuses on confidentiality and authentication, we omit the ANON-CCA proof, which remains the same for encryption scheme as in Hung et al. [6]. This signcryption scheme requires three additional multiplication operations for signcryption and unsigncryption, with the cost of signcryption being linear with the number of designated receivers and the cost of unsigncryption remaining constant for each designated receiver. In comparison to the other existing signcryption techniques listed at the end of this paper, the MCLS scheme avoids the key escrow problem and works in a multireceiver certificateless public key setting. Specifically, the main contributions are as follows.

- We design a Multireceiver Certificateless Signcryption (MCLS) scheme, that significantly extends the functionalities of the existing Efficient Anonymous Multireceiver Certificateless Encryption (AMCLE) scheme [6].
- We provide a detailed 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 Existential Unforgeability security against a Chosen Message Attack (EUF-MCLS-CMA).
- We evaluate the performance of the proposed MCLS scheme and present a comparison with other existing signcryption schemes.

The reminder of this paper is described as follows. Section 2 reviews the research related to the scheme. Section 3 introduces the fundamentals of bilinear pairings as well as mathematical assumptions. Section 4 describes the framework and security model in the MCLS scheme for two types of adversaries. Section 5 introduces the MCLS scheme. In Section 6, we perform a security analysis of the scheme under the assumption of hardness, and in Section 7, we compare it to existing schemes. Section 8 contains the conclusion.

2 Related Work

Barbosa and Farshim [2] proposed the first certificateless based signcryption scheme that provides confidentiality and authentication while protecting against Type-I and Type-II adversaries and is secure against insider attacks in a ROM. A Type-I adversary is a malicious user who can replace the public key of any

user but cannot access the master key of Trusted Authority (TA). A Type-II adversary is a malicious TA who can access the master key but cannot replace the public key of a user. The scheme is based on the bilinear pairing assumption. To prove the scheme's security, it employs Gap-Bilinear Diffie Hellman (G-BDH), Decisional Bilinear Diffie-Hellman (DBDH), and Computational Bilinear Diffie-Hellman (CBDH) assumptions and shown to be IND-CPA and sUF-CMA secure. Selvi et al. proposed an efficient and provably secure certificateless multireceiver signcryption scheme [14]. The scheme is based on the Strong (DH) Problem, Collusion Attack Algorithm with K-Traitors (k-CAA), Modified BDHI for K-Values (k-mBDHIP), and Gap-BDH Problem. The scheme employs bilinear pairing operations and compares the efficiency of signcryption and unsigncryption operations to that of identity-based schemes. The scheme proposed by Selvi et al. [14] is not secure against a Type-1 adversary and is improved as enhanced certificateless multireceiver signcryption scheme to prevent against Type-1 adversary [13].

However, Miao et al. proposed a cryptanalysis of a certificateless multireceiver signcryption scheme [11], in which the authors demonstrated that the scheme proposed in [13] is still insecure against a Type-I adversary and presented an attack on Selvi'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. [7] proposed an anonymous and provably secure certificateless multireceiver encryption (AMCLE) scheme which uses an Elliptic Curve Cryptography based technique under the CDH assumption. In this scheme, the encryption cost is quadric with the number of receivers, whereas the decryption cost is linear with the number of receivers, however, its security proof has a drawback that the simulator failed to successfully generate the challenge ciphertext and thus failed in the simulation. To overcome the key escrow problem and provide more efficiency, Hung et al. [6] proposed an Efficient Anonymous Multireceiver Certificateless Encryption (ACMLE) scheme that provides confidentiality and sender's anonymity. This scheme uses bilinear pairing under the BDDH, Gap-BDH, and CDH assumptions. To prove confidentiality, the scheme defines the IND-CLME-CCA and to achieve anonymity, the authors present ANON-CLME-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. [5] proposed an efficient certificateless ring signcryption scheme with conditional privacy preservation. The scheme employs a certificateless cryptographic technique and compares the results to identity-based cryptographic signature schemes.

Hung et al's. scheme provides efficient and anonymous multireceiver certificateless encryption based on bilinear pairing. In this paper, we substantially expand Hung et al.'s scheme and propose an efficient multireceiver certificateless signcryption that not only provides confidentiality but also authentication and non-repudiation.

3 Preliminaries and Assumptions

Here, we briefly review the basic definitions and properties of bilinear pairings and the related security assumptions on which the scheme is based. Let G_1 and G_2 be two cyclic additive groups and multiplicative groups respectively, over a prime order q where q is a large prime number. A pairing is a map: $\hat{e} : G_1 \times G_1 \rightarrow G_2$ which satisfies the bilinearity, computability, and non-degeneracy properties as follows.

- Bilinearity: For any $P, Q \in G_1$, $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ where $a, b \in Z_q^*$.
- Computable: For $P, Q \in G_1$, $\hat{e}(P, Q)$ can be efficiently computed.
- Non-degenerate: $\hat{e}(P, P) \neq 1$, for some $P \in G_1$.

Definition 1. *Decisional Bilinear Diffie-Hellman (DBDH) Assumption: On input $P, aP, bP, cP \in G_1$ and $R \in G_2$, the DBDH assumption holds if no PPT adversary A with non-negligible advantage can decide whether $R = \hat{e}(P, P)^{abc}$ or not. The advantage of A is defined as*

$$\begin{aligned} Adv^{DBDH} = Pr\left[A(P, aP, bP, cP, \hat{e}(P, P)^{abc}) = 1\right] - \\ Pr\left[A(P, aP, bP, cP, R) = 1\right] \ . \end{aligned} \tag{1}$$

Definition 2. *Computational Diffie-Hellman (CDH) Assumption: On input $P, a P, bP \in G_1$, the CDH assumption holds if no PPT adversary A with non-negligible advantage can compute abP. The advantage of A is defined as*

$$Adv^{CDH} = Pr\left[A(P, aP, bP) = abP\right] \ . \tag{2}$$

Definition 3. *GAP-Bilinear Diffie-Hellman (GBDH) Assumption: On input $P, aP, bP, cP \in G_1$, the Gap-BDH assumption holds if no PPT adversary A with non-negligible advantage can compute $\hat{e}(P, P)^{abc}$ with the help of the DBDH oracle, where $DBDH(P, aP, bP, cP, R) = 1$ if $\hat{e}(P, P)^{abc} = R$ and 0 otherwise. The advantage of A is defined as*

$$Adv^{Gap-BDH} = Pr\left[A(P, aP, bP, cP) = \hat{e}(P, P)^{abc}\right] \ . \tag{3}$$

Definition 4. *Decisional Bilinear Diffie-Hellman Inversion (DBDHI) Problem: On input $P, aP, bP, cP \in G_1$ and $R \in G_2$, the DBDHI assumption holds if no PPT adversary A with non-negligible advantage can decide whether $R = \hat{e}(P, P)^{ab^{-1}c}$ or not. The advantage of A is defined as*

$$\begin{aligned} Adv^{DBDHI} = Pr\left[A(P, aP, bP, cP, \hat{e}(P, P)^{ab^{-1}c}) = 1\right] - \\ Pr\left[A(P, aP, bP, cP, R) = 1\right] \ . \end{aligned} \tag{4}$$

4 Framework and Security Model

4.1 Framework

This paper adopts the certificateless signcryption scheme framework from AMCLE [6]. The AMCLE scheme allows a sender to produce the ciphertext of a

message for t designated receivers. The scheme has two roles; KGC and n number of users (a sender and t receivers) where $t \leq n$.

The scheme consists of seven polynomial-time algorithms.

Setup (1^λ). On input security parameter 1^λ, the KGC runs this algorithm to generate a master secret key s and public parameters PP. The public parameters PP are provided as input to other algorithms.

Partial private key (s, ID). On input master secret key s, public parameters PP, and user's identity $ID \in \{0,1\}^*$, the KGC runs this algorithm to generate a partial private key DID.

Set secret value (ID). On input user identity ID and public parameters PP, the user runs this algorithm and generates a user secret value x_{id}.

Set private key (DID, x_{id}). Taking partial private key DID and the secret value x_{id} as input, the user runs this algorithm to generate a full private key SID for the identity ID.

Set public key (x_{id}). Taking the secret value x_{id} as input, the user with identity ID runs this algorithm to generate a user public key PID.

Signcryption $(m, SID, ((ID_1, PID_1), ..., (ID_t, PID_t)))$. On input public parameters PP, a plaintext message m, sender's private key SID, and receiver's identity and public key $((ID_1, PID_1), ..., (ID_t, PID_t))$ where $t \leq n$, a sender with identity ID runs a probabilistic algorithm to generate a ciphertext CT.

Unsigncryption (CT, ID, SID, PID). On input public parameters PP, ciphertext CT, sender's identity ID, designated receiver's private key SID, and sender's public key PID, the receiver runs deterministic algorithm to generate a plaintext message m or "reject".

4.2 Security Model

For confidentiality, we define the Indistinguishability of Multireceiver Certificateless Signcryption against a Chosen Ciphertext Attack (IND-MCLS-CCA) from Hung et al.'s scheme. For authentication, we propose and define Existential Unforgeability against a Chosen Message Attack (EUF-MCLS-CMA). We consider two types of adversaries; Type-I and Type-II. A Type-I adversary is considered a common user who has no knowledge of KGC's master secret key but can replace the public key of any identity with a value of his/her own choice. A Type-II adversary is considered an insider adversary who has access to the master secret key of KGC but cannot replace the public key of a legitimate user. A Type-II adversary is also known as a malicious KGC. In Definition 5 (Game-I), we define the IND-MCLS-CCA-I for Type-I adversary and the IND-MCLS-CCA-II for Type-II adversary, and in Definition 6 (Game-II), we define the EUF-MCLS-CMA-I for Type-I adversary and the EUF-MCLS-CMA-II for Type-II adversary.

Definition 5. *The Indistinguishability of Multireceiver Certificateless Signcryption against Chosen Ciphertext Attack (IND-MCLS-CCA) requires that there exists no PPT Type-I and Type-II adversaries A which could distinguish ciphertexts. Therefore, the security game that captures confidentiality is based on the*

ciphertext indistinguishability. The advantage of A is defined as the probability that A wins the game.

Game-I (IND-MCLS-CCA-I, IND-MCLS-CCA-II): This Game is interaction between the challenger B and Type-I/Type-II adversary as follows.
Setup. The challenger B generates the master secret key s and public parameters PP. Then B gives PP to adversary A.
Phase-1. Without loss of generality in a certificateless (CL) setting, the Adversary A outputs t target identities denoted by ID_i^* for $i \in \{1, ..., t\}$ where $t \leq n$. The Adversary A further asks $q_i\{i = 0, ..., 6\}$ 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 Type-I adversary A has following constraints.

1. Adversary cannot access master secret key s.
2. The adversary is not allowed to ask a partial private key query for any of the challenger identities.

The Type-II adversary A has the following constraints.

1. Adversary cannot make public key replace query for the challenge identity.
2. Adversary is not allowed to make secret value extract queries.
3. If the public key replace query has been done for ID_i^*, then the secret value extract query for ID_i^* is not allowed.

Challenge. The adversary A outputs a target plaintext pair $\{m_0, m_1\}$. The challenger B picks $\beta \in \{0, 1\}$ at random and sets $CT^* = E(PP, ((ID_1, PID_1), ..., (ID_t, PID_t)), m_\beta)$ challenger sends CT^* to adversary A.
Phase-2. The adversary A can make further queries except that the target ciphertext CT^* is not allowed to appear in the unsigncryption queries.
Guess. Finally, A responds with its guess $\beta \in \{0, 1\}^*$. If $\beta = \beta'$, A wins the game. The advantage of Type-I adversary A is defined as

$$Adv_{\mathcal{A}}^{IND-MCLS-CCA-I} = \mid Pr\left[\beta = \beta'\right] - 1/2 \mid \quad . \tag{5}$$

The advantage of Type-II adversary A is defined as

$$Adv_{\mathcal{A}}^{IND-MCLS-CCA-II} = \mid Pr\left[\beta = \beta'\right] - 1/2 \mid \quad . \tag{6}$$

Definition 6. *For Existential Unforgeability Against Chosen Message Attack (EUF-MCLS-CMA), we define Game-II that is played between a challenger B and an adversary A. A certificateless multireceiver signcryption scheme is Type-I and Type-II EUF-CMA if every probabilistic PPT adversary A has a negligible advantage in winning Game-II.*

Game-II (EUF-MCLS-CMA-I, EUF-MCLS-CMA-II): This Game is interaction between the challenger B and Type-I/Type-II adversary as follows.

Setup. The challenger B generates the master secret key s and public parameters PP. Then B gives PP to adversary A.
Phase-1. The adversary first outputs a target identity denoted by ID_A^*. The Adversary A further asks $q_i\{i = 0, ..., 6\}$ 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 Type-I adversary A has the following constraints.

1. Adversary cannot access master secret key s.
2. The adversary is not allowed to ask a partial private key query for any of the challenger identities.

The Type-II adversary A has the following constraints.

1. Adversary cannot make public key replace query for the challenge identity.
2. Adversary is not allowed to make secret value extract queries.
3. If the public key replace query has been done for ID_A^*, then the secret value extract query for ID_A^* is not allowed.

Forgery. Adversary A outputs the forged signature under a target identity ID_A^*. A wins if unsigncryption does not return $\perp$.

5 Multireceiver Certificateless Signcryption Scheme

In this section, we define the MCLS scheme according to the framework defined in section 4.1. The main scheme is shown in Fig. 1.
Setup: Taking the security parameter λ as input, KGC initializes the system. It generates two large cyclic groups G_1 and G_2 of a large prime order $q \geq 2^\lambda$, a bilinear pairing $\hat{e} : G_1 \times G_1 \rightarrow G_2$, and selects a generator P of G_1. KGC defines seven hash functions $H_0 : \{0,1\}^* \rightarrow G_1$, $H_1, H_2 : G_2 \times G_1 \rightarrow \{0,1\}^w$, $H_3, H_4, H_5 : \{0,1\}^w \rightarrow \{0,1\}^w$, $H_6 : \{0,1\}^* \times G_1 \rightarrow Z_q^*$ for a positive integer w. KGC then chooses a master secret key $s \in Z_q^*$ at random, calculates system public key $P_{pub} = s.P$, chooses a symmetric encryption E_{sk} and a decryption D_{sk} function where sk is a symmetric key. KGC then publishes public parameters $PP = (G_1, G_2, e, P, q, P_{pub}, H_0, H_1, H_2, H_3, H_4, H_5, H_6, E_{sk}, D_{sk})$ and keeps the master secret key s.
Partial Private key: Taking the user's identity $ID \in \{0,1\}^*$ as input, the KGC computes $QID = H_0(ID)$ and the associated partial private key $DID = s.QID$. The KGC sends DID to the user via a secure channel.
Set Secret Value: User with identity $ID \in \{0,1\}^*$ selects a positive integer $x_{id} \in Z_q^*$ as a secret value.
Set Public Key: The user with $ID \in \{0,1\}^*$ takes x_{id} as input and generates the user public key $PID = x_{id}.P$.
Set Private Key: The user with $ID \in \{0,1\}^*$ takes the partial private key DID and secret value x_{id} as input and generates the full private key $SID = (DID, x_{id})$.
Signcryption: Suppose, a sender generates a ciphertext to transfer a message m

to t designated receivers with public keys $((ID_1, PID_1), ..., (ID_t, PID_t))$ where $t \leq n$. The sender runs the following steps.

- Chooses a value $r \in Z_q^*$ randomly and computes $U = r.P$, $F_i = r.PID_i$ for $i = 1, ..., t$, $h_i = H_1(X_a, m)$ where $X_a = F_i \cdot x_{id}$.
- Computes $K_i = \hat{e}(P_{pub}, QID_i)^r$, $QID_i = H_0(ID_i)$ and $T_i = H_2(K_i, F_i)$ for $i = 1, ..., t$.
- Picks an ephemeral value $\sigma \in \{0,1\}^w$ randomly and computes C_i for all $i = 1, ..., t$ $C_i = H_3(T_i) \parallel H_4(T_i) + \sigma$.
- Use the ephemeral value σ to compute symmetric key $sk = H_5(\sigma)$ and generate $V = Esk(m)$.
- Signs the message m as $Q = (r + h_i)x_{id}$ and sets $Q = \{Q_1, ..., Q_t\}$.
- To ensure data integrity, performs a hash operation $\bigwedge = H_6(m, \langle C_1, ..., C_t\rangle, Q, V, U, \sigma)$.
- Set the ciphertext $CT = (\langle C_1, ..., C_t\rangle, Q, V, U, \bigwedge)$.

Unsigncryption: The designated receiver with identity ID takes the ciphertext $CT = (\langle C_1, ..., C_t\rangle, Q, V, U, \bigwedge)$ as input, full private key $SID = (DID, x_{id})$ and runs the following steps.

- Computes $K = \hat{e}(U, DID)$.
- Computes $F = x_{id}.U$, $T = H_2(K, F)$ and $H_3(T)$.
- Uses $H_3(T)$ to find associated C_i for $i = 1, ..., t$ by the relation $C_i = H_3(T) \parallel W$ where $W = H_4(T) + \sigma$.
- Computes $\sigma' = W + H_4(T)$.
- Sets symmetric key $sk' = H_5(\sigma')$ and computes $m' = Dsk(V)$ and $\bigwedge' = H_6(m', \sigma', \langle C_1, ..., C_t\rangle, Q, V, U)$.
- If $\bigwedge' = \bigwedge$, then checks if $Q.P = F + h_i.PID$, hold or not. If it holds, receiver gets the message m, else returns 'reject'.

Correctness Analysis

1. $K = \hat{e}(P_{pub}, QID)^r = \hat{e}(s.P, QID)^r = \hat{e}(r.P, s.QID) = \hat{e}(U, D\ ID)$.
2. $F = r.PID = r.x_{id}.P = x_{id}.U$.
3. $Q.P = ((r+h_i)x_{id}).P = r.x_{id}.P + h_i.x_{id}.P = r.PID + h_i.PID = F + h_i.PID$

6 Security Analysis

Here, we illustrate that the MCLS scheme fulfills both confidentiality and unforgeability. For confidentiality, Theorems 1 and 2 below demonstrate that the scheme is secure against IND-MCLS-CCA Type-I and Type-II adversaries in the aforementioned Game-I in Definition 5. For unforgeability, Theorems 3 and 4 below demonstrate that the scheme is secure against EUF-MCLS-CMA Type-I and Type-II adversaries in the aforementioned Game-II in Definition 6.

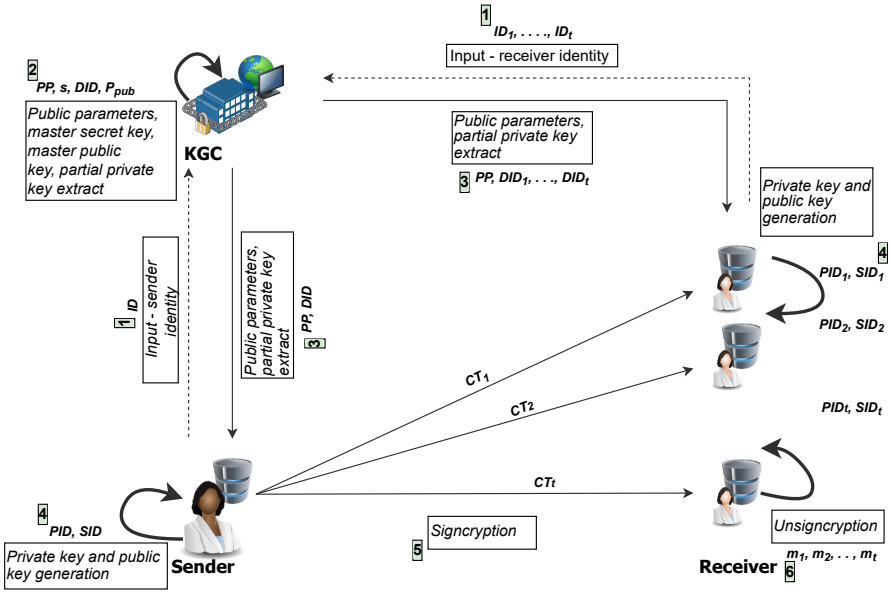

Fig. 1. The Multireceiver Certificateless Signcryption (MCLS) scheme

Theorem 1. *The MCLS scheme is provably secure against an IND-MCLS-CCA Type-I adversary. Assume that an IND-MCLS-CCA Type-I adversary A with a non-negligible advantage ϵ can break the MCLS scheme with running time τ, in ROM after $q_i\{i = 0, ..., 6\}$ 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. Then, there exists an algorithm that can solve the Gap-BDH problem with a non-negligible advantage ϵ' with running time τ' which are defined at the end of the Proof.*

Proof. To solve the mathematical difficult problem Gap-BDH, the challenger B is given an instance (P, aP, bP, cP) where P, aP, $bP, cP \in G_1$ with unknown $a, b, c \in Z_q^*$. Let $R = \hat{e}(P, P)^{abc}$ be the solution of the G-BDH problem. The challenger in Game-I (Definition 5) who would like to compute R by interacting with adversary A as follows.
Setup: B runs the initialized algorithm and generates public parameters $PP = \{G_1, G_2, \hat{e}, P, q, P_{pub}, H_0, H_1, H_2, H_3, H_4, H_5, H_6, E_{sk}, D_{sk}\}$ with $P_{pub} = aP$. The challenger B sends PP to adversary A.
Phase-1: Without loss of generality in a CL setting, the adversary first selects t target identities of receivers denoted by ID_i^* for $i \in \{1, ..., t\}$ where $t \leq n$ (in IND-MCLS-CCA-I, the target identity is the receiver's identity denoted by ID_i^* for $i \in \{1, ..., t\}$). The adversary A makes number of queries including $q_i\{i = 0, ..., 6\}$ hash queries, q_p query, q_r query, q_e query, q_s query, q_{sc} query, and

q_{usc} query. The challenger B sets empty lists PK^{list} to record public key values and maintains seven empty lists $(L_0, .., L_6)$ to record the responses of q_i queries. The challenger responds to adversary's queries by the following ways.
H_0 *query.* If there exists (ID, u, QID) in L_0, B returns QID to A. Otherwise, B performs the following steps.
Picks a value $u \in Z_q^*$ at random. If $ID = ID_i^*$ for some $i \in \{1, ..., t\}$, sets $QID = u.bP$, otherwise sets $QID = u.P$. Stores (ID, u, QID) in L_0 and responds with QID.
H_1 *query*: If there exists a record (m, X_a, h) in L_1, B returns h to A. Otherwise, B chooses a random string $h \in \{0,1\}^w$ and returns to A. It stores (m, X_a, h) in L_1.
H_2 *query*: If there exists (K, F, T) in the list L_2, B returns T to A. Otherwise, B picks a string $T \in \{0,1\}^w$ at random, stores (K, F, T) in L_2, and responds with T.
H_3 *query*: If there exists (T, x) in the list L_3, B returns x to A. Otherwise, B picks a string $x \in \{0,1\}^w$ at random, stores (T, x) in L_3, and responds with x.
H_4 *query*: If there exists (T, y) in the list L_4, B returns y to A. Otherwise, B picks a random string $y \in \{0,1\}^w$, stores (T, y) in L_4, and B returns y to A.
H_5 *query*: If there exists (k, w) in the list L_5, B returns w to A. Otherwise, B randomly picks a string $w \in \{0,1\}^w$, stores (k, w) in L_5, and responds with w.
H_6 *query*: If there exists $(m, \sigma, \langle C_1, ..., C_t \rangle, U, V, Q, \bigwedge)$ in the list L_6, B returns $\bigwedge$ to A. Otherwise, B picks a random value $\bigwedge \in Z_q^*$, stores the tuple $(m, \sigma, \langle C_1, ..., C_t \rangle, U, V, Q, \bigwedge)$ in L_6, and then returns $\bigwedge$ to A.
Public key retrieve query (q_p): If there exists (ID, PID, x_{id}) in PK^{list}, B returns PID to A. Otherwise, B randomly picks $x_{id} \in Z_q^*$, sets $PID = x_{id}.P$ and stores (ID, PID, x_{id}) in PK^{list} and provide PID to A.
Public key replace query (q_r): B replaces the associated tuple (ID, PID, x_{id}) in PK^{list} with the new tuple $(ID, PID', \perp)$. Since, the secret value x_{id} for PID' is unknown, B will set $\perp$ as x_{id}.
Partial private key query (q_e): If $ID = ID_i^*$, for some $i \in \{1, ..., t\}$, B returns $\perp$ because, ID_i^* is a target identity and a Type-I adversary is not allowed to ask for a partial private key query for the target identity. Otherwise, if (ID, u, QID) exists in L_0, B computes and returns $DID = u.P_{pub}$ to A. Otherwise, B randomly picks a value $u \in Z_q^*$, sets $QID = u.P$, and $DID = u.P_{pub}$, and stores (ID, u, QID) in L_0. B returns DID to A.
Secret value extract query (q_s): If (ID, PID, x_{id}) exists in PK^{list}, B returns x_{id} to the adversary A. Otherwise, B randomly picks $x_{id} \in Z_q^*$, sets $PID = x_{id}.P$, stores (ID, PID, x_{id}) in PK^{list} and returns x_{id} to A.
Signcryption query (q_{sc}): When B receives a signcrypt query with a message m, sender ID, and receiver's ID_i for $i \in \{1, ..., t\}$ and public key in a tuple $((ID_1, PID_1), ..., (ID_t, PID_t))$. B checks whether $ID = ID_i^*$ or not. If $ID \neq ID_i^*$, B performs normal signcryption as this scheme. Otherwise, B obtains the tuple (DID, x_{id}, PID) via q_p, q_e queries, and q_s and generates a ciphertext CT as follows.

- Pick a value $r \in Z_q^*$ randomly and compute $U = r.P$.

– Compute $F_i = r.PID_i$, $h_i = H_1(X_a, m)$, $X_a = F_i.x_{id}$ and add in L_1.
– Computes $K_i = \hat{e}(U, DID)$, $T_i = H_2(K_i, F_i)$ and adds in L_2.
– Picks an ephemeral value $\sigma \in \{0,1\}^w$ at random and computes $C_i = H_3(T_i) \parallel H_4(T_i) + \sigma$ and adds in L_3 and L_4.
– Use σ to compute symmetric key $sk = H_5(\sigma)$ and generate $V = E_{sk}(m)$.
– Compute $Q = (r + h_i)x_{id}$ and compute $\bigwedge = H_6(m, \sigma, \langle C_1, ..., C_t\rangle, Q, V, U)$ and update L_6.
– Set $C_T = (\langle C_1, ..., C_t\rangle, V, U, Q, \bigwedge)$.

Unsigncryption query (q_{usc}): If $ID \neq ID_i^*$ for $i \in \{1, ..., t\}$, B can obtain its full private key (DID, x_{id}) via the q_e and q_s queries, unsigncrypt CT and return m to A. Otherwise, B perform the following procedure.

– If $(m, \sigma, \langle C_1, ..., C_t\rangle, Q, V, U, \bigwedge)$ is not in L_6, B terminates. Otherwise, B obtains (m, σ) for possible utilization further in the following.
– B obtains QID from L_0 by issuing H_0 query.

For $k = 1, ..., t$, B runs the following steps.

– Pick the leftmost w bits of C_k and denote it by x_k.
– Pick the rightmost w bits of C_k, denote it by w_k.
– Compute $y_k = w_k + \sigma$.
– Find a common T_k such that both the tuples (T_k, x_k) and (T_k, y_k) lie in the L_3 and L_4, respectively. If no such T_k exists, return 'abort'.
– Search (K_k, F_k, T_k) associated with T_k from L_2. If not found, return 'abort'.
– Compute the value of h from L_1.
– Record the output of the query DBDH $(P, QID, P_{pub}, U, K_k)$ to the DBDH oracle.
– If DBDH $(P, PID, P_{pub}, U, K_k) = 1$, for some k, B compute $sk' = H_4(\sigma)$ and $m' = D'_{sk}(V)$.
– If $m' = m$, B returns m to the adversary A. In all other cases, B terminates.

Challenge: A gives a target plaintext pair (m_0, m_1) to B. B randomly chooses $\beta \in \{0,1\}$ and runs the following steps.

– Set $U^* = cP$.
– Choose $r^* \in Z_q^*$.
– $F_i^* = r^*.PID_i$, $X_a^* = F_i^*.x_{id}$, $h_i^* = H_1(X_a^*, m_\beta)$.
– Pick a string $\sigma \in \{0,1\}^w$ at random.
– For $i = 1, ..., t$, randomly pick $x_i^* \in \{0,1\}^w$ and $y_i^* \in \{0,1\}^w$, and compute $C_i^* = x_i^* \parallel (y_i^* \oplus \sigma^*)$.
– Compute $sk = H_4(\sigma^*)$, $V^* = E_{sk}(m_\beta)$, compute $Q^* = (r^* + h_i^*)x_{id}$ and set $\bigwedge^* = (\langle C_1^*, ..., C_t^*\rangle, V^*, U^*, Q^*)$.
– Finally, B returns $CT^* = (\langle C_1^*, ..., C_t^*\rangle, V^*, U^*, \bigwedge^*, Q^*)$.

Phase-2: The adversary A may ask further queries as in Phase-2 but CT^* is not allowed to appear in the unsigncryption query.
Guess: The adversary A responds with its guess $\beta' \in \{0,1\}$. If $\beta = \beta'$, A wins

the game.
The challenger will win the Game by obtaining $R = \hat{e}(P, P)^{abc}$ which is solution to the DBDH problem. The challenger solves the DBDH problem by obtaining the list L_2 for (K, F). Since, $QID_i = u_i.bP$, $P_{pub} = aP$, and $U^* = cP$, B can obtain $\hat{e}(P, P)^{abc}$ by evaluating $K_i^{ui^{-1}}$. Next, we evaluate the advantage of challenger B winning the Game-I (IND-MCLS-CCA-I) by calculating the probability of occurrence of the following events.

1. In the unsigncryption query if $(\langle C_1, ..., C_t \rangle, V, U, \bigwedge Q)$ cannot be found in L_6, B returns 'failure' and terminates. The probability is $1/qH_6$.
2. In the partial private key query, the game terminates if $ID \neq ID_i^*$, for some $i \in \{1, ..., t\}$. The probability is $1/q_e$.
3. In the unsigncryption query, the games aborts due to invalid message $m' \neq m$. The probability is q_{uns}/q.

Further, the challenger B will obtain the list L_2 for the some (K, F) with the probability $1/qH_2$. Hence, if an IND-CLMS-CCA-I adversary A can break MCLS scheme with a non-negligible advantage ϵ, then the Gap-BDH problem can be solved with a non-negligible advantage ϵ'

$$\epsilon' \geq \epsilon \left(\frac{1}{qH_6}\right)\left(\frac{1}{qH_2}\right)\left(1 - \frac{1}{q_e}\right)\left(1 - \frac{q_{uns}}{q}\right) \tag{7}$$

τ' is the required computation time while answering the queries in the aforementioned simulation Game-I. It turns out that $\tau' = \tau + O(q_o + q_p + q_e)\tau_1 + O(q_1 + q_2 + q_3 + q_4 + q_5 + q_6 + q_r + q_s + q_{usc})$ where τ_1 is the time to perform a scalar multiplication in G_1 and t is the number of target identities.

Theorem 2. *The scheme is provably secure against an IND-MCLS-CCA Type-II adversary with a non-negligible advantage ϵ can break the MCLS scheme with running time τ in ROM after $q_i\{i = 0, ..., 6\}$ hash queries including q_p queries to public key retrieve query, q_r public key replace query, q_s secret value extract query, and q_{usc} unsigncryption query respectively. Then, there is an algorithm B that can solve the CDH problem with a non-negligible advantage ϵ' with running time τ' defined as the end of the Proof.*

Proof. Assume that an algorithm B is given a random instance (P, aP, bP) of the CDH problem, where $P, aP, bP \in G_1$, within unknown $a, b \in Z_q^*$. Let $J = abP$ be the solution of the CDH problem. The algorithm B plays the challenger of Game-I (Definition 5) who would like to compute J by interacting with the adversary A as follows.
Setup: B runs the initialized algorithm and generates public parameters $PP = \{G_1, G_2, \hat{e}, P, q, P_{pub}, H_0, H_1, H_2, H_3, H_4, H_5, H_6, E_{sk}, D_{sk}\}$ with $P_{pub} = aP$. The challenger B sends PP to adversary A.
Phase-1: Without loss of generality in CL setting, the adversary first selects t target identities of denoted by ID_i^* for $i \in \{1, ..., t\}$ where $t \leq n$ (in IND-MCLS-CCA-II, the target identity is the receiver's identity denoted by ID_i^* for

$i \in \{1, ..., t\}$). The adversary A makes number of queries including a H_0 query, public key replace query, secret value extract query, and unsigncryption query. The challenger B sets empty lists PK^{list} to record public key values. Challenger B responds to all the queries as follows.
H_0 *query*: If there exists (ID, u, QID) in L_0, B returns QID to A. Otherwise, B picks a value $u \in Z_q^*$ randomly and computes $QID = uP$. Then, B Stores (ID, u, QID) in L_0 and responds with QID.
Public key retrieve query (q_p): If there exists (ID, PID, x_{id}) in the PK^{list}, B returns PID to A. Otherwise, B performs the following step.

- Picks a value $x_{id} \in Z_q^*$ at random.
- If $ID = ID_i^*$ for some $i \in \{1, .., t\}$, set $PID = x_{id}.a.P$ Otherwise, set $PID = x_{id}.P$, store (ID, PID, x_{id}) in the PK^{list} and return PID to A.

Public key replace query (q_r): If $ID = ID_i^*$ for some $i \in \{1, ..., t\}$, B reports failure and terminates because, ID_i^* is a target identity and Type-II adversary is not allowed to ask public key replace query for the target identity. Otherwise, B replaces the associated tuple (ID, PID, x_{id}) in the PK^{list} with a new tuple $(ID, PID', \perp)$.
Secret value extract query (q_s): If $ID = ID_i^*$ for some $i \in \{1, ..., t\}$, B returns $\perp$ because, in this case, ID_i^* is a target identity. If (ID, PID, x_{id}) exists in the PK^{list}, B returns x_{id} to the adversary A. Otherwise, B randomly picks $x_{id} \in Z_q^*$ sets $PID = x_{id}.P$, stores (ID, PID, x_{id}) in PK^{list}, and returns x_{id} to A.
Unsigncryption query (q_{usc}): If $ID \neq ID_i^*$, B can obtain its full private key (DID, x_{id}) via the q_e and q_s queries, unsigncrypt ciphertext and return m to A. Otherwise, B perform the following procedure.
If $(m, \sigma, \langle C_1, ..., C_t \rangle, Q, V, U, \bigwedge)$ is not in L_6, B terminates. Otherwise, B obtains (m, σ) for possible utilization further in the following.

- B obtains QID associated with ID from the list PK^{list} or by issuing public key retrieve query.

For $k = 1, ..., t$, B runs the following steps.

- Pick the leftmost w bits of C_k and denote it by x_k.
- Pick the rightmost w bits of C_k, denote it by w_k.
- Compute $y_k = w_k + \sigma$.
- Find a common T_k such that both the tuples (T_k, x_k) and (T_k, y_k) lie in the L_3 and L_4, respectively. If no such T_k exists, return 'abort'.
- Search the tuple (K_k, F_k, T_k) associate with T_k from L_2. If not found, return 'abort'.
- If $\hat{e}(P, F_k) = \hat{e}(U, PID)$, record the value k.
- If $\hat{e}(P, F_k) = \hat{e}(U, PID)$ for some $k \in \{1, ..., t\}$, B computes $sk' = H_4(\sigma)$ and $m' = D_{sk'}(V)$. If $m' = m$, B returns m to the adversary A. In all the other cases, B terminates.

Challenge: A gives a target plaintext pair (m_0, m_1) to B. Then, B randomly chooses $\beta \in \{0, 1\}$ and runs the following steps.

– Set $U^* = bP$.
– Choose $r^* \in Z_q^*$.
– $F_i^* = r^*.PID_i$, $X_a^* = F_i^*.x_{id}$, $h_i^* = H_1(X_a^*, m_\beta)$.
– For $i = 1, ..., t$, randomly pick $x_i^* \in \{0,1\}^w$ and $y_i^* \in \{0,1\}^w$, and compute $C_i^* = x_i^* \parallel (y_i^* \oplus \sigma^*)$.
– Computes $sk = H_4(\sigma^*)$, $V^* = E_{sk}(m_\beta)$, compute $Q^* = (r^* + h_i^*)x_{id}$, and set $\bigwedge^* = (\langle C_1^*, ..., C_t^* \rangle, V^*, U^*, Q^*)$.
– Finally B returns $CT^* = (\langle C_1^*, ..., C_t^* \rangle, V^*, U^*, \bigwedge^*, Q^*)$.

Phase-2: An adversary A may issue further queries as in Phase-2 with the restriction that CT^* is not allowed to appear in the unsigncryption query.
Guess: An adversary A responds with its guess $\beta' \in \{0,1\}$. If $\beta = \beta'$, A wins the game.
The challenger will win the Game by obtaining $J = abP$ which is the solution to the CDH problem. The challenger B solves the CDH problem by obtaining the list L_2 with some (K, F) such that $\hat{e}(P, F) = \hat{e}(U^*, PID_i)$ for some $i \in \{1, ..., t\}$. The challenger B can find such a F by verifying the equality $\hat{e}(P, F) = \hat{e}(U^*, PID_i)$, for all F appearing in the list L_2 and $i = \{1, ..., t\}$. Since, $U^* = bP$ and $PID_i = x_{id_i}.(aP)$, B can obtain $J = abP$ by evaluating $xid_i^{-1}.F_i$. Next, we evaluate the advantage of challenger B winning the Game-I (IND-MCLS-CCA-II) by calculating the probability of occurrence of the following events.

1. In the unsigncryption query, if $(\langle C_1, ..., C_t \rangle, V, U, \bigwedge, Q)$ cannot be found in L_6, B returns failure and terminates. The probability is $1/qH_6$.
2. In the public key replace query, the game terminates if $ID = ID_i^*$, for some $i \in \{1, ..., t\}$. The probability is $1/q_r$.
3. In the secret value extract query, the game terminates if $ID = ID_i^*$, for some $i \in \{1, ..., t\}$. The probability is $1/q_s$.
4. In the unsigncryption query, the games aborts due to invalid message $m' \neq m$. The probability is q_{uns}/q.

Further, the challenger B will obtain the list L_2 for the some (K, F) with the probability $1/qH_2$. Hence, if an IND-CLMS-CCA-II adversary A can break MCLS scheme with a non-negligible advantage ϵ, then the Gap-BDH problem can be solved with a non-negligible advantage ϵ'

$$\epsilon' \geq \epsilon \left(\frac{1}{qH_6}\right)\left(\frac{1}{qH_2}\right)\left(1 - \frac{1}{q_r}\right)\left(1 - \frac{1}{q_s}\right)\left(1 - \frac{q_{uns}}{q}\right) \quad . \tag{8}$$

In the following, we assess the required computation time τ' while answering queries in the aforementioned simulation game. It turns out that $\tau' = \tau + O(q_0 + q_p).\tau_1 + O(q_{usc}).\tau_2 + O(q_1 + q_2 + q_3 + q_4 + q_5 + q_6 + q_r + q_s)$, where τ_1 is the time to perform a scalar multiplication in G_1, τ_2 is the time to perform a pairing operation and t is the number of target identities.

Theorem 3. *The scheme is provably secure against EUF-MCLS-CMA Type-I adversary with a non-negligible advantage ϵ can break the MCLS scheme with running time τ in ROM after $q_i\{i = 0, ..., 6\}$ hash queries including q_p queries*

to public key retrieve query, q_r public key replace query, q_s secret value extract query, and q_{usc} unsigncryption query respectively. Then, there is an algorithm B that can solve the DBDHI problem with a non-negligible advantage ϵ' with running time τ' defined at the end of the Proof.

Proof. Assume that an algorithm B is given a random instance (P, aP, bP, cP) of the DBDHI problem, where $P, aP, bP, cP \in G_1$ with unknown $a, b, c \in Z_q^*$. Let $R = \hat{e}(P,P)^{ab^{-1}c}$ be the solution of DBDHI problem. The algorithm B plays the challenger in Game-II (Definition 6) who would like to compute R by interacting with the adversary A as follows.
Setup: B runs the initialized algorithm and generates public parameters $PP = \{G_1, G_2, \hat{e}, P, q, P_{pub}, H_0, H_1, H_2, H_3, H_4, H_5, H_6, E_{sk}, D_{sk}\}$ with $P_{pub} = aP$. The challenger B sends PP to adversary A.
Phase-1: The adversary first selects a target identity denoted by ID_A^* (in EUF-MCLS-CMA-I, the target identity is the sender's identity denoted by ID_A^*). The adversary A makes number of queries including a H_0 query, partial private key query, and signcryption query. The challenger B responds to these queries as follows.
$H_0(ID)$ *query*: If there exists (ID, u, QID) in the list L_0, B returns QID to A. Otherwise, B performs the following steps.

- Picks a value $u \in Z_q^*$ at random.
- If $ID = ID_A^*$, sets $QID = ub^{-1}P$. Otherwise, sets $QID = uP$, stores (ID, u, QID) in L_0 and responds with QID to adversary A.

Partial private key query (q_e): If $ID = ID_A^*$, B returns $\perp$ because, ID_A^* is a target identity and a Type-I adversary is not allowed to ask for a partial private key query for the target identity. Otherwise, if (ID, u, QID) exists in L_0, B computes and returns $DID = u.P_{pub}$ to A. Otherwise, B randomly picks a value $u \in Z_q^*$, sets $QID = u.P$, and $DID = u.P_{pub}$, and stores (ID, u, QID) in L_0. B returns DID to A.
Signcryption query (q_{sc}): When B receives a signcrypt query with a message m, sender ID, and receiver's identity ID_i for $i \in \{1, ..., t\}$ and public key in a tuple $((ID_1, PID_1), ..., (ID_t, PID_t))$. It checks if $ID = ID_A^*$. If $ID \neq ID_A^*$, the challenger B runs the normal signcryption algorithm. Otherwise, B obtains the tuple (DID, x_{id}, PID) via q_p, q_e, and q_s queries and generates a ciphertext CT via following procedure.

- Pick a value $r \in Z_q^*$ randomly and compute $U = r.P$.
- Compute $F_i = r.PID_i$, $h_i = H_1(X_a, m)$ where $X_a = F_i.x_{id}$ and adds in L_1.
- Compute $K_i = \hat{e}(U, DID)$, $T_i = H_2(K_i, F_i)$ and adds in L_2.
- Picks an ephemeral value $\sigma \in \{0,1\}^w$ at random and compute $C_i = H_3(T_i) \parallel H_4(T_i) + \sigma$ and adds in L_3 and L_4.
- Use σ to compute symmetric key $sk = H_5(\sigma)$ and generate $V = E_{sk}(m)$.
- Compute $Q = (r + h_i)x_{id}$ and compute $\bigwedge = H_6(m, \sigma, \langle C_1, ..., C_t \rangle, Q, V, U)$ and update L_6.
- Set $CT = (\langle C_1, ..., C_t \rangle, V, U, Q, \bigwedge)$.

Forgery: After the query phase completes, A outputs the challenge identity ID_A^*, a receiver's identity ID_i for $i \in \{1, ..., t\}$, a message m, and a challenge ciphertext $CT^* = (\langle C_1^*, ..., C_t^* \rangle, V^*, U^*, \bigwedge^*, Q^*)$. However, it cannot ask for the unsigncryption query for the challenge CT^* with the private key of any target identity.

If the game does not abort, the challenger fetches the list L_2 for (K, F) to obtain $R = \hat{e}(P, P)^{ab^{-1}c}$ which is the solution to the DBDHI problem. Since, $QID = ub^{-1}P$, $P_{pub} = aP$, and $U^* = cP$, B can obtain $R = \hat{e}(P, P)^{ab^{-1}c}$ by evaluating $K_i^{ui^{-1}}$. Hence, if the Game-II (EUF-MCLS-CMA-I) adversary A can break the MCLS scheme with a non-negligible advantage ϵ, the DBDHI problem can be solved with a non-negligible advantage ϵ'

$$\epsilon' \geq \epsilon \left(\frac{1}{qH_6}\right)\left(\frac{1}{qH_2}\right)\left(1 - \frac{1}{q_e}\right)\left(1 - \frac{q_{uns}}{q}\right) \tag{9}$$

τ' is the required computation time while answering the queries in the aforementioned simulation game. It turns out that $\tau' = \tau + O(q_0 + q_p + q_e)\tau_1 + O(q_1 + q_2 + q_3 + q_4 + q_5 + q_6 + q_r + q_s + q_{usc})$ where τ_1 is the time to perform a scalar multiplication in G_1 and t is the number of target identities.

Theorem 4. *The scheme is provably secure against EUF-MCLS-CMA Type-II adversary with a non-negligible advantage ϵ can break the MCLS scheme with running time τ in ROM after $q_i\{i = 0, ..., 6\}$ hash queries including q_p queries to public key retrieve query, q_r public key replace query, q_s secret value extract query, and q_{usc} unsigncryption query respectively. Then, there is an algorithm B that can solve the CDH problem with a non-negligible advantage ϵ' with running time τ' defined at the end of the Proof.*

Proof. Assume that an algorithm B is given a random instance (P, aP, bP) of the CDH problem, where $P, aP, bP \in G_1$, within unknown $a, b \in Z_q^*$. Let $J = abP$ be the solution of the CDH problem. The algorithm B plays the challenger of Game-II (Definition 6) who would like to compute J by interacting with the adversary A as follows.

Setup: B runs the initialized algorithm and generates public parameters $PP = \{G_1, G_2, \hat{e}, P, q, P_{pub}, H_0, H_1, H_2, H_3, H_4, H_5, H_6, E_{sk}, D_{sk}\}$ with $P_{pub} = aP$. The challenger B sends PP to adversary A.

Phase-1: The adversary first selects a target identity denoted by ID_A^* (in EUF-MCLS-CMA-II, the target identity is the sender's identity denoted by ID_A^*). The adversary A makes number of queries including a H_0 query, partial private key query, and signcryption query. The challenger B responds to these queries as follows.

Public key retrieve query (q_P): If there exists (ID, PID, x_{id}) in the list PK^{list}, B returns PID to A. Otherwise, B performs the following steps.

- Pick $x_{id} \in Z_q^*$ at random.
- If $ID = ID_A^*$, set $PID = x_{id}.aP$; otherwise, set $PID = x_{id}.P$.
- Store (ID, PID, x_{id}) in the PK^{list} and returns PID to A.

Signcryption query (q_{sc}): When B receives a signcrypt query with a message m, sender ID, and receiver's identity ID_i for $i \in \{1, ..., t\}$ and public key in a tuple $((ID_1, PID_1), ..., (ID_t, PID_t))$. It checks if $ID = ID_A^*$. If $ID \neq ID_A^*$, formal signcryption algorithm runs. Otherwise, B obtains the tuple (DID, x_{id}, PID) via q_p, q_e, and q_s and generates a ciphertext CT via following procedure.

- Pick a value $r \in Z_q^*$ randomly and compute $U = r.P$.
- Compute $F_i = r.PID_i$, $h_i = H_1(X_a, m)$ where $X_a = F_i.x_{id}$ and adds in L_1.
- Compute $K_i = \hat{e}(U, DID)$, $T_i = H_2(K_i, F_i)$ and adds in L_2.
- Picks an ephemeral value $\sigma \in \{0,1\}^w$ at random and compute $C_i = H_3(T_i) \parallel H_4(T_i) + \sigma$ and adds in L_3 and L_4.
- Use σ to compute symmetric key $sk = H_5(\sigma)$ and generate $V = E_{sk}(m)$.
- Compute $Q = (r + h_i)x_{id}$ and compute $\bigwedge = H_6(m, \sigma, \langle C_1, ..., C_t \rangle, Q, V, U)$ and update L_6.
- Set $CT = (\langle C_1, ..., C_t \rangle, V, U, Q, \bigwedge)$.

Forgery: After the query phase completes, A outputs the challenge sender identity ID_A^*, a receiver's identity ID_i for $i \in \{1, ..., t\}$, a message m, and a challenge ciphertext $CT^* = (\langle C_1^*, ..., C_t^* \rangle, V^*, U^*, \bigwedge^*, Q^*)$. However, it cannot ask for the unsigncryption query for the challenge CT^* with the private key of any target identity.
If the game does not abort, the challenger fetches the list L_2 for (K, F) such that $\hat{e}(P, F) = \hat{e}(U^*, PID)$. The challenger B can find such a F by verifying the equality $\hat{e}(P, F) = \hat{e}(U^*, PID)$. Since, $U^* = bP$, $PID = x_{id}(aP)$, B can obtains $J = abP$ by evaluating $F_i^2 X_a^{-1}$ which is the solution to the CDH problem. Hence, if the Game-II (EUF-MCLS-CMA-II) adversary A can break the proposed MCLS scheme with a non-negligible advantage ϵ, the CDH problem can be solved with a non-negligible advantage ϵ'

$$\epsilon' \geq \epsilon \left(\frac{1}{qH_6}\right)\left(\frac{1}{qH_2}\right)\left(1 - \frac{1}{q_r}\right)\left(1 - \frac{1}{q_s}\right)\left(1 - \frac{q_{uns}}{q}\right) \quad . \tag{10}$$

In the following, we assess the required computation time τ' while answering queries in the aforementioned simulation game. It turns out that $\tau' = \tau + O(q_0 + q_p).\tau_1 + O(q_{usc}).\tau_2 + O(q_1 + q_2 + q_3 + q_4 + q_5 + q_6 + q_r + q_s)$, where τ_1 is the time to perform a scalar multiplication in G_1, τ_2 is the time to perform a pairing operation and t is the number of target identities.

7 Performance Comparison and Discussion

Here, we compare the proposed MCLS scheme with the existing single receiver and multireceiver encryption and signcryption schemes which are mainly based on bilinear pairing operation [15], [12], [8], [9], [16], [6]. The notations are defined in Table 1. For single receiver signcryption schemes, Table 2 compares the computational cost of signcryption/unsigncryption, public key settings, and exemption from the key escrow problem with [9] and [8]. Li et al. [9] require

$2T_p + 9T_m + T_e$ total operations whereas, the proposed MCLS scheme requires total $2T_p + 6T_m + T_e$ operations for signcryption/unsigncryption and works in CLPKC settings. Karati et al. [8] has equal computational cost as MCLS scheme however, it works in IDPKC and does not provide exemption of the escrow problem. The computational cost of multireceiver signcryption / unsigncryption, public key settings, and exemption from the key escrow problem are compared with [12], [15], and [16]. Wang et al. [15] require total $(n+1)T_e + (n+2)T_m + 2T_p$

Table 1. Notations

Notations	Description
T_p	The time of executing a bilinear pairing operation $\hat{e} : G_1 \times G_1 \rightarrow G_2$.
T_m	The time of executing a scalar multiplication operation in G_1.
T_e	The time of executing an exponentiation in G_2 or an exponentiation operation in Z_q^*.
T_i	The time of executing modular inversion operation.
T_{pm}	The time of executing an multiplication operation in G.
n	The number of receivers.
IDPKC	Identity-based Public Key Cryptography.
CLPKC	Certificateless Public Key Cryptography.
Enc	Encryption.
Dec	Decryption.

operations for signcryption and unsigncryption however, works in IDPKC-PKC settings and are not exempt from the key escrow problem. Niu et al. [12] require $(n+3)T_m + 2(n+2)T_p + 2nT_e + T_{pa}$ total operations for multiple recipients and the scheme works in IDPKC for senders and CLPKC for receivers. Therefore, the sending entities are not exempt from the key escrow problem. Furthermore, Yang et al. [16] require total $3nT_m + 5nT_{pm} + nT_p + nT_e$ signcryption / unsigncryption operations whereas, it works in IDPKC and is not exempt from the key escrow.

Table 2. Comparison between MCLS scheme with the existing single and multi-receiver encryption and signcryption schemes based on bilinear pairings.

Scheme	Single receiver		Multireceiver		Public key settings	Exemption of key escrow
	Enc/Signcrypt	Dec/Unsigncrypt	Enc/Signcrypt	Dec/Unsigncrypt		
LI et al. (2019) [9]	$T_p + 4T_m + T_e$	$T_p + 5T_m$	-	-	IDPKC - CLPKC	Yes
Karati et al. (2018) [8]	$4T_e$	$2T_p + 2T_e + T_i$	-	-	IDPKC	No
Niu et al. (2017) [12]	-	-	$(n+2)T_m + 2nT_p + 2nT_e$	$4T_p + T_m + T_{pa}$	IDPKC - CLPKC	Yes
Wang et al. (2017) [15]	-	-	$(n+1)T_e + nT_m$	$2T_p + 2T_m$	IDPKC - PKC	No
Yang et al. (2022) [16]	-	-	$2nT_m + 2nT_{pm} + nT_e$	$nT_m + 3nT_{pm} + nT_p$	IDPKC	No
Hung et al. (2017)[6]	-	-	$nT_p + nT_e + (n+1)T_m$	$T_p + T_m$	CLPKC	Yes
Our scheme	$T_p + T_e + 4T_m$	$T_p + 2T_m$	$nT_p + nT_e + (2n+2)T_m$	$T_p + 2T_m$	CLPKC	Yes

From the multireceiver signcryption schemes the MCLS scheme requires total $(n+1)T_p + (2n+4)T_m + nT_e$ operations, works in certificateless settings, and exempts from the key escrow. The signcryption cost in the MCLS scheme is linear with the number of designated receivers, while the unsigncryption cost is constant for each receiver. Further, Hung et al.'s [6] multireceiver encryption scheme require $nT_p + nT_e + (n+1)T_m$ operations for encryption phase and $T_p + T_m$ operations for decryption. Therefore, Hung et al.'s scheme require total $(n+1)T_p + nT_e + (n+2)T_m$ operations for encryption and decryption. As compared to Hung et al.'s scheme, the MCLS require only three additional multiplication operations for signcryption and unsigncryption resulting in total $(n+1)T_p + (2n+4)T_m + nT_e$ operations, whereas, the signcryption cost is linear with the number of designated receivers and the unsigncryption cost is constant with the number of designated receivers. Finally, while the proposed scheme significantly extends Hung et al.'s efficient anonymous multireceiver certificateless encryption scheme into a multireceiver certificateless signcryption scheme (secure against a chosen message attack), this comes at a relatively small cost as shown in Table 2.

8 Conclusion

This paper presents a Multireceiver Certificateless Signcryption (MCLS) scheme to fulfill both confidentiality and authentication requirements, building on Hung et al.'s encryption [6] scheme. In the proposed scheme, the message is encrypted and signed with sender's private key, ensuring the message reliability and authenticity. While traditional multireceiver signcryption schemes require each receiver to verify the message, which increases computational cost, in this scheme, 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 IND-CCA (from Hung et al.'s scheme) and EUF-CMA (proposed) attacks in the random oracle model using the Gap-BDH, CDH, and DBDHI assumptions, respectively. Finally, we compare the proposed MCLS scheme's performance and functionality to existing single receiver and multireceiver signcryption approaches. In comparison to other existing single receiver and multireceiver signcryption techniques, the MCLS scheme is more efficient, while both avoiding the key escrow problem and work in multireceiver certificateless public key setting.

References

1. Al-Riyami, S.S., Paterson, K.G.: Certificateless public key cryptography. In: Laih, C. (ed.) Advances in Cryptology - ASIACRYPT 2003, 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, November 30 - December 4, 2003, Proceedings. Lecture Notes in Computer Science, vol. 2894, pp. 452–473. Springer (2003), https://doi.org/10.1007/978-3-540-40061-5_29

2. Barbosa, M., Farshim, P.: Certificateless signcryption. In: Abe, M., Gligor, V.D. (eds.) Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security, ASIACCS 2008, Tokyo, Japan, March 18-20, 2008. pp. 369–372. ACM (2008), https://doi.org/10.1145/1368310.1368364
3. Chen, L., Malone-Lee, J.: Improved identity-based signcryption. In: Vaudenay, S. (ed.) Public Key Cryptography - PKC 2005, 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, 2005, Proceedings. Lecture Notes in Computer Science, vol. 3386, pp. 362–379. Springer (2005), https://doi.org/10.1007/978-3-540-30580-4_25
4. Chow, S.S.M., Yiu, S., Hui, L.C.K., Chow, K.: Efficient forward and provably secure id-based signcryption scheme with public verifiability and public ciphertext authenticity. In: Lim, J.I., Lee, D.H. (eds.) Information Security and Cryptology - ICISC 2003, 6th International Conference, Seoul, Korea, November 27-28, 2003, Revised Papers. Lecture Notes in Computer Science, vol. 2971, pp. 352–369. Springer (2003), https://doi.org/10.1007/978-3-540-24691-6_26
5. Guo, R., Xu, L., Li, X., Zhang, Y., Li, X.: An efficient certificateless ring signcryption scheme with conditional privacy-preserving in vanets. J. Syst. Archit. **129**, 102633 (2022), https://doi.org/10.1016/j.sysarc.2022.102633
6. Hung, Y., Huang, S., Tseng, Y., Tsai, T.: Efficient anonymous multireceiver certificateless encryption. IEEE Syst. J. **11**(4), 2602–2613 (2017), https://doi.org/10.1109/JSYST.2015.2451193
7. Islam, S.H., Khan, M.K., Al-Khouri, A.M.: Anonymous and provably secure certificateless multireceiver encryption without bilinear pairing. Secur. Commun. Networks **8**(13), 2214–2231 (2015), https://doi.org/10.1002/sec.1165
8. 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. **5**(4), 2904–2914 (2018), https://doi.org/10.1109/JIOT.2017.2741580
9. Li, S., Tao, F., Shi, T.: Security analysis and improvement of hybrid signcryption scheme based on heterogeneous system. In: 14th International Conference on Computer Science & Education, ICCSE 2019, Toronto, ON, Canada, August 19-21, 2019. pp. 840–845. IEEE (2019), https://doi.org/10.1109/ICCSE.2019.8845053
10. Malone-Lee, J.: Identity-based signcryption. IACR Cryptol. ePrint Arch. p. 98 (2002), http://eprint.iacr.org/2002/098
11. Miao, S., Zhang, F., Zhang, L.: Cryptanalysis of a certificateless multi-receiver signcryption scheme. In: 2010 International Conference on Multimedia Information Networking and Security. pp. 593–597. IEEE (2010)
12. Niu, S., Niu, L., Yang, X., Wang, C., Jia, X.: Heterogeneous hybrid signcryption for multi-message and multi-receiver. PloS one **12**(9), e0184407 (2017)
13. Selvi, S.S.D., Vivek, S.S., Rangan, C.P.: A note on the certificateless multi-receiver signcryption scheme. IACR Cryptol. ePrint Arch. p. 308 (2009), http://eprint.iacr.org/2009/308
14. Selvi, S.S.D., Vivek, S.S., Shukla, D., Rangan, C.P.: Efficient and provably secure certificateless multi-receiver signcryption. In: Baek, J., Bao, F., Chen, K., Lai, X. (eds.) Provable Security, Second International Conference, ProvSec 2008, Shanghai, China, October 30 - November 1, 2008. Proceedings. Lecture Notes in Computer Science, vol. 5324, pp. 52–67. Springer (2008), https://doi.org/10.1007/978-3-540-88733-1_4
15. Wang, C., Liu, C., Li, Y., Qiao, H., Chen, L.: Multi-message and multi-receiver heterogeneous signcryption scheme for ad-hoc networks. Inf. Secur. J. A Glob. Perspect. **26**(3), 136–152 (2017), https://doi.org/10.1080/19393555.2017.1319523

16. 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. **6**(3), 1520–1531 (2022). https://doi.org/10.1109/TGCN.2022.3163596, https://doi.org/10.1109/TGCN.2022.3163596
17. Yu, Y., Yang, B., Huang, X., Zhang, M.: Efficient identity-based signcryption scheme for multiple receivers. In: Xiao, B., Yang, L.T., Ma, J., Müller-Schloer, C., Hua, Y. (eds.) Autonomic and Trusted Computing, 4th International Conference, ATC 2007, Hong Kong, China, July 11-13, 2007, Proceedings. Lecture Notes in Computer Science, vol. 4610, pp. 13–21. Springer (2007), https://doi.org/10.1007/978-3-540-73547-2_4
18. Zheng, Y.: Digital signcryption or how to achieve cost(signature & encryption) textlesstextless cost(signature) + cost(encryption). In: Jr., B.S.K. (ed.) Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings. Lecture Notes in Computer Science, vol. 1294, pp. 165–179. Springer (1997). https://doi.org/10.1007/BFb0052234, https://doi.org/10.1007/BFb0052234
19. Zheng, Y.: Signcryption or how to achieve cost (signature & encryption)¡¡ cost (signature)+ cost (encryption). In: Annu. Int. Cryptol. Conf (1999)