Leakage-Resilient Anonymous Multi-Recipient Signcryption Under a Continual Leakage Model

TUNG-TSO TSAI1, YUH-MIN TSENG2, (Member, IEEE), SEN-SHAN HUANG2, JIA-YI XIE2, AND YING-HAO HUNG3

1Department of Computer Science and Engineering, National Taiwan Ocean University, Keelung 202, Taiwan
2Department of Mathematics, National Changhua University of Education, Changhua 500, Taiwan
3Department of Mathematics, National Experimental High School at Hsinchu Science Park, Hsinchu 300, Taiwan

Corresponding author: Yuh-Min Tseng (ymtseng@cc.ncue.edu.tw)

This work was supported in part by the Ministry of Science and Technology, Taiwan, under Contract MOST110-2221-E-018-006-MY2, Contract MOST110-2221-E-018-007-MY2, and Contract MOST110-2222-E-019-001-MY2.

ABSTRACT A multi-recipient signcryption (MRSC) scheme possesses the functionalities of both multi-recipient public-key encryption and digital signature to ensure both integrity and confidentiality of transmitted messages. Moreover, an anonymous MRSC (AMRSC) scheme retains the functionalities of an MRSC scheme while offering privacy-preserving, namely, a recipient’s identity or public key being hidden to other recipients. In the past, numerous MRSC and AMRSC schemes based on various public-key cryptographies (i.e., public key infrastructure (PKI)-based, identity (ID)-based and certificateless (CL)) were proposed. Recently, an attacker can realize side-channel attacks to acquire partial bits of private keys participated in cryptographic computations. However, up to date, no MRSC or AMRSC scheme can resist side-channel attacks so that these schemes might suffer from such attacks and could be broken. To resist such attacks under a continual leakage model, we propose the first PKI-based leakage-resilient AMRSC (PKI-LR-AMRSC) scheme in this paper. In the proposed scheme, an attacker is permitted to continually acquire partial bits of private keys partook in computations of the PKI-LR-AMRSC scheme, and formal security proofs are given to show that the proposed scheme still retains the original security of AMRSC schemes. As compared with the relevant AMRSC schemes, our PKI-LR-AMRSC scheme not only resists side-channel attacks but also reduces the cost of executing the multi-signcryption and unsigncryption algorithms. In particular, the point is that the computational complexities of our scheme respectively require only $O(t)$ and $O(1)$ in executing the Multi-signcryption algorithm and the Unsigncryption algorithm, where $t$ is the number of recipients.

INDEX TERMS Anonymity, multi-recipient encryption, signature, side-channel attacks, leakage-resilience.

I. INTRODUCTION

As compared with unicast communication, multicast communication provides an efficient way to send massive contents to multiple recipients. Indeed, several multicast applications (e.g., digital content distribution, multimedia conference and pay-per-view TV) typically need a secure mechanism (e.g., multi-recipient encryption, termed as MRE scheme) to ensure that unauthorized recipients cannot decrypt these multicast contents [1], [2], [3], [4], [5], [6]. Moreover, based on his own signcryption scheme [7], Zheng [8] proposed a multi-recipient signcryption (MRSC) scheme that possesses the functionalities of multi-recipient encryption and digital signature to ensure both integrity and confidentiality of transmitted contents. Furthermore, for protecting recipient’s identity from concealing to other recipients, anonymous MRE (AMRE) schemes [9], [10] and anonymous MRSC (AMRSC) scheme [11] were proposed to combine privacy-preserving property into the original MRE or MRSC schemes.

Indeed, in all traditional cryptographic schemes based on various public-key cryptographies, there is an important prerequisite that a user’s private key cannot be disclosed to an attacker, even part of it. However, recently, an attacker can realize side-channel attacks [12], [13], [14] to acquire partial...
bits of private keys participated in each cryptographic computation. If an attacker can acquire partial bits of a private key participated in each computation, the entire private key will be eventually guessed by attackers so that these traditional cryptographic schemes will be broken. Therefore, the design of cryptographic schemes withstand side-channel attacks is an essential security topic. Fortunately, leakage-resilient cryptography is a novel alternative answer and numerous leakage-resilient cryptographic schemes have been proposed that will be reviewed later.

In the past, there are numerous MRSC and AMRSC schemes based on various public-key cryptographies, namely, public key infrastructure (PKI)-based, identity (ID)-based [15] or certificateless (CL) [16]. However, up to date, no MRSC or AMRSC scheme can resist side-channel attacks. In this paper, we will propose the first PKI-based leakage-resilient AMRSC (PKI-LR-AMRSC) scheme under a continual leakage model.

A. EVOLUTION OF MRSC AND AMRSC SCHEMES

Here, let us review the evolution of MRSC and AMRSC schemes based on various public-key cryptographies (i.e., public key infrastructure (PKI)-based, identity (ID)-based or certificateless (CL)) that include PKI-MRSC, PKI-AMRSC, ID-MRSC, ID-AMRSC, CL-MRSC and CL-AMRSC schemes.

As mentioned earlier, Zheng [8] proposed the first PKI-MRSC scheme based on the discrete logarithm problem, that possesses the functionalities of multi-recipient encryption and digital signature to ensure both integrity and confidentiality of transmitted messages. Based on Zheng’s scheme, Yavuz et al. [17] presented a new PKI-MRSC scheme suited for satellite multicast with highly dynamic property. Afterwards, numerous improved PKI-MRSC schemes [18], [19], [20], [21] were proposed to offer various properties, namely, multi-message multi-recipient signcryption, ciphertext verifiability or publicly verifiability. Based on bilinear pairing groups, several PKI-MRSC schemes [22], [23] were proposed. For achieving better performance, several efficient PKI-MRSC schemes [24], [25], [26], [27] based on elliptic curve or hyperelliptic curve cryptography have been proposed. Moreover, Wang et al. [11] proposed a PKI-AMRSC scheme to combine privacy-preserving property into the original PKI-MRSC scheme.

Based on the ID-based public-key setting, Duan and Cao [28] proposed the first ID-MRSC scheme. To enhance the security of Duan and Cao’s scheme, Tan [29] presented an improvement. Afterwards, several ID-MRSC schemes [30], [31], [32] were proposed to discuss the security of previous schemes and present related modifications. Indeed, in these ID-MRSC schemes mentioned above, their security proofs are based on the random oracle model. On the other hand, Zhang and Xu [33] proposed a secure ID-MRSC scheme without random oracles. Also, Selvi et al. [34] proposed an efficient ID-MRSC scheme using a pre-shared system key. However, Selvi et al.’s scheme has a drawback that the system becomes insecure if the pre-shared system key is compromised. For achieving better performance, Khullar et al. [35] presented an efficient ID-MRSC scheme based on elliptic curve cryptography. Moreover, Lal and Kushwah [36] proposed the first ID-AMRSC scheme to provide privacy-preserving property. Afterwards, numerous improved ID-AMRSC schemes [37], [38], [39] were proposed to enhance security or offer ciphertext verifiability property.

Based on the certificateless (CL) public-key setting, Selvi et al. [40] proposed the first CL-MRSC scheme. However, Miao et al. [41] presented a forgery attack on Selvi et al.’s scheme. Moreover, Wang et al. [42] proposed a new CL-MRSC scheme that offers multi-message multi-recipient signcryption to multicast various contents to multiple recipients. For achieving better performance, Win et al. [43] proposed an efficient CL-MRSC scheme based on elliptic curve cryptography. Furthermore, Pang et al. [44] presented an efficient CL-AMRSC scheme to offer verifiability for partial private key and privacy-preserving property. Afterwards, numerous improved CL-AMRSC schemes [45], [46], [47] were proposed to offer the public channel transmission of partial private key, provide multi-message multi-recipient signcryption, or suit for edge computing environments.

B. LEAKAGE-RESILIENT ENCRYPTION SCHEMES

As mentioned earlier, leakage-resilient cryptography is an alternative answer to withstand side-channel attacks. Let’s first introduce two leakage models of leakage-resilient cryptography, namely, bounded and continual (or unbounded). Indeed, in both models, the leaked bit length of a private key participated in each cryptographic computation is bounded and related to a security parameter. The bounded leakage model has an impractical restriction in the sense that the total bits of a private key disclosed to attackers are bounded to a fixed amount during system lifecycle [48], [49]. In the continual leakage model, an attacker is permitted to continually acquire partial bits of private keys participated in each computation so that this model has the leakage-unbounded property and is more acceptable [50], [51], [52], [53], [54], [55], [56], [57]. Numerous leakage-resilient encryption schemes under the continual leakage model based on PKI-based, ID-based or certificateless (CL) cryptographies are reviewed as follows.

Under the continual leakage model, Kiltz and Pietrzak [58] proposed the first PKI-based leakage-resilient encryption scheme. For reducing ciphertext size and computation cost, Galindo et al. [59] presented an improvement on Kiltz and Pietrzak’s scheme. Moreover, Brakerski et al. [60] presented the first leakage-resilient ID-based encryption scheme. In Brakerski et al.’s scheme, an attacker is permitted to acquire partial bits of a user’s private key only, but not the system secret key of the private key generator (PKG). Therefore, Yuen et al. [61] presented a modification on Brakerski et al.’s scheme to improve performance and security. In addition,
Li et al. [62] presented a new leakage-resilient ID-based encryption scheme in the standard model to eliminate the usage of hash functions. Later, Li et al. [63] considered the broadcast property to propose an ID-based broadcast encryption with continuous leakage resilience. To overcome the shortcomings in the ID-based public key systems, a certificate-based encryption with leakage resilience was proposed by Guo et al. [64]. Furthermore, Xiong et al. [65] proposed the first leakage-resilient certificateless encryption scheme which is only secure in the bounded leakage model. Hence, under the continual leakage model, Wu et al. [66] presented a new leakage-resilient certificateless encryption scheme. Based on Wu et al.’s scheme, Tseng et al. [67] further proposed a new leakage-resilient revocable certificateless encryption to outsource the revocation functionality to an authority who can eliminate the revocation computation load of the key generation center (KGC) in the certificateless cryptography. In addition, several attribute-based encryption schemes were proposed, such as, key-policy attribute-based encryption against continual auxiliary input leakage [68] and hierarchical attribute-based encryption with continuous leakage-resilience [69].

C. CONTRIBUTIONS

As mentioned earlier, up to date, there exists no leakage-resilient MRSC or AMRSC scheme based on PKI-based, ID-based or certificateless cryptographies. In this paper, the first PKI-based leakage-resilient AMRSC (PKI-LR-AMRSC) scheme under a continual leakage model is proposed. Based on the security notions of PKI-AMRSC schemes, we present new security notions of PKI-LR-AMRSC schemes by adding two leak queries (i.e., Multi-signcryption leak query and Unsigncryption leak query) used to simulate an attacker’s leakage ability. In the new security model, an attacker is permitted to continually acquire partial bits of users’ private keys participated in each computation. Therefore, we use the key update method in [50], [51], [53], and [56] to split each user’s private key into two parts which have to be updated before executing the Multi-signcryption or Unsigncryption algorithm in the proposed PKI-LR-AMRSC scheme. Due to the multiplicative blinding technique of the key update method, the leaked bits of the two parts participated in two computations are mutually independent so that our scheme has the leakage-unbounded property. Also, under the generic bilinear group (GBG) model [70], security analysis of the proposed scheme is proved to possess three security properties, namely, existential unforgeability, indistinguishability of encryptions and anonymous indistinguishability of encryptions. As compared with the previously proposed MRSC or AMRSC schemes, our scheme has three merits as presented below. (1) It is the first PKI-based leakage-resilient AMRSC scheme. (2) It has the leakage-unbounded property. (3) A recipient requires only constant computations for decrypting ciphertext.

D. ORGANIZATION

The rest of this paper is organized as follows. In Section 2, preliminaries are introduced. In Section 3, the new framework and security notions of PKI-LR-AMRSC schemes are presented. Our PKI-LR-AMRSC scheme is proposed in Section 4. In Section 5, security theorems and their formal proofs of our scheme are shown. Comparisons are demonstrated in Section 6. Conclusions and future work are drawn in Section 7.

II. PRELIMINARIES

A. BILINEAR GROUPS

Let \( \{ p, G_0, G_1, \hat{e}, g_0, g_1 \} \) be a parameter set of bilinear groups. \( G_0 = \langle g_0 \rangle \) and \( G_1 = \langle g_1 \rangle \) are two multiplicative groups of a prime order \( p \), where \( g_0 \) and \( g_1 \) are generators of \( G_0 \) and \( G_1 \), respectively. Moreover, \( \hat{e} : G_0 \times G_0 \rightarrow G_1 \) represents a bilinear map that have three properties as presented below.

- Bilinear: for \( a, b \in \mathbb{Z}_p^* \), \( \hat{e}(g_0^a, g_0^b) = \hat{e}(g_0, g_0)^{ab} \).
- Computable: for \( A, B \in G_0 \), \( \hat{e}(A, B) \) may be evaluated efficiently.
- Non-degenerate: \( g_1 = \hat{e}(g_0, g_0) \neq 1 \).

Note that the reader may refer to [15] for details about the parameter set of bilinear groups.

B. GENERIC BILINEAR GROUP MODEL

In 2005, Boneh et al. [70] introduced a security proof method for cryptographic schemes, called the generic bilinear group (GBG) model. In this method, a challenger first sets a parameter set of bilinear groups. Given \( \hat{e} : G_0 \times G_0 \rightarrow G_1 \), the discrete logarithm problem on \( G_0/G_1 \) would be resolved.

In the GBG model, two random injective mappings \( \xi_0 : \mathbb{Z}_p^* \rightarrow \Theta G_0 \) and \( \xi_1 : \mathbb{Z}_p^* \rightarrow \Theta G_1 \) are used, respectively, to encode each element of both \( G_0 \) and \( G_1 \) to a distinct bit string, where the sets \( \Theta G_0 \) and \( \Theta G_1 \) collect, respectively, the encoded bit strings of \( G_0 \) and \( G_1 \) with \( |\Theta G_0| = |\Theta G_1| = p \) and \( \Theta G_0 \cap \Theta G_1 = \phi \). Additionally, in the GBG model, to execute three group operations, namely, multiplication of \( G_0 \), multiplication of \( G_1 \) and bilinear map, the attacker must, respectively, issue three queries \( O_0, O_1 \) and \( O_z \) that have the following behaviors for \( a, b \in \mathbb{Z}_p^* \).

- \( O_0(\xi_0(a), \xi_0(b)) \rightarrow \xi_0(a + b \bmod p) \).
- \( O_1(\xi_1(a), \xi_1(b)) \rightarrow \xi_1(a + b \bmod p) \).
- \( O_z(\xi_0(a), \xi_0(b)) \rightarrow \xi_1(a \cdot b \bmod p) \).

It is worth mentioning that \( g_0 = \xi_0(1) \) and \( g_1 = \hat{e}(g_0, g_0) = \xi_1(1) \).

C. SECURITY ASSUMPTIONS

The security of the proposed PKI-LR-AMRSC scheme is based on two assumptions as presented below.

- **Discrete logarithm assumption**: Let \( \{ p, G_0, G_1, \hat{e}, g_0, g_1 \} \) denote a parameter set of bilinear groups. Given \( g_0^a \in G_0 \) or \( g_1^a \in G_1 \) for unknown \( a \in \mathbb{Z}_p^* \), no algorithm with
non-negligible probability can discover $a$ in polynomial time.

**Hash function assumption:** Assume that $H : \{0, 1\}^* \rightarrow \{0, 1\}^l$ is a secure hash function, where $l$ is a positive integer. $H$ must satisfy three properties below.

1. **One-way:** For $x \in \{0, 1\}^l$, it is difficult to find a bit string $B \in \{0, 1\}^*$ such that $H(B) = x$.
2. **Weak-collision resistant:** Given $B_1 \in \{0, 1\}^*$, it is difficult to find a distinct $B_2 \in \{0, 1\}^*$ such that $H(B_1) = H(B_2)$.
3. **Strong-collision resistant:** It is difficult to find two distinct bit strings $B_1, B_2 \in \{0, 1\}^*$ such that $H(B_1) = H(B_2)$.

## D. CONCEPT OF ENTROPY

For measuring the security influence by leaked bits of private keys participated in cryptographic computations, we introduce the entropy to evaluate the uncertainty for guessing these private keys. Here, a private key is viewed as a finite random variable. Let $D$ and $\Pr[D = d]$ respectively denote a private key (finite random variable) and the probability of $D = d$. Two kinds of min-entropies are introduced as follows.

1. **Min-entropy of $D$:**
   \[
   H_\infty(D) = -\log_d \Pr[D = d].
   \]

2. **Average conditional min-entropy of $D$ under a condition $C$:**
   \[
   \tilde{H}_\infty(D|C) = -\log_d \Pr[D = d|C].
   \]

In the following, two consequences (Lemmas 1 and 2) about the security influences by leaked bits of private keys were proved in literatures [50], [71].

**Lemma 1:** Let $f : D \rightarrow \{0, 1\}^l$ denote a leakage function for a finite random variable $D$, where $\tau$ is the maximal leaked bit length. Under the condition of this leakage function, we have $H_\infty(f(D)) \geq H_\infty(D) - \tau$.

**Lemma 2:** Assume that $D_1, D_2, \ldots, D_n$ are finite random variables. Let a polynomial $PD \in \mathbb{Z}_p[D_1, D_2, \ldots, D_n]$ has degree $e$. Let $P_t$ denote the probability distribution of $D_t = d_t \in \mathbb{Z}_p$ under a leakage function $f_t$ with a maximal leaked bit length $\tau$ such that $H_\infty(P_j) \geq \log p - \tau$, for $j = 1, 2, \ldots, n$. If all $P_t$ are mutually independent, we have $\Pr[PD(D) = d_1, D_2 = d_2, \ldots, D_n = d_n] = 0 \leq (e/p)^{2\tau}$ that is negligible if $\tau < (1 - \varsigma)\log p$, where $\varsigma$ is a positive decimal fraction.

## III. FRAMEWORK AND SECURITY NOTIONS

### A. FRAMEWORK

Traditional public-key cryptography is based on the construction of the public key infrastructure (PKI). An PKI architecture consists of two trusted third parties, namely, certificate authority (CA) and registration authority (RA). A user $ID_u$ first generates a private/public key pair ($PRK_u$, $PUK_u$) and sends the public key $PUK_u$ to the RA to request the certificate of $PUK_u$. The RA forwards $PUK_u$ to the CA after verifying the user’s credential. The CA generates and sends the certificate of $PUK_u$ to the user. Indeed, the functionalities of both the RA and the CA can be combined into one role, i.e., CA.

In the following, we define a new framework of PKI-based leakage-resilient anonymous multi-recipient signcryption (PKI-LR-AMRSC) schemes. A PKI-LR-AMRSC scheme consists of four algorithms, namely, System setup, Key generation, Multi-signcryption and Unsigncryption. To resist side-channel attacks under a continual leakage model, a user $ID_u$’s private key $PRK_u$ is first partitioned into two initial parts ($PRK_{u, 0, 1}$, $PRK_{u, 0, 2}$) by using the key update method based on the multiplicative blinding technique [50], [51], [53], [56]. Note that, in the $k$-round, the user $ID_u$’s current private key ($PRK_{u,k-1,1}$, $PRK_{u,k-1,2}$) must be updated to ($PRK_{u,k,1}$, $PRK_{u,k,2}$) before signing (i.e., multi-signcryption) or decrypting (i.e., unsigncryption) a message.

In the PKI-LR-AMRSC scheme, assume that a sender $ID_s$ would like to securely deliver a message $M$ to a nominated recipient set $NRS$ of $r$ recipients, i.e., $NRS = \{(ID_{s1}, PU_{K_{s1}}), (ID_{s2}, PU_{K_{s2}}), \ldots, (ID_{sr}, PU_{K_{sr}})\}$. The sender $ID_s$ with the current private key ($PRK_{s,j-1,1}$, $PRK_{s,j-1,2}$) takes as input $M$ and ($PU_{K_{s1}}, PU_{K_{s2}}, \ldots, PU_{K_{sr}}$) to run the multi-signcryption (MSC) algorithm. In the MSC algorithm, the sender $ID_s$ updates her/his current private key ($PRK_{s,j-1,1}$, $PRK_{s,j-1,2}$) to ($PRK_{s,j,1}$, $PRK_{s,j,2}$), and generates a ciphertext $CT = MSC(M, (PRK_{s,j,1}, PRK_{s,j,2}), (PU_{K_{s1}}, PU_{K_{s2}}, \ldots, PU_{K_{sr}}))$. For the unsigncryption (USC) algorithm, a nominated recipient $ID_{rs} \in NRS$ first updates her/his current private key ($PRK_{r,s-1,1}$, $PRK_{r,s-1,2}$) to ($PRK_{r,s,1}$, $PRK_{r,s,2}$), and obtains $M = USC(CT, (PRK_{r,s,1}, PRK_{r,s,2}))$ while the recipient’s public key $PU_{K_r}$ is hidden to the other recipients. The multi-signcryption (MSC) and unsigncryption (USC) processes of the PKI-LR-AMRSC scheme are presented in Figure 1. The detailed framework of the PKI-LR-AMRSC scheme is presented in Definition 1 below.

**Definition 1:** An PKI-LR-AMRSC scheme consists of four algorithms:
System setup: This algorithm is run by a trusted party (i.e. the CA). It takes as input a security parameter to generate and publish a parameter set \([p, G_0, G_1, \hat{e}, g_0, g_1]\) of bilinear groups introduced in Section 2.1. The trusted party also picks two symmetric cipher functions \(E_{sk}()\) and \(D_{sk}()\), where \(ck\) is a cipher key. Finally, the trusted party publishes public parameters \(PP\).

Key generation: This algorithm is run by a user \(ID_u\) to generate a private/public key pair \((PRK_u, PUK_u)\). The user \(ID_u\) also sets the initial private key \(PRK_u = (PRK_{u,0,1}, PRK_{u,0,2})\) by using the key update method based on the multiplicative blinding technique.

Multi-signcryption (MSC): This algorithm is run by a sender \(ID_s\) with current private key \((PRK_{s,j-1,1}, PRK_{s,j-1,2})\). The sender \(ID_s\) first updates her/his current private key \((PRK_{s,j-1,1}, PRK_{s,j-1,2})\) to \((PRK_{s,j,1}, PRK_{s,j,2})\). Note that, by the multiplicative blinding technique, we have \(PRK_s = PRK_{s,0,1} \cdot PRK_{s,0,2} = PRK_{s,1,1} \cdot PRK_{s,1,2} = \ldots = PRK_{s,t,1} \cdot PRK_{s,t,2}\). Without loss of generality, the sender \(ID_s\) takes as input a message \(M\) and a nominated recipient set \(NRS = \{(ID_1, PUK_1), (ID_2, PUK_2), \ldots, (ID_t, PUK_t)\}\) to run the MSC algorithm, and generates a ciphertext \(CT = MSC(M, (PRK_{s,1,1}, PRK_{s,1,2}), (PUK_1, PUK_2, \ldots, PUK_t))\).

Unsigncryption (USC): This algorithm is run by a nominated recipient \(ID_r \in NRS\) with current private key \((PRK_{r,j-1,1}, PRK_{r,j-1,2})\). The recipient \(ID_r\) first updates her/his current private key \((PRK_{r,j-1,1}, PRK_{r,j-1,2})\) to \((PRK_{r,j,1}, PRK_{r,j,2})\). Note that, by the multiplicative blinding technique, we have \(PRK_r = PRK_{r,0,1} \cdot PRK_{r,0,2} = PRK_{r,1,1} \cdot PRK_{r,1,2} = \ldots = PRK_{r,t,1} \cdot PRK_{r,t,2}\). The recipient \(ID_r\) takes as input the ciphertext \(CT\) and identity \(ID_s\) and obtains the message \(M = USC(CT, (PRK_{r,j,1}, PRK_{r,j,2}))\) while verifying \(CT\) signed by the sender \(ID_s\) using the public key \(PUK_s\).

**B. SECURITY NOTIONS**

Here, new security notions of PKI-LR-AMRSC schemes are defined as follows. As mentioned earlier, an attacker can realize side-channel attacks to acquire partial bits of private keys participated in cryptographic computations. In a PKI-LR-AMRSC scheme, attackers could acquire partial bits of both a sender \(ID_s\)’s current private key in the Multi-signcryption algorithm and a nominated recipient \(ID_r\)’s current private key in the Unsigncryption algorithm. Moreover, two leakage functions \(f_{MSC,i}\) and \(h_{MSC,i}\) are used to express the content about partial bits of the sender \(ID_s\)’s current private key \((PRK_{s,1,1}, PRK_{s,1,2})\) in the Multi-signcryption algorithm. Also, two leakage functions \(f_{USC,j}\) and \(h_{USC,j}\) for a nominated recipient \(ID_r\)’s current private key \((PRK_{r,1,1}, PRK_{r,1,2})\) in the Unsigncryption algorithm offer similar functionalities with \(f_{MSC,i}\) and \(h_{MSC,i}\). Furthermore, these four leakage functions satisfy \(|f_{MSC,i}|, |h_{MSC,i}|, |f_{USC,j}|\) and \(|h_{USC,j}| \leq \tau\), where \(\tau\) is the maximal output bit length of leaked partial bits of a private key. Finally, four leakage functions are defined as follows.

- \(\Delta_{MSC,i} = f_{MSC,i}(PRK_{s,1,1})\)
- \(\Delta_{hMSC,i} = h_{MSC,i}(PRK_{s,1,2})\)
- \(\Delta_{USC,j} = f_{USC,j}(PRK_{r,1,1})\)
- \(\Delta_{hUSC,j} = h_{USC,j}(PRK_{r,1,2})\)

In the PKI-LR-AMRSC scheme, the security notions are modeled by three leakage-resilient (LR) security games, namely, existential unforgeability against adaptive chosen-message attacks (LR-EUF-ACMA), anonymous indistinguishability of encryptions against chosen-ciphertext attacks (LR-ANON-CCA) and indistinguishability of encryptions against chosen-ciphertext attacks (LR-IND-CCA). All three security games are played by a challenger \(C\) and an attacker \(A\).

**Definition 2:** The PKI-LR-AMRSC scheme is LR-EUF-ACMA-secure if no probabilistic polynomial-time (PPT) attacker \(A\) with a non-negligible advantage can win the following LR-EUF-ACMA security game with a challenger \(C\).

- **Setup.** The challenger \(C\) takes as input a security parameter to perform the System setup algorithm to generate and publish a parameter set \([p, G_0, G_1, \hat{e}, g_0, g_1]\) of bilinear groups and two symmetric cipher functions \(E_{ck}()\) and \(D_{ck}()\), where \(ck\) is a cipher key.
- **Query.** The attacker \(A\) adaptively issues four queries to \(C\) as defined below.
  - **Multi-signcryption query:** Assume that \(A\) issues this query with taking as input a message \(M\), \(ID_s\) and \(NRS = \{(ID_1, PUK_1), (ID_2, PUK_2), \ldots, (ID_t, PUK_t)\}\). Let the sender \(ID_s\)’s current private key be \((PRK_{s,0,1}, PRK_{s,0,2})\). \(C\) updates this current private key \((PRK_{s,0,1}, PRK_{s,0,2})\) to \((PRK_{s,1,1}, PRK_{s,1,2})\) and returns a ciphertext \(CT = MSC(M, (PRK_{s,1,1}, PRK_{s,1,2}), (PUK_1, PUK_2, \ldots, PUK_t))\).
  - **Multi-signcryption leak query:** For this Multi-signcryption query with taking as input \(M\), \(ID_s\) and \(NRS = \{(ID_1, PUK_1), (ID_2, PUK_2), \ldots, (ID_t, PUK_t)\}\), \(A\) may request this leak query only once. Assume that \(A\) issues this query with input two leakage functions \(f_{MSC,i}\) and \(h_{MSC,i}\). \(C\) returns leaked bits \(\Delta_{MSC,i} = f_{MSC,i}(PRK_{s,1,1})\) and \(\Delta_{hMSC,i} = h_{MSC,i}(PRK_{s,1,2})\).
  - **Unsigncryption query:** Assume that \(A\) issues this query with input a ciphertext \(CT\) and a nominated recipient \(ID_r \in NRS\). Let the recipient \(ID_r\)’s current private key be \((PRK_{r,0,1}, PRK_{r,0,2})\). \(C\) updates this current private key \((PRK_{r,0,1}, PRK_{r,0,2})\) to \((PRK_{r,1,1}, PRK_{r,1,2})\) and returns a message \(M = USC(CT, (PRK_{r,j,1}, PRK_{r,j,2}))\).
  - **Unsigncryption leak query:** For this Unsigncryption query with input \(CT\) and \(ID_r\), \(A\) may request this query only once. Assume that \(A\) issues this query with input two leakage functions \(f_{USC,j}\) and \(h_{USC,j}\). \(C\) returns leaked bits \(\Delta_{USC,j} = f_{USC,j}(PRK_{r,1,1})\) and \(\Delta_{hUSC,j} = h_{USC,j}(PRK_{r,1,2})\).
  - **Forgery.** Finally, \(A\) outputs a tuple \((ID_s, PUK_s, M^*, NRS, CT^*)\) to \(C\). We say that \(A\) wins the security game
if the recipient ID_r \in NRS can obtain the message M^* while verifying CT signed by ID_r by using the public key PUK_s. Note that the Multi-signcryption query on (ID_s, M^*, NRS) has never been issued. The advantage of A is denoted as Adv_A.

**Definition 3:** The PKI-LR-AMRSC scheme is LR-IND-CCA-secure if no PPT attacker A with a non-negligible advantage can win the following LR-IND-CCA security game with a challenger C.

- **Setup.** The phase is the same with the Setup phase in Definition 2.
- **Query.** The phase is the same with the Query phase in Definition 2.
- **Challenge.** Finally, A sends a message pair (M_0, M_1) and a nominated recipient set NRS to C, where NRS = \{(ID_1, PUK_1), (ID_2, PUK_2), \ldots, (ID_t, PUK_t)\}. C selects a random value b \in \{0, 1\} and returns CT^b = MSC(M_b, (PRK_{s,i,1}, PRK_{s,i,2}), (PUK_1, PUK_2, \ldots, PUK_t)) to A.
- **Guess.** A outputs b' \in \{0, 1\} and wins the game if b' = b. The advantage that A wins the game is defined as Adv_A = |Pr[b = b'] - \frac{1}{2}|.

**Definition 4:** The PKI-LR-AMRSC scheme is LR-ANON-CCA-secure if no PPT attacker A with a non-negligible advantage can win the following LR-ANON-CCA security game with a challenger C.

- **Setup.** The phase is the same with the Setup phase in Definition 2.
- **Query.** The phase is the same with the Query phase in Definition 2.
- **Challenge.** Finally, A sends a message M and a nominated recipient set NRS to C, where NRS = \{(ID_1, PUK_1), (ID_2, PUK_2), \ldots, (ID_t, PUK_t)\}. C selects a random value b \in \{1, 2\} and returns CT^b = MSC(M, (PRK_{s,i,1}, PRK_{s,i,2}), (PUK_b, PUK_3, \ldots, PUK_t, PUK_{t+1})) to A.
- **Guess.** A outputs b' \in \{1, 2\} and wins the game if b' = b. The advantage that A wins the game is defined as Adv_A = |Pr[b = b'] - \frac{1}{2}|.

### IV. THE PROPOSED PKI-LR-AMRSC SCHEME

The proposed PKI-LR-AMRSC scheme consists of four algorithms as presented below.

- **System setup:** A trusted party (i.e. the CA) takes as input a security parameter to generate and publish a parameter set \{p, G_0, G_1, \hat{e}, g_0, g_1\} of bilinear groups introduced in Section 2.1. The CA picks two symmetric cipher functions E_{\hat{e}}() and D_{\hat{e}}(), where \hat{e} is a cipher key. The CA picks five hash functions, H_0: G_0 \rightarrow \{0, 1\}, H_1, H_2, H_3: \{0, 1\} \rightarrow \{0, 1\}, and H_4: \{0, 1\} \times G_0 \rightarrow \{0, 1\}, where I is a positive integer. The CA also chooses x, y \in \mathbb{Z}_p, and sets X = g_0^x and Y = g_0^y. Finally, the CA publishes public parameters PP = \{p, G_0, G_1, \hat{e}, g_0, g_1, H_0, H_1, H_2, H_3, H_4, E, D, X, Y\}.
- **Key generation:** A user ID_u randomly chooses \alpha \in \mathbb{Z}_p^* and computes a private/public key pair (PRK_{u} = g_0^{\beta}, PUK_{u} = \hat{e}(g_0, PRK_{u})). The user ID_u also chooses a random value \beta \in \mathbb{Z}_p and computes the initial private key (PRK_{u,0.1} = g_0^\beta, PRK_{u,0.2} = PRK_{u} \cdot g_0^{-\beta}), where PRK_{u} = PRK_{u,0.1} \cdot PRK_{u,0.2}.

- **Multi-signcryption (MSC):** Assume that a sender ID_s with current private key (PRK_{s,i-1,1}, PRK_{s,i-1,2}) would like to transmit a message M to a nominated recipient set NRS = \{(ID_1, PUK_1), (ID_2, PUK_2), \ldots, (ID_t, PUK_t)\}, where t < n. Here, n is the number of users in the system. The sender ID_s runs the following steps to generate a ciphertext CT.

1. Randomly choose \gamma \in \mathbb{Z}_p^* and update the current private key (PRK_{s,i,1,2} = (PRK_{s,i-1,1}, \gamma g_0^{\beta}, PRK_{s,i-1,2}, g_0^{-\beta})).
2. Randomly choose v \in \mathbb{Z}_p and compute R = g_0^v, S_u = (PUK_0)^\gamma and T_u = H_0(S_u), for u = 1, \ldots, t.
3. Randomly choose w \in \{0, 1\} and compute U_u = H_1(T_u) || H_2(T_u) || w, for u = 1, \ldots, t, where \{\|\}\ is the concatenation operand.
4. Compute ck = H_3(w) and generate C = E_{ck}(M) and \rho = H_4(M, w, U_1, U_2, \ldots, U_t, C, R).
5. Compute a signature \sigma = PRK_{s,i,2} \cdot T_S, where T_S = PRK_{s,i,1} \cdot (X \cdot Y^\rho).
6. Set the ciphertext CT = (\{(U_1, U_2, \ldots, U_t), C, R, \rho, \sigma\}.

- **Unsigncryption (USC):** A nominated recipient ID_r \in NRS with current private key (PRK_{r,j-1,1}, PRK_{r,j-1,2}) takes as input ID_r and CT = (\{(U_1, U_2, \ldots, U_t), C, R, \rho, \sigma\), and performs the following steps to obtain the message M and verify CT signed by the sender ID_s using the public key PUK_s.

1. Randomly choose \delta \in \mathbb{Z}_p^* and update the current private key (PRK_{r,j,1,2} = (PRK_{r,j-1,1}, \delta g_0^{\beta}, PRK_{r,j-1,2}, g_0^{-\beta})).
2. Compute T_{I_r} = \hat{e}(R, PRK_{r,j,1}) \cdot T_I, T_u = H_0(S_u), T_{H_1} = H_1(T_u) and T_{H_2} = H_2(T_u).
3. Use T_{H_1} to locate the corresponding U_u = T_{H_1} || T_{H_2} || w, u = 1, 2, \ldots, t, and remove T_{H_1} from U_u to get Temp = T_{H_2} || w.
4. Recover M = D_{\hat{e}}(C).
5. Compute the cipher key \hat{c}' = H_3(w') and get M' = D_{\hat{c}'}(C).
6. Compute \rho' = H_4(M', w', U_1, U_2, \ldots, U_t, C, R).
7. Return M' and “True” if both \rho' = \rho and \hat{e}(g_0, \sigma) = PUK_s \cdot \hat{e}(R, X \cdot Y^\rho) hold; otherwise reject this message.

The correctness of both S = (PUK_s) \cdot \hat{e}(g_0, \sigma) = PUK_s \cdot \hat{e}(R, X \cdot Y^\rho) are the following two equalities.

\[ S = \hat{e}(R, PRK_{r,j,2}) \cdot T_I \]
\[ = \hat{e}(R, PRK_{r,j,2}) \cdot \hat{e}(R, PRK_{r,j,1}) \]
\[ = \hat{e}(R, PRK_{r,j,2} \cdot PRK_{r,j,1}) \]
\[ = \hat{e}(g_0, PRK_{r}) \]
V. SECURITY ANALYSIS

According to the LR-EUF-ACMA, LR-IND-CCA and LR-ANON-CCA security games defined in Section 3.2, three theorems are established that the proposed PKI-LR-AMRSC scheme are LR-EUF-ACMA-secure, LR-IND-CCA-secure and LR-ANON-CCA-secure against attackers under the GBG model (i.e., discrete logarithm assumption) and the hash function assumption, respectively.

Theorem 1: Under the GBG model and hash function assumption, the proposed PKI-LR-AMRSC scheme is LR-UF-ACMA-secure.

Proof: In the LR-UF-ACMA security game played by an attacker $A$ and a challenger $C$, there are three phases as given below.

- Setup. $C$ performs the System setup algorithm to set $PP = \{p, G_0, G_1, \hat{e}, g_0, g_1, h_0, h_1, h_2, h_3, h_4, e, d, X, Y\}$. Also, $C$ constructs four lists $L_0$, $L_1$, $L_U$ and $L_M$ as follows.
  - $L_0$ and $L_1$ are created to record elements of $G_0$ and $G_1$, respectively.
    (1) A pair $(\mathbb{G}_{G_0, \psi, \theta}, \Theta_{G_0, \psi, \theta})$ in $L_0$ denotes an element of $G_0$, where $\mathbb{G}_{G_0, \psi, \theta}$ and $\Theta_{G_0, \psi, \theta}$, respectively, represent a multivariate polynomial and its corresponding bit string. Here, three indices $\Psi, \Phi, \theta$ indicate type $\Psi$, $\Phi$-th query and $\theta$-th element in $G_0$. Additionally, $(\mathbb{G}_{G_0, \Theta_{G_0, I, 0.0}}, 2X, \Theta_{G_0, I, 0.2})$ and $(\mathbb{Y}, \Theta_{G_0, I, 0.3})$ are initially recorded into $L_0$.
    (2) A pair $(\mathbb{G}_{G_1, \psi, \theta}, \Theta_{G_1, \psi, \theta})$ in $L_1$ denotes an element of $G_1$, where $\mathbb{G}_{G_1, \psi, \theta}$ and $\Theta_{G_1, \psi, \theta}$, respectively, represent a multivariate polynomial and its corresponding bit string. Three indices $\Psi, \Phi, \theta$ have the same meanings as those in $L_0$. The element $(\mathbb{G}_{G_1, \Theta_{G_1, I, 0.1}})$ is initially recorded into $L_1$.

For $L_0$ and $L_1$, two transforming rules between the multivariate polynomial $\mathbb{G}_{G_0, \psi, \theta} / \mathbb{G}_{G_1, \psi, \theta}$ and the corresponding bit string $\Theta_{G_0, \psi, \theta} / \Theta_{G_1, \psi, \theta}$ are presented as follows.

(1) Transforming rule-1: By taking $\mathbb{G}_{G_0, \psi, \theta} / \mathbb{G}_{G_1, \psi, \theta}$ as input, $C$ looks for $(\mathbb{G}_{G_0, \psi, \theta}, \Theta_{G_0, \psi, \theta}) / (\mathbb{G}_{G_1, \psi, \theta}, \Theta_{G_1, \psi, \theta})$ in $L_0/L_1$ and returns $\Theta_{G_0, \psi, \theta} / \Theta_{G_1, \psi, \theta}$ if found. Otherwise, $C$ selects a distinct bit string $\Theta_{G_0, \psi, \theta} / \Theta_{G_1, \psi, \theta}$ and records $(\mathbb{G}_{G_0, \psi, \theta}, \Theta_{G_0, \psi, \theta}) / (\mathbb{G}_{G_1, \psi, \theta}, \Theta_{G_1, \psi, \theta})$ in $L_0/L_1$.

(2) Transforming rule-2: By taking $\Theta_{G_0, \psi, \theta} / \Theta_{G_1, \psi, \theta}$ as input, $C$ looks for $(\mathbb{G}_{G_0, \psi, \theta}, \Theta_{G_0, \psi, \theta}) / (\mathbb{G}_{G_1, \psi, \theta}, \Theta_{G_1, \psi, \theta})$ in $L_0/L_1$ and returns $\Theta_{G_0, \psi, \theta} / \Theta_{G_1, \psi, \theta}$ if found. Otherwise, the security game is terminated.

- Query: $A$ adaptively issues various queries to $C$ at most $\lambda$ times as defined below.
  - $O_0$ query $(\Theta_{G_0, q_{j,n}}, \Theta_{G_0, q_{j,n}})$: For the $n$-th $O_0$ query,
    (1) Transform $(\Theta_{G_0, q_{j,n}}, \Theta_{G_0, q_{j,n}})$ to $(\mathbb{G}_{G_0, q_{j,n}}, \mathbb{G}_{G_0, q_{j,n}})$ in $L_0$ by Transforming rule-2.
    (2) Compute $\mathbb{G}_{G_0, q_{j,n}} = \mathbb{G}_{G_0, q_{j,n}} + \mathbb{G}_{G_0, q_{j,n}}$ if $OR = \text{"Mul."}$, and $\mathbb{G}_{G_0, q_{j,n}} = \mathbb{G}_{G_0, q_{j,n}} - \mathbb{G}_{G_0, q_{j,n}}$ if $OR = \text{"Div."}$.
    (3) Transform $\mathbb{G}_{G_0, q_{j,n}}$ to return $\Theta_{G_0, q_{j,n}}$ by Transforming rule-1.
  - $O_1$ query $(\Theta_{G_1, q_{j,n}}, \Theta_{G_1, q_{j,n}})$: For the $n$-th $O_1$ query,
    (1) Transform $(\Theta_{G_1, q_{j,n}}, \Theta_{G_1, q_{j,n}})$ to $(\mathbb{G}_{G_1, q_{j,n}}, \mathbb{G}_{G_1, q_{j,n}})$ in $L_1$ by Transforming rule-2.
    (2) Compute $\mathbb{G}_{G_1, q_{j,n}} = \mathbb{G}_{G_1, q_{j,n}} + \mathbb{G}_{G_1, q_{j,n}}$ if $OR = \text{"Mul."}$, and $\mathbb{G}_{G_1, q_{j,n}} = \mathbb{G}_{G_1, q_{j,n}} - \mathbb{G}_{G_1, q_{j,n}}$ if $OR = \text{"Div."}$.
    (3) Transform $\mathbb{G}_{G_1, q_{j,n}}$ to return $\Theta_{G_1, q_{j,n}}$ by Transforming rule-1.
  - $O_2$ query $(\Theta_{G_0, q_{j,n}}, \Theta_{G_0, q_{j,n}})$: For the $n$-th $O_2$ query,
    (1) Transform $(\Theta_{G_0, q_{j,n}}, \Theta_{G_0, q_{j,n}})$ to obtain $(\mathbb{G}_{G_0, q_{j,n}}, \mathbb{G}_{G_0, q_{j,n}})$ in $L_0$ by Transforming rule-1.
    (2) Compute $\mathbb{G}_{G_1, q_{j,n}} = \mathbb{G}_{G_0, q_{j,n}} - \mathbb{G}_{G_0, q_{j,n}}$.
    (3) Transform $\mathbb{G}_{G_1, q_{j,n}}$ to return $\Theta_{G_1, q_{j,n}}$ by Transforming rule-1.

- Multi-signcryption query: Assume that $A$ issues this query with input a message $M$, $ID_1$ and $NRS = \{ID_1, PUK_1\}, (ID_2, PUK_2), \ldots, (ID_l, PUK_l)\}$. Let a sender $ID_s$’s current private key be $PRK_{s_1,i-1,\ldots,2}$. $C$ performs the following steps to return a ciphertext $CT$.
  (1) Update the current private key $(ID_s, \mathbb{Z}_{PUK_i}, \mathbb{Z}_{PRK_{s}, (\mathbb{Z}_{PRK_{s}, s_1,i-1,\ldots,2})})$ to $(ID_s, \mathbb{Z}_{PUK_i}, \mathbb{Z}_{PRK_{s}, (\mathbb{Z}_{PRK_{s}, s_1,i-1,\ldots,2})})$ in $L_U$.
  (2) Choose a new variate $\mathbb{Z}$ in $G_0$ and a random string $\Theta_w \in \{0, 1\}^k$, and get $\Theta_{ck} = H_2(\Theta_w)$ and $C = E_{\Theta_{ck}}(M)$. 

\[ \hat{e}(g_0, PRK_i) \]
\[ (PUK_i) \]
\[ \hat{e}(g_0, \sigma) = \hat{e}(g_0, PRK_{i,2}, PRK_{i,1} \cdot (X \cdot Y)^\rho) \]
\[ \hat{e}(g_0, PRK_i, (X \cdot Y)^\rho) \]
\[ \hat{e}(g_0, PRK_i, (X \cdot Y)^\rho) \]
\[ = PUK_i \cdot \hat{e}(g_0^\rho, X \cdot Y^\rho) \]
\[ = PUK_i \cdot \hat{e}(g_0^\rho, X \cdot Y^\rho). \]
(3) For $u = 1, \ldots, t$, compute $\Xi S_u = \Xi R \cdot \Xi PUK_u$, and get $\Theta T_u = H_0(\Xi S_u), \Theta H_1(\Theta T_u), \Theta H_2(\Theta T_u)$ and $\Theta U_u = \Theta H_1(\Theta T_u) \land (\Theta H_2(\Theta T_u) \land \Theta U)$. 
(4) Choose a new variate $\Xi \rho$ in $G_0$ and compute $\Xi \sigma = \Xi PPK_\xi + \Xi R(\Xi X + \Xi \cdot \Xi Y)$. 
(5) For $u = 1, \ldots, t$, add $(\Xi R, \Xi S_u, \Theta T_u, \Theta H_1(\Theta T_u), \Theta H_2(\Theta T_u), \Theta U_u, \Theta c, C, \Theta \rho, \Xi \sigma)$ in $L_M$. 
(6) Transform $\Xi R, \Xi \rho$ and $\Xi \sigma$ to obtain $\Theta R, \Theta \rho$ and $\Theta \sigma$. 
(7) Return $CT = (\Theta U_1, \Theta U_2, \ldots, \Theta U_t), C, \Theta R, \Theta \rho, \Theta \sigma)$. 
• **Multi-signcryption leak query:** For this Multi-signcryption query with input $M, ID_1$’s current private key $(PRK_{r_1,j-1,1}, PRK_{r_1,j-1,2})$ and $NRS = \{(ID_1, PUK_1), (ID_2, PUK_2), \ldots,(ID_s, PUK_s)\}$, $\mathcal{A}$ may request this leak query only once. Assume that $\mathcal{A}$ issues this query along with $f_{MSC,j}$ and $h_{MSC,j}$. $C$ returns leaked partial bits $\Delta f_{MSC,j} = f_{MSC,j}(PRK_{r_1,j-1,1})$ and $\Delta h_{MSC,j} = h_{MSC,j}(PRK_{r_1,j-2})$. 
• **Unsigncryption query:** Assume that $\mathcal{A}$ issues this query with input a ciphertext $CT = ((\Theta U_1, \Theta U_2, \ldots, \Theta U_t), C, \Theta R, \Theta \rho, \Theta \sigma)$ and a nominated recipient $ID_r$. Let the recipient $ID_r$’s current private key be $(PRK_{r,j-1,1}, PRK_{r,j-1,2})$. 
(1) Update the current private key $(ID_r, \Xi PUK_r, \Xi PPRK_s, \Xi PPRK_{r,j-1,1}, \Xi PPRK_{r,j-1,2})$ to $(ID_r, \Xi PUK_r, \Xi PPRK_s, \Xi PPRK_{r,j-1,1}, \Xi PPRK_{r,j-1,2})$ in $L_U$. 
(2) Transform $\Theta R$ to get $\Xi R$ in $L_0$ and compute $\Xi S = \Xi R \cdot \Xi PUK_r$. 
(3) Use $\Xi R$ and $\Xi S$ to search $(\Xi R, \Xi S, \Theta T, \Theta H_1(\Theta T), \Theta H_2(\Theta T), \Theta U, \Theta c, C, \Theta \rho, \Xi \sigma)$ in $L_M$. 
(4) Returns $\Theta c$ and $M = D_{\Theta c}(C)$. 
• **Unsigncryption leak query:** For this Unsigncryption query with input $CT$ and a nominated recipient $ID_r$ with the current private key $(PRK_{r,1,1}, PRK_{r,1,2})$, $\mathcal{A}$ may request this leak query only once. Assume that $\mathcal{A}$ issues this query along with $f_{USC,j}$ and $h_{USC,j}$. $C$ returns leaked partial bits $\Delta f_{USC,j} = f_{USC,j}(PRK_{r,1,1})$ and $\Delta h_{USC,j} = h_{USC,j}(PRK_{r,1,2})$. 
- **Forgery.** $A$ outputs a tuple $(ID_s, \Theta PUK_s, M^*, NRS, CT^* = ((\Theta U_1, \Theta U_2, \ldots, \Theta U_t), C, \Theta R, \Theta \rho, \Theta \sigma))$ to $C$. It is said that $A$ wins the security game if a recipient $ID_r \in NRS$ can obtain the message $M^*$ while verifying $CT$ signed by $ID_r$ by using the public key $PUK_s$. Note that the Multi-signcryption query on $(ID_s, M^*, NRS)$ has never been issued.

In the following, let us first evaluate the advantage $Adv_{A-w}$, that $A$ wins the LR-UF-ACMA security game without requesting any leak query. Based on the evaluation of $Adv_{A-w}$, we can evaluate the advantage $Adv_A$ that $A$ wins the LR-UF-ACMA security game with requesting the Multi-signcryption leak query and Unsigncryption leak query.

To evaluate $Adv_{A-w}$, the numbers and the maximal degrees of elements in $L_0$ and $L_1$ are first countered as follows.

(1) The total number of elements in $L_0$ and $L_1$, denoted by $|L_0| + |L_1|$, satisfies the inequality $|L_0| + |L_1| \leq 4 + \lambda_o + 3\lambda_{ms} \leq 3\lambda$ due to the following argumentations. 
- There are 3 and 1 elements that are initially recorded in $L_0$ and $L_1$, respectively.
- Let $\lambda_o$ denote the total times of issuing $O_0, O_1$ and $O_2$ queries. Then, at most $\lambda_o$ elements are recorded in $L_0$ or $L_1$.
- Let $\lambda_{ms}$ denote the times of issuing the Multi-signcryption query. Then, at most $3\lambda_{ms}$ elements are recorded in $L_0$ or $L_1$.

(2) In $L_0$, the maximal degree is 3 due to the following argumentations.
- In the Setup phase, $\Xi g_0, \Xi X$ and $\Xi Y$ have degree 1.
- In the $O_q$ query, $\Xi g_0,q,n,k$ has the maximal degree of $\Xi g_0,q,n,i$ and $\Xi g_0,q,n,j$.
- In the Multi-signcryption query, $\Xi R, \Xi S_u, \Xi \rho$ and $\Xi \sigma$ have degrees 1, 2, 1 and 3, respectively.

(3) In $L_1$, the maximal degree is 6 due to the following argumentations.
- In the Setup phase, $\Xi g_1$ has degree 1.
- In the $O_1$ query, $\Xi g_1,q,n,k$ has the maximal degree of $\Xi g_1,q,n,i$ and $\Xi g_1,q,n,j$.
- In the $O_2$ query, $\Xi g_1,q,n,k$ has degree 6 since both $\Xi g_0,q,n,i$ and $\Xi g_0,q,n,j$ have degree 3 in $L_0$ and $\Xi g_1,q,n,k = \Xi g_0,q,n,i = \Xi g_0,q,n,j$.

**Evaluation of $Adv_{A-w}$:** If one of the following two circumstances occurs, $A$ wins the LR-UF-ACMA security game.

**Circumstance 1:** $A$ discovers a collision in $L_0$ or $L_1$, with its probability denoted by $Pr[C - 1]$. Let’s first measure the collision probability in $L_0$. Assume that the amount of all variates in $L_0$ is $a$. Then choose a random values $r_i \in Z_p^*$ for $i = 1, 2, \ldots, a$. Assume that $\Xi g_{0,j}$ and $\Xi g_{0,k}$ are two distinct polynomials in $L_0$ and compute $\Xi g_{0,j}(r_1, r_2, \ldots, r_i) = \Xi g_{0,j} - \Xi g_{0,k}$. If $\Xi g_{0,i}(r_1, r_2, \ldots, r_i) = 0$, the collision in $L_0$ occurs. By Lemma 2, the probability is at most $3/p$ since $L_0$ has the maximal polynomial degree 3 and no partial bits $(\tau = 0)$ are leaked to attackers. Additionally, there are $(\mid L_0^t\mid)$ different pairs of $(\Xi g_{0,i}, \Xi g_{0,k})$ so that the collision probability in $L_0$ is $(3/p)(\mid L_0^t\mid)$. By similar arguments, the collision probability in $L_1$ is $(6/p)(\mid L_1^t\mid)$. Since $|L_0| + |L_1| \leq 3\lambda$, we have 
$$Pr[C - 1] \leq \frac{3}{p}(\frac{|L_0|}{2} + \frac{6}{p}(\frac{|L_1|}{2}) \leq \frac{6}{p}(\frac{|L_0| + |L_1|)^2}{2} \leq 54\lambda^2/p.$$
\(\Theta R, \Theta \sigma, \Theta \sigma\), with its probability denoted by \(\Pr[C - 2]\). 
\(\mathcal{C}\) transforms \(\Theta PUK_{i}, \Theta R, \Theta \sigma\) and \(\Theta \sigma\) to obtain their polynomials \(\Sigma PUK_{i}, \Sigma R, \Sigma \rho\) and \(\Sigma \sigma\). A valid tuple must satisfy the equality \(\Sigma g_{0} = \Sigma g_{0} = \Sigma PUK_{i} + \Sigma R - (\Sigma X + \Sigma Y \cdot \Sigma \rho)\), namely, \(\Sigma f = \Sigma g_{0} - \Sigma \sigma - \Sigma PUK_{i} + \Sigma R - (\Sigma X + \Sigma Y \cdot \Sigma \rho) = 0\). Since \(\Sigma f\) has degree at most 3, the probability is at most \(3/p\) by Lemma 2, namely, \(\Pr[C - 2] = 3/p\).

By the arguments above, \(Adv_{A-w} = \Pr[C - 1] + \Pr[C - 2] \leq 54\lambda^{2}/p + 3/p = O(\lambda^{2}/p)\), and \(Adv_{A-w}\) is negligible if \(\lambda = poly(\log p)\).

**Evaluation of \(Adv_{A}\):** Based on the evaluation of \(Adv_{A-w}\), we can evaluate the advantage \(Adv_{A}\) that \(\mathcal{A}\) wins the LR-UC-ACMA security game with requesting the *Multi-signcryption leak query* and *Unsigncryption leak query*.

(1) By the *Multi-signcryption leak query*, \(\mathcal{A}\) can acquire partial bits of the sender ID\(_{r}\)'s current private key \((PRK_{r,i,1}, PRK_{r,i,2})\), namely, \(\Delta_{\text{MSC},i} = f_{\text{MSC},i}(PRK_{r,i,1})\) and \(\Delta_{\text{MSC},i} = h_{\text{MSC},i}(PRK_{r,i,2})\) such that \(|f_{\text{MSC},i}|, |h_{\text{MSC},i}| \leq \tau\). By the multiplicative blinding technique, we have \(PRK_{r} = PRK_{r,0,1}, PRK_{r,0,2,1} = PRK_{r,0,1,1} \cdot PRK_{r,0,1,2} = \ldots = PRK_{r,0,1,1} \cdot PRK_{r,0,1,2}\). Additionally, leaked bits of \(PRK_{r,i-1,1}\) and \(PRK_{r,i-1,2}\) are independent of these bits of \(PRK_{r,i-1,1}\) and \(PRK_{r,i-1,2}\). Hence, \(\mathcal{A}\) acquires at most 2\(\tau\) bits of \(PRK_{r}\).

(2) By the *Unsigncryption leak query*, \(\mathcal{A}\) may acquire partial bits of the receiver ID\(_{r}\)'s current private key \((PRK_{r,i,1}, PRK_{r,i,2})\), namely, \(\Delta_{\text{USC},i} = f_{\text{USC},i}(PRK_{r,i,1})\) and \(\Delta_{\text{USC},i} = h_{\text{USC},i}(PRK_{r,i,2})\) such that \(|f_{\text{USC},i}|, |h_{\text{USC},i}| \leq \tau\). By the multiplicative blinding technique, we have \(PRK_{r} = PRK_{r,0,1}, PRK_{r,0,2,1} = PRK_{r,0,1,1} \cdot PRK_{r,0,1,2} = \ldots = PRK_{r,0,1,1} \cdot PRK_{r,0,1,2}\). Additionally, leaked bits of \(PRK_{r,i-1,1}\) and \(PRK_{r,i-1,2}\) are independent of these bits of \(PRK_{r,i-1,1}\) and \(PRK_{r,i-1,2}\). Hence, \(\mathcal{A}\) acquires at most 2\(\tau\) bits of \(PRK_{r}\).

By the arguments above, we define two events below.

(1) Let \(EVPRK\) denote the event that \(\mathcal{A}\) acquires \(PRK_{u}\) (i.e., \(PRK_{u}\) or \(PRK_{r}\)) by \(\Delta_{\text{MSC},i}, \Delta_{\text{USC},i}, \Delta_{\text{MSC},i}\), and \(\Delta_{\text{USC},i}\). Also, \(EVPRK\) is the complement event of \(EVPRK\).

(2) Let \(EVF\) denote the event that \(\mathcal{A}\) forges a valid tuple \((ID_{s}, \Theta PUK_{s}, M^{*}, NRS, CT^{*} = \langle \langle \Theta U_{1}, \Theta U_{2}, \ldots, \Theta U_{i}\rangle, C, \Theta R, \Theta \rho, \Theta \sigma\rangle\).

Hence, \(Adv_{A}\) satisfies

\[
Adv_{A} = \Pr[EVF] = \Pr[EVF \land \neg EVPRK] + \Pr[EVF \land \neg EVPRK] \leq \Pr[EVPRK] + \Pr[EVF \land \neg EVPRK].
\]

By the *Multi-signcryption leak query* or *Unsigncryption leak query*, \(\mathcal{A}\) acquires at most 2\(\tau\) bits of \(PRK_{u}\) (i.e., \(PRK_{u}\) or \(PRK_{r}\)). By Lemma 2, we have \(\Pr[EVPRK] \leq Adv_{A-w} \cdot 2^{2\tau} \leq O(\lambda^{2}/p) \cdot 2^{2\tau}\) due to \(Adv_{A-w} = O(\lambda^{2}/p)\). The probability \(\Pr[EVF \land \neg EVPRK]\) indicates that \(\mathcal{A}\) acquires no useful information about \(PRK_{u}\) so that \(\Pr[EVF \land \neg EVPRK] = Adv_{A-w} = O(\lambda^{2}/p)\). Hence, we have

\[
Adv_{A} \leq \Pr[EVPRK] + \Pr[EVF \land \neg EVPRK] \leq O(\lambda^{2}/p) + O(\lambda^{2}/p) = O(\lambda^{2}/p) \cdot 2^{2\tau}.
\]

By Lemma 2, \(Adv_{A}\) is negligible if \(\lambda = poly(\log p)\). □

**Theorem 2:** Under the GBG model and hash function assumption, the proposed PKI-LR-AMRSC scheme is LR-IND-CCA-secure.

**Proof:** In the LR-IND-CCA security game played by an attacker \(\mathcal{A}\) and a challenger \(C\), there are four phases as given below.

- **Setup.** The phase is the same with the *Setup* phase in the proof of Theorem 1.
- **Query.** The phase is the same with the *Query* phase in the proof of Theorem 1.
- **Challenge.** In this phase, \(\mathcal{A}\) sends a message pair \((M_{0}, M_{1})\) and a nominated recipient set NRS to \(C\), where \(NRS = \{ID_{1}, ID_{2}, ID_{3}\}, \ldots, (ID_{t}, ID_{4})\) \}. \(C\) selects a random bit \(b \in \{0, 1\}\) and returns \(CT^{*} = \text{MSC}(M_{b}, (PRK_{s,1,1}, PRK_{s,1,2}), (PRK_{1,1}, PRK_{2,1}, \ldots, PRK_{t,1}))\) to \(\mathcal{A}\).
- **Guess.** \(\mathcal{A}\) outputs \(b' \in \{0, 1\}\) and wins the game if \(b' = b\). The advantage that \(\mathcal{A}\) wins the game is defined as \(Adv_{A} = |\Pr[b' = b'\}| - 1/2\).

Let \(Adv_{A-w}\) denote the advantage that \(\mathcal{A}\) wins the LR-IND-CCA security game without requesting any leak query. Also, let \(Adv_{A}\) denote the advantage that \(\mathcal{A}\) wins the LR-IND-CCA security game with requesting the Multi-signcryption leak query and Unsigncryption leak query.

**Evaluation of \(Adv_{A-w}\):** If one of the following two circumstances occurs, \(\mathcal{A}\) wins the LR-IND-CCA security game.

**Circumstance 1:** \(\mathcal{A}\) discovers a collision in \(L_{0}\) or \(L_{1}\), with the probability denoted by \(\Pr[C - 1]\). By similar arguments of Circumstance 1 in the proof of Theorem 1, we have \(\Pr[C - 2] = 54\lambda^{2}/p\).

**Circumstance 2:** In this circumstance, we evaluate the probability of \(b' = b\) in the Guess phase, and clearly we have the probability \(\Pr[C - 2] \leq 1/2\).

By the arguments above, we obtain \(Adv_{A-w} \leq |\Pr[C - 1]| + \Pr[C - 2] - 1/2 = 54\lambda^{2}/p = O(\lambda^{2}/p)\), and so \(Adv_{A-w}\) is negligible if \(\lambda = poly(\log p)\).

**Evaluation of \(Adv_{A}\):** Based on the evaluation of \(Adv_{A-w}\), we evaluate the advantage \(Adv_{A}\) that \(\mathcal{A}\) wins the LR-IND-CCA security game with requesting the Multi-signcryption leak query and Unsigncryption leak query. It is obvious that if a user’s private key \(PRK_{u}\) (i.e., \(PRK_{u}\) or \(PRK_{r}\)) was obtained, the challenge message \(M_{b}\) (i.e., \(M_{0}\) or \(M_{1}\)) would be correctly decrypted. There are two events as discussed below.
TABLE 1. Comparisons between the related schemes and our scheme.

| Scheme          | Public-key setting | Cost of Multi-signcryption algorithm | Cost of Unsigncryption algorithm | Recipient anonymity | Ability of withstanding side-channel attacks | Leakage-unbounded property |
|-----------------|--------------------|-------------------------------------|----------------------------------|---------------------|---------------------------------------------|----------------------------|
| Yu et al.’s scheme [27] | PKI-based          | $O(t^2)$                            | $O(t)$                           | No                  | No                                          | No                         |
| Wang et al.’s scheme [11] | PKI-based          | $O(t^2)$                            | $O(t)$                           | Yes                 | No                                          | No                         |
| Pang et al.’s scheme [39] | ID-based           | $O(t^2)$                            | $O(t)$                           | Yes                 | No                                          | No                         |
| Pang et al.’s scheme [44] | Certificateless    | $O(t^2)$                            | $O(t)$                           | Yes                 | No                                          | No                         |
| The proposed scheme | PKI-based          | $O(t)$                             | $O(1)$                           | Yes                 | Yes                                         | Yes                        |

(1) Let $EVPRK$ represent the event that $A$ acquires $PRK_{id}$ (i.e., $PRK_s$ or $PRK_r$) by $\Delta f_{MSC,i}$, $\Delta h_{MSC,i}$, $\Delta f_{USC,j}$ and $\Delta h_{USC,j}$. Also, $EVPKR$ is the complement event of $EVPRK$.

(2) Let $EVB$ represent the event that $A$ outputs a random bit $b' = b$.

By the two events defined above, $Adv_A$ satisfies

$$Adv_A = |Pr[EVB] - 1/2| = |Pr[EVB \land EVPRK] + Pr[EVB \land EVPKR] - 1/2| \leq |Pr[EVPRK] + Pr[EVB \land EVPKR] - 1/2| \leq O((\lambda^2/p) \cdot 2^{2t}).$$

By similar arguments in the proof of Theorem 1, we have $Pr[EVPRK] \leq O((\lambda^2/p) \cdot 2^{2t})$. The probability $Pr[EVB \land EVPKR]$ indicates that $A$ acquires no useful information about $PRK_{id}$ so that $Pr[EVB \land EVPKR] = 1/2$. Therefore, $Adv_A \leq |Pr[EVPRK] + Pr[EVB \land EVPKR] - 1/2| \leq O((\lambda^2/p) \cdot 2^{2t})$. □

**Theorem 3:** Under the GBG model and hash function assumption, the proposed PKI-LR-AMRSC scheme is LR-ANON-CCA-secure.

**Proof:** In the LR-ANON-CCA security game played by an attacker $A$ and a challenger $C$, there are four phases as given below.

- **Setup.** The phase is the same with the Setup phase in the proof of Theorem 1.
- **Challenge.** The phase is the same with the Query phase in the proof of Theorem 1.
- **Challenge.** In this phase, $A$ sends a message $M$ and a nominated recipient set $MRS$ to $C$, where $NRS = \{(ID_1, PK_{id_1}), (ID_2, PK_{id_2}), \ldots, (ID_t, PK_{id_t})\}$. $C$ selects a random bit $b \in \{1, 2\}$ and returns $CT^* = MSC(M, PRK_{id_1}, PRK_{id_2}, \ldots, PRK_{id_t})$ to $A$.
- **Guess.** $A$ outputs $b' \in \{1, 2\}$ and wins the game if $b' = b$. The advantage that $A$ wins the game is defined as $Adv_A = |Pr[b = b'] - 1/2|$. Let $Adv_{A-W}$ denote the advantage that $A$ wins the LR-ANON-CCA security game without requesting any leak query. Also, let $Adv_{A}$ denote the advantage that $A$ wins the LR-ANON-CCA security game with requesting the Multi-signcryption leak query and Unsigncryption leak query.

TABLE 2. Comparisons of public key and ciphertext sizes between the related schemes and our scheme.

| Scheme          | Public-key size | Ciphertext size |
|-----------------|-----------------|-----------------|
| Yu et al.’s scheme [27] | $|G_o|$ | $(t+1)|Z_p| + |G_o|$ |
| Wang et al.’s scheme [11] | $|G_o|$ | $(t+7)|Z_p| + 3|G_o|$ |
| Pang et al.’s scheme [39] | $|G_o|$ | $(t+1)|Z_p| + 3|G_o|$ |
| Pang et al.’s scheme [44] | $2|G_o|$ | $(t+2)|Z_p| + 3|G_o|$ |
| The proposed scheme | $|G_o|$ | $(t+2)|Z_p| + 2|G_o|$ |

By similar arguments in the proof of Theorem 2, we can obtain $Adv_{A-W} = O(\lambda^2/p)$ and $Adv_A \leq Adv_{A-W} \cdot 2^{2t} = O(\lambda^2/p) \cdot 2^{2t}$. □

**VI. COMPARISONS**

Table 1 lists the comparisons among the proposed PKI-LR-AMRSC scheme with PKI-MRSC, PKI-AMRSC, ID-AMRSC and CL-AMRSC schemes [11], [27], [39], [44] in terms of the public-key setting, the cost of multi-signcryption algorithm, the cost of unsigncryption algorithm, recipient anonymity, the ability of withstanding side-channel attacks, and leakage-unbounded property. For recipients of the schemes in [11], [27], [39], and [44], a sender computes a key $k_r$ by using each recipient $ID_r$’s public key (for $r = 1, 2, \ldots, t$), and produces a Lagrange polynomial of degree $t$, $f(x) = \prod_{i=1}^{t}(x - k_r) + ck(mod p) = b_0 + b_1x + \ldots + b_{t-1}x^{t-1} + x^t$, where $t$ is the number of recipients and $ck$ is a cipher key selected by the sender. Afterwards, each recipient $ID_r$ may use her/his private key to compute the corresponding key $k_r$ and the encryption key $ck = f(k_r)$. Hence, the required costs of the multi-encryption and unsigncryption algorithms, respectively, are quadric and linear with $t$. In our scheme, the required cost of the multi-encryption algorithm is linear with $t$, whereas the required cost of the unsigncryption algorithm is constant. That is, the computational complexities of our scheme, respectively, require only $O(t)$ and $O(1)$ in executing the Multi-signcryption algorithm and the Unsigncryption algorithm. The point is that the proposed scheme is the first LR-AMRSC scheme withstanding side-channel attacks and possesses leakage-unbounded property even though some bilinear pairing operations are...
required. Additionally, Table 2 lists the comparisons between our LR-AMRSC scheme with PKI-MRSC, PKI-AMRSC, ID-AMRSC and CL-AMRSC schemes [11], [27], [39], [44] in terms of public key size and ciphertext size. Indeed, all schemes have $O(t)$ complexity. Next, let’s discuss the computational cost saving for the Multi – signcryption algorithm. We first refer to the literature [72] to define $T_m$, $T_e$ and $T_h$ as the cost of performing an exponentiation operation, a multiplication operation and a hash operation, respectively. Following the simulation results [73], we have $T_m = 2.758$ ms, $T_e = 0.4746$ ms and $T_h = 0.0126$ ms. Hence, our scheme requires $5T_m + 5T_e + 2T_h + t(T_e + 3T_h) = 16.1882 + t \cdot 0.5124$ ms for $t$ recipients on the Multi – signcryption algorithm. According to similar analysis of computational cost saving [74], we compute the computational cost saving of performing the Multi-signcryption algorithm as $[(t \cdot 16.1882 + t \cdot 0.5124) – (16.1882 + t \cdot 0.5124)]/(t \cdot 16.1882 + t \cdot 0.5124)$ for $t = 1, 2, 4, 6, 8$ and 10 in Table 3.

VII. CONCLUSION AND FUTURE WORK

Indeed, up to date, there exists no multi-recipient signcryption (MRSC) or anonymous MRSC (AMRSC) schemes with leakage-resilient property. In the paper, we have proposed the first PKI-based leakage-resilient AMRSC (PKI-LR-AMRSC) scheme under the continual leakage model. A new security model of PKI-LR-AMRSC schemes was defined, which consists of three security games, namely, LR-EUF-ACMA, LR-IND-CCA and LR-ANON-CCA. In these security games, both the Multi-signcryption leak query and the Unsigncryption leak query are used to simulate an attacker’s leakage ability. In the proposed scheme, an attacker is permitted to continually acquire partial bits of users’ private keys participated in cryptographic computations (i.e., Multi-signcryption and Unsigncryption algorithms) by the Multi-signcryption leak query and the Unsigncryption leak query. According to the LR-EUF-ACMA, LR-IND-CCA and LR-ANON-CCA security games, three theorems have been demonstrated to show that the proposed PKI-LR-AMRSC scheme are LR-EUF-ACMA-secure, LR-IND-CCA-secure and LR-ANON-CCA-secure against attackers, respectively. In the future, we expect that the research of leakage-resilient MRSC and AMRSC schemes based on ID-based or certificateless cryptography would become a significant topic.

REFERENCES

[1] Y. Dodis and N. Fazio, “Public key broadcast encryption for stateless receivers,” in Proc. DRM, in Lecture Notes in Computer Science, vol. 2696, 2002, pp. 61–80.
[2] D. Boneh, C. Gentry, and B. Waters, “Collusion resistant broadcast encryption with short ciphertexts and private keys,” in Proc. CRYPTO, in Lecture Notes in Computer Science, vol. 3621, 2005, pp. 258–275.
[3] K. Kurosawa, “Multi-recipient public-key encryption with shortened ciphertext,” in Proc. PKC, in Lecture Notes in Computer Science, vol. 2274, 2002, pp. 48–63.
[4] M. Bellare, A. Boldyreva, and D. Pointcheval, “Multi-recipient encryption schemes: Security notions and randomness re-use,” in Proc. PKC, in Lecture Notes in Computer Science, vol. 2567, 2003, pp. 85–99.
[5] S. Islam, N. Muslim, and J. W. Atwood, “A survey on multicasting in software-defined networking,” IEEE Commun. Surveys Tuts., vol. 20, no. 1, pp. 355–387, 1st Quart., 2018.
[6] S. Pizzi, C. Suraci, A. Iera, A. Molinaro, and G. Araniti, “A sideline-aided approach for secure multicast service delivery: From human-oriented multimedia traffic to machine type communications,” IEEE Trans. Broadcast., vol. 67, no. 1, pp. 313–323, Mar. 2021.

7. Y. Zheng, “Digital signcryption or how to achieve cost(signature & encryption) ≪ cost(signature) + cost(encrypting),” in Proc. Annu. Int. Crytlog. Conf., in Lecture Notes in Computer Science, vol. 1294, 1997, pp. 165–179.

8. Y. Zheng, “Signcryption and its applications in efficient public key solutions,” in Proc. Int. Workshop Inf. Security, in Lecture Notes in Computer Science, vol. 1396, 1998, pp. 291–312.

9. L. Harn, C.-C. Chang, and H.-L. Wu, “An anonymous multi-receiver encryption based on RSA,” Int. J. Netw. Secur., vol. 15, no. 4, pp. 307–312, 2013.

10. M. Zhang and T. Takagi, “Efficient constructions of anonymous multireceiver encryption protocol and their deployment in group E-mail systems with privacy preservation,” IEEE Syst. J., vol. 7, no. 3, pp. 410–419, Sep. 2013.

11. Q. Wang, M. He, and X. Zheng, “Privacy-preserving communication for vehicular with multi receiver conditionally anonymously ring signcryption,” in Proc. 3rd Int. Conf. Mater. Eng., Manuf. Technol. Control, 2016, pp. 496–501.

12. P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in Proc. CRYPTO, in Lecture Notes in Computer Science, vol. 1666, 1999, pp. 388–397.

13. D. Brumley and D. Boneh, “Remote timing attacks are practical,” Comput. Netw., vol. 48, no. 5, pp. 701–716, 2005.

14. E. Bihani, Y. Carmeli, and A. Shamir, “Bug attacks,” in Proc. CRYPTO, in Lecture Notes in Computer Science, vol. 5157, 2008, pp. 221–240.

15. D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” in Proc. CRYPTO, in Lecture Notes in Computer Science, vol. 2139, 2001, pp. 213–229.

16. S. Al-Riyami and K. Paterson, “Certificateless public key cryptography,” in Proc. ASIACRYPT, in Lecture Notes in Computer Science, vol. 2849, 2003, pp. 452–473.

17. A. Yavuz, F. Alagz, and E. Anarim, “SAT05–6: NAMEPS–N-tier satellite multiscar security protocol based on signcryption schemes,” in Proc. IEEE Globecom, Nov./Dec. 2006, pp. 1–6.

18. H. M. Elkamchouchi, A.-A.-M. Emarah, and E. A. A. Hagras, “A new efficient public key multi-message multi-recipient signcryption (PK-MM-MRSC) scheme for provable secure communications,” in Proc. Int. Conf. Comput. Eng. Syst., Nov. 2007, pp. 89–94.

19. Y. Han and X. Gui, “Multi-recipient signcryption for secure group communication,” in Proc. 4th IEEE Conf. Ind. Electron. Appl., May 2009, pp. 161–165.

20. H. Elkamchouchi, M. Nasr, and R. Ismail, “A new efficiently public verifiable signature scheme and its multiple recipients variant for firewalls implementation,” in Proc. Nat. Radio Sci. Conf., Mar. 2009, pp. 1–9.

21. F. Ahmed, A. Masood, and F. Kaura, “An efficient multi recipient signcryption scheme offering non repudiation,” in Proc. 10th IEEE Int. Conf. Comput. Inf. Technol., Jun. 2010, pp. 1577–1581.

22. F. Li, Y. Hu, and S. Liu, “Efficient and provably secure multi-recipient signcryption from bilinear pairings,” Wuhan Univ. J. Natural Sci., vol. 12, no. 1, pp. 17–20, Jan. 2007.

23. Y. Han, X. Gui, X. Yang, and H. Yang, “Parallel multi-recipient signcryption for multicast networks,” in Proc. 3rd Int. Workshop Educ. Technol. Comput. Sci., 2010, pp. 128–131.

24. Y. Han, X. Yang, and Y. Hu, “Signcryption based on elliptic curve and its multi-party schemes,” in Proc. 3rd Int. Conf. Inf. Secur., 2004, pp. 216–217.

25. I. Ullah, N. Ul-Amin, H. Khattak, S. Ullah, and A. Khan, “Multi receiver proxy signcryption based on hyper elliptic curve cryptography,” Int. J. Comput. Sci. Inf. Secur., vol. 14, no. 12, pp. 1003–1008, 2016.

26. A. Sadat, R. Ahmad, I. Ullah, H. Khattak, and S. Ullah, “Multi-receiver signcryption based on hyper elliptic curve cryptosystem,” J. Appl. Environ. Biol. Sci., vol. 7, no. 12, pp. 194–200, 2017.

27. X. Yu, W. Zhao, and D. Tang, “Efficient and provably secure multi-receiver signcryption scheme using implicit certificate in edge computing,” J. Syst. Archit., vol. 126, May 2022, Art. no. 102457.
S. Selvi, S. Vivek, R. Gopalakrishnan, N. Karuturi, and C. Rangan, “Cryptanalysis of ID-based signcryption for multiple receivers,” in Proc. Int. Cryptol. ePrint Arch., vol. 2008, Art. no. 228.

F. Li, X. Xiong, and X. Nie, “A new multi-receiver ID-based signcryption scheme for group communications,” in Proc. Int. Conf. Autonomic Trusted Comput., in Lecture Notes in Computer Science, vol. 4610, 2007, pp. 13–21.

S. Selvi, S. Vivek, R. Gopalakrishnan, N. Karuturi, and C. Rangan, “Cryptanalysis of ID-based signcryption scheme for multiple receivers,” IACR Cryptol. ePrint Arch., vol. 2008, Art. no. 228.

J.-D. Wu, Y.-M. Tseng, and S.-S. Huang, “An identity-based authenticated key exchange protocol resilient to continuous key leakage,” IEEE Syst. J., vol. 13, no. 4, pp. 3968–3979, Dec. 2019.

J.-D. Wu, Y.-M. Tseng, S.-S. Huang, and T.-T. Tsai, “ Leakage-resilient revocable identity-based signature with cloud revocation authority,” in Proc. IEEE Conf. Inf. Sci., vol. 31, no. 3, pp. 597–620, 2020.

Y. Tseng, J.-D. Wu, S.-S. Huang, and T.-T. Tsai, “ Leakage-resilient output revocable certificateless signature with a cloud revocation server,” Infor. Technol. Control, vol. 49, no. 4, pp. 464–481, Dec. 2020.

T.-C. Hsieh, Y.-M. Tseng, and S.-S. Huang, “A leakage-resilient certificateless authenticated key exchange protocol withstanding side-channel attacks,” IEEE Access, vol. 8, pp. 121795–121810, 2020.

T.-T. Tsai, Y.-H. Chuang, Y.-M. Tseng, S.-S. Huang, and Y.-H. Hung, “A leakage-resilient ID-based authenticated key exchange protocol with a revocation mechanism,” IEEE Access, vol. 9, pp. 128633–128647, 2021.

A.-L. Peng, Y.-M. Tseng, and S.-S. Huang, “An efficient leakage-resilient authenticated key exchange protocol suitable for IoT devices,” IEEE Syst. J., vol. 15, no. 4, pp. 5343–5354, Dec. 2021.

Q. Yu, J. Li, and S. Ji, “Fully secure ID-based signature scheme with continuous leakage resilience,” Secur. Commun. Netw., vol. 2022, pp. 1–12, Jan. 2022.

E. Kiltz and K. Pietrzak, “Leakage resilient ElGamal encryption,” in Proc. ASIACRYPT, in Lecture Notes in Computer Science, vol. 6477, 2010, pp. 595–612.

D. Galindo, J. Großschädl, Z. Liu, P. K. Vadnala, and S. Vivek, “Implementation of a leakage-resilient ElGamal key encapsulation mechanism,” J. Cryptograph. Eng., vol. 6, no. 3, pp. 229–238, Sep. 2016.

Z. Brakerski, Y. T. Kalai, J. Katz, and V. Vaikuntanathan, “ Cryptography resilient to continual memory leakage,” in Proc. 51st Annu. IEEE Symp. Found. Comput. Sci., Oct. 2010, pp. 501–510.

T.-H. Yuen, S. S. M. Chow, Y. Zhang, and S.-M. Yu, “Identity-based encryption resilient to continual auxiliary leakage,” in Proc. EUROCYPTR, in Lecture Notes in Computer Science, vol. 7237, 2012, pp. 117–134.

J. Li, Y. Guo, Q. Yu, Y. Lu, and Y. Zhang, “Provably secure identity-based encryption resilient to post-challenge continuous auxiliary input leakage,” Secur. Commun. Netw., vol. 9, no. 10, pp. 1016–1024, 2016.

J. Li, Q. Yu, and Y. Zhang, “Identity-based broadcast encryption with continuous leakage resilience,” Inf. Sci., vol. 429, pp. 177–193, Mar. 2018.

Y. Guo, J. Li, Y. Lu, Y. Zhang, and F. Zhang, “Provably secure certificate-based encryption with leakage resilience,” Theor. Comput. Sci., vol. 711, pp. 1–10, Feb. 2018.

H. Xiong, T. H. Yuen, C. Zhang, S. M. Yu, and Y.-J. He, “Leakage-resistant certificateless public key encryption,” in Proc. 1st ACM Workshop Asia Public-Key Cryptogr. (AsiaPKC), 2013, pp. 13–22.

J.-D. Wu, Y.-M. Tseng, S.-S. Huang, and W.-C. Chou, “Leakage-resistant certificateless key encapsulation scheme,” Informatica, vol. 29, no. 1, pp. 125–155, Jan. 2018.

Y.-M. Tseng, S.-S. Huang, T.-T. Tsai, Y.-H. Chuang, and Y.-H. Hung, “Leakage-resistant revocable certificateless encryption with an outsourced revocation authority,” Informatica, vol. 33, no. 1, pp. 151–179, 2019.

J. Li, Q. Yu, and Y. Zhang, “Key-policy attribute-based encryption against continual auxiliary input leakage,” Inf. Sci., vol. 470, pp. 175–188, Jan. 2019.

J. Li, Q. Yu, and Y. Zhang, “Hierarchical attribute based encryption with continuous leakage-resilience,” Inf. Sci., vol. 484, pp. 113–134, May 2019.

D. Boneh, X. Boyen, and E. J. Goh, “Hierarchical identity based encryption with constant size ciphertext,” in Proc. EUROCYPTR, in Lecture Notes in Computer Science, vol. 3494, 2005, pp. 440–456.

Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” SIAM J. Comput., vol. 38, no. 1, pp. 97–139, 2008.

L. Pang, H. Li, L. Gao, and Y. Wang, “Completely anonymous multi-reipient signcryption scheme with public verification,” PLoS ONE, vol. 8, no. 5, May 2013, Art. no. e63562.

Y. Li, Q. Cheng, X. Li, and X. Li, “A secure anonymous identity-ased scheme in new authentication architecture for mobile edge computing,” IEEE Syst. J., vol. 15, no. 1, pp. 935–946, Mar. 2021.
TUNG-TSO TSAI received the Ph.D. degree from the Department of Mathematics, National Changhua University of Education, Taiwan, in 2014, under the supervision of Prof. Yuh-Min Tseng. He is currently an Assistant Professor at the Department of Computer Science and Engineering, National Taiwan Ocean University, Taiwan. His research interests include applied cryptography, pairing-based cryptography, and leakage-resilient cryptography.

YUH-MIN TSENG (Member, IEEE) is currently the Vice President and a Professor at the Department of Mathematics, National Changhua University of Education, Taiwan. He has published over 100 scientific journal articles on various research areas of cryptography, security, and computer networks. His research interests include cryptography, network security, computer networks, and leakage-resilient cryptography. He is a member of IEEE Computer Society, IEEE Communications Society, and the Chinese Cryptology and Information Security Association (CCISA). He serves as the editor for several international journals.

SEN-SHAN HUANG received the Ph.D. degree from the University of Illinois at Urbana–Champaign, in 1997, under the supervision of Prof. Bruce C. Berndt. He is currently a Professor at the Department of Mathematics, National Changhua University of Education, Taiwan. His research interests include number theory, cryptography, and leakage-resilient cryptography.

JIA-YI XIE received the B.S. and M.S. degrees in mathematics from the National Changhua University of Education, Taiwan, in 2020 and 2022, respectively. Her research interests include applied cryptography, information security, network security, and leakage-resilient cryptography.

YING-HAO HUNG received the Ph.D. degree from the Department of Mathematics, National Changhua University of Education, Taiwan, in 2017, under the supervision of Prof. Yuh-Min Tseng. His research interests include applied cryptography and pairing-based cryptography.