Symmetry **2015**, *7*, 1856-1881; doi:10.3390/sym7041856

OPEN ACCESS

symmetry

ISSN 2073-8994

www.mdpi.com/journal/symmetry

Article

Anonymous Multi-Receiver Identity-Based Authenticated Encryption with CCA Security

Chun-I Fan * and Yi-Fan Tseng

Department of Computer Science and Engineering, National Sun Yat-sen University, No. 70, Lienhai Road, Kaohsiung 804, Taiwan; E-Mail: yftseng1989@gmail.com

* Author to whom correspondence should be addressed; E-Mail: cifan@mail.cse.nsysu.edu.tw; Tel.: +886-7525-2000 (ext. 4346); Fax: +886-7525-4301.

Academic Editor: Vladimir Shpilrain

Received: 12 September 2015 / Accepted: 8 October 2015 / Published: 16 October 2015

Abstract: In a multi-receiver encryption system, a sender chooses a set of authorized receivers and sends them a message securely and efficiently, as the message is well encrypted and only one ciphertext corresponding to the message is generated no matter how many receivers the sender has chosen. It can be applied to video conferencing systems, pay-per-view channels, remote education, and so forth. Due to privacy considerations, an authorized receiver may not expect that his identity is revealed. In 2010, anonymous multi-receiver identity-based (ID-based) encryption was first discussed, and furthermore, many works on the topic have been presented so far. Unfortunately, we find that all of those schemes fail to prove the chosen ciphertext attacks (CCA) security in either confidentiality or anonymity. In this manuscript, we propose the first anonymous multi-receiver ID-based authenticated encryption scheme with CCA security in both confidentiality and anonymity. In the proposed scheme, the identity of the sender of a ciphertext can be authenticated by the receivers after a successful decryption. In addition, the proposed scheme also is the first CCA-secure one against insider attacks. Moreover, only one pairing computation is required in decryption.

Keywords: anonymity; multi-receiver encryption; chosen-ciphertext attacks; identity-based encryption; bilinear pairing

---

1. Introduction

Multi-receiver encryption makes it possible for a sender to compute and transmit only one ciphertext corresponding to a message for multiple receivers. It greatly decreases communication cost, so that it is popular among some advanced services, such as video conferencing, pay-per-view TV [1–3] and remote education. In order to prevent unauthorized access, messages are encrypted, and the encryption keys change every session. When a new member joins the communication group, the system will assign a long-term key to him, and the key will be revoked once the member leaves the group. The system must deal with key management effectively. Another important issue in such services is the authentication of the sender, which can guarantee the source and legality of the digital products. Many researchers focused on this topic and have proposed interesting results [4–6].

In 2001, Boneh and Franklin [7] first proposed an ID-based encryption scheme from the Weil pairing. In 2005, Du *et al.* [6] presented an ID-based broadcast encryption scheme for key distribution. They used matrix operations for encryption and decryption. In 2005, Wang and Wu [5] proposed an ID-based multicast encryption scheme, which has a key generation center and a group center. No users need any computation during the rekeying process. However, the sender must be the group center. In the same year, Baek *et al.* [4] proposed a multi-receiver ID-based encryption scheme along with a formal definition and security model for this kind of scheme. They proved the security in the selective ID model using random oracles [8]. Their second scheme was employed in the REACT technique proposed by Okamoto and Pointcheval [9].

In some situations, such as ordering sensitive TV programs, the customers may expect that their identities are not revealed. In consideration of protecting users' privacy, Fan *et al.* [10] first introduced the concept of anonymous mutli-receiver ID-based encryption (AMRIBE) in 2010. They also proposed a multi-receiver ID-based encryption scheme using Lagrange interpolating polynomials in order to achieve anonymity for every receiver such that nobody knows who the receivers are except the sender. However, Chien [11] pointed out that Fan *et al.*'s scheme does not hold the anonymity. An attacker can identify the identity of a receiver. Chien indicated that the security model defined in [10] does not cover all of the multi-receiver environments. Additionally, he also proposed an improved AMRIBE scheme.

Recently, many results of AMRIBE have been proposed [11–31]. After examining these results, however, we find that none of them satisfies the CCA (chosen ciphertext attacks) security in both confidentiality and anonymity. A major reason is that they are vulnerable to the insider attacks in anonymity, that is a selected receiver, called an insider, can derive the identities of the other receivers selected by the sender in those schemes.

Therefore, in view of the aforementioned reasons, we propose a novel type of multi-receiver encryption called anonymous multi-receiver identity-based authenticated encryption (AMRIBAE). A concrete encryption scheme has also been proposed, which achieves the CCA security in both confidentiality and anonymity, such that it is immune to not only outsider (*i.e.*, unselected receiver) but insider attacks, as well. Let t be the number of the selected receivers of a ciphertext. In our scheme, even if the unselected receivers collude with any $(t-1)$ selected receivers, the anonymity of the non-colluding selected receiver is still preserved. Furthermore, we also prove that the proposed scheme achieves sender authentication, *i.e.*, the identity of the sender of a ciphertext can be confirmed

by the selected receivers. In addition, we provide complete proofs with problem reduction to formally demonstrate the CCA security. Furthermore, our scheme is decryption efficient due to only one pairing computation.

Anonymous Multi-Receiver ID-Based Encryption vs. Anonymous Dynamic Broadcast ID-Based Encryption

In [32], Delerablée *et al.* introduced the concept of dynamic broadcast encryption. In a dynamic broadcast encryption system, a sender can arbitrarily select some or all of the users who have enrolled in the system as the receivers of a ciphertext that he or she is about to generate, and it is unnecessary for the system to re-compute the private keys of the enrolled users whenever a new user joins the system. A multi-receiver encryption system can also achieve this; however, a non-dynamic broadcast encryption system cannot. In a non-dynamic system, all of the enrolled users should be the receivers of every ciphertext in the system, that is the receiver set contains all enrolled users, and it is always fixed for every ciphertext. In addition, the receiver set should be determined before private key generation, which will imply that the private keys of all enrolled users must be re-computed whenever a new user joins the non-dynamic system. Although a non-dynamic broadcast encryption scheme [33–35] might not be as flexible as a dynamic one, those schemes usually provide shorter ciphertext or constant-size ciphertext. Besides, in an ID-based encryption system, the identities of the users also act as their public keys, which will largely simplify the management of the public keys as compared to a non-ID-based one, such as [36].

This research will aim at anonymous multi-receiver ID-based encryption, which can be regarded as anonymous dynamic broadcast ID-based encryption. In this manuscript, we will discuss dynamic and ID-based schemes [10,11,14,16,18–21,23,25–29,31] and compare them to our work.

2. Related Works

In order to protect users' privacy, Fan *et al.* [10] first introduced anonymous multi-receiver identity-based encryption (AMRIBE) in 2010. Their scheme was constructed by using Lagrange interpolating polynomials. However, it cannot achieve anonymity against outside and inside attackers. The cryptanalysis on Fan *et al.*'s scheme [10] has been presented in [11,13,25].

In 2012, Wang *et al.* proposed an AMRIBE scheme [25] by improving Fan *et al.*'s scheme. Unfortunately, their scheme did not achieve anonymity against inside attackers. The cryptanalysis on Wang *et al.*'s scheme [25] has been shown in [17,29]. In the same year, Tseng *et al.* proposed an AMRIBE scheme and claimed that their scheme is CCA secure in both confidentiality and anonymity [21,22]. However, we found that they demonstrated the security without considering all possible attackers. In the proof of the security, they assume that the attacker must compute the symmetric encryption/decryption key corresponding to the challenge ciphertext before it wins the CCA game. That is to say, the proof does not cover the type of attackers that win the CCA game, but have not computed the key of the challenge ciphertext. The details are shown in the Appendix.

In 2013, Zhang and Takagi proposed two AMRIBE schemes [31]. They designed a deployment in an e-mail delivery system and provided some experimental results. However, their first scheme cannot achieve anonymity against inside attackers [28], and they did not provide any security proof for their

second scheme. Besides, Zhang and Mao proposed an improved AMRIBE scheme [28] based on Zhang *et al.*'s scheme [31] in 2013. They claimed that their scheme has the CCA security. However, we have found some mistakes in their security proofs due to the inconsistency between a hash function and the hash oracle corresponding to the function, where the details are shown in the Appendix.

In 2014, there were three AMRIBE schemes [23,26,27] proposed by Tseng *et al.*, Wang and Zhang *et al.*, respectively. Nevertheless, we have found some mistakes in their security proof, and the details are shown in the Appendix.

The other works [11,12,14,16,18–20,29] either have the CPA (chosen plaintext attacks) security only or have not provided the proof for the security. The security of all of the above schemes has been summarized in Section 6 Table 3.

3. Preliminaries

In this section, we define anonymous multi-receiver ID-based authenticated encryption and review some hard problems and assumptions. In addition, we propose a modified decisional bilinear Diffie–Hellman (DBDH) assumption, called the M-DBDH assumption, and prove that the assumption holds if the 1-weak decisional bilinear Diffie–Hellman inversion (1-wDBDHI) problem is hard.

Definition 1. An anonymous multi-receiver identity-based authenticated encryption (AMRIBAE) scheme consists of the following algorithms:

- Setup is an algorithm that takes as input a security parameter l. It returns a master secret key msk and system parameters $params$.
- KeyExtract is an algorithm that takes as input $params$, msk and a user's identity $ID_i \in \{0,1\}^*$ and then returns the secret key d_i of the user.
- Encrypt is an algorithm that takes as input $params$, a message M, the identity ID_s of the sender, the private key d_s of the sender and an identity set $\{ID_1, ID_2, \ldots, ID_t\}$ and returns a ciphertext C. We write $C = Encrypt(params, ID_s, ID_1, ID_2, \ldots, ID_t, M, d_s)$.
- Decrypt is an algorithm that takes as input $params$, a ciphertext C and the secret key d_i of user ID_i and returns a message M. We write $M = Decrypt(params, C, d_i)$.

Let G_1 and G_2 be two cyclic groups of prime order q, P be a generator of G_1 and $e : G_1 \times G_1 \to G_2$ be a bilinear mapping.

Definition 2 (The Bilinear Diffie–Hellman (BDH) Problem)**.** Given (P, aP, bP, cP) for some random $a, b, c \in \mathbb{Z}_q^*$, compute $e(P,P)^{abc}$.

Definition 3 (The Decisional Bilinear Diffie–Hellman (DBDH) Problem)**.** Given (P, aP, bP, cP, Z) for some random $a, b, c \in \mathbb{Z}_q^*$ and $Z \in_R \{e(P,P)^{abc}, Y \in_R G_2 \backslash e(P,P)^{abc}\}$, decide if $Z = e(P,P)^{abc}$.

Definition 4 (The DBDH Assumption [7])**.** Define that an algorithm $\mathcal{A}$ with output $\beta \in \{0,1\}$ has advantage ϵ in solving the DBDH problem if:

$$\left| Pr[\mathcal{A}(P, aP, bP, cP, e(P,P)^{abc}) = 1] - Pr[\mathcal{A}(P, aP, bP, cP, Z) = 1] \right| \geq \epsilon$$

where $a, b, c \in_R \mathbb{Z}_q^*$ and $Z \in_R \{e(P,P)^{abc}, Y \in_R G_2 \backslash e(P,P)^{abc}\}$. We say that the DBDH assumption holds if no polynomial-time algorithm has a non-negligible advantage in solving the DBDH problem.

Definition 5 (The l-Weak Decisional Bilinear Diffie–Hellman Inversion (l-wDBDHI) Problem [37])**.** Given $(P, \overrightarrow{Y}, cP, Z)$, where $Z \in_R \{e(P,P)^{b^{l+1}c}, Y \in_R G_2 \backslash e(P,P)^{abc}\}$ and $\overrightarrow{Y} = (bP, b^2P, \ldots, b^lP)$, decide if $Z = e(P,P)^{b^{l+1}c}$.

Definition 6 (The l-Weak Decisional Bilinear Diffie–Hellman Inversion (l-wDBDHI) Assumption [37])**.** Define that an algorithm $\mathcal{A}$ with output $\beta \in \{0,1\}$ has advantage ϵ in solving the l-wDBDHI problem if:

$$\left| Pr[\mathcal{A}(P, \overrightarrow{Y}, cP, e(P,P)^{b^{l+1}c}) = 1] - Pr[\mathcal{A}(P, \overrightarrow{Y}, cP, Z) = 1] \right| \geq \epsilon.$$

We say that the l-wDBDHI assumption holds if there exists no polynomial-time adversary that has a non-negligible advantage in solving the l-wDBDHI problem.

Definition 7 (The Modified Decisional Bilinear Diffie–Hellman (M-DBDH) Problem)**.** Given $(P, aP, bP, cP, e(P,P)^{b^2c}, Z)$ for some random $a, b, c \in \mathbb{Z}_q^*$ and $Z \in_R \{e(P,P)^{abc}, Y \in_R G_2 \backslash e(P,P)^{abc}\}$, decide if $Z = e(P,P)^{abc}$. Define that an algorithm $\mathcal{A}$ with output $\beta \in \{0,1\}$ has advantage ϵ in solving the M-DBDH problem if:

$$\left| Pr[\mathcal{A}(P, aP, bP, cP, e(P,P)^{b^2c}, e(P,P)^{abc}) = 1] - Pr[\mathcal{A}(P, aP, bP, cP, e(P,P)^{b^2c}, Z) = 1] \right| \geq \epsilon$$

where $a, b, c \in_R \mathbb{Z}_q^*$ and $Z \in_R \{e(P,P)^{abc}, Y \in_R G_2 \backslash e(P,P)^{abc}\}$.

Theorem 8. *No polynomial-time algorithm has a non-negligible advantage in solving the M-DBDH problem if the* 1*-wDBDHI assumption holds.*

Proof. If there exists a polynomial-time algorithm $\mathcal{A}$ with non-negligible advantage ϵ in solving the M-DBDH problem, then we can construct a polynomial-time algorithm $\mathcal{B}$ with non-negligible advantage in solving the 1-wDBDHI problem as follows. Given a 1-wDBDHI instance (P, bP, cP, Z), $\mathcal{B}$ forms an M-DBDH instance via the following operations:

1. Randomly choose $a \in \mathbb{Z}_q^*$, and compute aP.
2. Compute $Z_1 = e(bP, cP)^a$.
3. Set the M-DBDH instance as (P, aP, bP, cP, Z, Z_1), and input it into $\mathcal{A}$.

Let β be the output of $\mathcal{A}$. $\mathcal{B}$ will confirm that $Z = e(P,P)^{b^2c}$ by outputting one as the answer of the 1-wDBDHI instance if $\beta = 1$; otherwise, $\mathcal{B}$ will output zero.

Since:

$$\left| Pr[\mathcal{A}(P, aP, bP, cP, e(P,P)^{b^2c}, e(P,P)^{abc}) = 1] - Pr[\mathcal{A}(P, aP, bP, cP, e(P,P)^{b^2c}, W) = 1] \right| \geq \epsilon$$

where $W \in_R \{e(P,P)^{abc}, X \in_R G_2 \backslash e(P,P)^{abc}\}$,

$$\left| Pr[\mathcal{A}(P, aP, bP, cP, e(P,P)^{b^2c}, e(P,P)^{abc}) = 1] - \frac{1}{2} \right|$$

$$\geq \left| Pr[\mathcal{A}(P, aP, bP, cP, e(P,P)^{b^2c}, e(P,P)^{abc}) = 1] - Pr[\mathcal{A}(P, aP, bP, cP, e(P,P)^{b^2c}, W) = 1] \right| \geq \epsilon.$$

Let $T \in_R \{e(P,P)^{b^2c}, X \in_R G_2 \backslash e(P,P)^{abc}\}$. Thus, we have that:

$$\begin{aligned}
&\left|Pr[\mathcal{B}(P,bP,cP,e(P,P)^{b^2c}) = 1] - Pr[\mathcal{B}(P,bP,cP,T) = 1]\right| \\
&= \left|Pr[\mathcal{A}(P,aP,bP,cP,e(P,P)^{b^2c}, e(P,P)^{abc}) = 1]\right. \\
&\quad -(\frac{1}{2}Pr[\mathcal{B}(P,bP,cP,e(P,P)^{b^2c}) = 1] \\
&\quad \left. +\frac{1}{2}Pr[\mathcal{B}(P,bP,cP,X) = 1])\right| \\
&= \left|\frac{1}{2}Pr[\mathcal{A}(P,aP,bP,cP,e(P,P)^{b^2c}, e(P,P)^{abc}) = 1] - \frac{1}{4}\right| \geq \frac{\epsilon}{2}.
\end{aligned}$$

It turns out that the polynomial-time algorithm $\mathcal{B}$ has a non-negligible advantage $\frac{\epsilon}{2}$ in solving the 1-wDBDH problem. □

Definition 9 (The M-DBDH Assumption)**.** We say that the M-DBDH assumption holds if no polynomial-time algorithm has non-negligible advantage in solving the M-DBDH problem.

By Theorem 8, the M-DBDH assumption holds.

4. Our Scheme

In this section, we will present an anonymous multi-receiver identity-based authenticated encryption scheme with provable CCA security in both confidentiality and anonymity against not only outsider, but also insider attacks. Our scheme can be viewed as a key encapsulation mechanism. The notations used in the proposed scheme are defined in Table 1.

Table 1. The notations.

Notation	Meaning
G_1	a cyclic additive group of prime order q
G_2	a cyclic multiplicative group of prime order q
e	a bilinear mapping; $e : G_1 \times G_1 \to G_2$
P	a generator of G_1
KGC	the key generation center
P_{pub}	the public key of KGC
M	a message
ID_i	the identity of user i
Q_i	the hashed value of ID_i
d_i	the private key of ID_i

The proposed scheme is described as follows.

- **Setup**

  The key generation center (KGC) performs the following operations:

1. Choose an integer $\alpha \in \mathbb{Z}_q^*$ randomly as the master secret key, and set $P_{pub} = \alpha P$.
2. Choose three cryptographic one-way hash functions, $H : \{0,1\}^* \to G_1$, $H_1 : G_2 \to \mathbb{Z}_q^*$, and $H_2 : \{0,1\}^* \times \mathbb{Z}_q^* \to \mathbb{Z}_q^*$.
3. Compute $\Omega = e(P, P)$.
4. Publish the system parameters $params = \{G_1, G_2, e, q, P, P_{pub}, H, H_1, H_2, \Omega\}$ and keep the master key α secret.

- **KeyExtract**
  When user i joins the system, KGC will compute $Q_i = H(ID_i)$ and the private key $d_i = \alpha Q_i$ of the user, and then, KGC will send d_i to user i in a secure manner.

- **Encrypt**
  A sender, say ID_s, produces the ciphertext of a message by performing the following steps:

  1. Choose a message $M \in G_2$, and select a set of t receivers $\{ID_1, \cdots, ID_t\}$.
  2. Choose $k \in \mathbb{Z}_q^*$ at random, and compute $r = H_2(M, k)$.
  3. For $i = 1$ to t, compute $Q_i = H(ID_i)$ and $v_i = H_1(e(rQ_i, d_s))$.
  4. Compute $f(x) = k - \prod_{i=1}^{t}(x - v_i) = \sum_{i=0}^{t-1} c_i x^i + x^t \bmod q$.
  5. Compute $U = rP, V = rQ_s$ and $W = M \cdot \Omega^{-k}$.
  6. Set the ciphertext $C = (c_0, c_1, \ldots, c_{t-1}, U, V, W, ID_s)$.

- **Decrypt**
  After receiving the ciphertext $C = (c_0, c_1, \ldots, c_{t-1}, U, V, W, ID_s)$, a selected receiver, say ID_i, can decrypt C as follows.

  1. Compute $v_i' = H_1(e(V, d_i))$.
  2. Compute $k' = f(v_i') = \sum_{j=0}^{t-1} c_j (v_i')^j + (v_i')^t \bmod q$.
  3. Compute $M' = W \cdot \Omega^{k'}$.
  4. Accept M' if $U = H_2(M', k')P$. If the receiver wants to authenticate the identity of the sender, he can check whether $e(U, H(ID_s)) = e(V, P)$.

The proposed scheme also is illustrated in Figure 1, and the correctness is demonstrated as follows.

$$\begin{aligned} v_i' &= H_1(e(V, d_i)) \\ &= H_1(e(rQ_s, \alpha Q_i)) \\ &= H_1(e(rQ_i, \alpha Q_s)) \\ &= H_1(e(rQ_i, d_s)) \\ &= v_i \end{aligned}$$

and

$$k' = f(v_i') = f(v_i) = k.$$

Thus, the selected receiver ID_i can successfully recover the message by computing $M' = W \cdot \Omega^{k'} = W \cdot \Omega^k = M$, so that $U = H_2(M, k)P = H_2(M', k')P$.

After successfully recovering the message, we have $e(V, d_i) = (rH(ID'_s), \alpha Q_i) = e(rQ_i, \alpha Q_s) = e(rQ_i, d_s)$ for some identity ID'_s, which convinces the receiver that the ciphertext is encrypted with the private key of ID'_s. Additionally, the equation $e(U, H(ID_s)) = e(V, P)$ can guarantee that $V = rQ_s = rH(ID_s)$, which means $ID'_s = ID_s$. This feature makes it possible for the receivers to authenticate the sender of the ciphertext they received. Besides, according to [38], in an anonymous multi-receiver encryption scheme, the length of a ciphertext will at least linearly grow with the number of the receivers. Thus, the ciphertext length of our scheme might be optimal in the aspect of [38].

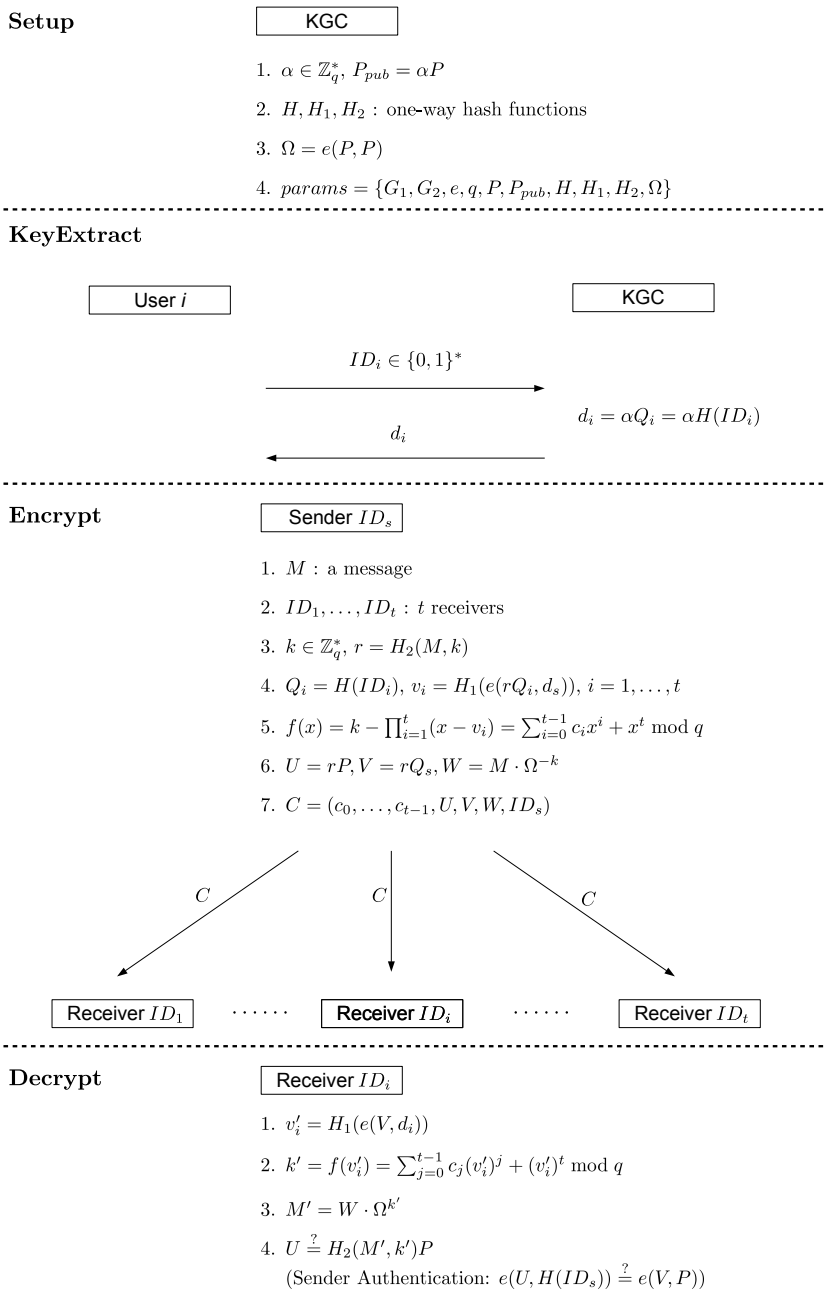

Figure 1. The proposed anonymous multi-receiver identity-based authenticated encryption (AMRIBAE) scheme.

5. Security Models and Proofs

In this section, we will define the security models and the security notions for anonymous multi-receiver identity-based authenticated encryption. The security notions are the "indistinguishability of encryptions under selective multi-ID, chosen-ciphertext attacks" (IND-sMID-CCA) and the "anonymous indistinguishability of encryptions under selective multi-ID, chosen-ciphertext attacks" (Anon-sMID-CCA). We then will prove that our proposed scheme is provably CCA secure in confidentiality and anonymity against insider and outsider attacks.

Definition 10 (The IND-sMID-CCA Game)**.** Let $\mathcal{A}$ be a polynomial-time attacker. $\mathcal{A}$ interacts with a simulator $\mathcal{S}$ in the following game.

Initialization. $\mathcal{A}$ chooses a set of identities $ID^* = \{ID_1^*, ID_2^*, \ldots, ID_t^*\}$ and sends ID^* to $\mathcal{S}$.
Setup. $\mathcal{S}$ runs the *Setup* algorithm to generate $params$ and msk. $\mathcal{S}$ then sends $params$ to $\mathcal{A}$.
Phase 1. $\mathcal{A}$ issues the following queries.

- Hash query: $\mathcal{S}$ operates hash functions on the inputs given by $\mathcal{A}$ and returns the hashed values.
- KeyExtract (ID_i): $\mathcal{A}$ sends an identity ID_i to $\mathcal{S}$ and $\mathcal{S}$ returns the private key of ID_i where KeyExtract (ID_j) cannot be queried if $ID_j \in ID^*$.
- Encrypt ($ID_s, ID_1, \cdots, ID_u, M$): $\mathcal{A}$ sends a sender's identity ID_s, a receiver set $\{ID_1, \cdots, ID_u\}$ and a message M to $\mathcal{S}$. $\mathcal{S}$ returns a ciphertext C to $\mathcal{A}$.
- Decrypt (C, ID_i): $\mathcal{A}$ sends an identity ID_i and a ciphertext C to $\mathcal{S}$, and $\mathcal{S}$ returns the message M.

Challenge. $\mathcal{A}$ submits a sender's identity ID_s and (M_0, M_1) to $\mathcal{S}$, with restrictions that M_0, M_1 are two distinct messages of the same length, $ID_s \notin ID^*$, and KeyExtract (ID_s) has not been queried before. $\mathcal{S}$ then randomly chooses $\beta \in \{0, 1\}$ and generates C^* = Encrypt $(ID_s, ID_1^*, \ldots, ID_t^*, M_\beta)$. Finally, $\mathcal{S}$ sends C^* to $\mathcal{A}$.
Phase 2. $\mathcal{A}$ issues the queries defined in Phase 1, excluding the Decrypt queries with $C = C^*$ and $ID_i \in ID^*$ and the query KeyExtract (ID_s).
Guess. Finally, $\mathcal{A}$ outputs $\beta' \in \{0, 1\}$ and wins the game if $\beta' = \beta$.

The advantage of $\mathcal{A}$ winning the game is defined as:

$$\mathbf{Adv}^{\text{IND-sMID-CCA}}(\mathcal{A}) = \left| Pr[\beta' = \beta] - \frac{1}{2} \right|.$$

An anonymous multi-receiver identity-based authenticated encryption scheme is said to be IND-sMID-CCA secure if there exists no polynomial-time attacker that can win the IND-sMID-CCA game with non-negligible advantage. The model of this game is shown in Figure 2.

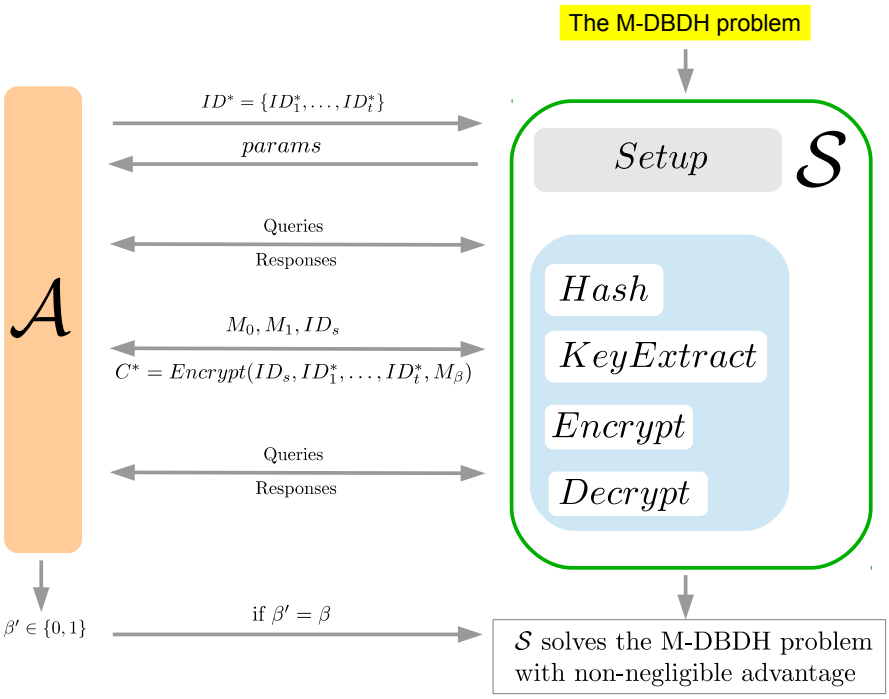

Figure 2. The indistinguishability of encryptions under selective multi-ID, chosen-ciphertext attacks (IND-sMID-CCA) game.

Definition 11 (The Anon-sMID-CCA Game)**.** Let $\mathcal{A}$ be a polynomial-time attacker. $\mathcal{A}$ interacts with a simulator $\mathcal{S}$ in the following game.

Initialization. $\mathcal{A}$ chooses two identities $\{ID_0^*, ID_1^*\}$ and sends them to $\mathcal{S}$.
Setup. $\mathcal{S}$ runs the *Setup* algorithm to generate $params$ and msk. $\mathcal{S}$ then sends $params$ to $\mathcal{A}$.
Phase 1. $\mathcal{A}$ issues the following queries.

- Hash query: $\mathcal{S}$ operates hash functions on the inputs given by $\mathcal{A}$ and returns the hashed values.
- KeyExtract (ID_i): $\mathcal{A}$ sends an identity ID_i to $\mathcal{S}$, and $\mathcal{S}$ returns the private key of ID_i where neither KeyExtract (ID_0^*) nor KeyExtract (ID_1^*) can be queried.
- Encrypt $(ID_s, ID_1, \cdots, ID_u, M)$: $\mathcal{A}$ sends a sender's identity ID_s, a receiver set $\{ID_1, \cdots, ID_u\}$ and a message M to $\mathcal{S}$. $\mathcal{S}$ returns a ciphertext C to $\mathcal{A}$.
- Decrypt (C, ID_i): $\mathcal{A}$ sends an identity ID_i and a ciphertext C to $\mathcal{S}$, and $\mathcal{S}$ returns the message M.

Challenge. $\mathcal{A}$ submits a sender's identity ID_s, a message M and a set of identities $\{ID_2, ID_3, \ldots, ID_t\}$ to $\mathcal{S}$ with restrictions that $ID_s \notin \{ID_0^*, ID_1^*\}$ and KeyExtract (ID_s) has not been queried before. $\mathcal{S}$ then randomly chooses $\beta \in \{0,1\}$ and generates C^* = Encrypt $(ID_s, ID_\beta^*, ID_2, \ldots, ID_t, M)$. Finally, $\mathcal{S}$ sends C^* to $\mathcal{A}$.
Phase 2. $\mathcal{A}$ issues the queries defined in Phase 1, excluding Decrypt (C^*, ID_0^*), Decrypt (C^*, ID_1^*) and KeyExtract (ID_s).
Guess. Finally, $\mathcal{A}$ outputs $\beta' \in \{0,1\}$ and wins the game if $\beta' = \beta$.

The advantage of $\mathcal{A}$ winning the game is defined as:

$$\mathbf{Adv}^{\text{Anon-sMID-CCA}}(\mathcal{A}) = \left| Pr[\beta' = \beta] - \frac{1}{2} \right|.$$

An anonymous multi-receiver identity-based authenticated encryption scheme is said to be Anon-sMID-CCA secure if there exists no polynomial-time attacker that can win the Anon-sMID-CCA game with non-negligible advantage. The model of this game is shown in Figure 3.

Note that there is a restriction that KeyExtract (ID_s) cannot be queried in both the IND-sMID-CCA game and the ANON-sMID-CCA game. This is to model that the adversary cannot collude with the sender, since the confidentiality and the anonymity will be meaningless when the collusion happens.

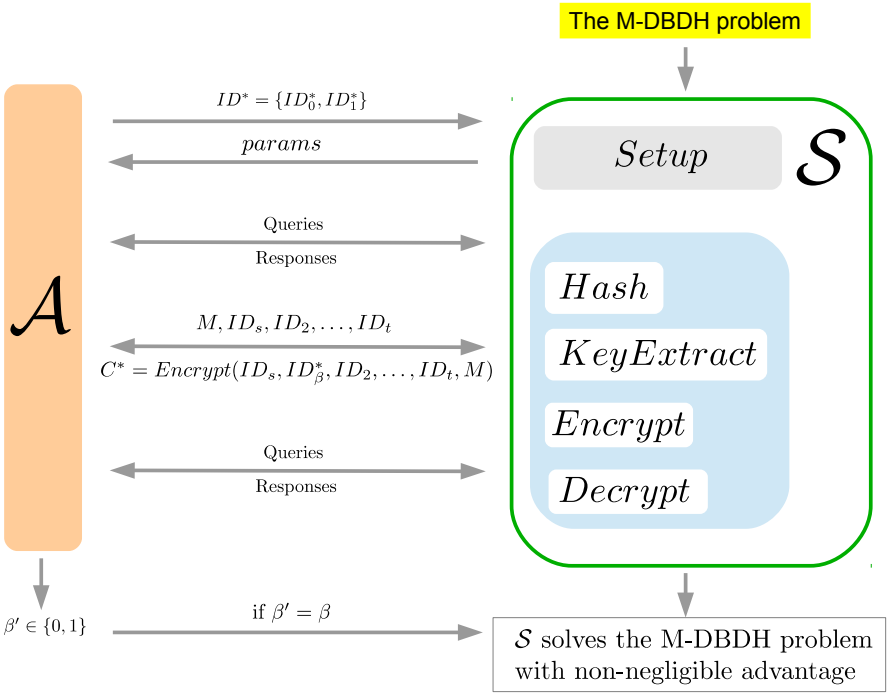

Figure 3. The anonymous (Anon)-sMID-CCA game.

Definition 12 (The Sender Authentication Game)**.** Let $\mathcal{A}$ be a polynomial-time attacker. $\mathcal{A}$ interacts with a simulator $\mathcal{S}$ in the following game.

Initialization. $\mathcal{A}$ chooses two identities $\{ID_s^*, ID_R^*\}$ and sends them to $\mathcal{S}$.
Setup. $\mathcal{S}$ runs the *Setup* algorithm to generate $params$ and msk. $\mathcal{S}$ then sends $params$ to $\mathcal{A}$.
Phase 1. $\mathcal{A}$ issues the following queries.

- Hash query: $\mathcal{S}$ operates hash functions on the inputs given by $\mathcal{A}$ and returns the hashed values.
- KeyExtract (ID_i): $\mathcal{A}$ sends an identity ID_i to $\mathcal{S}$ and $\mathcal{S}$ returns the private key of ID_i where neither KeyExtract (ID_s^*) nor KeyExtract (ID_R^*) can be queried.
- Encrypt ($ID_s, ID_1, \cdots, ID_u, M$): $\mathcal{A}$ sends a sender's identity ID_s, a receiver set $\{ID_1, \cdots, ID_u\}$ and a message M to $\mathcal{S}$. $\mathcal{S}$ returns a ciphertext C to $\mathcal{A}$.
- Decrypt (C, ID_i): $\mathcal{A}$ sends an identity ID_i and a ciphertext C to $\mathcal{S}$, and $\mathcal{S}$ returns the message M.

Forgery. $\mathcal{A}$ outputs a ciphertext C^* with restrictions that the sender is ID_s^* and ID_R^* is one of the receivers, and C^* was not outputted by querying the Encrypt oracle. $\mathcal{A}$ wins the game if C^* is a valid ciphertext.

The advantage of $\mathcal{A}$ winning the game is defined as:

$$\mathbf{Adv}^{\mathrm{SA}}(\mathcal{A}) = Pr[Decrypt(C, ID_R^*) \neq \perp].$$

An anonymous multi-receiver identity-based authenticated encryption scheme is said to satisfy sender authentication if there exists no polynomial-time attacker that can win the sender authentication game with non-negligible advantage. The model of this game is shown in Figure 4.

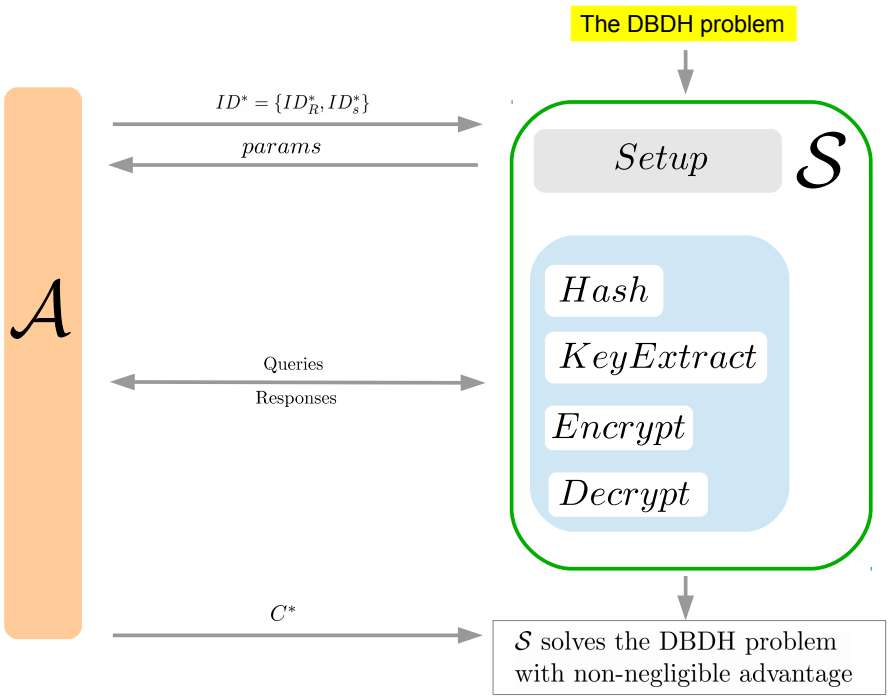

Figure 4. The sender authentication game.

Theorem 13. *(Confidentiality) The proposed AMRIBAE scheme is IND-sMID-CCA secure in the random oracle model if the M-DBDH assumption holds.*

Proof. The basic concept of the proof is a proof by contradiction. Assume that the proposed scheme is not IND-sMID-CCA secure, *i.e.*, there exists a polynomial-time adversary $\mathcal{A}$ that wins the IND-sMID-CCA game with non-negligible advantage. Then, we will construct a polynomial-time algorithm $\mathcal{S}$ that has non-negligible advantage in solving the M-DBDH problem.

First, $\mathcal{S}$ is given $< q, G_1, G_2, e, P, aP, bP, cP, e(P,P)^{b^2c}, Z >$, which is an instance of the M-DBDH problem. $\mathcal{S}$ simulates the game for $\mathcal{A}$ as follows:

Initialization. $\mathcal{A}$ outputs a target identity set $ID^* = \{ID_1^*, \cdots, ID_t^*\}$.
Setup. $\mathcal{S}$ sets $P_{pub} = cP$, computes $\Omega = e(P,P)$ and outputs $\{G_1, G_2, e, q, P, P_{pub}, H, H_1, H_2, \Omega\}$ as the public parameters where H, H_1 and H_2 are three random oracles controlled by $\mathcal{S}$.
Phase 1. $\mathcal{S}$ maintains H-list, H_1-list and H_2-list to store the results of querying H, H_1 and H_2, respectively. In this phase, $\mathcal{A}$ can issue the following queries:

- H-query:
  This oracle takes an identity $ID_j \in \{0,1\}^*$ as input. If there exists a record (ID_j, Q_j, q_j) in H-list, return Q_j. Otherwise, do the following:
  1. Randomly select $q_j \in \mathbb{Z}_q^*$.
  2. If $ID_j \in ID^*$, compute $Q_j = q_j(bP)$; else $Q_j = q_jP$.
  3. Return Q_j, and add (ID_j, Q_j, q_j) into H-list.
- H_1-query:
  This oracle takes X_j as input, where $X_j \in G_2$. If there exists a record (X_j, v_j) in H_1-list, return v_j. Otherwise, do the following:
  1. Randomly choose $v_j \in \mathbb{Z}_q^*$.
  2. Add (X_j, v_j) to H_1-list.
  3. Return v_j.
- H_2-query:
  This oracle takes $M_j \in G_2$ and an integer $k_j \in \mathbb{Z}_q^*$ as input. If there exists a record (M_j, k_j, r_j, U_j) in H_2-list, return r_j. Otherwise, do the following:
  1. Randomly choose $r_j \in \mathbb{Z}_q^*$, and compute $U_j = r_jP$.
  2. Add (M_j, k_j, r_j, U_j) to H_2-list.
  3. Return r_j.
- KeyExtract:
  This oracle takes an identity ID_j as input. Call $H(ID_j)$ and retrieve q_j from H-list. Then, $\mathcal{S}$ does the following:
  - If $ID_j \in ID^*$, return "reject".
  - Otherwise, compute $d_j = q_j(cP)$ and return d_j.
- Encrypt:
  This oracle takes $u+1$ identities $(ID_s, ID_1, \ldots, ID_u)$ and a message M as input. Upon receiving an Encryptquery, $\mathcal{S}$ does the following:
  1. Choose $k, r \in \mathbb{Z}_q^*$ at random, and set $H_2(M, k) = r$.
  2. For $i = 1$ to u,
     - if $ID_s \notin ID^*$, compute $v_i = H_1(e(Q_i, d_s)^r)$, where d_s is the private key of the sender ID_s;
     - if $ID_s \in ID^*$ and $ID_i \notin ID^*$, compute $v_i = H_1(e(d_i, Q_s)^r)$, where d_i is the private key of the receiver ID_i;
     - if $ID_s, ID_i \in ID^*$, compute $v_i = H_1((e(P,P)^{b^2c})^{rq_sq_i})$.
  3. Compute $f(x) = k - \prod_{i=1}^{u}(x - v_i) = \sum_{i=0}^{u-1} c_i x^i + x^u \bmod q$.
  4. Compute $U = rP, V = rQ_s$, and $W = M \cdot e(P,P)^{-k}$.
  5. Set the ciphertext $C = (c_0, c_1, \ldots, c_{u-1}, U, V, W, ID_s)$, and return C.

- Decrypt:
  This oracle takes an identity ID_j and a ciphertext C as input. Upon receiving a Decryptquery, denoted by Decrypt(C, ID_j) where $C = (c_0, \ldots, c_{u-1}, U, V, W, ID_s)$, $\mathcal{S}$ does the following:
  1. Search H_2-list to get (M_i, k_i, r_i, U_i) with $U_i = U$. If not found, return "reject".
  2. Search H-list to get (ID_s, Q_s, q_s) with $e(U, Q_s) = e(P, V)$. If not found, return "reject".
  3. This step can be separated into three cases:
     - if $ID_s \notin ID^*$, compute $v_j = H_1(e(Q_j, d_s)^{r_i})$;
     - if $ID_s \in ID^*$ and $ID_j \notin ID^*$, compute $v_j = H_1(e(d_j, Q_s)^{r_i})$;
     - if $ID_s, ID_j \in ID^*$, compute $v_j = H_1((e(P, P)^{b^2c})^{r_i q_s q_j})$.
  4. Compute $k = c_0 + c_1 v_j + \cdots + c_{u-1} v_j^{u-1} + v_j^u \bmod q$.
  5. Check whether $k_i = k$ and $M_i = W \cdot \Omega^k$ or not. If not, return "reject". Otherwise, return M_i.

Challenge. $\mathcal{A}$ sends (M_0, M_1) and a sender's identity ID_s to $\mathcal{S}$, with restrictions that M_0, M_1 are two distinct messages with the same length, $ID_s \notin ID^*$, and KeyExtract (ID_s) has never been queried. $\mathcal{S}$ performs the following operations:

1. Choose $\beta \in \{0, 1\}$ randomly.
2. For $i = 1$ to t, call $H(ID_i^*)$, and retrieve q_i^* from H-list.
3. Call $H(ID_s)$, and retrieve q_s from H-list.
4. Choose $k \in \mathbb{Z}_q^*$, and set $U^* = aP$ and $V^* = q_s(aP)$.
5. For $i = 1$ to t, compute $v_i = H_1(Z^{q_i^* q_s})$.
6. Compute $f(x) = k - \prod_{i=1}^{t}(x - v_i) = \sum_{i=0}^{t-1} c_i x^i + x^t \bmod q$ and $W^* = M_\beta \cdot \Omega^{-k}$.
7. Set the ciphertext $C^* = (c_0, c_1, \ldots, c_{t-1}, U^*, V^*, W^*, ID_s)$, and send C^* to $\mathcal{A}$.

Phase 2. $\mathcal{A}$ makes queries as those in Phase 1. However, if $\mathcal{A}$ issues a Decrypt query with input $C = C^*$ and $ID_i \in ID^*$ or the query KeyExtract (ID_s), $\mathcal{S}$ will return "reject".
Guess. Finally, $\mathcal{A}$ outputs $\beta' \in \{0, 1\}$. If $\beta' = \beta$, then $\mathcal{S}$ outputs one. Otherwise, $\mathcal{S}$ randomly chooses $\bar{\beta} \in \{0, 1\}$ and outputs $\bar{\beta}$.

If $Z = e(P, P)^{abc}$, then $Z^{q_i^* q_s} = e(P, P)^{abcq_i^* q_s} = e(q_i^*(bP), q_s(cP))^a = e(Q_i^*, d_s)^a$ for $i = 1$ to t. Therefore, C^* is a correct ciphertext. Otherwise, Z is an element randomly chosen in G_2. As the construction above, $\mathcal{S}$ correctly simulates the IND-sMID-CCA game. If $\mathcal{A}$ wins the IND-sMID-CCA game with non-negligible advantage, at least ϵ, $\left|Pr[\beta' = \beta] - \frac{1}{2}\right| \geq \epsilon$ under a correct simulation of the game, *i.e.*, $\left|Pr[\mathcal{A}(\Omega) = \beta' = \beta] - \frac{1}{2}\right| \geq \epsilon$, where Ω is a correct AMRIBAE scheme. Thus, we have that:

$$Pr[\mathcal{S}(P, aP, bP, cP, e(P, P)^{b^2c}, e(P, P)^{abc}) = 1]$$

$$= Pr[\mathcal{A}(\Omega) = \beta] + \frac{1}{2}(1 - Pr[\mathcal{A}(\Omega) = \beta])$$

$$= \frac{1}{2} Pr[\mathcal{A}(\Omega) = \beta] + \frac{1}{2}$$

and

$$Pr[\mathcal{S}(P, aP, bP, cP, e(P, P)^{b^2c}, Z) = 1]$$

$$= \frac{1}{2}Pr[\mathcal{S}(P, aP, bP, cP, e(P,P)^{b^2c}, e(P,P)^{abc}) = 1]$$
$$+\frac{1}{2}Pr[\mathcal{S}(P, aP, bP, cP, e(P,P)^{b^2c}, X \in_R G_2 \backslash e(P,P)^{abc}) = 1]$$
$$= \frac{1}{2}(\frac{1}{2}Pr[\mathcal{A}(\Omega) = \beta] + \frac{1}{2}) + \frac{1}{2}(\frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2})$$
$$= \frac{1}{4}Pr[\mathcal{A}(\Omega) = \beta] + \frac{5}{8}.$$

We can obtain:

$$\left|Pr[\mathcal{S}(P, aP, bP, cP, e(P,P)^{b^2c}, e(P,P)^{abc}) = 1] - Pr[\mathcal{S}(P, aP, bP, cP, e(P,P)^{b^2c}, Z) = 1]\right|$$
$$= \left|\frac{1}{4}Pr[\mathcal{A}(\Omega) = \beta] - \frac{1}{8}\right| = \frac{1}{4}\left|Pr[\mathcal{A}(\Omega) = \beta] - \frac{1}{2}\right| \geq \frac{\epsilon}{4}.$$

Therefore, $\mathcal{S}$ solves the M-DBDH problem with non-negligible advantage $\frac{\epsilon}{4}$ within polynomial time. □

Theorem 13 ensures the CCA security of confidentiality against the outside attackers (unselected receivers). In confidentiality, no inside attackers exist (selected receivers), because every selected receiver can decrypt the ciphertext.

Theorem 14. *(Anonymity) The proposed AMRIBAE scheme is Anon-sMID-CCA secure in the random oracle model if the M-DBDH assumption holds.*

Proof. Assume that the proposed scheme is not Anon-sMID-CCA secure, that is there exists a polynomial-time adversary $\mathcal{A}$ that wins the Anon-sMID-CCA game with non-negligible advantage. We will construct a polynomial-time algorithm $\mathcal{S}$ that has non-negligible advantage in solving the M-DBDH problem.

First, $\mathcal{S}$ is given $< q, G_1, G_2, e, P, aP, bP, cP, e(P,P)^{b^2c}, Z >$, which is an instance of the M-DBDH problem. $\mathcal{S}$ simulates the game for $\mathcal{A}$ as follows:

Initialization. $\mathcal{A}$ outputs a target identity set $ID^* = \{ID_0^*, ID_1^*\}$.
Setup. $\mathcal{S}$ sets $P_{pub} = cP$, computes $\Omega = e(P,P)$ and outputs $\{G_1, G_2, e, q, P, P_{pub}, H, H_1, H_2, \Omega\}$ as the public parameters, where H, H_1 and H_2 are three random oracles controlled by $\mathcal{S}$.
Phase 1. $\mathcal{S}$ maintains H-list, H_1-list and H_2-list to store the results of querying H, H_1 and H_2, respectively. In this phase, $\mathcal{A}$ can issue the H, H_1, H_2, KeyExtract, Encrypt and Decrypt queries. The simulations are the same as those in the proof of Theorem 13.
Challenge. $\mathcal{A}$ sends a message M, $t-1$ receivers' identities $\{ID_2, ID_3, \ldots, ID_t\}$ and a sender's identity ID_s to $\mathcal{S}$ with restrictions that $ID_s \notin ID^*$ and KeyExtract (ID_s) has never been queried. $\mathcal{S}$ does the following:

1. Choose $\beta \in \{0, 1\}$ randomly.
2. For $i = 2$ to t, call $H(ID_i)$, and retrieve q_i from H-list.
3. Call $H(ID_\beta^*)$, and retrieve q_β^* from H-list.
4. Call $H(ID_s)$, and retrieve q_s from H-list.
5. Choose $k \in \mathbb{Z}_q^*$, and set $U^* = aP$ and $V^* = q_s(aP)$.

6. For $i = 2$ to t, compute $v_i = H_1(e(q_i U^*, q_s(cP)))$.
7. Compute $v_\beta = H_1(Z^{q_\beta^* q_s})$.
8. Compute $f(x) = k - (x - v_\beta)\prod_{i=2}^{t}(x - v_i) = \sum_{i=0}^{t-1} c_i x^i + x^t \bmod q$ and $W^* = M \cdot \Omega^{-k}$.
9. Set the ciphertext $C^* = (c_0, c_1, \ldots, c_{t-1}, U^*, V^*, W^*, ID_s)$ and send C^* to $\mathcal{A}$.

Phase 2. $\mathcal{A}$ makes queries as those in Phase 1. However, if $\mathcal{A}$ issues a Decrypt query with input $C = C^*$ and $ID_i \in ID^*$ or KeyExtract (ID_s), $\mathcal{S}$ will return "reject".
Guess. Finally, $\mathcal{A}$ outputs $\beta' \in \{0, 1\}$. If $\beta' = \beta$, then $\mathcal{S}$ outputs one. Otherwise, $\mathcal{S}$ randomly chooses $\bar{\beta} \in \{0, 1\}$ and outputs $\bar{\beta}$.

If $Z = e(P, P)^{abc}$, then $Z^{q_\beta^* q_s} = e(P, P)^{abcq_\beta^* q_s} = e(q_\beta^*(bP), q_s(cP))^a = e(Q_\beta^*, d_s)^a$ for $\beta \in \{0, 1\}$. Therefore, C^* is a correct ciphertext. Otherwise, Z is an element randomly chosen in G_2. As the construction above, $\mathcal{S}$ correctly simulates the Anon-sMID-CCA game. If $\mathcal{A}$ wins the game with non-negligible advantage at least ϵ, $\left|Pr[\beta' = \beta] - \frac{1}{2}\right| \geq \epsilon$ under a correct simulation of the game, *i.e.*, $\left|Pr[\mathcal{A}(\Omega) = \beta' = \beta] - \frac{1}{2}\right| \geq \epsilon$, where Ω is a correct AMRIBAE scheme. Thus, we have that:

$$\begin{aligned}
&\left|Pr[\mathcal{S}(P, aP, bP, cP, e(P, P)^{b^2 c}, e(P, P)^{abc}) = 1 - Pr[\mathcal{S}(P, aP, bP, cP, e(P, P)^{b^2 c}, Z) = 1]\right| \\
&= \left|(\frac{1}{2}Pr[\mathcal{A}(\Omega) = \beta] + \frac{1}{2}) - (\frac{1}{4}Pr[\mathcal{A}(\Omega) = \beta] + \frac{5}{8})\right| \\
&= \left|\frac{1}{4}Pr[\mathcal{A}(\Omega) = \beta] - \frac{1}{8}\right| = \frac{1}{4}\left|Pr[\mathcal{A}(\Omega) = \beta] - \frac{1}{2}\right| \geq \frac{\epsilon}{4}.
\end{aligned}$$

Therefore, $\mathcal{S}$ solves the M-DBDH problem with non-negligible advantage $\frac{\epsilon}{4}$ within polynomial time. □

Theorem 14 guarantees the CCA security of anonymity against both the outside attackers (unselected receivers) and the inside attackers (selected receivers) in the proposed scheme. In other words, even if an adversary compromises with any $t - 1$ receivers, the anonymity of the remaining receiver is still preserved in the proposed scheme. In this proof, we do not cover the following extreme case. Assume that the total number of users in the system is N. The extreme case occurs when a user (sender) encrypts a message for other $N - 2$ selected users (receivers), so that there would be only one unselected user, and this unselected user can no doubt figure out the identities of the $N - 2$ receivers.

Theorem 15. *(Sender authentication) The proposed AMRIBAE scheme satisfies sender authentication in the random oracle model if the DBDH assumption holds.*

Proof. Assume that there exists a polynomial-time adversary $\mathcal{A}$ that wins the sender authentication game with non-negligible advantage. Then, we will construct a polynomial-time algorithm $\mathcal{S}$ that has non-negligible advantage in solving the DBDH problem.
First, $\mathcal{S}$ is given $< q, G_1, G_2, e, P, aP, bP, cP, Z >$, which is an instance of the DBDH problem. $\mathcal{S}$ simulates the game for $\mathcal{A}$ as follows:

Initialization. $\mathcal{A}$ outputs an identity set $ID^* = \{ID_s^*, ID_R^*\}$.
Setup. $\mathcal{S}$ sets $P_{pub} = cP$, computes $\Omega = e(P, P)$ and outputs $\{G_1, G_2, e, q, P, P_{pub}, H, H_1, H_2, \Omega\}$ as the public parameters, where H, H_1 and H_2 are three random oracles controlled by $\mathcal{S}$.

Phase 1. $\mathcal{S}$ maintains H-list, H_1-list and H_2-list to store the results of querying H, H_1 and H_2, respectively. In this phase, $\mathcal{A}$ can issue the following queries:

- H-query:
  This oracle takes an identity $ID_j \in \{0,1\}^*$ as input. If there exists a record (ID_j, Q_j, q_j) in H-list, return Q_j. Otherwise, do the following:
  1. Randomly select $q_j \in \mathbb{Z}_q^*$.
  2. If $ID_j = ID_s^*$, compute $Q_j = q_j(aP)$; else if $ID_j = ID_R^*$, compute $Q_j = q_j(bP)$; else $Q_j = q_jP$.
  3. Return Q_j and add (ID_j, Q_j, q_j) into H-list.
- The simulation of H_1-query and H_2-query are the same as those in the proof of Theorem 13.
- KeyExtract:
  This oracle takes an identity ID_j as input. Call $H(ID_j)$, and retrieve q_j from H-list. Then, $\mathcal{S}$ does the following:
  - If $ID_j \in ID^*$, return "reject".
  - Otherwise, compute $d_j = q_j(cP)$, and return d_j.
- Encrypt:
  This oracle takes $u+1$ identities $(ID_s, ID_1, \ldots, ID_u)$ and a message M as input. Upon receiving an Encrypt query, $\mathcal{S}$ does the following:
  1. Choose $k, r \in \mathbb{Z}_q^*$ at random, and set $H_2(M,k) = r$.
  2. For $i = 1$ to u,
     - if $ID_s \notin ID^*$, compute $v_i = H_1(e(Q_i, d_s)^r)$, where d_s is the private key of the sender ID_s;
     - if $ID_s \in ID^*$ and $ID_i \notin ID^*$, compute $v_i = H_1(e(d_i, Q_s)^r)$, where d_i is the private key of the receiver ID_i;
     - if $ID_s, ID_i \in ID^*$, compute $v_i = H_1(Z^{rq_sq_i})$.
  3. Compute $f(x) = k - \prod_{i=1}^{u}(x - v_i) = \sum_{i=0}^{u-1} c_i x^i + x^u \bmod q$.
  4. Compute $U = rP, V = rQ_s$ and $W = M \cdot \Omega^{-k}$.
  5. Set the ciphertext $C = (c_0, c_1, \ldots, c_{u-1}, U, V, W, ID_s)$, and return C.
- Decrypt:
  This oracle takes an identity ID_j and a ciphertext C as input. Upon receiving a Decrypt query, denoted by Decrypt (C, ID_j), where $C = (c_0, \ldots, c_{u-1}, U, V, W, ID_s)$, $\mathcal{S}$ does the following:
  1. Search H_2-list to get (M_i, k_i, r_i, U_i) with $U_i = U$. If not found, return "reject".
  2. Search H-list to get (ID_s, Q_s, q_s) with $e(U, Q_s) = e(P, V)$. If not found, return "reject".
  3. This step can be separated into three cases:
     - if $ID_s \notin ID^*$, compute $v_j = H_1(e(Q_j, d_s)^{r_i})$;
     - if $ID_s \in ID^*$ and $ID_j \notin ID^*$, compute $v_j = H_1(e(d_j, Q_s)^{r_i})$;
     - if $ID_s, ID_j \in ID^*$, compute $v_j = H_1(Z^{r_iq_sq_j})$.
  4. Compute $k = c_0 + c_1v_j + \cdots + c_{u-1}v_j^{u-1} + v_j^u \bmod q$.

5. Check whether $k_i = k$ and $M_i = W \cdot \Omega^k$ or not. If not, return "reject". Otherwise, return M_i.

Forgery. Finally, $\mathcal{A}$ outputs $C^* = (c_0, c_1, \ldots, c_{t-1}, U^*, V^*, W^*, ID_s^*)$, where C^* was not outputted by querying the Encrypt oracle. Then, $\mathcal{S}$ performs the following.

1. Search H_2-list to get (M_i, k_i, r_i, U_i) with $U_i = U^*$.
2. Call $H(ID_s^*)$ and $H(ID_R^*)$ to retrieve q_s^* and q_R^* from H-list.
3. Compute $v = H_1(Z^{q_s^* q_R^* r_i})$.
4. Compute $k = c_0 + c_1 v + \cdots + c_{t-1} v^{t-1} + v^t \bmod q$.
5. Check whether $k_i = k$ and $M_i = W \cdot \Omega^k$ or not. If it is, $\mathcal{A}$ wins the game.

$\mathcal{S}$ outputs 1 if $\mathcal{A}$ wins the game. Otherwise, $\mathcal{S}$ outputs 0. Assume $\mathcal{A}$ wins the game with a non-negligible advantage at least ϵ under a correct simulation. To analyze the advantage of solving the DBDH problem, we define the following events.

E_1: The game has been correctly simulated.
E_2: $\mathcal{A}$ wins the game.

Then, we have that:

$$\begin{aligned} &Pr[\mathcal{S}(P, aP, bP, cP, e(P,P)^{abc}) = 1] \\ &= Pr[E_1 \wedge E_2] = Pr[E_1] Pr[E_2 | E_1] \\ &\geq 1 \cdot \epsilon = \epsilon \end{aligned}$$

and

$$\begin{aligned} &\left| Pr[\mathcal{S}(P, aP, bP, cP, e(P,P)^{abc}) = 1] - Pr[\mathcal{S}(P, aP, bP, cP, Z) = 1] \right| \\ &= \left| \frac{1}{2} Pr[\mathcal{S}(P, aP, bP, cP, e(P,P)^{abc}) = 1] \right| \geq \frac{1}{2}\epsilon. \end{aligned}$$

Therefore, $\mathcal{S}$ solves the DBDH problem with non-negligible advantage $\frac{\epsilon}{2}$ within polynomial time. □

Theorem 15 guarantees that the proposed scheme satisfies sender authentication. In other words, even if an adversary compromises with any $t-1$ receivers, the adversary cannot impersonate a sender to send a valid ciphertext.

6. Comparisons

In this section, we compare the proposed scheme to [10,11,14,16,18–21,23,25–29] and [31] in performance and security. According to [39–41] and [42], we can obtain that $T_p \approx 5T_e$, $T_s \approx 29T_m$, $T_e \approx 240T_m$, $T_h \approx 23T_m$ and $T_a \approx 0.12T_m$, shown in Table 2, which summarizes the comparison in the computation cost of encryption/decryption and the ciphertext length for multiple receivers. Especially, our scheme is efficient in decryption.

The security comparison is shown in Table 3. The schemes of [11,29] and the second scheme of [31] lack the proofs for confidentiality and anonymity. The scheme [19] did not provide the proof for anonymity, but it is CPA secure in confidentiality. The schemes [14,16,18] and [20] are CPA secure in both confidentiality and anonymity, where the proof of [20] is under a standard model. The scheme [10] is CCA secure in confidentiality, but it is not with anonymity, which has been indicated in [11,13,25]. The scheme of [25] and the first scheme of [31] are CCA secure in confidentiality and anonymity against outsider attacks; however, the authors of [17,29] and [28], respectively, have shown that they are not with anonymity against insider attacks. In addition, we demonstrate that there exist some problems in the proofs of the schemes [21–23,26–28], where the details are shown in the Appendix. Our scheme is the first one that can achieve the CCA security under the random oracle model against outside attackers and inside attackers simultaneously. The confidentiality and anonymity of our scheme have been formally proven in Section 5.

Table 2. Performance comparison.

	Encryption Cost	**Decryption Cost**	**Ciphertext Length**
[10]	$(2t+3)T_h + 2tT_m + (t^2+2)T_s$ $+(t^2-t)T_a + tT_{poly} + T_p + T_e$ $\approx (29t^2+48t+1567)T_m + tT_{poly}$	$4T_h + (t+2)T_s$ $+tT_a + 2T_p$ $\approx (29t+2550)T_m$	$(t+2)u + w$
[11]	$(2t+1)T_h + (t+1)T_s + tT_p$ $\approx (1275t+52)T_m$	$tT_h + tT_s + tT_p$ $\approx 1252tT_m$	$(t+2)u + w$
[25]	$(2t+3)T_h + 2tT_m + (2t^2+t+1)T_s$ $+2(t^2-t)T_a + tT_{poly} + T_p + tT_e$ $\approx (58t^2+317t+1298)T_m + tT_{poly}$	$4T_h + (2t+2)T_s$ $+2tT_a + 2T_p$ $\approx (58t+2550)T_m$	$(2t+2)u + w$
[21]	$(t+1)T_h + 2T_s + tT_p + T_{poly}$ $\approx (1223t+81)T_m + T_{poly}$	$T_h + tT_m + T_p$ $\approx (t+1223)T_m$	$t\|q\| + u + w$
[18]	$(t+2)T_s + (t+1)T_p + T_{CRT}$ $\approx (1229t+1258)T_m + T_{CRT}$	T_p $\approx 1200T_m$	$t\|q\| + 2u + w$
[16]	$tT_h + (t+1)T_e + (2t+5)T_s + (t+1)T_e$ $\approx (1521t+1585)T_m$	$T_h + T_e + t(2T_p + T_e + T_s)$ $\approx (2669t+1223)T_m$	$(t+2)u + w$
[29]	$(2t+4)T_h + 2tT_m + (t^2+t+1)T_s$ $+2(t^2-t)T_a + tT_{poly} + T_p + tT_e$ $\approx (29t^2+317t+1233)T_m + tT_{poly}$	$4T_h + (t+1)T_s$ $+tT_a + 2tT_p$ $\approx (2429t+121)T_m$	$(2t+2)u + w$

Table 2. *Cont.*

	Encryption Cost	Decryption Cost	Ciphertext Length
[31]-Scheme 1	$(t+1)T_h + 2tT_e + 2T_s$ $+tT_a + 2tT_p$ $\approx (1703t + 1281)T_m$	$(t+1)T_h + T_s$ $+T_a + 2T_p$ $\approx (23t + 2452)T_m$	$(t+2)u + w$
[31]-Scheme 2	$(t+1)T_h + 2tT_e + 2T_s$ $+tT_a + 2tT_p$ $\approx (1703t + 1281)T_m$	$(t+1)T_h + T_s$ $+T_a + 2T_p$ $\approx (23t + 2452)T_m$	$(t+2)u + w$
[14]	$(2t+1)T_h + (3t+2)T_s$ $+T_e + nT_a$ $\approx (133t + 1281)T_m$	$t(T_p + T_a + T_h)$ $\approx 1223tT_m$	$(t+1)v + w$
[19]	$tT_h + t^2T_m + (t+4)T_s$ $+(t+1)T_e + T_{poly}$ $\approx (t^2 + 1252t + 1316)T_m$	$T_h + T_{poly}$ $+2T_a + (t+1)T_s + 4T_p$ $\approx (29t + 4852)T_m + T_{poly}$	$(t+3)u + v$
[28]	$(2t+1)T_h + (t+1)T_m$ $+tT_e + (2t+2)T_s$ $\approx (1305t + 82)T_m$	$(t+1)T_h + (t+1)T_p + tT_s$ $\approx (1252t + 1223)T_m$	$(t+2)u + w$
[20]	$tT_h + (t+1)T_m + (t^2+1)T_s$ $+(t^2-t)\|ID\|T_a + T_e + tT_{poly}$ $\approx (29t^2 + 24t + 270)T_m + tT_{poly}$	$T_h + T_m + T_e$ $+tT_a + tT_s + 2T_p$ $\approx (29t + 2664)T_m$	$(t+1)u + v$
[23]	$(3t+1)T_h + 2T_s + tT_p$ $\approx (1269t + 81)T_m$	$2T_h + T_e$ $\approx 1246T_m$	$(t+1)u + \|q\| + w$
[27]	$(2t+2)T_h + 4T_s + tT_p + T_{poly}$ $\approx (1246t + 162)T_m + T_{poly}$	$3T_h + tT_m + 3T_p + T_s + T_a$ $\approx (t + 3698)T_m$	$t\|q\| + 3u + \|ID\|$
[26]	$(t+2)T_h + (t+2)T_s + tT_p$ $\approx (1252t + 104)T_m$	$4T_h + tT_s + T_e$ $\approx (29t + 1292)T_m$	$(t+2)u + w$
Ours	$(2t+1)T_h + 4T_s + tT_p + T_{poly}$ $\approx (1246t + 139)T_m + T_{poly}$	$2T_h + tT_m + T_p + T_s$ $\approx (t + 1275)T_m$	$t\|q\| + 2u + v$

•T_p: the cost of a pairing operation; •T_h: the cost of a hash operation; •T_m: the cost of a modular multiplication in $\mathbb{Z}_q^*$; •T_e: the cost of a modular exponentiation in $\mathbb{Z}_q^*$; •T_s: the cost of a scalar multiplication in an additive group or an exponentiation in a multiplicative group; •T_a: the cost of an addition in an additive group or a multiplication in a multiplicative group; •T_{poly}: the cost of constructing a polynomial; •T_{CRT}: the cost of applying the Chinese remainder theorem; •t: the number of receivers; •$|ID|$: the bit length of an identity; •q: a large prime; •u: the bit length of an element in an additive group; •v: the bit length of an element in a multiplicative group; •w: the bit length of a symmetric encryption key.

Table 3. Properties comparison. CPA, chosen plaintext attack.

	Confidentiality	Anonymity		Security	Sender
		Outsider	Insider	Model	Authentication
[10]	CCA	△	△	ROM	No
[11]	–	–	–	–	No
[25]	CCA	CCA	△	ROM	No
[21,22]	△	△	△	ROM	No
[18]	CPA	CPA	CPA	ROM	No
[29]	–	–	–	–	No
[16]	CPA	CPA	CPA	ROM	No
[31]-Scheme 1	CCA	CCA	△	ROM	No
[31]-Scheme 2	–	–	–	–	No
[14]	CPA	CPA	CPA	ROM	No
[19]	CPA	–	–	ROM	No
[28]	△	△	△	ROM	No
[20]	CPA	CPA	CPA	STD	No
[23]	△	△	△	ROM	No
[27]	△	△	△	ROM	Yes
[26]	–	△	△	ROM	No
Ours	CCA	CCA	CCA	ROM	Yes

△: the authors claimed that their scheme is CCA secure, but it has some security flaws or there exist some problems in the security proofs.

7. Conclusions

In consideration of privacy preservation, Fan *et al.* first introduced the concept of anonymous multi-receiver identity-based encryption in 2010. Many works on the topic have been proposed recently. It is an interesting topic and worthy of study in both practical and theoretical aspects, because customers always pay much attention to their privacy in modern societies.

However, there is no anonymous multi-receiver identity-based encryption scheme proposed in the literature that possesses complete CCA security. In order to cope with the problem, we have proposed a new anonymous multi-receiver identity-based encryption scheme, which is provably CCA secure in both confidentiality and anonymity against not only outside attackers, but also inside attackers. Furthermore, the proposed scheme has also achieved sender authentication. All of the properties of our scheme are guaranteed based on the DBDH assumption and the M-DBDH assumption, whose hardness has been proven in this paper.

Acknowledgments

This work was partially supported by the Ministry of Science and Technology of the Taiwan under grants MOST 104-2221-E-110-043 and “Aim for the Top University Plan” of the National Sun Yat-sen University and Ministry of Education, Taiwan.

Author Contributions

The authors contributed equally to this work.

Conflicts of Interest

The authors declare no conflict of interest.

Appendix

A.1. Cryptanalysis to Other AMRIBEs

The notations used in this section are shown in Table 4.

Table 4. The notations.

Notation	Meaning
G_1	a cyclic groups of prime order q
G_2	a cyclic groups of prime order q
e	a bilinear mapping; $e : G_1 \times G_1 \rightarrow G_2$
P	a generator of G_1
KGC	the key generation center
P_{pub}	the public key of KGC
M	the message that the sender wants to send
(E_k, D_k)	a secure symmetric encryption scheme with secret key k
Q_i	the hash value of ID_i

A.1.1. Comment on Tseng *et al.*'S Scheme [21,22]

In 2012, Tseng *et al.* proposed an AMRIBE scheme with provable security, which is briefly described and discussed as follows. The detailed description of the scheme and the proofs can be referred to [21].

Comments

The simulation will be terminated when the challenger B receives a five-tuple $(P, QID_i, P_{pub}, cP, X_j)$ from the adversary A and $e(QID_i, cP_{pub}) = X_j$ is true. If so, B will solve the gap-BDH problem by outputting $(X_j)^{u_i^{-1}}$, which equals $e(P, P)^{abc}$. Since $U = cP$ in the challenge phase, if A can compute X_j, it implies that he or she is capable of computing $v_i = H_1(X_j)$ and getting the symmetric encryption/decryption key $k = f(v_i)$ corresponding to the challenge ciphertext, and thus, he or she will be able to win the CCA game. However, the proof only aims at the attackers who are capable of getting the key, k, before winning the CCA game. The authors have not considered the attackers who can win the game without getting the key. As a result, their proof does not cover all possible attackers. Besides, the same problem exists in the proof for anonymity, too. Similar situations happen in the schemes of [23,27].

A.1.2. Comment on Tseng *et al.*'s Scheme [23]

In their proofs, the authors have not considered the attackers who can win the game without getting the key. As a result, their proof does not cover all possible attackers. The comment is similar to that of [21].

A.1.3. Comment on Zhang *et al.*'s Scheme [27]

In their proofs, the authors have not considered the attackers who can win the game without getting the key. As a result, their proof does not cover all possible attackers. The comment is similar to that of [21].

A.1.4. Comment on Zhang *et al.*'s Scheme [28]

In 2013, Zhang and Mao proposed an AMRIBE scheme as follows. The details of the scheme and the proofs can be referred to [28].

Comments

In the proof of confidentiality, the H_1 oracle is queried by the adversary with two input elements of G_1. Additionally, the two elements must be recorded in order to simulate the decryption oracle. However, the hash function H_1 has only one input element of G_2 in the proposed scheme. Therefore, they cannot simulate the decryption oracle successfully, and thus, the proof is incorrect. The same mistake also exists in the proof of anonymity.

A.1.5. Comment on Wang's Scheme [26]

In 2014, Wang proposed an AMRIBE scheme as follows. The detailed description of the scheme can be referred to [26].

The Simulation of the CCA Game for Confidentiality

We only show the $Decrypt$ oracle here.

$Decrypt$: $\mathcal{C}$ is given the ciphertext-receiver pair (C, ID_j) where $C = (R_{1_i}, \ldots, R_{t_i}, U_{1_i}, U_{2_i}, V_i)$. If ID_j does not belong to the challenge identity set S_a, $\mathcal{C}$ gets d_i and decrypts C. If $ID \in S_a$, $\mathcal{C}$ looks for the table T_{H_3}. If there exists the records $(*, R_{1_i}, \ldots, R_{t_i}, U_{1_i}, U_{2_i}, l^*)$, $*, l^*$ are default. If $* = \sigma_j$, $\mathcal{C}$ checks whether $H(\sigma_j)P \stackrel{?}{=} U_{2_i}$. If it holds, go to the next step. Otherwise, $\mathcal{C}$ checks the next record until it holds. Suppose that the satisfied record is $* = \sigma^*$ and the corresponding hash value is l^*. $\mathcal{C}$ computes $M^* = D_{l^*}(V_i)$. If there exists the record $(M^*, \sigma, U_{1_i}, U_{2_i}, z^*)$, where z^* is default, $\mathcal{C}$ returns M^*. Otherwise, fail.

Comments

An adversary can make the $Decrypt$ oracle perform decryption incorrectly as follows.

1. Choose a receiver set $\{ID_{d_1}, ID_2, \ldots, ID_t\}$, where ID_{d_1} is the target identity.

2. Choose σ, r to compute $R_{d_1}, R_2, \ldots, R_t$ and U_1 as that in the $Encrypt$ algorithm of their scheme.
3. Choose σ', M, and compute $U_2 = H(\sigma')P$, $l = H_3(\sigma', R_{d_1}, R_2, \ldots, R_t, U_1, U_2)$.
4. Query $H_4(M, \sigma', U_1, U_2)$.
5. Set $V = E_l(M)$ and $C = (R_{d_1}, R_2, \ldots, R_t, U_1, U_2, V)$.

The ciphertext C is invalid since σ used to compute R_i and σ' used to compute l and U_2 are not identical, so that the authorized receivers $ID_2, \ldots, ID_t$ cannot decrypt C. However, if the adversary queries Decrypt (C, ID_{d_1}), the simulator will successfully perform the Decrypt oracle and return M.

References

1. Arul, T.; Shoufan, A. Consumer Opinions on Short-Interval Charging for Pay-TV over IPTV. In Proceedings of the 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Fukuoka, Japan, 26–29 March 2012; pp. 147–153.
2. Msgna, M.G.; Markantonakis, K.; Mayes, K.; Akram, R.N. Subscriber Centric Conditional Access System for Pay-TV Systems. In Proceedings of the 2013 IEEE 10th International Conference on e-Business Engineering (ICEBE), Coventry, UK, 11–13 September 2013; pp. 450–455.
3. Liu, Y.; Duan, J.; Tang, Q.; Zhang, Y. A Simple and Efficient Re-Scrambling Scheme for DTV Programs. *IEEE Trans. Multimed.* **2014**, *16*, 137–146.
4. Baek, J.; Safavi-Naini, R.; Susilo, W. Efficient Multi-Receiver Identity-Based Encryption and Its Application to Broadcast Encryption. In Proceedings of the 8th International Conference on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, 23–26 January 2005; pp. 380–397.
5. Wang, L.; Wu, C.K. Efficient identity-based multicast scheme from bilinear pairing. *IEEE Proc. Commun.* **2005**, *152*, 877–882.
6. Du, X.; Wang, Y.; Ge, J.; Wang, Y. An ID-based broadcast encryption scheme for key distribution. *IEEE Trans. Broadcast.* **2015**, *51*, 264–266.
7. Boneh, D.; Franklin, M. Identity-based encryption from the weil pairing. In Proceedings of the 21st Annual International Cryptology Conference, Santa Barbara, CA, USA, 19–23 August 2001; pp. 213–229.
8. Bellare, M.; Rogaway, P. Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols. In Proceedings of the 1st ACM Conference on Compute and Communications Security, Fairfax, VA, USA, 3–5 November 1993; pp. 62–73.
9. Okamoto, T.; Pointcheval, D. REACT: Rapid Enhenced-Security Asymmetric Cryptosystem Transform. In *Topics in Cryptology CT-RSA 2001*; Springer-Verlag Berling Heiderlberg: New York, NY, USA, 2001; pp. 159–175.
10. Fan, C.I.; Huang, L.Y.; Ho, P.H. Anonymous Multireciever identity-based encryption. *IEEE Trans. Comput.* **2010**, *59*, 1239–1249.
11. Chien, H.Y. Improved anonymous multi-receiver identity-based encryption. *Comput. J.* **2012**, *55*, 439–446.
12. Chen, Z.; Li, S.; Wang, C.; Shen, Y. Two constructions of multireceiver encryption supporting constant keys, short ciphertexts, and identity privacy. *Int. J. Netw. Secur.* **2012**, *14*, 270–279.

13. Chen, Z.; Li, S.; Wang, C.; Zhang, M. Comments on FHH anonymous multireceiver encryption. *Int. J. Netw. Secur.* **2014**, *16*, 285–288.
14. Cui, H.; Mu, Y.; Guo, F. Server-aided identity-based anonymous broadcast encryption. *Int. J. Netw. Secur.* **2013**, *8*, 29–39.
15. Harn, L.; Chang, C.C.; Wu, H.L. An anonymous multi-receiver encryption based on RSA. *Int. J. Netw. Secur.* **2013**, *15*, 307–312.
16. Hur, J.; Park, C.; Hwang, S.O. Privacy-preserving identity-based broadcast encryption. *Inf. Fusion* **2012**, *13*, 296–303.
17. Li, H.; Pang, L. Cryptanalysis of Wang et al's improved anonymous multi-receiver identity-based encryption scheme. *IET Inf. Secur.* **2013**, *8*, 8–11.
18. Muthulakshmi, A.; Anitha, R.; Rohini, S.; Princy, K. Identity Based Privacy Preserving Dynamic Broadcast Encryption for multi-privileged group. In *Recent Trends in Computer Networks and Distributed Systems Security*; Spring: Berlin Heidelberg, Germany, 2012; Volume 335, pp. 272–282.
19. Pang, L.; Guo, L.; Pei, Q.; Gui, J.; Wang, Y. A new ID-based multi-recipient public-key Encryption Scheme. *Chin. J. Electron.* **2013**, *22*, 89–92.
20. Ren, Y.; Niu, Z.; Zhang, X. Fully anonymous identity-based broadcast encryption without random oracles. *Int. J. Netw. Secur.* **2014**, *16*, 256–264.
21. Tseng, Y.M.; Huang, Y.H.; Chang, H.J. Privacy-preserving multireceiver ID-based encryption with provable security. *Int. J. Commun. Syst.* **2014**, *27*, 1034–1050.
22. Tseng, Y.M.; Huang, Y.H.; Chang, H.J. CCA-Secure Anonymous Multi-Receiver ID-Based Encryption. In 26th International Conference on Advanced Information Networking and Applications Workshops, Fukuoka, Japan, 26–29 March 2012; pp. 177–182.
23. Tseng, Y.M.; Tsai, T.T.; Huang, S.S.; Chien, H.Y. Efficient anonymous multi-receiver ID-based encryption with constant decryption cost. In Proceedings of the 2014 International Conference on Information Science, Electronics and Electrical Engineering (ISEEE), Sapporo, Japan, 26–28 April 2014; pp. 131–137.
24. Wang, H. Insecurity of "Improved Anonymous Multi-Receiver Identity-Based Encryption". *Comput. J.* **2013**, doi:10.1093/comjnl/bxt052.
25. Wang, H.; Zhang, Y.; Xiong, H.; Qing, B. Crytanalysis and improvements of an anonymous multi-receiver identity-based encryption scheme. *IET Inf. Secur.* **2012**, *6*, 20–27.
26. Wang, H. Provably Secure Anonymous Multi-receiver Identity-Based Encryption with Shorter Ciphertext. In Proceedings of the 2014 IEEE 12th International Conference on Dependable, Autonomic and Secure Computing (DASC), Dalian, China, 24–27 August 2014; pp. 85–90.
27. Zhang, B.; Sun, T.; Yu, D. ID-Based Anonymous Multi-Receiver Key Encapsulation Mechanism with Sender Authentication. In *Algorithm and Architectures for Parallel Processing*; Lecture Notes in Computer Science; Springer-Verlag Berlin Heidelberg: New York, NY, USA, 2014; Volume 8631, pp. 645–658.
28. Zhang, J.; Mao, J. An improved anonymous multi-receiver identity-based encryption Scheme. *Int. J. Commun. Syst.* **2015**, *28*, 645–658.

29. Zhang, J.; Xu, Y. Comment on Anonymous Multi-Receiver Identity-Based Encryption Scheme. In Proceedings of the 4th International Conference on Intelligent Networking and Collaborative Systems, Barcelona, Spain, 19–21 September 2012; pp. 473–476.
30. Zhang, J.; Xu, Y.; Zou, J. Comment on Wang et al.'s anonymous multi-receiver ID-based encryption scheme and its improved schemes. *Int. J. Intell. Inf. Database Syst.* **2013**, *7*, 400–413.
31. Zhang, M.; Takagi, T. Efficient constructions of anonymous multireceiver encryption protocol and their deployment in group E-Mail systems with privacy preservation. *IEEE Syst. J.* **2013**, *7*, 410–419.
32. Delerablée, C.; Paillier, P.; Pointcheval, D. Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size or Decryption Keys. In *Pairing-Based Cryptography—Pairing 2007*; Takagi, T., Ed.; Springer, Berlin, Germany, 2007; Volume 4575, pp. 39–59.
33. Delerablée, C. Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys. In *Advances in Cryptology-EUROCRYPT 2007*; Springer: Berlin Heidelberg, Germany, 2007; pp. 200–215.
34. Nelly, F.; Perera, I.M. Outsider-Anonymous Broadcast Encryption with Sublinear Ciphertexts. In Proceedings of the 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, 21–23 May 2012; pp. 225–242.
35. Zhang, L.; Wu, Q.; Mu, Y. Anonymous Identity-Based Broadcast Encryption with Adaptive Security. In Proceedings of the 5th International Symposium, CSS 2013, Zhangjiajie, Hunan, China, 13–15 November 2013; pp. 258–271.
36. Libert, B.; Paterson, K.G.; Quaglia, E.A. Anonymous Broadcast Encryption: Adaptive Security and Efficient Construction in the Standard Model. In Proceedings of the 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, 21–23 May 2012; pp. 225–242.
37. Boneh, D.; Boyen, X.; Goh, E.J. Hierarchical Identity Based Encryption with Constant Size Ciphertext. In *Advances in Cryptology-EUROCRYPT 2005*; Springer: Berlin Heidelberg, Germany, 2005; pp. 440–456.
38. Kiayias, A.; Samari, K. Lower Bound for Private Broadcast Encryption. In *Information Hiding*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 176–190.
39. Neal, K.; Alfred, M.; Vanstone, S. The state of elliptic curve cryptography. *Des. Codes Cryptogr.* **2000**, *19*, 173–193.
40. Menezes, A.J.; Vanstone, S.A.; van Oorschot, P.C. *Handbook of Applied Cryptography*; CRC Press, Inc.: Boca Raton, FL, USA, 2001.
41. Scott, M. Implementing Cryptographic Pairings. In Proceedings of the Pairing-Based Cryptography, Tokyo, Japan, 2–4 July 2007; pp. 177–196.
42. Zhang, Y.; Liu, W.; Lou, W.; Fang, Y. Securing mobile Ad Hoc networks with certificateless public keys. *IEEE Trans. Depend.z Secur. Comput.* **2006**, *3*, 386–399.