Hindawi
Security and Communication Networks
Volume 2021, Article ID 5519721, 11 pages
https://doi.org/10.1155/2021/5519721

Research Article

Anonymous Multireceiver Identity-Based Encryption against Chosen-Ciphertext Attacks with Tight Reduction in the Standard Model

Yi-Fan Tseng[1] **and Chun-I Fan**[2,3,4]

[1]*Department of Computer Science, National Chengchi University, Taipei 11605, Taiwan*
[2]*Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung 80424, Taiwan*
[3]*Information Security Research Center, National Sun Yat-sen University, Kaohsiung 80424, Taiwan*
[4]*Intelligent Electronic Commerce Research Center, National Sun Yat-sen University, Kaohsiung 80424, Taiwan*

Correspondence should be addressed to Chun-I Fan; cifan@mail.cse.nsysu.edu.tw

Received 17 February 2021; Revised 6 April 2021; Accepted 24 May 2021; Published 15 June 2021

Academic Editor: Stelvio Cimato

Multireceiver identity-based encryption is a cryptographic primitive, which allows a sender to encrypt a message for multiple receivers efficiently and securely. In some applications, the receivers may not want their identities to be revealed. Motivated by this issue, in 2010, Fan et al. first proposed the concept of anonymous multireceiver identity-based encryption (AMRIBE). Since then, lots of literature studies in this field have been proposed. After surveying the existing works, however, we found that most of them fail to achieve provable anonymity with tight reduction. A security proof with tight reduction means better quality of security and better efficiency of implementation. In this paper, we focus on solving the open problem in this field that is to achieve the ANON-IND-CCA security with tight reduction by giving an AMRIBE scheme. The proposed scheme is proven to be IND-MID-CCA and ANON-MID-CCA secure with tight reduction under a variant of the DBDH assumption. To the best of our knowledge, this is the first scheme proven with tight reducible full CCA security in the standard model.

1. Introduction

Identity-based encryption (IBE) is a large class of public key encryption in modern cryptography. The concept of IBE was first proposed by Shamir [1] in 1984, and the first practical construction was independently proposed by Boneh and Franklin [2] and Cocks [3] in 2001. In an IBE scheme, a user can use any string as her/his public key, such as national identifier number and e-mail address.

It is a natural question to ask how to design a multireceiver IBE to encrypt a message with better efficiency compared with individually encrypting to each user in terms of either computation cost or communication cost. Such a cryptographic primitive is popular in advanced applications such as video conferencing, pay-per-view TV [4–8], and distance education. The notion of multireceiver identity-based encryption (MRIBE) was first considered by Beak et al. [9] in 2005. In an MRIBE scheme, the input of the encryption algorithm is a set of identities rather than a single identity. A user who is selected in the set is able to decrypt the ciphertext. MRIBE then drew the attention of the research community, and lots of results [10, 11] have been proposed.

Another notion similar to MRIBE is identity-based broadcast encryption (IBBE) [12–14]. An IBBE scheme is usually designed in the sense of key encapsulation mechanism (KEM), where the encryption algorithm takes as input only a set of identities and outputs a header and an encryption key. To encrypt a message, one then uses the encryption key with a data encryption mechanism (DEM), such as DES and AES. A user whose identity is selected in the set can use her/his private key together with the header to recover the encryption key. On the other hand, an

encryption scheme can be regarded as a key encapsulation mechanism by simply setting a ciphertext as the header and the corresponding plaintext as the encryption key. In this paper, we will treat MRIBE and IBBE as the identical notion.

In some situations, such as ordering sensitive TV programs, the customers may expect that their identities are not revealed. In consideration of privacy-preserving, Fan et al. [15] first introduced the concept of anonymous multireceiver ID-based encryption (AMRIBE) in 2010. Anonymity is defined as that no one should know the identities of the receivers except the encryptor. They also proposed a multireceiver ID-based encryption scheme using Lagrange interpolating polynomials. Unfortunately, their scheme was pointed out to be flawed by Chien [16] in 2012. In Fan et al. scheme, anyone given a ciphertext is able to reveal the receivers. Chien further indicated that the security model defined in [15] does not cover all of the multireceiver scenarios. He also proposed an improved AMRIBE scheme in [16]. Since then, many results of AMRIBE have been proposed [17–25].

After examining these AMRIBE schemes, we found that there is no AMRIBE scheme achieving full-ID security with tight reduction against chosen-ciphertext attacks. Filling the gap is significant for the researches of AMRIBE in terms of both theoretical and practical aspects.

Most of the existing AMRIBEs are only proven to be secure in the weaker "selective-ID" model, where the attacker must commit a target receiver set that it will attack at the beginning of the security game. The selective-ID model might not be appropriate for the attack model in a realistic environment, since the attackers should be able to adaptively choose their target after learning some information of the system. This characteristic is captured by another stronger model called "full-ID" model, where the attacker chooses the target at the challenge phase rather than at the beginning. In [26, 27], Boneh and Boyen show that a selective-ID secure IBE can also be proven to be full-ID secure. Roughly speaking, a challenger can make a guess on which identity, said ID^*, will be targeted at the challenge phase before it starts the simulation. If the adversary makes a query with ID^* or does not activate the challenge phase with ID^*, then the simulation is aborted. However, the proof strategy makes the reduction "lossy," i.e., the reduction is not tight. Let N be the number of allowed identities, then the reduction will lose a factor of N. That is, if the adversary wins the security game with advantage ϵ, then the challenger only guarantees to solve the underlying hard problem with advantage $\epsilon' \leq (\epsilon/N)$ (actually the analysis should take the running times into consideration. Here, we simply assume that the running times of the adversary and the challenger are asymptotically equivalent). More details can be referred to [26, 28].

A lossy reduction is not merely a theoretic problem; it also relates to the efficiency and efficacy of the entire system. We give a simple example for the (informal) analysis as follows. If we want to build an IBE system based on the DBDH assumption with 80-bit security level, and assume $N = 2^{160}$, then we need to adopt a DBDH-hard group whose order is 2^{240} due to the lossiness. This will make the entire system inefficient since we need a longer bit representation for the group of larger order [29]. Therefore, achieving tight reduction is a significant goal for an encryption scheme, since it affects both security and efficiency. The tight reduction allows one to construct an encryption scheme with the same security level as the underlying hard assumption. We refer the readers to [30] for more detailed examples.

The consequence of a lossy reduction will be much more worse when it comes to more complex primitives, such as AMRIBE. In the security game of AMRIBE, an adversary activates the challenge phase with t receivers, where t can be any positive number smaller than the number of the total possible identities. Assume that we set an identity to be an n-bits string, then a challenger needs to guess the target receiver set from $\sum_{t=1}^{2^n} \binom{2^n}{t} = 2^{2^n}$ different combinations. This makes the scheme impractical, since either the bit length of the representation for the underlying group will be exponentially large, or the reduction will be successful only with negligible advantage in the security proof.

1.1. Contributions. For both practical and theoretical reasons mentioned above, in this paper, we propose the first AMRIBE scheme achieving full-ID security in confidentiality and anonymity with tight reduction. It is worth noting that the security of our scheme is proven in the standard model, i.e., without random oracles. The random oracle model [31] is a heuristic and idealized model used to help people to prove the security of cryptographic primitives. In the security proofs, one usually models a cryptographic hash function as a random oracle. However, there are schemes proven secure in the random oracle models while being insecure when implementing the random oracle with any hash function in the real world [32, 33]. To the best of our knowledge, our scheme is the first and only one to achieve IND-MID-CCA/ANON-MID-CCA security (the abbreviation of "Indistinguishability under full-multi-ID chosen-ciphertext attacks" and "Anonymity under full-multi-ID chosen-ciphertext attacks") with tight reduction in the standard model. Besides, compared with other existing schemes, the encryption cost is low. Therefore, our scheme fits the scenario that a sender needs frequently to send messages for large amount of users, such as e-mail systems with receiver anonymity.

1.2. Organization. The remainder of this paper is organized as follows. Section 2 presents some preliminaries, specifically our security notions and the complexity assumptions that will be used in the security proofs. In Section 3, we introduce our AMRIBE scheme. Section 4 provides security proofs for the confidentiality and anonymity of our proposed scheme. Next, we show the comparison between our scheme and the existing works in properties and performances in Section 5. Finally, Section 6 concludes our work and provides future research directions.

2. Preliminaries

2.1. Notations. In this paper, we use multiplicative group representation. For $[m, n]$ where $m < n$, we mean the successive integer set from m to n, i.e., $\{m, m+1, \ldots, n\}$. Furthermore, for an integer n, $[n]$ denotes the integer set

$\{1, 2, \ldots, n\}$. For a set S, by "$x \xleftarrow{\$}$ " we mean "choose x uniformly from S". For an algorithm $\mathscr{A}$, by "$x \longleftarrow \mathscr{A}$," we denote "$x$ is the output of $\mathscr{A}$". For a bit-string s, we denote the i-th bit of s as $s[i]$.

2.2. Bilinear Mapping

Definition 1. Let $\mathbb{G}, \widehat{\mathbb{G}}$, and $\mathbb{G}_T$ be three multiplicative cyclic groups of prime order p. A bilinear map (pairing) e: $\mathbb{G} \times \widehat{\mathbb{G}} \longrightarrow \mathbb{G}_T$ satisfies the following properties in which $g, \widehat{g}$ is a generator of $\mathbb{G}, \widehat{\mathbb{G}}$, respectively.

(i) Bilinearity: $e(g^a, \widehat{g}^b) = e(g, \widehat{g})^{ab}$, $\forall a, b \in \mathbb{Z}_p$.

(ii) Nondegeneracy: if $e(g, \widehat{g}) = 1_{\mathbb{G}_T}$, the identity element of $\mathbb{G}_T$, then either g is the identity of $\mathbb{G}$ or $\widehat{g}$ is the identity of $\widehat{\mathbb{G}}$.

(iii) Computability: there exists an efficient algorithm to compute the function e.

In this paper, we use type 3 pairings [34, 35], where $\mathbb{G} \neq \widehat{\mathbb{G}}$ and no efficient computable isomorphisms $\widehat{\mathbb{G}}$ between $\mathbb{G}$ are known.

2.3. Complexity Assumptions.

The security of the proposed scheme is based on a variant of the decisional bilinear Diffie–Hellman (DBDH) problem, called DBDH-3 problem [36–39]. Let $\mathbb{G}, \widehat{\mathbb{G}}$, and $\mathbb{G}_T$ be three multiplicative cyclic groups of prime order p, where $g, \widehat{g}$ is a generator of $\mathbb{G}, \widehat{\mathbb{G}}$, respectively. Let e: $\mathbb{G} \times \widehat{\mathbb{G}} \longrightarrow \mathbb{G}_T$ be a type 3 pairing.

Definition 2 (a variant of DBDH problem in type 3 pairing groups—DBDH-3). Given $(g, \widehat{g}, \widehat{g}^a, \widehat{g}^b, g^b, g^c, \widehat{g}^c, Z)$, where $a, b, c \xleftarrow{\$}$ decide whether $Z = e(g, \widehat{g})^{abc}$ or a random element in $\mathbb{G}_T$.

We say that an algorithm $\mathscr{B}$ that outputs a bit has the advantage ϵ in solving the DBDH-3 problem if

$$\left|\Pr\left[\mathscr{B}\left(g, \widehat{g}, \widehat{g}^a, \widehat{g}^b, g^b, g^c, \widehat{g}^c, e(g, \widehat{g})^{abc}\right) = 1\right] - \Pr\left[\mathscr{B}\left(g, \widehat{g}, \widehat{g}^a, \widehat{g}^b, g^b, g^c, \widehat{g}^c, Z \longleftarrow \mathbb{G}_T\right) = 1\right]\right| \geq \epsilon. \quad (1)$$

Definition 3 (the DBDH-3 assumption). We say that the (τ, ϵ)-DBDH-3 assumption holds if no τ-time algorithm has advantage at least ϵ in solving the DBDH-3 problem. We occasionally drop (τ, ϵ) for simplicity.

2.4. Anonymous Multireceiver Identity-Based Encryption.

An AMRIBE scheme consists of the following algorithms:

(i) Setup(1^λ): this algorithm takes as input a security parameter λ and outputs the master secret key msk and the system parameter param. Note that all algorithms except Setup will implicitly take param as one of the inputs, and thus, we will omit the term param for simplicity.

(ii) KeyExtract(msk, ID): this algorithm takes as inputs the master secret key msk and an identity ID and then outputs the private key d_{ID} for user ID.

(iii) Encrypt(S, M): this algorithm takes as inputs an identity set $S = \{\mathrm{ID}_1, \ldots, \mathrm{ID}_t\}$ for any positive t and a message M and then outputs a ciphertext C.

(iv) Decrypt(C, d_{ID}): this algorithm takes as inputs a ciphertext and a private key for ID and then outputs a message M or a dedicated error symbol $\perp$.

Correctness. For all $C \longleftarrow$ Ecrypt(S, M), $d_{\mathrm{ID}} \longleftarrow$ KeyExtract(msk, ID):

(i) If ID $\in S$, then $M \longleftarrow$ Decrypt(C, d_{ID})

(ii) If ID $\in S$, then $\perp \longleftarrow$ Decrypt(C, d_{ID})

2.4.1. Confidentiality. Next, we will give the security definition for confidentiality. Consider the following game played between a challenger $\mathscr{C}$ and an adversary $\mathscr{A}$. The security game consists of four phases as follows:

Setup: $\mathscr{C}$ generates the system parameter params and sends it to $\mathscr{A}$.

Phase 1: $\mathscr{A}$ is allowed to make queries from the following oracles:

KeyExtract: $\mathscr{A}$ makes a KeyExtract query with an identity ID, and $\mathscr{C}$ returns the private key d_{ID} to $\mathscr{A}$
Decrypt: $\mathscr{A}$ makes a Decrypt query with a ciphertext C and an identity ID, and $\mathscr{C}$ returns the result of Decrypt(C, d_{ID})

Challenge: the adversary submits two messages M_0, M_1 with the same length and a target identity set $\mathrm{ID}^* = \{\mathrm{ID}_1^*, \ldots, \mathrm{ID}_t^*\}$ for any positive integer t, with the restriction that all identities in ID^* should not be submitted to KeyExtract oracle in Phase 1. $\mathscr{C}$ then randomly chooses $\beta \in \{0, 1\}$ and generates $C^* \longleftarrow$Encrypt(ID^*, M_β). Finally, C^* is returned to $\mathscr{A}$.

Phase 2: $\mathscr{A}$ is allowed to make queries as in Phase 1, except for *KeyExtract* queries with ID $\in \mathrm{ID}^*$ and Decrypt queries with $(C^*, \mathrm{ID} \in \mathrm{ID}^*)$.

Guess: finally, $\mathscr{A}$ outputs a bit β' and wins the game if $\beta' = \beta$.

One can observe that the above game is modelled for the security notion IND-MID-CCA. The security games for IND-sMID-CCA and IND-MID-CPA can be obtained by forcing $\mathscr{A}$ to commit ID^* before Setup and disallowing $\mathscr{A}$ to query Decrypt oracle, respectively. The advantage of $\mathscr{A}$ winning the game is defined as

$$\mathbf{Adv}^{\mathrm{IND-MID-CCA}}(\mathscr{A}) = \left|\Pr[\beta' = \beta] - \frac{1}{2}\right|. \quad (2)$$

We say that an AMRIBE scheme is (τ, ϵ)-IND-MID-CCA secure if all τ-time adversaries have at most advantage ϵ in winning the above IND-MID-CCA game.

2.4.2. Anonymity. Next, we define the anonymity for an AMRIBE. Consider the following game played between a challenger $\mathscr{C}$ and an adversary $\mathscr{A}$. The security game consists of four phases as follows:

Setup: $\mathscr{C}$ generates the system parameter params and sends it to $\mathscr{A}$.

Phase 1: $\mathscr{A}$ is allowed to make queries from the following oracles:

KeyExtract: $\mathscr{A}$ makes a KeyExtract query with an identity ID, and $\mathscr{C}$ returns the private key d_{ID} to $\mathscr{A}$
Decrypt: $\mathscr{A}$ makes a Decrypt query with a ciphertext C and an identity ID, and $\mathscr{C}$ returns the result of $\mathrm{Decrypt}(C, d_{\mathrm{ID}})$

Challenge: the adversary submits a message M, a target identity set $\mathrm{ID}^* = \{\mathrm{ID}_0^*, \mathrm{ID}_1^*\}$, and an identity set $\{\mathrm{ID}_2^*, \ldots, \mathrm{ID}_t^*\}$ for any positive integer t, with the restriction that all identities in ID^* should not be submitted to KeyExtract oracle in Phase 1. $\mathscr{C}$ then randomly chooses $\beta \in \{0,1\}$, sets $S_\beta^* = \{\mathrm{ID}_\beta^*, \mathrm{ID}_2^*, \ldots, \mathrm{ID}_t^*\}$, and generates $C^* \longleftarrow \mathrm{Encrypt}(S_\beta^*, M)$. Finally, C^* is returned to $\mathscr{A}$.

Phase 2: $\mathscr{A}$ is allowed to make queries as in Phase 1, except for KeyExtract queries with $\mathrm{ID} \in \mathrm{ID}^*$ and Decrypt queries with $(C^*, \mathrm{ID} \in \mathrm{ID}^*)$.

Guess: finally, $\mathscr{A}$ outputs a bit β' and wins the game if $\beta' = \beta$.

The above game is modelled for the security notion ANON-MID-CCA (the security games for ANON-sMID-CCA and ANON-MID-CPA can be obtained by forcing $\mathscr{A}$ to commit ID^* before Setup and disallowing $\mathscr{A}$ to query Decrypt oracle, respectively). The advantage of $\mathscr{A}$ winning the game is defined as follows:

$$\mathrm{Adv} - \mathrm{ANON} - \mathrm{MID} - \mathrm{CCA}\mathscr{A} = \left|\Pr[\beta' = \beta] - \frac{1}{2}\right|. \quad (3)$$

We say that an AMRIBE scheme is (τ, ϵ)-ANON-MID-CCA secure if all τ-time adversaries have at most advantage ϵ in winning the above ANON-MID-CCA game.

Remark 1. Note that this definition is actually modelled against insider adversaries, since $\mathscr{A}$ is allowed to query the private key for $\{\mathrm{ID}_2^*, \ldots, \mathrm{ID}_t^*\}$, and the encrypted message M is chosen by $\mathscr{A}$.

Remark 2. The ANON-MID-CCA game defined above is slightly different from some existing works, such as [19, 20, 22]. In their definition, $\mathscr{A}$ submits two different identity sets S_0^*, S_1^*, where $|S_0^*| = |S_1^*|$, with the restriction that all $\mathrm{ID} \in S_0^* \Delta S_1^* = (S_0^*/S_1^*) \cup (S_1^*/S_0^*)$ have not been queried to KeyExtract oracle. In our model, one can image that $S_0^* = \{\mathrm{ID}_0^*, \mathrm{ID}_2^*, \ldots, \mathrm{ID}_t^*\}$ and $S_1^* = \{\mathrm{ID}_1^*, \mathrm{ID}_2^*, \ldots, \mathrm{ID}_t^*\}$, and thus, $S_0^* \Delta S_1^* = \{\mathrm{ID}_0^*, \mathrm{ID}_1^*\}$, where $|S_0^* \Delta S_1^*|$ is minimal. Actually, our model may be a stronger model since we allow an adversary to query as much private keys as possible, as long as the trivial way to win the game is prevented from the adversary.

2.5. Tight Security Reduction. In this section, we introduce the notion of tight security reduction. To prove the security of a cryptographic primitive, we usually construct a reduction between the security of the primitive and a well-studied hard assumption. That is, if there is an algorithm $\mathscr{A}$ breaks the security of the primitive, then there exists an algorithm $\mathscr{C}$ that makes black-box use of $\mathscr{A}$ to solve the hard problem. Assume that the algorithm $\mathscr{A}$ breaks the primitive with advantage $\epsilon_{\mathscr{A}}$ in time $\tau_{\mathscr{A}}$, and the algorithm $\mathscr{C}$ breaks the assumption with advantage $\epsilon_{\mathscr{C}}$ in time $\tau_{\mathscr{C}}$. In a conventional sense [40], a reduction is said to be tight if $\epsilon_{\mathscr{C}} \approx \epsilon_{\mathscr{A}}$ and $\tau_{\mathscr{C}} \approx \tau_{\mathscr{A}}$. Another weaker notion of tight reduction is defined in [30, 41]. The quality of a reduction can also be measured by the ratio between $(\tau_{\mathscr{A}}/\epsilon_{\mathscr{A}})$ and $(\tau_{\mathscr{C}}/\epsilon_{\mathscr{C}})$. Let

$$\frac{\tau_{\mathscr{C}}}{\epsilon_{\mathscr{C}}} = \ell \cdot \left(\frac{\tau_{\mathscr{A}}}{\epsilon_{\mathscr{A}}}\right). \quad (4)$$

In the above equation, "ℓ" is the "loss" for the reduction. A reduction is efficient if the loss ℓ is polynomially bounded. If ℓ is constant, then the reduction is said to be weakly tight. From this definition, we can see why an efficient (or ideally, tight) reduction is important. We briefly explain the reason. Assume that $\tau_{\mathscr{C}} \approx \tau_{\mathscr{A}}$, then we have

$$\epsilon_{\mathscr{C}} = \frac{\epsilon_{\mathscr{A}}}{\ell}. \quad (5)$$

If ℓ is exponentially large, then $\epsilon_{\mathscr{C}}$ may be negligible; even if the adversary's advantage $\epsilon_{\mathscr{A}}$ is nonnegligible, we cannot base the security of our protocol on the underlying complexity assumptions.

3. Anonymous Multireceiver Identity-Based Encryption with Tight Reduction

In this section, we demonstrate a novel AMRIBE scheme with tight reduction. The proposed AMRIBE scheme is, to the best of our knowledge, the first such scheme with full security under tight reduction in the standard model.

3.1. The Proposed AMRIBE with Tight Reduction. Let $\mathbb{G}, \widehat{\mathbb{G}}$, and $\mathbb{G}_T$ be three cyclic multiplicative groups with prime order p and $g, \widehat{g}$ be the generators of $\mathbb{G}, \widehat{\mathbb{G}}$, respectively. In this scheme, we adopt type 3 pairing, i.e., e: $\mathbb{G} \times \widehat{\mathbb{G}} \longrightarrow \mathbb{G}_T$. The proposed scheme consists of the following algorithms:

Setup (1^λ): taking as input a security parameter 1^λ, KGC performs as follows:

(1) Choose $\alpha, \beta \xleftarrow{\$}$.

(2) Choose two cryptographic hash functions H: $\{0,1\}^* \longrightarrow \{0,1\}^n$ and H_1: $\{0,1\}^* \longrightarrow \mathbb{Z}_p$, where n is a positive integer.

(3) Compute $\Omega = e(g, \widehat{g})^{\alpha\beta}$, $\Lambda = e(g, \widehat{g})^{\alpha(\beta-1)}$.

(4) For $i \in [n]$, choose $\nu_i \xleftarrow{\$}$ and compute $I_i = g^{\nu_i}, \widehat{I}_i = \widehat{g}^{\nu_i}$.

(5) Choose $\phi, \psi \xleftarrow{\$}$, and compute $\widehat{\Phi} = \widehat{g}^{\phi}, \widehat{\Psi} = \widehat{g}^{\psi}$.

(6) Publish the system parameter

$$\text{param} = \left(\mathbb{G}, \widehat{\mathbb{G}}, \mathbb{G}_T, e, p, g, \Omega, \Lambda, \{I_i\}_{i\in[n]}, \widehat{\Phi}, \widehat{\Psi}, H, H_1\right). \tag{6}$$

and keep secret the master secret key $\text{msk} = (\widehat{g}, \widehat{g}^{\alpha}, \{\widehat{I}_i\}_{i\in[n]})$.

KeyExtract(msk, ID): taking as input the master secret key $\text{msk} = (\widehat{g}, \widehat{g}^{\alpha}, \{\widehat{I}_i\}_{i\in[n]})$ and an identity ID, KGC computes the private key for ID as follows. For convenience, given an identity ID, where the corresponding hash value $H(\text{ID})$ is h_{ID}, we define a function $\widehat{F}(\text{ID}) = \prod_{i\in[n]} \widehat{I}_i^{h_{\text{ID}}[i]}$.

(1) Choose $r \xleftarrow{\$}$

(2) Compute $\widehat{F}(\text{ID})$

(3) Set the private key $d_{\text{ID}} = (\widehat{d}_{\text{ID},0}, \widehat{d}_{\text{ID},1}) = (\widehat{g}^{\alpha}(\widehat{F}(\text{ID}))^r, \widehat{g}^r)$

Encrypt(S, M): taking as input an identity set $S = \{\text{ID}_1, \ldots, \text{ID}_t\}$ for a positive integer t and a message $M \in \mathbb{G}_T$, the sender performs as follows. For convenience, given an identity ID, where the corresponding hash value $H(\text{ID})$ is h_{ID}, we define a function $F(\text{ID}) = \prod_{i\in[n]} I_i^{h_{\text{ID}}[i]}$.

(1) Choose $s \xleftarrow{\$}$.

(2) For $i \in [t]$, compute $F(\text{ID}_i)$.

(3) Compute $C_0 = M \cdot \Omega^s, C_1 = \Lambda^s, C_2 = g^s, C_{3,i} = F(\text{ID}_i)^s$ for $i \in [t]$, and $K = (\Lambda^s/\Omega^s)$.

(4) Compute $h = H_1(C_0, C_1, C_2, C_{3,1}, \ldots, C_{3,t}, K, M)$, and $\widehat{\Gamma} = (\widehat{\Phi} \cdot \widehat{\Psi}^h)^s$.

(5) The ciphertext is $C = (C_0, C_1, C_2, \{C_{3,i}\}_{i\in[t]}, \widehat{\Gamma})$.

Decrypt(C, d_{ID}): taking as input a ciphertext $C = (C_0, C_1, C_2, \{C_{3,i}\}_{i\in[t]}, \widehat{\Gamma})$ and a private key d_{ID}, a user ID performs as follows. For $i \in [t]$, compute $K' = (e(C_{3,i}, \widehat{d}_{\text{ID},1})/e(C_2, \widehat{d}_{\text{ID},0}))$ and $M' = (C_0/C_1) \cdot K'$. Then the user computes $h = H_1(C_0, C_1, C_2, C_{3,1}, \ldots, C_{3,t}, K', M')$ and checks whether $e(C_2, \widehat{\Phi} \cdot \widehat{\Psi}^h) = e(g, \widehat{\Gamma})$. If the equality holds, then output M'. If the equality does not hold for all $i \in [t]$, then output $\perp$.

Correctness. Assume that $\text{ID} \in S$ (say $\text{ID} = \text{ID}_i$) and $h_{\text{ID}} = H(\text{ID})$. Note that $e(F(\text{ID}), \widehat{g}) = e(g, \widehat{F}(\text{ID}))$ since the discrete logarithms of both sides are equal. We have

$$K' = \frac{e\left(C_{3,i}, \widehat{d}_{\text{ID},1}\right)}{e\left(C_2, \widehat{d}_{\text{ID},0}\right)} = \frac{e\left(F(\text{ID}_i)^s, \widehat{g}^r\right)}{e\left(g^s, \widehat{g}^{\alpha}(\widehat{F}(\text{ID}))^r\right)} = \frac{e\left(\left(\prod_{j\in[n]} I_j^{h_{\text{ID}}[j]}\right)^s, \widehat{g}^r\right)}{e\left(g^s, \widehat{g}^{\alpha}\left(\prod_{j\in[n]} \widehat{I}_j^{h_{\text{ID}}[j]}\right)^r\right)} = \frac{1}{e(g, \widehat{g})^{\alpha s}} = \frac{\Lambda^s}{\Omega^s} = K, \tag{7}$$

and thus

$$M' = \frac{C_0}{C_1} \cdot K' = \frac{M \cdot e(g, \widehat{g})^{\alpha\beta s}}{e(g, \widehat{g})^{\alpha(\beta-1)s} e(g, \widehat{g})^{\alpha s}} = M. \tag{8}$$

Besides, the integrity of the ciphertext and the message can be verified by whether $e(C_2, \widehat{\Phi} \cdot \widehat{\Psi}^h) = e(g, \widehat{\Gamma})$.

Remark 3. In the computations of $F(\text{ID}) = \prod_{i\in[n]} I_i^{h[i]}$ ($\widehat{F}(\text{ID}) = \prod_{i\in[n]} I_i^{h[i]}$), it seems that lots of scalar operations for $\mathbb{G}$ ($\widehat{\mathbb{G}}$) must be performed. However, we can construct an index set $\mathcal{I}_{\text{ID}} = \{i | h[i] = 1\}$, where $h = H(\text{ID})$ before computing $F(\text{ID})$ ($\widehat{F}(\text{ID})$). We then compute $F(\text{ID}) = \prod_{i\in\mathcal{I}_{\text{ID}}} I_i$ ($\widehat{F}(\text{ID}) = \prod_{i\in\mathcal{I}_{\text{ID}}} \widehat{I}_i$). Therefore, we can compute $F(\text{ID})$ ($\widehat{F}(\text{ID})$) using only at most n cheap group operations.

4. Security Proofs

Theorem 1. *The proposed AMRIBE scheme is (τ, ϵ)-IND-MID-CCA secure in the standard model if the (τ', ϵ')-DBDH-3 assumption holds, where $\epsilon = \epsilon'$ and $\tau = \tau' - \mathcal{O}(q_D \cdot T_P)$ (q_D is the maximum number of Decrypt queries and T_P is the time required for a pairing).*

Proof. Given $(g, \widehat{g}, \widehat{g}^a, \widehat{g}^b, g^b, g^c, \widehat{g}^c, Z)$, the challenger $\mathscr{C}$ simulates the following game for the adversary $\mathscr{A}$:

Setup: $\mathscr{C}$ performs as follows:

(1) Choose two cryptographic hash functions $H: \{0,1\}^* \longrightarrow \{0,1\}^n$ and $H_1: \{0,1\}^* \longrightarrow \mathbb{Z}_p$, where n is the length of an identity.

(2) Set $\Omega = e(g^b, \widehat{g}^a), \Lambda = e((g^b/g), \widehat{g}^a) = e(g, \widehat{g})^{a(b-1)}$.

(3) For $i \in [n]$, choose $\nu_i \xleftarrow{\$}$ and compute $I_i = g^{\nu_i}, \widehat{I}_i = \widehat{g}^{\nu_i}$.

(4) Choose $\phi, \psi \xleftarrow{\$}$, and compute $\widehat{\Phi} = \widehat{g}^{\phi}, \widehat{\Psi} = \widehat{g}^{\psi}$.

(5) Set the master secret key $\text{msk} = (\widehat{g}, \widehat{g}^a, \{\widehat{I}_i\}_{i\in[n]})$.

(6) Send the system parameter

$$\text{param} = \left(\mathbb{G}, \widehat{\mathbb{G}}, \mathbb{G}_T, e, p, g, \Omega, \Lambda, \{I_i\}_{i\in[n]}, \widehat{\Phi}, \widehat{\Psi}, H, H_1\right) \text{ to } \mathscr{A}. \tag{9}$$

Phase 1: in this phase, $\mathscr{A}$ is allowed to make queries from KeyExtract and Decrypt oracles. Since $\mathscr{C}$ knows the master secret key msk, it can easily answer KeyExtract and Decrypt queries as the same way as the proposed scheme.

Challenge: $\mathscr{A}$ sends (M_0, M_1) and a set of receivers $\text{ID}^* = \{\text{ID}_1^*, \ldots, \text{ID}_t^*\}$ for a positive integer t to $\mathscr{C}$, where M_0, M_1 are two distinct messages with the same length, and

KeyExtract(ID_i^*) has not been queried in Phase 1 for $i \in [t]$. Then $\mathscr{C}$ performs as follows:

(1) Choose $\beta \xleftarrow{\$}$ compute $C_0 = M_\beta \cdot Z$

(2) Compute $C_1 = (Z/e(g^c, \widehat{g}^a)), K = (1/e(g^c, \widehat{g}^a))$

(3) Set $C_2 = g^c$

(4) For $i \in [t]$, let $h_i^* = H(\mathrm{ID}_i^*)$, compute $C_{3,i} = (g^c)^{\sum_{j \in [n]} \nu_j h_i^*[j]}$

(5) Compute $h = H_1(C_0, C_1, C_2, C_{3,1}, \ldots, C_{3,t}, K, M_\beta)$, and $\widehat{\Gamma} = (\widehat{g}^c)^{\phi + \psi h}$

(6) Output the challenge ciphertext $C^* = (C_0, C_1, C_2, \{C_{3,i}\}_{i \in [t]}, \widehat{\Gamma})$

Phase 2: $\mathscr{A}$ makes the same queries as Phase 1. However, $\mathscr{A}$ is unable to query Decrypt(C^*, ID) and KeyExtract(ID) for $\mathrm{ID} \in \mathrm{ID}^*$.

Guess: finally, $\mathscr{A}$ outputs a bit β' and wins the game if $\beta' = \beta$. Then, $\mathscr{C}$ outputs 1 if $\mathscr{A}$ wins the game; otherwise, outputs 0.

Perfect simulation: since $\mathscr{C}$ has full control on the master secret key msk, KeyExtract oracle and Decrypt oracle can be simulated perfectly. As for the challenge ciphertext C^*, we implicitly set $s = c$. If $Z = e(g, \widehat{g})^{abc}$, then we have that

(i) $C_0 = M_\beta \cdot Z = M_\beta \cdot e(g^b, \widehat{g}^a)^c = M_\beta \cdot \Omega^c$

(ii) $C_1 = (Z/e(g^c, \widehat{g}^a)) = (e(g, \widehat{g})^{abc}/e(g, \widehat{g})^{ac}) = (e(g, \widehat{g})^{a(b-1)})^c = \Lambda^c$

(iii) $C_2 = g^c$

(iv) For $i \in [t], C_{3,i} = (g^c)^{\sum_{j \in [n]} \nu_j h_i^*[j]} = (\prod_{j \in [n]} (g^{\nu_i})^{h_i^*[j]})^c = (\prod_{j \in [n]} I_j^{h_i^*[j]})^c$

(v) $\widehat{\Gamma} = (\widehat{g}^c)^{\phi + \psi h} = (\widehat{g}^\phi \cdot \widehat{g}^{\psi h})^c = (\widehat{\Phi} \cdot \widehat{\Psi}^h)^c$

Therefore, the challenge ciphertext C^* is well formed. If Z is a random element in $\mathbb{G}_T$, then the distribution of β is independent from $\mathscr{A}$'s view, and thus, the advantage will be 0.

Probability analysis: we then analyse the advantage that $\mathscr{C}$ breaks the DBDH-3 assumption. If $Z = e(g, \widehat{g})^{abc}$, we have $\mathrm{Adv}^{\mathrm{IND-MID-CCA}}(\mathscr{A}) = |\Pr[\beta' = \beta] - (1/2)| \geq \epsilon$. If Z is a random element in $\mathbb{G}_T$, we have $\mathrm{Adv}^{\mathrm{IND-MID-CCA}}(\mathscr{A}) = |\Pr[\beta' = \beta] - (1/2)| = 0$. Therefore, we have

$$\begin{aligned} &\left|\Pr\left[\mathscr{C}\left(g, \widehat{g}, \widehat{g}^a, \widehat{g}^b, g^b, g^c, \widehat{g}^c, Z = e(g,g)^{abc}\right) = 1\right] - \Pr\left[\mathscr{C}\left(g, \widehat{g}, \widehat{g}^a, \widehat{g}^b, g^b, g^c, \widehat{g}^c, Z \xleftarrow{} \mathbb{G}_T\right) = 1\right]\right| \\ &= \left|\Pr\left[\beta' = \beta | Z = e(g,g)^{abc}\right] - \Pr\left[\beta' = \beta | Z \xleftarrow{} \mathbb{G}_T\right]\right| \geq \left|\frac{1}{2} + \epsilon - \frac{1}{2}\right| \geq \epsilon. \end{aligned} \tag{10}$$

Time complexity: let q_D be the maximum numbers of the Decrypt queries. Since in each Decrypt query, $\mathscr{C}$ needs to perform at most $4u$ pairings, where u is the size of the receiver set, we have that $\tau' = \tau + \mathcal{O}(q_D \cdot T_P)$, where T_P is the time required for a paring.

Tightness analysis: according to the definition given in Section 2.5, a reduction is said to be tight if $\epsilon' \approx \epsilon$ and $\tau' \approx \tau$. From the above analysis, we have that $\epsilon = \epsilon'$ and $\tau = \tau' - \mathcal{O}(q_D \cdot T_P)$. Since the DBDH-3 problem is an assume-to-be-hard problem, we have $\tau' = \mathcal{O}(\exp(\lambda))$, where λ is the security parameter and $\exp(\lambda)$ is an exponential function in λ. On the other hand, $q_D = \mathcal{O}(\mathrm{poly}(\lambda))$ and $T_p = \mathcal{O}(\mathrm{poly}'(\lambda))$, where $\mathrm{poly}(\lambda)$ and $\mathrm{poly}(\lambda)$ are polynomials of λ. Therefore, we know that $\tau \approx \tau'$. □

One may wonder that, since the reduction algorithm is able to generate a private key for any ID and accept any IDs for the challenge ciphertext, whether it is possible that the reduction algorithm generates a private key for $\mathrm{ID} \in \mathrm{ID}^*$ and decrypt C^* to check if $Z = (g, \widehat{g})^{abc}$. Note that our proof strategy is slightly similar to that of [28]. The challenge ciphertext is structured such that, if we decrypt C^* with the private key for $\mathrm{ID} \in \mathrm{ID}^*$, the decryption procedure will succeed no matter the value of Z is. In the decryption algorithm, we recover the message $M = (C_0/C_1) \cdot K$. In the reduction algorithm, we can see that both $C_2, C_{3,i}$ are valid no matter the value of Z is. Thus, if we compute $K = (e(C_{3,i}, \widehat{d}_{\mathrm{ID},1})/e(C_2, \widehat{d}_{\mathrm{ID},0}))$, then we will have $K = (1/e(g, \widehat{g})^{ac})$. It leads that

$$\frac{C_0}{C_1} \cdot K = \frac{M_\beta \cdot Z}{(Z/e(g^c, \widehat{g}^a))} \cdot \frac{1}{e(g, \widehat{g})^{ac}} = M_\beta. \tag{11}$$

Theorem 2. *The proposed AMRIBE scheme is (τ, ϵ)-ANON-MID-CCA secure in the standard model if the (τ', ϵ')-DBDH-3 assumption holds, where $\epsilon = \epsilon'$ and $\tau = \tau' - \mathcal{O}(q_D \cdot T_P)$ (q_D is the maximum number of Decrypt queries and T_P is the time required for a pairing).*

Proof. Given $(g, \widehat{g}, \widehat{g}^a, \widehat{g}^b, g^b, g^c, \widehat{g}^c, Z)$, the challenger $\mathscr{C}$ simulates the following game for the adversary $\mathscr{A}$:

Setup: $\mathscr{C}$ performs as follows.

(1) Choose two cryptographic hash functions $H: \{0,1\}^* \longrightarrow \{0,1\}^n$ and $H_1: \{0,1\}^* \longrightarrow \mathbb{Z}_p$, where n is a positive integer.

(2) Set $\Omega = e(g^b, \widehat{g}^a), \Lambda = e((g^b/g), \widehat{g}^a) = e(g, \widehat{g})^{a(b-1)}$.

(3) For $i \in [n]$, choose $\nu_i \xleftarrow{\$}$ and compute $I_i = g^{\nu_i}, \widehat{I}_i = \widehat{g}^{\nu_i}$.

(4) Choose $\phi, \psi \xleftarrow{\$}$, and compute $\widehat{\Phi} = \widehat{g}^\phi, \widehat{\Psi} = \widehat{g}^\psi$.

(5) Set the master secret key msk $= (\widehat{g}, \widehat{g}^a, \{\widehat{I}_i\}_{i \in [n]})$.

(6) Send the system parameter

$$\mathrm{param} = \left(\mathbb{G}, \widehat{\mathbb{G}}, \mathbb{G}_T, e, p, g, \Omega, \Lambda, \{I_i\}_{i \in [n]}, \widehat{\Phi}, \widehat{\Psi}, H, H_1\right) \text{ to } \mathscr{A}. \tag{12}$$

Phase 1: in this phase, $\mathscr{A}$ is allowed to make queries from KeyExtract and Decrypt oracles. Since $\mathscr{C}$ knows the master

secret key msk, it can easily answer KeyExtract and Decrypt queries as the same way as the proposed scheme.

Challenge: $\mathcal{A}$ sends M, $\mathrm{ID}^* = \{\mathrm{ID}_0^*, \mathrm{ID}_1^*\}$, and a set of identities $\{\mathrm{ID}_2^*, \ldots, \mathrm{ID}_t^*\}$ for a positive integer t to $\mathcal{C}$, where $\mathrm{KeyExtract}(\mathrm{ID}_i^*)$ has not been queried in Phase 1 for $\mathrm{ID}_i^* \in \mathrm{ID}^*$. Then $\mathcal{C}$ performs as follows:

(1) Choose $\beta \xleftarrow{\$}$ compute $C_0 = M \cdot Z$

(2) Compute $C_1 = (Z/e(g^c, \widehat{g}^a)), K = (1/e(g^c, \widehat{g}^a))$

(3) Set $C_2 = g^c$

(4) For $i \in [2, t] \cup \{\beta\}$, let $h_i^* = H(\mathrm{ID}_i^*)$, compute $C_{3,i} = (g^c)^{\sum_{j\in[n]} \nu_j h_i^*[j]}$

(5) Compute $\widehat{\Gamma} = (\widehat{g}^c)^{\phi+\psi h}$, where $h = H_1(C_0, C_1, C_2, C_{3,\beta}, C_{3,2}, \ldots, C_{3,t}, K, M)$

(6) Output the challenge ciphertext $C^* = (C_0, C_1, C_2, \{C_{3,i}\}_{i\in[2,t]\cup\{\beta\}}, \widehat{\Gamma})$

Phase 2: $\mathcal{A}$ makes the same queries as Phase 1. However, $\mathcal{A}$ is unable to query $\mathrm{Decrypt}(C^*, \mathrm{ID})$ and $\mathrm{KeyExtract}(\mathrm{ID})$ for $\mathrm{ID} \in \mathrm{ID}^*$.

Guess: finally $\mathcal{A}$ outputs a bit β' and wins the game if $\beta' = \beta$. Then $\mathcal{C}$ outputs 1 if $\mathcal{A}$ wins the game; otherwise outputs 0.

Perfect simulation: since $\mathcal{C}$ has full control on the master secret key msk, KeyExtract oracle and Decrypt oracle can be simulated perfectly. As for the challenge ciphertext C^*, we implicitly set $s = c$. If $Z = e(g, \widehat{g})^{abc}$, then we have that

(i) $C_0 = M \cdot Z = M \cdot e(g^b, \widehat{g}^a)^c = M \cdot \Omega^c$

(ii) $C_1 = (Z/e(g^c, \widehat{g}^a)) = (e(g, \widehat{g})^{abc}/e(g, \widehat{g})^{ac}) = (e(g, \widehat{g})^{a(b-1)})^c = \Lambda^c$

(iii) $C_2 = g^c$

(iv) For $i \in [2, t] \cup \{\beta\}, C_{3,i} = (g^c)^{\sum_{j\in[n]} \nu_j h_i^*[j]} = (\prod_{j\in[n]} (g^{\nu_i})^{h_i^*[j]})^c = (\prod_{j\in[n]} I_j^{h_i^*[j]})^c$

(v) $\widehat{\Gamma} = (\widehat{g})^{\phi+\psi h} = (\widehat{g}^{\phi} \cdot \widehat{g}^{\psi h})^c = (\widehat{\Phi} \cdot \widehat{\Psi}^h)^c$

Therefore, the challenge ciphertext C^* is well formed. If Z is a random element in $\mathbb{G}_T$, then the distribution of β is independent from $\mathcal{A}$'s view, and thus, the advantage will be 0.

Probability analysis: we then analyse the advantage that $\mathcal{C}$ breaks the DBDH-3 assumption. If $Z = e(g, \widehat{g})^{abc}$, we have $\mathrm{Adv}^{\mathrm{ANON-MID-CCA}}(\mathcal{A}) = |\Pr[\beta' = \beta] - (1/2)| \geq \epsilon$. If Z is a random element in $\mathbb{G}_T$, we have $\mathrm{Adv}^{\mathrm{ANON-MID-CCA}}(\mathcal{A}) = |\Pr[\beta' = \beta] - (1/2)| = 0$. Therefore, we have

$$\begin{aligned} &\left|\Pr\left[\mathcal{C}\left(g, \widehat{g}, \widehat{g}^a, \widehat{g}^b, g^b, g^c, \widehat{g}^c, Z = e(g,g)^{abc}\right) = 1\right] - \Pr\left[\mathcal{C}\left(g, \widehat{g}, \widehat{g}^a, \widehat{g}^b, g^b, g^c, \widehat{g}^c, Z \xleftarrow{} \mathbb{G}_T\right) = 1\right]\right| \\ &= \left|\Pr\left[\beta' = \beta | Z = e(g,g)^{abc}\right] - \Pr\left[\beta' = \beta | Z \xleftarrow{} \mathbb{G}_T\right]\right| \geq \left|\frac{1}{2} + \epsilon - \frac{1}{2}\right| \geq \epsilon. \end{aligned} \tag{13}$$

Time complexity: let q_D be the maximum numbers of the Decrypt queries. Since in each Decrypt query, $\mathcal{C}$ needs to perform at most $4u$ pairings, where u is the size of the receiver set, we have that $\tau' = \tau + \mathcal{O}(q_D \cdot T_P)$, where T_P is the time required for a paring.

Tightness analysis: according to the definition given in Section 2.5, a reduction is said to be tight if $\epsilon' \approx \epsilon$ and $\tau' \approx \tau$. From the above analysis, we have that $\epsilon = \epsilon'$ and $\tau = \tau' - \mathcal{O}(q_D \cdot T_P)$. Since the DBDH-3 problem is an assume-to-be-hard problem, we have $\tau' = \mathcal{O}(\exp(\lambda))$, where λ is the security parameter and $\exp(\lambda)$ is an exponential function in λ. On the other hand, $q_D = \mathcal{O}(\mathrm{poly}(\lambda))$ and $T_p = \mathcal{O}(\mathrm{poly}'(\lambda))$, where $\mathrm{poly}(\lambda)$ and $\mathrm{poly}'(\lambda)$ are polynomials of λ. Therefore, we know that $\tau \approx \tau'$. □

5. Comparisons

In this section, we give comparisons of our schemes with the existing schemes in both properties and efficiency. The notations used in this section are shown in Table 1, and the comparisons for the properties and performances between our scheme and the existing works are shown in Tables 2 and 3, respectively. For convenience, we set the following scenario to quantize the efficiency. When a sender wants to share a file with t receivers, she/he first encrypts a symmetric key using the Encrypt algorithm of an AMRIBE scheme and then encrypts the file with this symmetric key. The "Encryption cost" means the computation cost to generate the ciphertext for the symmetric key, and the "Ciphertext Length" is the bit length of the ciphertext for the symmetric key. When a receiver wants to recover the shared file, she/he first recovers the symmetric key using the Decrypt algorithm of the AMRIBE scheme and then recovers the shared file. The "Decryption Cost" in the following tables means the computation cost to recover the symmetric key. In the comparison of computation cost, we mainly consider the costs of some heavy operations, such as scalar operation in $\mathbb{G}, \widehat{\mathbb{G}}, \mathbb{G}_T$ and pairing, and omit some lightweight operations, such as hash function and symmetric encryption. The reason is that the former is much more costly than the latter. To better evaluate the efficiency, we may assume that the number of receivers for a ciphertext to be $t = 100$ and an identity is a string with $n = 80$ bits. From [42], we have that $(T_s, T_G, T_P) = (0.55\,\mathrm{ms}, 5.16\,\mathrm{ms}, 5.05\,\mathrm{ms})$ and $|\mathbb{G}| = |\widehat{\mathbb{G}}| = |\mathbb{G}_T| = 256$ bits in prime order groups of 128-bit security level. Besides, we consider the implementation of a Map-To-Point function given in [2] as the Map-To-Point

Table 1: The notations.

$T_s = 0.55$ ms	The cost of a scalar operation in $\mathbb{G}(\widehat{\mathbb{G}})$
$T_G = 5.16$ ms	The cost of a scalar operation in $\mathbb{G}_T$
$T_P = 5.05$ ms	The cost of a pairing operation
$T_{\text{MTP}} = 3.3$ ms	The cost of a Map-To-Point function
$\kappa = 256$ bits	The length of a symmetric key/symmetric ciphertext
$\eta = 256$ bits	The length of the output of a hash function
$\lvert\mathbb{G}\rvert = 256$ bits	The length of an element in $\mathbb{G}$
$\lvert\mathbb{G}_T\rvert = 256$ bits	The length of an element in $\mathbb{G}_T$
$\lvert\widehat{\mathbb{G}}_p\rvert = 128$ bits	The length of an element in $\mathbb{Z}_p$
$\lvert\text{ID}\rvert = 80$ bits	The length of an identity
ROM/STD	The random oracle model/the standard model
Ful/Sel	The full-ID model/The selective-ID model
Ours	The proposed AMRIBE

Table 2: Property comparison for AMRIBE.

	Confidentiality	Anonymity		Security Model	Tightness	Ful/Sel
		Outsider	Insider			
[15]	CCA	◇	◇	ROM	Yes	Sel
[18]	CCA	CCA	◇	ROM	Yes	Ful
[43]	◇	◇	◇	ROM	No	Sel
[44]	◇	◇	◇	ROM	Yes	Sel
[45]	◇	◇	◇	ROM	Yes	Sel
[46]	◇	◇	◇	ROM	No	Sel
[47]	CCA	CCA	◇	ROM	Yes	Sel
[48]	◇	◇	◇	ROM	Yes	Sel
[49]	◇	◇	◇	ROM	No	Ful
[50]	CCA	CCA	◇	ROM	No	Sel
[17]	CCA	CCA	CCA	ROM	Yes	Sel
Ours	CCA	CCA	CCA	STD	Yes	Ful

function used in these papers, and we have $T_{\text{MTP}} \approx 6T_s \approx 3.3$ ms. Some of the existing schemes use a symmetric encryption function to encrypt the message. For convenience, we assume that the message length and the symmetric key length are 256 bits. Also we assume that the lengths of the outputs of hash functions and symmetric encryption function in these schemes are 256 bits.

Here, we compare the proposed AMRIBE schemes with the existing AMRIBE schemes [15, 18, 43–50], whose CCA security has been claimed by their authors. The results are shown in Tables 2 and 3. The computation costs for decryption shown in Table 3 are evaluated in the worst case. That is, a receiver must try all t ciphertext components for successful decryption if necessary.

From Table 2, one can observe that our scheme is the first one achieving full security against chosen-ciphertext attacks with tight reduction in the standard model. As we mentioned in the Introduction, those properties are significant in both theoretic and practical points of view. Besides, from Table 3, we can see that, compared with other existing schemes, the encryption cost is low. Therefore, our scheme fits the scenario that a sender needs frequently to send messages for large amount of users, such as e-mail systems with receiver anonymity. However, the efficiency of the proposed scheme can be further improved in decryption cost, i.e., the decryption is almost the slowest among the existing schemes. Another disadvantage is that ours can only be implemented in groups supporting type 3 pairings, which is an additional requirement compared to other schemes.

The symbol "◇" in Table 2 means that the scheme is claimed to achieve CCA security, but some problem is found. All the cryptanalysis for these schemes can be found in [17, 49, 51, 52], except for [18, 19]. We will give the cryptanalysis for [18, 19] in Section 5.1.

Although the authors of [53] have claimed that their scheme achieves IND-CCA security, they did not prove the anonymity. Therefore, their work is not included in Tables 2 and 3.

Note that we do not list the schemes of [54, 55] in our comparison table because their schemes do not meet the basic requirement of identity-based encryption. In [54], Chen et al. proposed two schemes, and in both of their schemes, KeyGen algorithm needs a receiver set as one of the inputs. However, it is impossible for a user to know the receiver set which will be decided in the future. There are two possibilities: one is that the KGC must be online to generate private keys when a user needs to decrypt and the other is that all the ciphertext must be encrypted for a fixed group. Both assumptions are not practical and against the basic requirements of IBE. The problems of schemes in [55] are the same as that of [54].

Some of the existing schemes [25, 56] are claimed to be CCA secure; however, they actually achieve only CPA security. The reason is that, in their proofs, the partitioning paradigm is used. That is, all the identities will be separated into two disjoint groups, say group A and group B. The challenger can only generate private keys for IDs of group A, while generate challenge ciphertexts for IDs of group B. When an adversary queries private keys with IDs of group B or challenge ciphertexts with IDs of group A, the challenger aborts the simulation. Therefore, if an adversary is only allowed to make decryption queries with IDs of group A, then that is actually equivalent to CPA security only.

5.1. Anonymity Analysis on He et al.'s AMRIBE Scheme. In 2016, He et al. proposed generic construction of AMRIBE [18], which is the preliminary version of [19]. The generic constructions given in the two papers are the same. Due to the page limitation, we give only a high-level overview on the cryptanalysis of He et al.'s AMRIBE scheme. We refer the readers to [18, 19] for more details. The idea of our cryptanalysis is similar to that in [49], where Zhang et al. presented an algorithm for an insider adversary to break the anonymity of the scheme of Zhang and Takagi [50].

In He et al.'s scheme, the component associated with the encrypted message in a ciphertext is with the form $C_1 = (C^0_{\text{ID}_1}, C^1_{\text{ID}_1}) \| \ldots \| (C^0_{\text{ID}_t}, C^1_{\text{ID}_t})$. The message M is encrypted in $C^1_{\text{ID}_i}$ with the encryption algorithm of an IND-CPA secure IBE scheme, i.e., $C^1_{\text{ID}_i} \longleftarrow \widehat{\text{IBE}}.\text{Enc}(\text{Param}, \text{ID}, \text{svk} \| \delta \| M)$, and $C^0_{\text{ID}_i} = H_2(e(g_1, H(\text{ID}_i))^r)$ is used for a selected receiver to confirm whether herself is one of the receivers. However, in order to prove the IND-MID-CCA

Table 3: Efficiency comparison for AMRIBE.

	Ciphertext length	Encryption cost	Decryption cost
[15]	$\kappa + \eta + (t+2)\lvert\mathbb{G}\rvert \approx 26624$ bits	$T_p + tT_{\mathrm{MTP}} + (t^2+3)T_s \approx 5836.7$ ms	$2T_P + tT_s \approx 65.1$ ms
[18]	$2\lvert\mathbb{G}\rvert + 3t\eta \approx 77312$ bits	$2tT_p + 4T_s + tT_{\mathrm{MTP}} \approx 1342.2$ ms	$2T_P + 2T_s \approx 11.2$ ms
[43]	$\lvert\mathbb{G}\rvert + t\lvert\mathbb{Z}_p\rvert + \kappa + 2\eta \approx 26624$ bits	$tT_p + 2T_s + tT_{\mathrm{MTP}} \approx 836.1$ ms	$T_p \approx 5.05$ ms
[44]	$\lvert\mathbb{G}\rvert + t\lvert\mathbb{Z}_p\rvert + \kappa + \eta \approx 26368$ bits	$tT_p + 2T_s + tT_{\mathrm{MTP}} \approx 836.1$ ms	$T_p \approx 5.05$ ms
[45]	$\lvert\mathbb{G}\rvert + \kappa(2t+1)\eta \approx 51968$ bits	$tT_p + 2T_s tT_{\mathrm{MTP}} \approx 836.1$ ms	$T_p \approx 5.05$ ms
[46]	$2\lvert\mathbb{G}\rvert + \kappa + t\eta \approx 26368$ bits	$tT_p + 3T_s + tT_{\mathrm{MTP}} \approx 836.65$ ms	$T_p + T_s \approx 5.6$ ms
[47]	$(2t+1)\lvert\mathbb{G}\rvert + \kappa + \eta \approx 51968$ bits	$T_p + tT_{\mathrm{MTP}} + (2t^2+2)T_s \approx 11336.15$ ms	$2T_p(2t-1)T_s \approx 119.55$ ms
[48]	$3\lvert\mathbb{G}\rvert + \lvert\mathrm{ID}\rvert + t\lvert\mathbb{Z}_p\rvert \approx 13648$ bits	$tT_p + 4T_s + (t+1)T_{\mathrm{MTP}} \approx 840.5$ ms	$3T_p \approx 15.15$ ms
[49]	$(t+2)\lvert\mathbb{G}\rvert + \kappa \approx 26368$ bits	$tT_p + tT_{\mathrm{MTP}} + (t+4)T_s \approx 892.2$ ms	$2T_p + T_s \approx 10.65$ ms
[50]	$(t+2)\lvert\mathbb{G}\rvert + \kappa \approx 26368$ bits	$(t+1)T_p + tT_{\mathrm{MTP}} + (t+2)T_s \approx 896.15$ ms	$2tT_p + T_s \approx 10.65$ ms
[17]	$(t+1)\lvert\mathbb{Z}_p\rvert + 2\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert + \lvert\mathrm{ID}\rvert \approx 13776$ bits	$tT_p + (t+2)T_s + T_G + (t+1)T_{\mathrm{MTP}} \approx 899.56$ ms	$T_p + T_G + T_s + T_s \approx 10.76$ ms
Ours	$2\lvert\mathbb{G}_T\rvert + (t+2)\lvert\mathbb{G}\rvert \approx 26624$ bits	$(t+3)T_s + 2T_G \approx 66.97$ ms	$(t+3)T_P + T_s \approx 520.7$ ms

security, the scheme is designed such that $r = H_3(\delta, M)$, which means an insider adversary is able to recover r after successful decryption. Therefore, given an identity ID*, an insider adversary can easily check whether ID* is also one of the receivers by checking if there exists $j \in [t]$, such that $C^1_{\mathrm{ID}_j} = H_2(e(g_1, H(\mathrm{ID}^*))^r)$.

6. Conclusion

Multireceiver identity-based encryption is a one-to-many encryption mechanism which encrypts a message to multiple receivers at the same time efficiently and securely. Such encryption is useful in many applications, e.g., pay-per-view TV, video conferencing, and distance education. Under certain circumstances, users may wish to protect their identities from revealing. To deal with this issue, Fan et al. first proposed the notion of anonymous multireceiver identity-based encryption and gave a concrete AMRIBE scheme. Since then, lots of research studies on these topics have been proposed.

In this paper, we give a novel fully secure AMRIBE scheme. To the best of our knowledge, it is the first and only scheme that achieves the IND-MID-CCA and the ANON-MID-CCA security in the standard model with tight reduction. Moreover, compared with other existing schemes, the encryption cost is low. Therefore, our scheme fits the scenario that a sender needs frequently to send messages for large amount of users, such as e-mail systems with receiver anonymity. There are still some improvements that can be made to our schemes in the future. For instance, the efficiency of the proposed AMRIBE with tight reduction may be further improved, especially in the decryption cost. Besides, due to the thread of the supreme computing power of quantum computers, the researches of postquantum cryptographic primitives are becoming significant. Lots of postquantum ID-based schemes [57–59] are proposed in the literature as well. Hence, another direction for our future research could be figuring out an AMRIBE scheme achieving tight security and CCA security in postquantum setting.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was partially supported by the Ministry of Science and Technology of Taiwan under grants MOST 110-2218-E-110-007-MBK, MOST 109-2221-E-110-044-MY2, MOST 110-2923-E-110-001-MY3, MOST 108-2218-E-004-002-MY2, MOST 109-2221-E-004-011-MY3, and MOST 109-3111-8-004-001. It also was financially supported by the Information Security Research Center at National Sun Yat-sen University in Taiwan and the Intelligent Electronic Commerce Research Center from The Featured Areas Research Center Program within the framework of the Higher Education Sprout Project by the Ministry of Education (MOE) in Taiwan.

References

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of CRYPTO 84 on Advances in Cryptology*, pp. 47–53, Springer-Verlag, New York, NY, USA, 1985.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '01*, pp. 213–229, Springer-Verlag, London, UK, August 2001.

[3] C. Cocks, "An identity based encryption scheme based on quadratic residues," in *Proceedings of the 8th IMA International Conference on Cryptography and Coding*, pp. 360–363, Springer-Verlag, London, UK, December 2001, http://dl.acm.org/citation.cfm?id=647995.742435.

[4] T. Arul, *Channel Switching-Triggered Charging for Pay-TV over IPTV*, http://tuprints.ulb.tu-darmstadt.de/6680/PhD Thesis, Darmstadt University of Technology, Darmstadt, Germany, 2017, http://tuprints.ulb.tu-darmstadt.de/6680/ PhD Thesis.

[5] T. Arul and A. Shoufan, "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*, pp. 147–153, WAINA, Fukuoka, Japan, March 2012.

[6] T. Arul and A. Shoufan, "Subscription-free pay-tv over IPTV," *Journal of Systems Architecture*, vol. 64, pp. 37–49, 2016.

[7] Y. Liu, J. Duan, Q. Tang, and Y. Zhang, "A simple and efficient re-scrambling scheme for dtv programs," *IEEE Transactions on Multimedia*, vol. 16, no. 1, pp. 137–146, 2014.

[8] M. G. Msgna, K. Markantonakis, K. Mayes, and R. N. Akram, "Subscriber centric conditional access system for pay-tv systems," in *Proceedings of the 2013 IEEE 10th International Conference on e-Business Engineering*, pp. 450–455, Coventry, UK, September 2013.

[9] J. Baek, R. Safavi-Naini, and W. Susilo, "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, PKC'05*, pp. 380–397, Springer-Verlag, Berlin, Germany, 2005.

[10] C.-D. Jung, S.-B. Yoon, C. Sur, and K. H. Rhee, "Efficient multi-receiver identity-based encryption scheme from bilinear pairing," *The Journal of the Korean Institute of Information and Communication Engineering*, vol. 11, no. 1, 2007.

[11] L. Wang and C.-K. Wu, "Efficient identity-based multicast scheme from bilinear pairing," *IEEE Proceedings - Communications*, vol. 152, no. 5, pp. 877–882, 2005.

[12] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in *Proceedings of the Advances in Cryptology–ASIACRYPT*, pp. 200–215, Springer, Berlin, Germany, 2007.

[13] X. Du, Y. Wang, J. Ge, and Y. Wang, "An ID-based broadcast encryption scheme for key distribution," *IEEE Transactions on Broadcasting*, vol. 51, no. 2, pp. 264–266, 2005.

[14] R. Sakai and J. Furukawa, "Identity-based broadcast encryption," https://eprint.iacr.org/2007/217Report 2007/217, Cryptology ePrint Archive, Berlin, Germany, 2007, https://eprint.iacr.org/2007/217Report 2007/217.

[15] C. I. Fan, L. Y. Ling-Ying Huang, and P. H. Pei-Hsiu Ho, "Anonymous multireceiver identity-based encryption," *IEEE Transactions on Computers*, vol. 59, no. 9, pp. 1239–1249, 2010.

[16] H.-Y. Chien, "Improved anonymous multi-receiver identity-based encryption," *The Computer Journal*, vol. 55, no. 4, pp. 439–446, 2012.

[17] C.-I. Fan and Y.-F. Tseng, "Anonymous multi-receiver identity-based authenticated encryption with CCA security," *Symmetry*, vol. 7, no. 4, pp. 1856–1881, 2015, http://www.mdpi.com/2073-8994/7/4/1856.

[18] K. He, J. Weng, M. H. Au, Y. Mao, and R. H. Deng, "Generic anonymous identity-based broadcast encryption with chosen-ciphertext security," vol. 9723, pp. 207–222, in *Proceedings, Part II, of the 21st Australasian Conference on Information Security and Privacy*, vol. 9723, pp. 207–222, Springer-Verlag, New York, NY, USA, 2016.

[19] K. He, J. Weng, Y. Mao, and H. Yuan, "Anonymous identity-based broadcast encryption technology for smart city information system," *Personal and Ubiquitous Computing*, vol. 21, no. 5, pp. 841–853, 2017.

[20] J. Lai, Y. Mu, F. Guo, and R. Chen, "Fully privacy-preserving ID-based broadcast encryption with authorization," *The Computer Journal*, vol. 60, no. 12, pp. 1809–1821, 2017.

[21] J. Lai, Y. Mu, F. Guo, W. Susilo, and R. Chen, "Anonymous identity-based broadcast encryption with revocation for file sharing," in *Proceedings of the Information Security and Privacy*, pp. 223–239, Springer International Publishing, Cham, Switzerland, 2016.

[22] J. Lai, Y. Mu, F. Guo, W. Susilo, and R. Chen, "Fully privacy-preserving and revocable ID-based broadcast encryption for data access control in smart city," *Personal and Ubiquitous Computing*, vol. 21, no. 5, pp. 855–868, 2017.

[23] P. Xu, J. Li, W. Wang, and H. Jin, "Anonymous identity-based broadcast encryption with constant decryption complexity and strong security," in *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, ASIA CCS '16*, pp. 223–233, ACM, New York, NY, USA, 2016.

[24] J. Zhang and J. Mao, "Anonymous multi-receiver broadcast encryption scheme with strong security," *International Journal of Embedded Systems*, vol. 9, no. 2, pp. 177–187, 2017.

[25] F.-C. Zhou, M.-Q. Lin, Y. Zhou, and Y.-X. Li, "Efficient anonymous broadcast encryption with adaptive security," *KSII Transactions on Internet and Information Systems*, vol. 9, no. 11, pp. 4680–4700, 2015.

[26] D. Boneh and X. Boyen, "Efficient selective-ID secure identity-based encryption without random oracles," in *Proceedings of the Advances in Cryptology - EUROCRYPT 2004, volume 3027 of LNCS*, Springer-Verlag, Berlin, Germany, pp. 223–238, 2004.

[27] D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," in *Advances in Cryptology–CRYPTO 2004*, M. Franklin, Ed., Springer, Berlin, Germany, pp. 443–459, 2004.

[28] C. Gentry, "Practical identity-based encryption without random oracles," in *Advances in Cryptology-EUROCRYPT 2006*, S. Vaudenay, Ed., pp. 445–464, Springer, Berlin, Germany, 2006.

[29] N. Attrapadung, "Dual system encryption framework in prime-order groups via computational pair encodings," vol. 10032, pp. 591–623, in *Proceedings, Part II, of the 22Nd International Conference on Advances in Cryptology—ASIACRYPT 2016*, vol. 10032, , Springer-Verlag, New York, NY, USA, 2016.

[30] C. Bader, T. Jager, Y. Li, and S. Schäge, "On the impossibility of tight cryptographic reductions," in *Advances in Cryptology – EUROCRYPT 2016*, Marc Fischlin and Coron Jean-Sébastien, Eds., Springer, Berlin, Germany, pp. 273–304, 2016.

[31] M. Bellare and P. Rogaway, "Random oracles are practical," in *Proceedings of the 1st ACM Conference on Computer and Communications Security, CCS '93*, pp. 62–73, ACM, New York, NY, USA, 1993.

[32] M. Bellare, A. Boldyreva, and A. Palacio, "An uninstantiable random-oracle-model scheme for a hybrid-encryption problem," in *Advances in Cryptology - EUROCRYPT 2004*, C. Cachin and J. L. Camenisch, Eds., pp. 171–188, Springer, Berlin, Heidelberg, 2004.

[33] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited," *Journal of the ACM*, vol. 51, no. 4, pp. 557–594, 2004.

[34] S. D. Galbraith, K. G. Paterson, and N. P. Smart, "Pairings for cryptographers," *Discrete Applied Mathematics*, vol. 156, no. 16, pp. 3113–3121, 2008, http://www.sciencedirect.com/science/article/pii/S0166218X08000449.

[35] N. P. Smart and F. Vercauteren, "On computable isomorphisms in efficient asymmetric pairing-based systems," *Discrete Applied Mathematics*, vol. 155, no. 4, pp. 538–547, 2007, http://www.sciencedirect.com/science/article/pii/S0166218X06003271.

[36] S. Chatterjee and A. Menezes, "On cryptographic protocols employing asymmetric pairings - the role of Ψ revisited," *Discrete Applied Mathematics*, vol. 159, no. 13, pp. 1311–1322,

2011, http://www.sciencedirect.com/science/article/pii/S0166218X11001648.

[37] S. Chatterjee and P. Sarkar, "Practical hybrid (hierarchical) identity-based encryption schemes based on the decisional bilinear diffie-hellman assumption," *International Journal of Applied Cryptography*, vol. 3, no. 1, pp. 47–83, 2013.

[38] C.-I. Fan, V. S.-M. Huang, and H.-M. Ruan, "Arbitrary-state attribute-based encryption with dynamic membership," *IEEE Transactions on Computers*, vol. 63, no. 8, pp. 1951–1961, 2014.

[39] J. H. Park and D. H. Lee, "An efficient ibe scheme with tight security reduction in the random oracle model," *Designs, Codes and Cryptography*, vol. 79, no. 1, pp. 63–85, 4 2016.

[40] J. Katz and N. Wang, "Efficiency improvements for signature schemes with tight security reductions," in *Proceedings of the 10th ACM Conference on Computer and Communications Security, CCS '03*, pp. 155–164, ACM, New York, NY, USA, 2003.

[41] N. Attrapadung, J. Furukawa, T. Gomi, G. Hanaoka, H. Imai, and R. Zhang, "Efficient identity-based encryption with tight security reduction," in *Cryptology and Network Security*, D. Pointcheval, Yi Mu, and K. Chen, Eds., pp. 19–36, Springer, Berlin, Germany, 2006.

[42] A. Guillevic, "Comparing the pairing efficiency over composite-order and prime-order elliptic curves," in *Proceedings of the Applied Cryptography and Network Security*, pp. 357–372, Banff, Canada, 2013.

[43] Y.-M. Tseng, Y.-H. Huang, and H.-J. Chang, "CCA-secure anonymous multi-receiver ID-based encryption," in *Proceedings of the 2012 26th International Conference on Advanced Information Networking and Applications Workshops*, pp. 177–182, Fukuoka-shi, Japan, March 2012.

[44] Y.-M. Tseng, Y.-H. Huang, and H.-J. Chang, "Privacy-preserving multireceiver ID-based encryption with provable security," *International Journal of Communication Systems*, vol. 27, no. 7, pp. 1034–1050, 2012.

[45] Y.-M. Tseng, T.-T. Tsai, S.-S. Huang, and H.-Y. Chien, "Efficient anonymous multi-receiver ID-based encryption with constant decryption cost," in *Proceedings of the 2014 International Conference on Information Science*, pp. 131–137, Auckland, New Zealand, April 2014.

[46] H. Wang, "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*, pp. 85–90, Dalian, China, August 2014.

[47] H. Wang, Y. Zhang, H. Xiong, and B. Qin, "Cryptanalysis and improvements of an anonymous multi-receiver identity-based encryption scheme," *IET Information Security*, vol. 6, no. 1, pp. 20–27, 2012.

[48] B. Zhang, T. Sun, and D. Yu, "ID-based anonymous multi-receiver key encapsulation mechanism with sender authentication," in *Proceedings of the Algorithms and Architectures for Parallel Processing*, pp. 645–658, Springer, Cham, Switzerland, October 2014.

[49] J. Zhang and J. Mao, "An improved anonymous multi-receiver identity-based encryption scheme," *International Journal of Communication Systems*, vol. 28, no. 4, pp. 645–658, 2015.

[50] M. Zhang and T. Takagi, "Efficient constructions of anonymous multireceiver encryption protocol and their deployment in group e-mail systems with privacy preservation," *IEEE Systems Journal*, vol. 7, no. 3, pp. 410–419, 2013.

[51] H. Li and L. Pang, "Cryptanalysis of Wang et al. improved anonymous multi-receiver identity-based encryption scheme," *IET Information Security*, vol. 8, no. 1, pp. 8–11, 2014.

[52] J. Zhang and Y. Xu, "Comment on anonymous multi-receiver identity-based encryption scheme," in *Proceedings of the 2012 Fourth International Conference on Intelligent Networking and Collaborative Systems*, pp. 473–476, Bucharest, Romania, September 2012.

[53] L. Pang, L. Guo, Q. Pei, J. Gui, and Y. Wang, "A new ID-based multi-recipient public-key encryption scheme," *Chinese Journal of Electronics*, vol. 22, no. 1, pp. 89–92, 2013.

[54] Z. Chen, S. Li, C. Wang, and Y. Shen, "Two constructions of multireceiver encryption supporting constant keys, short ciphertexts, and identity privacy," *International Journal of Network Security*, vol. 14, no. 9, 2012.

[55] L. Zhang, Q. Wu, and Y. Mu, "Anonymous identity-based broadcast encryption with adaptive security," in *Proceedings of the Cyberspace Safety and Security*, pp. 258–271, Springer International Publishing, Cham, Switzerland, November 2013.

[56] A. Muthulakshmi, R. Anitha, S. Rohini, and K. Princy, "Identity based privacy preserving dynamic broadcast encryption for multi-privileged groups," in *Recent Trends in Computer Networks and Distributed Systems Security*, S. M. Thampi, A. Y. Zomaya, T. Strufe, M. Jose, A. Calero, and Tony Thomas, Eds., Springer, Berlin, Germany, pp. 272–282, 2012.

[57] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (h)ibe in the standard model," in *Advances in Cryptology–EUROCRYPT 2010*, H. Gilbert, Ed., Springer, Berlin, Germany, pp. 553–572, 2010.

[58] Z. Li, C. Ma, and D. Wang, "Towards multi-hop homomorphic identity-based proxy re-encryption via branching program," *IEEE Access*, vol. 5, pp. 16214–16228, 2017.

[59] Z. Li, C. Ma, and D. Wang, "Achieving multi-hop pre via branching program," *IEEE Transactions on Cloud Computing*, vol. 8, no. 1, pp. 45–58, 2020.