Two Constructions of Multireceiver Encryption Supporting Constant Keys, Short Ciphertexts, and Identity Privacy

Zhenhua Chen[1], Shundong Li[1], Chunzhi Wang[2], Yanping Shen[3]
(Corresponding author: Zhenhua Chen)

School of Computer Sciences, Shaanxi Normal University, Xi'an 710062, China[1]
College of Computer Science and Engineering, Hubei University of Technology, Wuhan 430068, China[2]
Institute of Disaster Prevention, Langfang 101601, China[3]
(Received May 1, 2012; revised and accepted May 14, 2012)

Abstract

Multireceiver encryption enables a sender to encrypt a message and transmit the ciphertext to a set of authorized users while no one outside this set can decrypt the message, which is known as an efficient protocol to achieve a secure multicast data communication among multiple authorized users. In this work, we construct two identity-based multireceiver encryption schemes (one is based on composite order groups whose order is a product of three primes and the other is based on prime order of asymmetric bilinear groups where the isomorphisms between two groups are not efficiently computable) that support: (1)unbounded recipient in multireceiver set that does not pre-establish the maximum number of multireceiver users in advance in the setup algorithm; (2)identity privacy that no one outside the multireceiver set can derive the identities of multireceiver users, and (3)higher computing and communicating performance, i.e., short ciphertexts, fix-length public parameters and constant keys. The security analysis, including semantic security and identity privacy, are presented in selective security model under the mathematical assumptions of (bilinear) subgroup decisional problems in composite order model and decisional BDH problems in prime order of asymmetric bilinear groups in the standard model.
Keywords: multireceiver encryption, unbounded user, identity privacy, constant ciphertext

1 Introduction

Multireceiver encryption is an efficient fashion in sending a message securely in such a way that more than one designated recipients can decrypt it. Multireceiver encryption enables a sender to encrypt a message and transmit it to a subset of authorized users, which is known as an efficient protocol to achieve a secure multicast among the authorized user set while no one outside this set can decrypt the message [1, 16]. Multireceiver encryption has lots of application requirements such as TV pay [20], wireless broadcast [26], mobile devices [25] and smart card [26].

Identity-based cryptography, first introduced by Shamir [21], is one of fundamental primitives in modern cryptography that allows to use the recipient identity as a public key, avoids the burden deployment of public key infrastructure. User's public key is derived from some known aspect of his/her identity, such as email address, IP address and ID card number etc, which eliminates the dependence of public key distribution problem in public key infrastructure.

Multireceiver encryption [3, 8, 10, 19, 27, 29, 30] allows a sender to send a encrypted message to a set of recipient S, and only the user in set S can decrypt the ciphertext using his private key. In identity-based multireceiver encryption schemes, a broadcaster typically encrypts a message by combining public identities of receivers in S and system parameters.

In traditional identity-based multireceiver encryption, one shortcoming is that anyone can guess the identity of recipient from the ciphertext. The cryptographic primitive of identity-based encryption allows a sender to encrypt a message for a receiver using only the receiver's identity as a public key. However, in this case, the ciphertext will leak the identity information in the recipient set, since the adversary may test the identity in the ciphertext even though s/he does not aware of the message in the ciphertext [10]. Identity privacy encryption [4, 14], which hides the recipient identity of decryptor private key holder, is an effect methodology to protect the recipient's privacy. Informally, identity privacy encryption holds the security property that the adversary cannot distinguish an encrypted ciphertext of a randomly chosen identity by an adversary. In particular, the adversary is unable to decide whether a ciphertext was encrypted for a chosen identity by the adversary, or for a random identity string.

1.1 Related Work

The formal concept of the identity-based broadcast encryption was first presented by Delerablée in [8]. This concept is related to encryption scheme in identity-based setting, in which the maximal size of a multireceiver set is $\ell = 1$. Delerablée [8] also proposed an IBBE scheme with constant size ciphertexts and private keys. But the size of public key is linear to the maximum number of multireceiver set S.

Ren and Gu [19] proposed an IBBE scheme against chosen-ciphertext attack (CCA) in the full security model in the standard model. However, Wang et al. [23] showed that the private key can be forged in Ren and Gu's scheme [19].

Hur et al. [16] constructed a privacy-preserving identity-based multireceiver encryption scheme against active attacks by hiding the identities in the ciphertext. But the public parameters and ciphertext size are linear to the number of multireceiver users.

Gentry and Waters [13] presented a new technique, namely semi-static model, to obtain adaptive security model in multireceiver encryption scheme. They realized a generic two-key transformation from semi-statically secure systems to adaptively secure systems that have comparable-size ciphertexts. Also, they presented three IBBE schemes with semi-static or adaptive security, but the security relies on the complex assumptions that were dependent on the depth of multireceiver users in receiver set S and the number of queries requested by the adversary [27]. Daza et al. [7] proposed a threshold multireceiver encryption with CCA2 security. Wang and Bi [22] proposed a lattice-based identity-based multireceiver encryption that was motivated by the technique of lattice basis delegation techniques [6].

Hur et al. [16] constructed an IBBE with receiver identity privacy, however, their scheme does not support constant ciphertext and fix-length public parameters. Fan et al. [10] constructed an anonymous multireceiver encryption by deploying a secret sharing scheme to hide receivers' identity. Recently, Zhang et al. [27] constructed an IBBE scheme with constant private key and ciphertext with adaptive security. However, in their scheme, the multireceiver set must be sequential. Informally, for a decryption key that generated by recipient set $S = \{I_1, I_2\}$, it is intractable to decrypt the ciphertext that encrypted with broadcasting identities set $S' = \{I_2, I_1\}$. The main reason is that the Zhang et al.'s scheme is derived from a variant of a hierarchical identity-based encryption [17, 18]. Hu et al. [15] proposed an identity-based broadcast encryption scheme without random oracles heuristic and it achieved chosen plaintext security in selective identity model. The proposed scheme is a good and efficient hybrid encryption scheme, which captures $\mathcal{O}(1)$-size ciphertexts, public parameters and private keys.

In 2009, Waters [24] proposed a dual system encryption methodology to achieve fully secure (hierarchical) identity-based encryption systems from simple assumptions. Lewko and Waters [17] spread the dual system encryption technique to obtain a fully secure hierarchical IBE scheme with constant size ciphertext. Moreover, the proofs rely on the simple constant-size assumptions which is independent to the queries number that the adversary requests. Recently, Lewko and Waters [18] improve the constructions of a hierarchical IBE and an attribute-based encryption with *unbounded* delegation depth, which hold the short public parameters.

1.2 Motivation and Results

Most of the identity-based multireceiver encryptions have a weakness that they had to provide a constant N as the maximum multireceiver user number in multireceiver set [3, 8, 19, 27]. This setting will be performed in the setup algorithm and be published as the system public parameters. However, it is inflexible and impractical if we deploy this scheme in different multireceiver set-size environments because it will consume excess bandwidth when dispensing the preestablished maximum system public parameters. That is, the size of public parameters will grow linearly to the pre-established user number and the receiver number cannot exceed this value. Meanwhile, to protect the multireceiver identities privacy, we should hide the receiver identities in the multireceiver ciphertext.

In this work, we proposed two identity-based multireceiver encryption schemes that support unbounded multireceiver users and protect the identity privacy of receiver, and they also possess the cryptographic properties such as fixed length public parameters, short ciphertexts and constant private keys. By virtue of the technique in [18], we produce $\leq s$ samples and be raised to the same exponent $r \in \mathbb{Z}_n$ to achieve unbounded user (is less than order n) without considering pre-determinated maximum in setup phase. In the first scheme, we introduce a composite order group to achieve identity privacy property. In the second scheme, we deploy an asymmetric bilinear group where the isomorphisms between two groups are not computable to implement the same properties in the first scheme. Informally, our contribution is described as follows:

1) We formalize the model of identity-based multireceiver encryption with unbounded receiver set and identity privacy. Besides the semantic security, we also give the identity privacy game description for the identity-based multireceiver encryption. Identity privacy is a security property by which an adversary is unable to determine the identity with which the ciphertext was produced. That is, the recipient's identity is anonymous from the adversary's point of view.

2) We explore two concrete multireceiver encryption schemes with identity privacy that support unbounded receiver set. The first one is constructed in bilinear composite order groups whose order is a product of three primes, and the other one is constructed in asymmetric bilinear prime order groups

where the isomorphisms between two groups are not efficiently computable. The proposed schemes achieve unbounded receiver set key generation and receiver identities encryption that do not fix a maximum multireceiver user number in advance. Our schemes are constructed by virtue of the techniques of unbounded hierarchical IBE in [18]. The security (includes semantic security and identity privacy) is provable selective secure in static model of (bilinear) subgroup decisional problems and asymmetric DBDH problems in the standard model.

3) Compared with related schemes, our schemes have comparative advantage in constant ciphertexts, fixed length public parameters, and short keys. Furthermore, the proposed schemes hold the receiver set identities privacy preservation by virtue of the property of identity privacy.

2 Mathematics Background

2.1 Asymmetric Bilinear Map in Prime Order Groups

Let λ be a security parameter and $\mathbb{G} = \langle g \rangle, \hat{\mathbb{G}} = \langle \hat{g} \rangle$ and $\mathbb{G}_2$ be multiplicative cyclic groups of prime order p where $p > 2^\lambda$ and $\mathbb{G} \neq \hat{\mathbb{G}}$. The asymmetric admissible bilinear map $\hat{e}_1 : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_2$ has the properties: for all $u \in \mathbb{G}$, $v \in \hat{\mathbb{G}}$ and $\alpha, \beta \in \mathbb{Z}_n$, it holds that $\hat{e}_2(u^\alpha, v^\beta) = \hat{e}_2(u^\beta, v^\alpha) = \hat{e}_2(u, v^\beta)^\alpha = \hat{e}_2(u, v)^{\alpha\beta}$ and $\hat{e}_2$ is non-trivial, i.e., $\hat{e}_2(g, \hat{g}) \neq 1_{\mathbb{G}_2}$, that is, $\hat{e}_2(g, \hat{g})$ is a generator of $\mathbb{G}_2$.

Moveover, we require that there does not exist an efficient and computable homomorphism ψ such that $\psi(\mathbb{G}) \to \hat{\mathbb{G}}$ or $\psi(\hat{\mathbb{G}}) \to \mathbb{G}$ [9, 12].

2.2 Symmetric Bilinear Map in Composite Order Groups

Composite order bilinear groups were first introduced in [2]. Let $\mathbb{G} = \langle g \rangle$ and $\mathbb{G}_2$ be two cyclic multiplicative groups of composite order $n = lcm(p_1, p_2, p_3)$. $\hat{e}_1$ be an admissible bilinear map from $\mathbb{G}^2$ to $\mathbb{G}_2$, i.e., for all $u, v \in \mathbb{G}$ and $\alpha, \beta \in \mathbb{Z}_n$, it holds that $\hat{e}_1(u^\alpha, v^\beta) = \hat{e}_1(u^\beta, v^\alpha) = \hat{e}_1(u, v^\beta)^\alpha = \hat{e}_1(u, v)^{\alpha\beta}$ and $\hat{e}_1$ is non-trivial, i.e., $\hat{e}_1(g, g) \neq 1_{\mathbb{G}_2}$.

We use the notation $\mathbb{G}_{p_1}, \mathbb{G}_{p_2}$ and $\mathbb{G}_{p_3}$ to denote the subgroups of $\mathbb{G}$ with prime order p_1, p_2, p_3, respectively. Similarly, we use the notation $\mathbb{G}_{t,p}, \mathbb{G}_{t,p_2}, \mathbb{G}_{t,p_3}$ to denote as the subgroups of $\mathbb{G}_2$ with p_1, p_2, p_3, respectively. We denote by $\mathbb{G} = \mathbb{G}_{p_1} \times \mathbb{G}_{p_2} \times \mathbb{G}_{p_3}$, and $\mathbb{G}_2 = \mathbb{G}_{2,p_1} \times \mathbb{G}_{2,p_2} \times \mathbb{G}_{2,p_3}$, respectively.

Lemma 1. ***Orthogonality subgroups*** *If $g_{p_1} \in \mathbb{G}_p, g_{p_2} \in \mathbb{G}_{p_2}$, and $g_{p_3} \in \mathbb{G}_{p_3}$ be the generators of $\mathbb{G}_{p_1}, \mathbb{G}_{p_2}, \mathbb{G}_{p_3}$, respectively, then $g_{p_1 p_2}$ be the generator of $\mathbb{G}_{p_3}$, $g_{p_1 p_3}$ be the generator of $\mathbb{G}_{p_2}$, and so on.*

In particular, for all random elements $h_{p_1} \in \mathbb{G}_{p_1}$, $h_{p_2} \in \mathbb{G}_{p_2}$, and $h_{p_3} \in \mathbb{G}_{p_3}$ which satisfy $h_{p_1} = g_{p_1}^\alpha, h_{p_2} = g_{p_2}^\beta$, and $h_{p_3} = g_{p_3}^\gamma$ for some integers $\alpha, \beta, \gamma \in \mathbb{Z}_n$. It has,

$$\begin{aligned} & \hat{e}_1(h_{p_1} h_{p_2}, h_{p_3}) \\ = \; & \hat{e}_1(g_{p_1}^\alpha g_{p_2}^\beta, g_{p_3}^\gamma) \\ = \; & \hat{e}_1(g_{p_1}, g_{p_2}) \hat{e}_1(g_{p_2}, g_{p_3}) = 1 \end{aligned} \quad (1)$$

Definition 1. ***Canceling group*** *[11] Let $\mathcal{G}$ be a bilinear group generator. We say that $\mathcal{G}$ is r-canceling if it also outputs groups $G_2, \ldots, G_r \subset \mathbb{G}$ and $\hat{G}_2, \ldots, \hat{G}_r \subset \hat{\mathbb{G}}$, such that*

1) $\tilde{\mathbb{G}} = G_1 \times G_2 \times \ldots \times G_r$ and $\hat{\mathbb{G}} = \hat{G}_1 \times \hat{G}_2 \times \ldots \times \hat{G}_r$,

2) $\hat{e}_1(g_i, g_j) = 1$ for all $g_i \in G_i$, $\hat{g}_j \tilde{\in} \hat{G}_j$ and $i \neq j$.

3 Identity-based Multireceiver Encryption with Identity Privacy

In this section, we present a formal definition of an identity-based multireceiver encryption scheme (IBME) and its security notion. The IBME is comprised of four probabilistic polynomial-time algorithms $\prod = (Stp, Ext, Enc, Dec)$. Notice that *Stp* algorithm and *Ext* algorithm are performed by public key generator (PKG), *Enc* algorithm is performed by a sender and *Dec* algorithm is performed by a user in multireceiver set S.

3.1 Formal Model of IBME with Identity Privacy

$\prod$.***Stp*** (1^λ): The setup algorithm takes the security parameter λ as input and outputs the public parameters mk and the system master key msk.

$\prod$.***Ext*** (mk, msk, I_i, S): The key generation algorithm takes the master key, a multireceiver user set $S = \{I_1, I_2, \ldots, I_N\}$, an identity I_i such that $I_i \in S$, and the public parameters mk as input and outputs a private key Sk_{I_i}.

$\prod$.***Enc*** (mk, S, m): The encryption algorithm takes a message m, a multireceiver identity set $S = \{I_1, I_2, \ldots, I_N\}$, and the public parameters mk as input and outputs a ciphertext Ct.

$\prod$.***Dec*** (mk, Ct, Sk_{I_i}): The decryption algorithm takes a ciphertext Ct, a private key Sk_{I_i} associated with an identity I_i, and the public parameters mk as input, and outputs the decrypted message m if $I_i \in S$ and outputs $\perp$ otherwise.

Remark 1. *An identity-based multireceiver encryption holds unbounded receiver set if the cardinality of the receiver set S is not fixed in advance. That is, in the above model, N is not previous determined and also not a constant.*

The completeness of a multireceiver encryption scheme has the following consistency and correctness property: For all correctly produced mk, msk and a user with private key Sk_{I_i}, generates $Ct \leftarrow \prod.Enc\ (mk, S, m)$ and $m' \leftarrow \prod.Dec(mk, Ct, Sk_{I_i})$. If $I_i \in S$ holds then $m = m'$. Otherwise, $m \neq m'$ except for a negligible probability, i.e.,

$$Pr\left[\begin{array}{l}(mk, msk) \leftarrow \prod.Stp(1^\lambda)\\ S \leftarrow \{I_1, I_2, \ldots\}\\ Sk_{I_i} \leftarrow \prod.Ext(mk, msk, I_i, S)\\ Ct \leftarrow \prod.Enc(mk, S, m)\\ m = \prod.Dec(mk, Ct, Sk_{I_i})\end{array}\right] > 1 - negl(\lambda) \quad (2)$$

where $negl(\lambda)$ is a negligible function such that there exists an integer λ' that for every $\lambda' > \lambda$ it satisfies $f(\lambda') < 1/negl(\lambda)$.

3.2 Security Models

We will present two IBME encryption schemes with unbounded multireceiver users. All of our proposed schemes capture the security of *semantic security* and *identity privacy*. On cryptographic side, they also support *constant public parameters*, *constant keys*, *short ciphertexts* together with *unbounded receiver*.

Definition 2. ***Semantic Security Game*** *Semantic security is the usual security notion for an encryption scheme, which means that no non-trivial information about the message can be feasibly gleaned from the ciphertext. Semantic security is equivalent to the definition of ciphertext indistinguishability. Formally, indistinguishability means that adversary cannot distinguish two different message ciphertexts after he performs a lot of key extraction queries, which is formally defined as the* IND-IBME-CPA *game as in Figure 1(a).*

The advantage for $\mathscr{A}$ under an IND-IBME-CPA game against multireceiver encryption scheme $\prod$ is defined as

$$Adv^{ind}_{\prod,\mathscr{A}}(\lambda) = |Pr[(b = b')] - \frac{1}{2}| \quad (3)$$

Definition 3. ***Confidentiality*** *An identity-based multireceiver encryption is semantic secure against chosen-plaintext attacks if all probabilistic polynomial-time adversaries $\mathscr{A}$ achieve at most a negligible advantage $Adv^{ind}_{\prod,\mathscr{A}}$ in*IND-IBME-CPA *game.*

Definition 4. ***Identity privacy game*** *This game ensures that a distinguisher $\mathscr{D}$ cannot distinguish a ciphertext intended for one multireceiver set from a ciphertext intended for another multireceiver set. Formally, distinguisher $\mathscr{D}$ must be unable to decide whether a ciphertext was encrypted for a chosen multireceiver set, or for a random multireceiver set. Identity privacy game* KP-IBME-CPA *is formally defined as in Figure 1(b).*

The advantage for distinguisher under a KP-IBME-CPA game is defined as

$$Adv^{kp}_{\prod,\mathscr{D}}(\lambda) = |Pr[(b = b')] - \frac{1}{2}| \quad (4)$$

Definition 5. ***Identity privacy*** *An identity-based multireceiver encryption has the identity privacy if all probabilistic polynomial-time distinguishers achieve at most a negligible advantage $Adv^{kp}_{\prod,\mathscr{D}}$ in* KP-IBME-CPA *game.*

4 $\prod_1$: Construction in Composite Order Groups

We explore two concrete IBME schemes. The former one is based on the bilinear group of composite order $ord(\mathbb{G}) = n = p_1p_2p_3$ that p_1, p_2 and p_3 are distinct primes. The latter one is based on the asymmetric bilinear group of prime order p such that the isomorphisms between two groups are not efficiently computable. In this section, we construct a multireceiver encryption scheme $\prod_1$ with identity privacy in composite order model that is based on a canceling group in definition 1. Please refer to Example 3.7 in [11] to output a bilinear group of composite order.

4.1 Proposed Scheme in Composite Order Groups

$\prod_1$.*Stp* 1) Takes as input a security parameter λ, PKG first runs the algorithm $\mathcal{G}$ to generate the composite order group description $(p_1, p_2, p_3, \mathbb{G}_{p_1}, \mathbb{G}_{p_2}, \mathbb{G}_{p_3}, \mathbb{G}_{2,p_1}, \mathbb{G}_{2,p_2}, \mathbb{G}_{2,p_3}, \hat{e}_1)$, and sets $n = p_1p_2p_3$;

2) Selects a random generator g of group $\mathbb{G}$;

3) At random picks $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{Z}_n$, $g, u, v, w \leftarrow \mathbb{G}_{p_1}$, and $X_2 \leftarrow \mathbb{G}_{p_2}, X_3 \leftarrow \mathbb{G}_{p_3}$;

4) Computes $U = uX_3^{\gamma_1}$, $V = vX_3^{\gamma_2}$, $W = wX_3^{\gamma_3}$;

5) At random picks $\alpha, \beta \leftarrow \mathbb{Z}_n$ and computes $\Omega = \hat{e}_1(g, v)^{\alpha\beta}$;

6) Keeps the master key msk=$(g, u, v, w, X_2, g^{\alpha\beta})$;

7) Sets and publishes the system parameters $mk = (n, \mathbb{G}, \mathbb{G}_2, \hat{e}_1, U, V, W, X_3, \Omega)$.

$\prod_1$.*Ext* Let S be the recipient user set such that $S = \{I_1, I_2, \ldots\}$. PKG does the following to generate the private key of identity I_i that $I_i \in S$.

1) Picks $r \in \mathbb{Z}_n$, and $Y_1, Y_2, Y_3 \in \mathbb{G}_{p_2}$ randomly;

2) Computes Sk_1=$g^{\alpha\beta}(wu^{I_i})^rY_1$, $Sk_2 = v^rY_2$, Sk_3= $(\prod_{j \in S \setminus \{I_i\}} u^{I_j})^rY_3$;

3) Outputs $Sk_{I_i} = (Sk_1, Sk_2, Sk_3)$ as the private key of user I_i.

$\prod_1$.*Enc* To send a massage $m \in \mathbb{G}_2$ to a receiver user set S securely, a sender does the following to produce the ciphertext Ct.

1) Randomly picks $s \leftarrow \mathbb{Z}_n$, and at random selects elements $Z_1, Z_2 \leftarrow \mathbb{G}_{p_3}$; Note that the random elements in $\mathbb{G}_{p_3}$ can be produced by raising X_3 to random exponent in $\mathbb{Z}_n$, i.e., at random picks $\upsilon_1, \upsilon_2 \leftarrow \mathbb{Z}_n$ to compute $Z_1 = X_3^{\upsilon_1}, Z_2 = X_3^{\upsilon_2}$;

IND-IBME-CPA	KP-IBME-CPA
$Exp^{\text{IND-IBME-CPA}}_{\prod,\mathscr{A}}(\lambda)$	$Exp^{\text{KP-IBME-CPA}}_{\prod,\mathscr{D}}(\lambda)$
$(I^*, st) \leftarrow \mathscr{A}_0(.)$	$(I_0^*, I_1^*, st) \leftarrow \mathscr{D}_0(.)$
$mk \leftarrow I^*, st, \prod Stp(\lambda)$	$mk \leftarrow I_0^*, I_1^*, st, \prod Stp(\lambda)$
$(m_0, m_1, st') \leftarrow \mathscr{A}_1^{\mathcal{O}_{Ext}}(st, mk)$	$(m, st') \leftarrow \mathscr{D}_1^{\mathcal{O}_{Ext}}(st, mk)$
$b \leftarrow \{0,1\}$	$b \leftarrow \{0,1\}$
$Ct^* \leftarrow \prod Enc(mk, I^*, m_b)$	$Ct^* \leftarrow \prod Enc(mk, I_b^*, m)$
$b' \leftarrow \mathscr{A}_2^{\mathcal{O}_{Ext}}(mk, Ct^*, st')$	$b' \leftarrow \mathscr{D}_2^{\mathcal{O}_{Ext}}(mk, Ct^*, st')$
return $(b' = b)$	return $(b' = b)$

† During the IND-IBME-CPA game, $\mathscr{A}_1, \mathscr{A}_2$ run under the restriction that they cannot query the key extraction and on the challenged identity I^*

‡ During the KP-IBME-CPA game, $\mathscr{D}_1, \mathscr{D}_2$ run under the restriction that they cannot query the key extraction on the challenged identity I_0^* and I_1^*

Figure 1(a) Indistinguishability game **Figure 1(b) Identity privacy game**

2) Computes $C = m \times \Omega^s$;
3) Computes $C_1 = V^s Z_1$;
4) Computes $C_2 = (W \prod_{i \in S} U^{I_i})^s Z_2$;
5) Outputs the multireceiver ciphertext as $Ct = (C, Hdr)$ where $Hdr = (C_1, C_2)$.

$\prod_1$.***Dec*** A user I_i in multireceiver set S can use his private key $Sk_{I_i} = (Sk_1, Sk_2, Sk_3)$ to decrypt the ciphertext Ct. The user I_i proceeds as follows

1) Parses the ciphertext as $Ct = (C_0, Hdr) = (C, C_1, C_2)$;
2) Recovers the message m by computing

$$m = C \cdot \hat{e}_1(Sk_2, C_2)\hat{e}_1(Sk_1 Sk_3, C_1)^{-1}$$

Remark 2. *In the key generation algorithm of this scheme, the multireceiver set S is unbounded. That is, set $S(S \leq n)$ may has arbitrary number of users.*

Remark 3. *Actually, in practical multi-user system, the receiver number is far below from the security parameter n. In this construction, we assume that there is a hard problem in factoring $n = p_1 p_2 p_3$. That is, n is at least 1024-bit (equal to AES-80 security) in practical application which means it can accommodate over 1.79×10^{308} users in a multireceiver system.*

4.2 Correctness

If a user I_i carries a valid private key $Sk_{I_i} = (Sk_1, Sk_2, Sk_3)$ for decrypting a ciphertext Ct, it has

4.3 Security Proof

Our first scheme $\prod_1$ is constructed in composite order groups. In this subsection, we present the security proof. The security in composite order groups is based on the following assumptions, which are derived from the variant of (bilinear) subgroup decisional problems. These assumptions are analyzed in detail in [11, 17].

Assumption 1. *For a given composite order group generating $\mathcal{G}$, the Assumption 1 is stated as the following.*

$$\left[\begin{array}{l} (p_1, p_2, p_3, \mathbb{G}_{p_1}, \mathbb{G}_{p_2}, \mathbb{G}_{p_3}, \mathbb{G}_2, \hat{e}_1) \leftarrow \mathcal{G}(\lambda) \\ n \leftarrow p_1 p_2 p_3, \mathbb{G} \leftarrow \mathbb{G}_{p_1} \times \mathbb{G}_{p_2} \times \mathbb{G}_{p_3} \\ g \leftarrow \mathbb{G}_{p_1}, X_2, Y_2, Z_2 \leftarrow \mathbb{G}_{p_2},\ X_3 \leftarrow \mathbb{G}_{p_3}, \alpha, \beta, s \leftarrow \mathbb{Z}_n \\ T_0 \leftarrow \hat{e}_1(g, g^{\alpha\beta})^s,\ T_1 \leftarrow \mathbb{G}_2 \\ \Gamma \leftarrow (g, g^{\alpha\beta} X_2, X_3, g^s Y_2, Z_2, n, \mathbb{G}, \mathbb{G}_2, \hat{e}_1) \end{array}\right]$$

After given the challenge pair (Γ, T_0, T_1) to adversary $\mathscr{A}$, $\mathscr{A}$ outputs b' and succeeds if $b = b'$ in Assumption 1. The advantage of $\mathscr{A}$ in solving Assumption 1 in groups generated by $\mathcal{G}$ is

$$Adv^1_{\mathcal{G},\mathscr{A}}(\lambda) := |Pr[\mathscr{A}(\Gamma, T_0) = true] - Pr[\mathscr{A}(\Gamma, T_1) = true]|$$

Definition 6. *A group generator $\mathcal{G}$ satisfies the Assumption 1 if the advantage $Adv^1_{\mathcal{G},\mathscr{A}}(\lambda)$ in solving this problem is negligible in probabilistic polynomial-time.*

Assumption 2. *For a given composite order group generating $\mathcal{G}$, let the following distribute be $P(\lambda)$.*

$$\left[\begin{array}{l} (p_1, p_2, p_3, \mathbb{G}_{p_1}, \mathbb{G}_{p_2}, \mathbb{G}_{p_3}, \mathbb{G}_2, \hat{e}_1) \leftarrow \mathcal{G}(\lambda) \leftarrow \mathcal{G}(\lambda) \\ n \leftarrow p_1 p_2 p_3, \mathbb{G} \leftarrow \mathbb{G}_{p_1} \times \mathbb{G}_{p_2} \times \mathbb{G}_{p_3} \\ g \leftarrow \mathbb{G}_{p_1}, X_3 \leftarrow \mathbb{G}_{p_3}, T_0 \leftarrow \mathbb{G}_{p_1 p_2},\ T_1 \leftarrow \mathbb{G}_{p_1 p_2 p_3} \\ \Gamma \leftarrow (g, X_3, n, \mathbb{G}, \mathbb{G}_2, \hat{e}_1) \end{array}\right]$$

After given the challenge pair (Γ, T_0, T_1) to adversary $\mathscr{A}$, $\mathscr{A}$ outputs b' and succeeds if $b = b'$ in Assumption 2. The advantage of $\mathscr{A}$ in solving Assumption 2 in groups generated by $\mathcal{G}$ is

$$Adv^2_{\mathcal{G},\mathscr{A}}(\lambda) := |Pr[\mathscr{A}(\Gamma, T_0) = true] - Pr[\mathscr{A}(\Gamma, T_1) = true]|$$

Definition 7. *A group generator $\mathcal{G}$ satisfies the Assumption 2 if the advantage $Adv^2_{\mathcal{G},\mathscr{A}}(\lambda)$ is negligible in probabilistic polynomial-time.*

$$
\begin{aligned}
C \cdot \frac{\hat{e}_1(Sk_2, C_2)}{\hat{e}_1(Sk_1 Sk_3, C_1)} &= \frac{m\hat{e}_1(g,v)^{\alpha\beta s} \times \hat{e}_1(v^r Y_2, (W\prod_{i\in S} U^{I_i})^s Z_2))}{\hat{e}_1(g^{\alpha\beta}(wu^{I_i})^r Y_1(\prod_{j\in S\setminus\{I_i\}} u^{I_j})^r Y_3, V^s Z_1))} \\
&= \frac{m\hat{e}_1(g,v)^{\alpha\beta s} \times \hat{e}_1(v^r Y_2, (W\prod_{i\in S} U^{I_i})^s Z_2)}{\hat{e}_1(g^{\alpha\beta} w^r (\prod_{j\in S} u^{I_j})^r Y_1 Y_3, V^s Z_1))} \\
&= \frac{m\hat{e}_1(g,v)^{\alpha\beta s} \times \hat{e}_1(v^r, (W\prod_{i\in S} U^{I_i})^s)\hat{e}_1(v^r Y_2, Z_2)}{\hat{e}_1(g^{\alpha\beta}, v^s)\hat{e}_1((\prod_{j\in S} u^{I_j})^r, V^s)\hat{e}_1(g^{\alpha\beta}, Z_1)\hat{e}_1((\prod_{j\in S} u^{I_j})^r, Z_1)\hat{e}_1(Y_1 Y_3, V^s Z_1)} \\
&= \frac{m\hat{e}_1(v^r, Z_2)}{\hat{e}_1(g^{\alpha\beta}, Z_1)\hat{e}_1((\prod_{j\in S} u^{I_j})^r, Z_1)} \\
&= m
\end{aligned}
$$

Assumption 3. *For a given composite order group generating $\mathcal{G}$, the Assumption 3 is stated as the following.*

$$
\left[\begin{array}{l}
(p_1, p_2, p_3, \mathbb{G}_{p_1}, \mathbb{G}_{p_2}, \mathbb{G}_{p_3}, \mathbb{G}_2, \hat{e}_1) \leftarrow \mathcal{G}(\lambda) \\
n \leftarrow p_1 p_2 p_3, \mathbb{G} \leftarrow \mathbb{G}_{p_1} \times \mathbb{G}_{p_2} \times \mathbb{G}_{p_3} \\
g, X_1 \leftarrow \mathbb{G}_{p_1}, X_2, Y_2 \leftarrow G_{p_2}, X_3, Y_3 \leftarrow \mathbb{G}_{p_3} \\
T_0 \leftarrow \mathbb{G},\ T_1 \leftarrow \mathbb{G}_{p_1 p_3} \\
\Gamma \leftarrow (g, X_1 X_2, X_3, Y_2 Y_3, n, \mathbb{G}, \mathbb{G}_2, \hat{e}_1)
\end{array}\right]
$$

After given the challenge pair (Γ, T_0, T_1) to adversary $\mathscr{A}$, $\mathscr{A}$ outputs b' and succeeds if $b = b'$ in Assumption 3. The advantage of $\mathscr{A}$ in solving Assumption 3 in groups generated by $\mathcal{G}$ is

$$Adv^3_{\mathcal{G},\mathscr{A}}(\lambda) := |Pr[\mathscr{A}(\Gamma, T_0) = true] - Pr[\mathscr{A}(\Gamma, T_1) = true]|$$

Definition 8. *A group generator $\mathcal{G}$ satisfies the Assumption 3 if the advantage $Adv^3_{\mathcal{G},\mathscr{A}}(\lambda)$ is negligible in probabilistic polynomial-time.*

To understand our construction, it is necessarily to describe the role of each of subgroups $\mathbb{G}_{p_1}, \mathbb{G}_{p_2}, \mathbb{G}_{p_3}$. The $\mathbb{G}_{p_1}$ subgroup is used to prevent an adversary from manipulating components of either a ciphertext Ct or a key Sk_{I_i} and then evaluating a query on the improperly formed inputs.

The $\mathbb{G}_{p_2}$ subgroup is to hide the factors for secret key and to keep the privacy of a private key. Due to the indistinguishability of the key between $\mathbb{G}_{p_1 p_2}$ and $\mathbb{G}$, thus we can obtain the identity privacy of the keys. The $\mathbb{G}_{p_3}$ subgroup is to hide factors from other subgroups in the ciphertexts. The elements in $\mathbb{G}_{p_2}$ and $\mathbb{G}_{p_3}$ are bilinear orthogonal, that is, $\hat{e}_1(X_2, X_3)$=1 for all $X_2 \in \mathbb{G}_{p_2}$ and $X_3 \in \mathbb{G}_{p_3}$. This is crucial to extract the message from the ciphertext.

We prove the security of confidentiality under a hybrid experiment over a sequence of games which are defined as follows:

Game$_0$ This game is the real scheme with the game definition in 3.2 such that $\Gamma_0 :\ Ct = (C, C_1, C_2)$;

Game$_1$ This game is like the Game$_0$ except that the component C in ciphertext is a random element in $\mathbb{G}_2$ such that $\Gamma_1 :\ Ct = (C \cdot R' = R_0, C_1, C_2)$;

Game$_2$ This game is like the Game$_1$ except that the component C_1 is replaced by a random element in $\mathbb{G}$. i.e., $\Gamma_2 :\ Ct = (R_0, C_1 \cdot R'_1 = R_1, C_2)$;

Game$_3$ This game is like the Game$_2$ except that the component C_2 is replaced by a random element in $\mathbb{G}$. i.e., $\Gamma_3 :\ Ct = (R_0, R_1, C_2 \cdot R'_2 = R_2)$;

In Game$_3$, the ciphertext components are randomly elements in corresponding subgroups, which means that the adversary cannot obtain any information from the ciphertext, including the plaintext and the receivers' identities. We show that the security proof consists of the indistinguishability between each sequential games as above.

Theorem 1. *If a composite order group generator $\mathcal{G}$ satisfies the security assumptions 1,2 and 3, then the proposed multireceiver encryption scheme $\prod_1$ is secure against adaptive chosen message attacks and holds the identity privacy.*

Proof. If the Assumptions 1, 2 and 3 hold for a composite group generator $\mathcal{G}$, we have proved by the lemmata 2, 3, 4 that the real security game Game$_0$ is indistinguishable from Game$_3$, in which the value of b is information-theoretically hidden.

In Game$_3$, the ciphertext components are indistinguishable to random elements in groups $\mathbb{G}_2$ or $\mathbb{G}$. Meanwhile, the payload of message is encoded in C and the identities attribute is encoded in $Hdr = (C_1, C_2)$. By Lemma 1, we show that the adversary cannot distinguish the ciphertext encrypted from a chosen message or a random message string. By Lemma 2 and 3, we indicate that the adversary cannot derive the identities of ciphertext since the components in Game$_3$ are distinguishable to randomly picked elements. Hence the adversary can obtain no advantage in guessing the plaintext and receivers' identities in the ciphertext Ct. □

Lemma 2. *If an adversary $\mathscr{A}$ has non-negligible advantage ϵ_0 in time t_0 in distinguishing Γ_1 from Γ_0, then there exists a probabilistic polynomial-time algorithm to break Assumption 1 with advantage $(\Theta(t_0), \epsilon_0)$.*

Proof. Assume that challenger $\mathscr{C}$ received an Assumption 1 instance, $\mathscr{C}$ works as

Init At random picks $\alpha, \beta, a, b, c \in \mathbb{Z}_n$, and sets $u = g^a, w = g^b, v = g^c$. Then challenger $\mathscr{C}$ generates the other system parameters and sends them to the adversary $\mathscr{A}$.

Stage-1 When $\mathscr{A}$ makes a key extraction query for identity I_i, $\mathscr{C}$ answers $Sk_{I_i} = [g^{\alpha\beta}(hu^{I_i})^{r_1}, g^{r_1}, g^{r_2}, v^{r_2}(\prod_{j\in S\setminus\{I_i\}} u^{I_j})^{r_1}]$ for randomly picked $r_1, r_2 \in \mathbb{Z}_n$. It is fully simulated since $\mathscr{C}$ knows the master key $g^{\alpha\beta}$.

Challenge When the adversary $\mathscr{A}$ provides two challenge message m_0, m_1 and a challenge multireceiver set $S^* = \{I_1^*, \ldots, I_N^*\}$ such that all members in S^* will not be queried, $\mathscr{C}$ outputs the challenge ciphertext as $Ct^* = [m_b \cdot \hat{e}_1(g,T)^{\alpha\beta}, T, T^s, T^{a\Sigma_{j\in S} I_j^* + b + s}]$ for randomly picked $b \in \{0,1\}$ and $s \in \mathbb{Z}_n$.

Stage-2 $\mathscr{A}$ continues to make a bounded number of queries like in Stage 1 with the restriction that $I_i \notin S^*$.

Output Finally, $\mathscr{A}$ outputs b' as the guess of challenged ciphertext Ct^*.

If $T \in \mathbb{G}_{p_1p_2}$ then Ct^* is a valid ciphertext. Otherwise, if $T \in \mathbb{G}_{p_1p_2p_3}$, then Ct^* is a semi-functional ciphertext of $\mathbb{G}$. If adversary $\mathscr{A}$ can succeed in guessing the challenged ciphertext Ct, then $\mathscr{C}$ can break the Assumption 1 with the same advantage. □

Lemma 3. *If an attacker can distinguish the* Γ_1 *and* Γ_2 *with advantage* ϵ_2 *in time* t_2 *after he performs at most* q_2 *key extraction queries, then there exist an algorithm to solve the Assumption 2 problem with the advantage* $(\Theta(t_2), \epsilon_2)$.

Lemma 4. *If an attacker can distinguish the* Γ_2 *and* Γ_3 *with advantage* ϵ_3 *in time* t_3 *after he performs at most* q_3 *key extraction queries, then there exist an algorithm to solve the Assumption 3 problem with the advantage* $(\Theta(t_3), \epsilon_3)$.

Proof. Assume there exists an attacker $\mathscr{A}$ who has non-negligible advantage ϵ_3 to distinguish Γ_3 and Γ_2, then we can construct an algorithm $\mathscr{B}$ to solve the Assumption 2 problem which uses $\mathscr{A}$ as a subroutine.

At first, $\mathscr{A}$ commits two multireceiver user set $S_0 = \{I_1, \ldots\}, S_1 = \{I_1', \ldots\}$, $\mathscr{B}$ randomly flips a coin $\zeta \xleftarrow{\$} \{0,1\}$. $\mathscr{B}$ randomly picks $\alpha, \beta, \gamma_1, \gamma_2, \gamma_3 \xleftarrow{\$} Z_n$, and computes $U = g^u X_2^{\gamma_1}, V = g^v X_2^{\gamma_2}, W = g^w X_2^{\gamma_3}$. $\mathscr{B}$ sets the system public parameters as $(n, U, V, W, X_3, \mathbb{G}, \mathbb{G}_t, \hat{e}_1)$

After $\mathscr{A}$'s key queries is over, $\mathscr{B}$ randomly picks $Z_1, Z_2 \xleftarrow{\$} \mathbb{G}_{p_3}$, and outputs the challenge ciphertext Ct_{S_ζ} as

$$\left[\ C_0 = m\Omega,\ C_1 = T \times Z_1,\ C_2 = T^{\sum_{i\in S_\zeta} I_i} Z_2\ \right]$$

Finally, $\mathscr{A}$ outputs the guess ζ for the ciphertext Ct_{S_ζ}. If $\zeta = 0$, then $\mathscr{B}$ outputs 0 as the Assumption 3 decision that $T = T_0 \in \mathbb{G}$. Otherwise, if $\zeta = 1$ then $\mathscr{B}$ outputs 1 as the solution that T is a random element in $\mathbb{G}_{p_1p_3}$. $\mathscr{B}$ has the same advantage ϵ_1 in solving the Assumption 2 problem. □

5 $\prod_2$: Construction in Prime Order Groups

In this section, we construct another identity-based multi-receiver encryption scheme $\prod_2 = (Stp, Ext, Enc, Dec)$ in prime order groups that holds the same properties in $\prod_1$. We consider an asymmetric bilinear group that there is no efficiently computable isomorphism between two groups $\mathbb{G}$ and $\hat{\mathbb{G}}$.

5.1 Concrete Scheme in Prime Order Groups

$\prod_2$.***Stp*** 1) On input a security parameter λ, PKG generates the asymmetric group description $(p, g, \hat{g}, \mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_2, \hat{e}_2)$, where $g, \hat{g}$ are the generators of group $\mathbb{G}, \hat{\mathbb{G}}$ of order p, respectively;

2) At random picks $\alpha, \beta, \gamma_1, \gamma_2, \gamma_3 \in \mathbb{Z}_p$, computes $g_1 = g^\alpha, u = g^{\gamma_1}, v = g^{\gamma_2}, w = g^{\gamma_3}$;

3) Computes $\hat{g}_1 = \hat{g}^\beta, \hat{u} = \hat{g}^{\gamma_1}, \hat{v} = \hat{g}^{\gamma_2}, \hat{w} = \hat{g}^{\gamma_3}$;

4) Sets the system parameters $mk = (p, g, g_1, u, v, w, \hat{g}, \hat{g}_1, \mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_2, \hat{e}_2)$;

5) Keeps the master key $msk = (\hat{g}^{\alpha\beta}, \hat{u}, \hat{v}, \hat{w})$.

$\prod_2$.***Ext*** To produce a private key for a user with identity $I_i \in \mathbb{Z}_n$ who is a member of recipient set S where $S = \{I_1, I_2, \ldots\}$ denotes as the recipient set, PKG performs as follows.

1) At random picks $r_1, r_2 \in \mathbb{Z}_p$;

2) Computes

$$Sk_1 = \hat{g}^{\alpha\beta}(\hat{v}\hat{u}^{I_i})^{r_1}\hat{w}^{r_2}, Sk_2 = \hat{g}^{r_1},$$
$$Sk_3 = \hat{g}^{r_2}, Sk_4 = \Big(\prod_{j\in S\setminus\{I_i\}} \hat{u}^{I_j}\Big)^{r_1}$$

3) Outputs $Sk_{I_i} = (Sk_1, Sk_2, Sk_3, Sk_4)$ as the private key for user I_i.

$\prod_2$.***Enc*** To encrypt a massage $m \in \mathbb{G}_2$ to a multireceiver user set S, sender does the following.

1) At random picks $s \leftarrow \mathbb{Z}_p$;

2) Computes $C = m \times \hat{e}_2(g_1, \hat{g}_1)^s$;

3) Computes $C_1 = g^s$;

4) Computes $C_2 = (v\prod_{i\in S} u^{I_i})^s$;

5) Computes $C_3 = w^s$;

6) Outputs the ciphertext $Ct = (C, Hdr)$ where $Hdr = (C_1, C_2, C_3)$.

$\prod_2$.***Dec*** A user in set S may use his private key $Sk_{I_i} = (Sk_1, Sk_2, Sk_3, Sk_4)$ to decrypt the ciphertext Ct.

1) Parses the ciphertext as $Ct = (C_0, Hdr) = (C, C_1, C_2, C_3)$;
2) Recovers the message m by computing

$$m = C \cdot \frac{\hat{e}_2(Sk_2, C_2)\hat{e}_2(Sk_3, C_3)}{\hat{e}_2(Sk_1 Sk_4, C_1)}$$

5.2 Security Analysis

The security of our $\prod_2$ scheme is based on the asymmetric decisional bilinear Diffie-Hellman (Asymmetric DBDH) assumption. Notice that the asymmetric strong DBDH assumption is derived from the external computational Diffie-Hellman (XDH) assumption and the asymmetric DBDH assumption.

Definition 9. ***Asymmetric DBDH*** *For given $g \in \mathbb{G}$, $\hat{g} \in \hat{\mathbb{G}}$, $a, b, c \in \mathbb{Z}_p$, and $T \in \mathbb{G}_2$, it is hard to distinguish $(g, g^a, g^c, \hat{g}, \hat{g}^a, \hat{g}^b, g^{abc})$ and $(g, g^a, g^c, \hat{g}, \hat{g}^a, \hat{g}^b, T)$.*

Definition 10. ***Asymmetric strong DBDH*** *For given $g \in \mathbb{G}$, $\hat{g} \in \hat{\mathbb{G}}$, $a, b, c \in \mathbb{Z}_p$, and $T \in \mathbb{G}_2$, it is hard to distinguish $(g, g^a, g^{ab}, g^c, \hat{g}, \hat{g}^a, \hat{g}^b, g^{abc})$ and $(g, g^a, g^{ab}, g^c, \hat{g}, \hat{g}^a, \hat{g}^b, T)$.*

The proof proceeds by a hybrid argument across a number of games. Let $Ct = (C, Hdr) = (C, C_1, C_2, C_3)$ denote the challenge ciphertext given to the adversary during a real attack game. Additionally, let R be a random element of $\mathbb{G}_2$ and R_0, R_1 be random elements of $\mathbb{G}$. We define the following hybrid experiments, which differ in how the challenge ciphertext is generated:

Game$_0$ This game is the real scheme with the game definition in 3.2 such that $\Gamma_0 : \ Ct = (C, C_1, C_2, C_3)$;

Game$_1$ This game is like Game$_0$ except that the component C in ciphertext is replaced by a random element in $\mathbb{G}_2$;

Game$_2$ This game is like Game$_1$ except that the component C_1 is replaced by a random element in $\mathbb{G}$;

Game$_3$ This game is like Game$_2$ except that the component C_2 is replaced by a random element in $\mathbb{G}$;

Game$_4$ This game is like Game$_3$ except that the component C_3 is replaced by a random element in $\mathbb{G}$.

We will give the indistinguishability between Game$_i$ and Game$_{i+1}$ for $i = 0, 1, 2, 3$.

Theorem 2. *If the asymmetric bilinear group generator $\mathcal{G}$ makes the asymmetric (strong) DBDH assumptions hold, the scheme $\prod_2$ in prime order of asymmetric bilinear groups holds semantic security and identity privacy.*

Proof. If the Asymmetric DBDH and Asymmetric strong DBDH Assumptions hold for asymmetric bilinear group generator $\mathcal{G}$, then we prove that the real security game Game$_0$ is indistinguishable from Game$_4$, in which the value of b is information-theoretically hidden. In Game$_4$, the ciphertext components are indistinguishable to random elements in groups $\mathbb{G}_2$ or $\mathbb{G}$. Meanwhile, the payload of message is encoded in C and the identities attribute is encoded in Hdr. Hence the adversary can obtain no advantage in breaking the proposed multireceiver encryption scheme. □

6 Performance Evaluation

In this section, we will analyze the performance of proposed schemes with related schemes. The comparison of related schemes is presented in Table 1. First we consider the schemes in prime order groups that shown in Table 1, there are six schemes that achieve the constant private keys and ciphertexts simultaneously, that are [8, 13, 15, 27, 28] and ours $\prod_2$. During these schemes, only Hu et al.'s scheme [15] and ours $\prod_2$ hold the unbounded multireceiver users, however, the Hu et al.'s scheme cannot support identity privacy property.

We discuss two schemes proposed by Zhang et al. [28] and ours $\prod_1$ that deploy in composite order groups. In [28], the elements in multireceiver set S must be labeled in sequentce, this is because that the Zhang et al.'s scheme is derived from a variant of a hierarchical IBE [17]. At the same time, our $\prod_1$ obtains the unbounded multireceiver and identity privacy abilities.

As for the security, our schemes are provable semantic secure against chosen-plaintext attack in the standard model. We can use a generalized transformation method [5] to construct stronger security schemes to obtain the security of non-malleability and IND-CCA2.

7 Conclusion

We constructed two identity-based multireceiver encryption schemes that supports unbounded receiver users. The proposed schemes achieve the security properties of semantic security and recipient identity privacy, higher computation and communication efficiency of fixed length public parameters, constant private keys and short ciphertexts. As our schemes need not deploy the maximum number of receiver set in advance, they can accommodate unbounded multireceiver user deployment that is flexible in secure communication for dynamic multicast environments.

Acknowledgments

The authors would like to express their deep appreciation for the valuable comments provided by anonymous reviewers. This work is supported by the Na-

Table 1: Performance comparison of the related schemes

schemes	Constant keys	Constant ciphertext	Unbounded user	Semantic security	Key privacy	Security model	Prime order/ composite order
[3]	X	✓	X	cpa	X	selective/std	prime
[8]	✓	✓	X	cpa	X	selective/rom	prime
[13]-1	✓	✓	X	cpa	X	semi-static/std	prime
[13]-2	✓	✓	X	cpa	X	adaptive/rom	prime
[13]-3	✓	X	X	cpa	X	sublinear/std	prime
[15]	✓	✓	✓	cpa	X	selective/std	prime
[16]	✓	X	X	cpa	✓	selective/rom	prime
[19]†	X	✓	X	cca	X	adaptive/std	prime
[27]	✓	✓	X	cpa	X	adaptive/std	composite
[28]	✓	✓	X	cca	X	adaptive/std	prime
our $\prod_1$	✓	✓	✓	cpa	✓	selective/std	composite
our $\prod_2$	✓	✓	✓	cpa	✓	selective/std	prime

† Wang et al. [23] showed that the private keys can be forged.
cpa:chosen-plaintext attack; cca: chosen-ciphertext attack;
STD: in the standard model; ROM: in the random oracle model;

tional Natural Science Foundation of China under Grants 60973134, 61173164, 61170135, 61070189, NSF of Science and Technology Department of Hubei Province under Grant 2010CDA011 and Project of Educational Department of Hubei Province under Grant D20111409.

References

[1] D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In *Cypto'05*, volume 3621 of *LNCS*, pages 258–275, 2005.

[2] D. Boneh, E. Goh, and K. Nissim. Evaluating 2-dnf formulas on ciphertexts. In *TCC'05*, volume 3378 of *LNCS*, pages 325–341, 2005.

[3] D. Boneh and M. Hamburg. Generalized identity based and boradcast encryption schemes. In *Asiacrypt'08*, volume 5350 of *LNCS*, pages 455–470, 2008.

[4] X. Boyen and B. Waters. Anonymous hierarchical identity-based encryption without random oracles. In *Crypto'06*, volume 4117 of *LNCS*, pages 290–307, 2006.

[5] R. Canetti, S. Halevi, and J. Katz. Chosen-ciphertext security from identity-based encryption. In *Eurocrypt'04*, volume 3027 of *LNCS*, pages 207–222, 2004.

[6] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert. Bonsai trees, or how to delegate a lattice basis. In *Eurocrypt'10*, volume 6110 of *LNCS*, pages 523–552, 2010.

[7] V. Daza, J. Herranz, P. Morillo, and C. Rfols. Cca2-secure threshold broadcast encryption with shorter ciphertexts. In *Provsec'07*, volume 4784 of *LNCS*, pages 35–50, 2007.

[8] C. Delerabl. Identity based broadcast encryption with constant size ciphertexts and private keys. In *Asiacrypt'07*, volume 4833 of *LNCS*, pages 200–215, 2007.

[9] C. Delerabl. Anonymity from asymmetry: new constructions for anonymous hibe. In *CT-RSA 2010*, volume 5985 of *LNCS*, pages 148–164, 2010.

[10] C. Fan, L. Y. Huans, and P. H. Ho. Anonymous multireceiver identity-based encryption. *IEEE Trans. on Computers*, 59(9):1239–1249, 2010.

[11] D. M. Freeman. Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In *Eurocrypt2010*, LNCS, pages 44–61, 2010.

[12] S.D. Galbraith, K.G. Paterson, and N.P. Smart. Pairings for cryptosystems. *Discrete Applied Mathematics*, 156(16):3113–3121, 2008.

[13] C. Gentry and B. Waters. Adaptive security in broadcast encryption systems. In *Eurocrypt'09*, volume 5479 of *LNCS*, pages 171–188, 2009.

[14] J. Herranz, F. Laguillaumie, and C. Rafols. Relations between semantic security and anonymity in identity-based encryption. *Information Processing Letters*, 111:453–460, 2011.

[15] L. Hu, Z. Liu, and X. Cheng. Efficient identity-based broadcast encryption without random oracles. *Journal of Computers*, 5(3):331–336, 2010.

[16] J. Hur, C. Park, and S. O. Hwang. J. hur, c. park, and s. o. hwang. *Information Fusion*, 13(4):296–303, 2012.

[17] A. Lewko and B. Waters. New techniques for dual system encryption and fully secure hibe with short ciphertexts. In *TCC'10*, volume 5978 of *LNCS*, pages 455–479, 2010.

[18] A. Lewko and B. Waters. Unbounded hibe and attribute-based encryption. In *Eurocrypt'11*, volume 6632 of *LNCS*, pages 547–567, 2011.

[19] Y. Ren and D. Gu. Fully cca2 secure identity based broadcast encryption without random oracles. *Information Processing Letter*, 109:527–533, 2009.

[20] P. Roelse. Dynamic subtree tracing and its application in pay-tv systems. *International Journal of Information Security*, 10(3):173–187, 2011.

[21] A. Shamir. Identity-based cryptosystems and signature schemes. In *Crypto'84*, volume 196 of *LNCS*, pages 47–53, 1984.

[22] J. Wang and J. Bi. Lattice-based identity-based broadcast encryption. 2010.

[23] X. Wang, J. Weng, X. Yang, and Y. Yang. Cryptanalysis of an identity based broadcast encryption scheme without random oracles. *Information Processing Letter*, 111:461–464, 2011.

[24] B. Waters. Dual system encryption: realizing fully secure ibe and hibe under simple assumptions. In *Crypto'09*, volume 5677 of *LNCS*, pages 619–636, 2009.

[25] J. H. Yang and C. C. Chang. A low computational-cost electronic payment scheme for mobile commerce with large-scale mobile users. *Wireless Personal Communications*, 63(1):83–99, 2012.

[26] X. Yi and L. Batten. Wireless broadcast encryption based on smart cards. *Wireless Networks*, 16(1):153–165, 2010.

[27] L. Zhang, Y. Hu, and Q. Wu. Adaptively secure identity-based broadcast encyrption with constant size private key and ciphertexts from the subgroups. *Mathematical and Computer Modeling*, 55(1-2):12–18, 2012.

[28] L. Zhang, Q. Wu, and Y. Hu. New constructions of identity-based broadcast encryption without random oracles. *KSII Trans. on Internet and Information Systems*, 5(2):428–439, 2011.

[29] M. Zhang, B. Yang, and T. Takagi. Group-oriented setting's multisigncryption scheme with threshold designcryption. *Information Sciences*, 181:4041–4050, 2011.

[30] M. Zhang, B. Yang, and T. Takagi. Reconciling and improving of multi-receiver signcryption protocols with threshold decryption. *Security and Communication Networks*, Doi: 10.1002/sec.509, 2012.

Zhenhua Chen received her B.S. degree from Lanzhou University in 1998, and the M.S. degree from Nanjing University of Science Technology in 2007. She is currently studying at School of Computer Sciences, Shaanxi Normal University as a Ph.D. candidate. She had been worked at Institute of Huaiyin Technology from 1998 to 2007 and at Beijing University of Technology as a associate professor from 2007 to 2011 respectively. Her research interests include cryptography and information security.

Shundong Li received his Ph. D. degree from Xi'an Jiaotong University in 2003, and had been studied in Tsinghua University as Postdoctors from 2003 to 2005. From 2005 to July 2007he had been a associate professor at Beijing Normal University. He is currently a professor and supervisor of Ph.D. at School of Computer Science, Shaanxi Normal University. His research interests focus on secure multi-party computation and confidential data mining.

Chunzhi Wang is a Ph.D, professor. She is currently working at College of Computer Science and Engineering, Hubei University of Technology. Her research interests focus on network security.

Yanping Shen is now working at Institute of Disaster Prevention. Her research focuses on the network security.