Anonymous Identity-Based Encryption with Identity Recovery

Xuecheng Ma¹,², Xin Wang¹,², and Dongdai Lin¹

¹ State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
² School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
{maxuecheng}@iie.ac.cn

Abstract. Anonymous Identity-Based Encryption can protect privacy of the receiver. However, there are some situations that we need to recover the identity of the receiver, for example a dispute occurs or the privacy mechanism is abused. In this paper, we propose a new concept, referred to as Anonymous Identity-Based Encryption with Identity Recovery (AIBEIR), which is an anonymous IBE with identity recovery property. There is a party called the Identity Recovery Manager (IRM) who has a secret key to recover the identity from the ciphertext in our scheme. We construct it with an anonymous IBE and a special IBE which we call it testable IBE. In order to ensure the semantic security in the case where the identity recovery manager is an adversary, we define a stronger semantic security model in which the adversary is given the secret key of the identity recovery manager. To our knowledge, we propose the first AIBEIR scheme and prove the security in our defined model.

Keywords: IBE, anonymous, identity recovery, testable

1 Introduction

Public key encryption is one of the most important primitives in cryptography, which was presented in the great paper titled “New Directions in Cryptography” in 1976 [DH76]. Public key encryption solves the problem that the sender and the receiver should share a common secret key which is not known to the adversary before communicating. One of the disadvantages in public key encryption is using certificate to bind the public key to the identity of its owner. The issue of management of certificates is complex and cumbersome.

In 1984, Shamir [Sha84] introduced the concept of Identity-Based Encryption (IBE) which solved the problem. IBE is a generalization of public key encryption where the public key of a user can be arbitrary string such as an e-mail address. The first realizations of IBE are given by [SOK00, BF01] using groups equipped with bilinear maps. Since then, realizations from bilinear maps

* A preliminary version of this work will appear in the proceedings of ACISP 2018
from quadratic residues modulo composite \[ \text{Coc01,BGH07} \], from lattices \[ \text{GPV08,CHKP10,ABB10,Boy10} \] and from the computational Diffie-Hellman assumption \[ \text{DG17} \] have been proposed.

In order to protect the privacy of the receiver, Boyen \[ \text{Boy03} \] first explicitly stated the concept of anonymous IBE\(^3\), where the ciphertext does not leak the identity of the recipient. In fact, \[ \text{BF01} \] is the first anonymous IBE scheme although they did not state it explicitly. Since then, there are some follow-up works realized from bilinear maps \[ \text{BW06} \], from quadratic residues modulo composite \[ \text{AG09} \], from lattices \[ \text{GPV08,ABB10} \] and from the computational Diffie-Hellman assumption \[ \text{BLSV17} \].

Anonymous IBE protects the privacy of the message and the receiver’s identity in the meantime, but we can only recover the message. However, there are some situations where we need to recover the identity of the receiver, for example a dispute occurs or the privacy mechanism is abused. In a mail system, there is a need to keep the receiver anonymous for everyone except the mail server who will forward the mail to the receiver. So can we extract the identity from an anonymous IBE ciphertext with some secret information? In this paper, we present a new primitive called anonymous identity-based encryption with identity recovery (AIBEIR) which can solve this problem. AIBEIR is a special anonymous IBE which has an additional property that the identity recovery manager can recover the identity with a secret key. But the identity recovery manager can not get any information of the message from the ciphertext. Formally, AIBEIR is semantic secure even when the identity recovery manager is the adversary.

1.1 Motivations

On the one hand, anonymity protects user’s privacy. On the other hand, unconditional privacy may lose supervision and cause illegal behavior. To balance the anonymity and accountability in anonymous IBE schemes, PKG can send the recovery key to a manager who takes charge of recovering identities of suspected ciphertexts. A similar notion was presented in group signature where a group manager can reveal the member identity registered to is group. But there is a subtlety that signature can be verified while general encryption does not have verifiable property. If a mole want to communicate with his partners, he will choose other secure encryption schemes other than encryption schemes with recovery property. In fact, it is inefficient if every ciphertext should be verified before delivering. So we can just restrict that the anonymous IBE with recovery is the only choice. For example, in the army, the internal communication tool is deployed with anonymous IBE with recovery. If some ciphertext is suspected to contain sensible data which is not allowed to send to the recipient.

In fact, anonymous IBE with recovery identity subdivides the privacy which makes the ciphertext anonymous for all users except some privileged supervisors. Imagine that how can an anonymous IBE encryption under the destination IP

\(^3\) In fact, Boyen gave an identity-based signcryption with a formalization of sender and recipient anonymity
address be transferred. Routers with recovery key can recover the corresponding identities of the ciphertext which makes it viable. Similarly, in a mail system deployed with anonymous IBE, the server does not know which one is the recipient.

1.2 Our Contributions

We propose a new cryptographic primitive called anonymous IBE with identity recovery. We first define the model and security notions of AIBEIR. We then present a method to convert an anonymous IBE into AIBEIR with the help of testable IBE and prove that the new scheme satisfies the security we defined. A testable IBE is an IBE which can test whether ciphertext $c$ is a ciphertext under identity $id$ given $c$ and $id$. It is obvious that a testable IBE is not anonymous. We will show that [BB04a,Wat05] and their variations are testable IBEs. AIBEIR consists of four parties, a Private Key Generator(PKG), an Identity Recovery Manager(IRM), a sender, and a receiver. There are five procedures in an AIBEIR scheme. They are setup procedure, extract procedure, encrypt procedure, decrypt procedure, and recover procedure.

Besides correctness and anonymity, we introduce two new security notions in AIBEIR. The first is a stronger semantic security, where the identity recovery manager is the adversary. The second is recovery, which ensures that the recovery is reliable and no adversary can fool the identity recovery manager. Finally, we prove the security of our AIBEIR scheme according to our security notions. To the best of our knowledge, our construction is the first anonymous IBE scheme with the identity recovery property.

To construct an AIBEIR scheme, we first encrypt the plaintext by a testable IBE and encrypt the testable IBE ciphertext using an anonymous IBE. Moreover, we encrypt the receiver’s identity under the recovery manager’s identity. The anonymity is guaranteed by the anonymous IBE and the stronger CPA security is guaranteed by the security of the testable IBE. Given the master secret key of the anonymous IBE, identity recovery manager obtains the identity and the testable IBE ciphertext by decrypting corresponding ciphertext, respectively. Then, check whether the testable IBE ciphertext is under the identity and output the identity if the test algorithm outputs 1.

1.3 Related Work

Identity-based cryptosystems were introduced by Shamir [Sha84]. The first realizatons of IBE were given by Boneh, Franklin [BF01] and Sakai et al [SOK00]. Boneh and Franklin gave the security model and their proposal is the first anonymous IBE. The anonymity was first noticed by Boyen [Boy03]. Another view of Anonymous IBE is as a combination of identity-based encryption with the property of key privacy, which was introduced by Bellare et al [BBDP01]. A similar concept called Identity-Based Group Encryption(IBGE) was presented by Xiling et al [LRL+16]. Traceability in their scheme is similar to recovery in ours. But there are some differences between IBGE and AIBEIR. On the one hand,
we do not have Verify algorithm which is used to verify whether the ciphertext belongs to the group. On the other hand, our construction is implemented by IBEs while they utilized PKE, IBE and ZKP (Zero-Knowledge Proofs) to construct their scheme. We do not think their scheme is a “pure” IBE because of the use of PKE. Recently, [GSRD17] pointed that the zero-knowledge proof used in [LRL+16] leaks much more information, due to which the verifier who is honest but curious will be able to identify the designated recipient. They proposed a construction with six random oracles.

1.4 Organization

This paper is organized as follows. In Sect. 2, we introduce definitions that we use throughout the paper including a definition of anonymous identity-based encryption and testable identity-based encryption. In Sect. 3, we show the syntax and security of the new primitive anonymous identity-based encryption with identity recovery. In Sect. 4, we present the construction of AIBEIR and prove its security. We conclude the paper in Sect. 5.

2 Preliminaries and Definitions

We denote \( s \leftarrow \mathcal{S} \) as the operation of assigning to \( s \) an element selected uniformly at random from set \( \mathcal{S} \). The notation \( x \leftarrow A(\cdot) \) denotes the operation of running an algorithm \( A \) with some given input and assigning the output to \( x \). A function \( \text{negl}: \mathbb{N} \rightarrow \mathbb{R} \) is negligible if for every positive polynomial \( \text{poly} \) and sufficiently large \( \lambda \), it holds that \( \text{negl}(\lambda) < 1/\text{poly}(\lambda) \). We use \( 0^\ell \) to denote the zero vector whose length is \( \ell \). If \( a \) is a vector, \( |a| \) denotes its length.

2.1 Bilinear Groups

Let \( G_1, G_2 \) and \( G_T \) be multiplicative cyclic groups of prime order \( p \). Let \( g_1, g_2 \) be generators of groups \( G_1 \) and \( G_2 \), respectively, and \( e: G_1 \times G_2 \rightarrow G_T \) be a bilinear map that holds the following features:

- Bilinearity: \( e(u^a, v^b) = e(u, v)^{ab} \) for all \( u \in G_1, v \in G_2 \) and \( a, b \in \mathbb{Z}_p \).
- Non-degeneracy: \( e(g_1, g_2) \neq 1_{G_T} \).
- Computability: there exists an efficient algorithm to compute \( e(u, v) \) for any input pair \( u \in G_1, v \in G_2 \).

We assume a symmetric bilinear map such that \( G_1 = G_2 = G \) and \( g_1 = g_2 = g \).

2.2 Identity-Based Encryption

Let \( \lambda \) be a security parameter. An identity-based encryption is a tuple of algorithms \( \Pi_{IBE} = (\text{IBE.Setup}, \text{IBE.Extract}, \text{IBE.Encrypt}, \text{IBE.Decrypt}) \) with the following properties:
Anonymous Identity-Based Encryption with Identity Recovery

- **Setup**($1^\lambda$): This is a polynomial time algorithm which takes as input $1^\lambda$ and outputs the system parameter $mpk$ and a master secret key $msk$.
- **Extract**($id, msk$): This is a polynomial time algorithm which takes as input user’s identity $id$ and master secret key $msk$, and outputs the user’s corresponding private key $sk_{id}$.
- **Encrypt**($m, id, mpk$): This is a polynomial time algorithm which takes as input a message $m$ in the message space, system parameter $mpk$, the receiver’s identity $id$ and outputs a ciphertext $c$ in the ciphertext space.
- **Decrypt**($mpk, c, sk_{id}$): This is a polynomial time algorithm which takes as input system parameter $mpk$, ciphertext $c$, user’s private key $sk_{id}$, outputs the message $m$ in the message space.

**Correctness.** We require correctness of decryption: that is, for all $\lambda$, all identity $id$ in the identity space, all $m$ in the specified message space, $\Pr[\text{Decrypt}(mpk, sk_{id}, \text{Encrypt}(m, id, mpk))] = m = 1 - \text{negl}(\lambda)$ holds, where the probability is taken over the randomness of the algorithms.

**Anonymity and Semantic security.** When the ciphertext can not reveal information of the message, we say that the cryptosystem is chosen-plaintext secure. We say that the cryptosystem is anonymous if the ciphertext can not reveal information of the identity of the receiver. We combine these two notions.

**Definition 1** An IBE scheme is anonymous against chosen-identity and chosen-plaintext attacks if there does not exist any polynomial adversary $A$ who has non-negligible advantage in the following game:

**Setup:** The challenger takes as input a security parameter $\lambda$ (in unary) and runs the **Setup** algorithm of the IBE. It provides $A$ with the system parameters $mpk$ while keeping the master secret key $msk$ to itself.

**Phase 1:** The adversary $A$ can make any polynomial key-extraction queries defined as follows: key-extraction query ($id$): The adversary $A$ can choose an identity $id$ and sends it to the challenger. The challenger generates a secret key $sk_{id}$ of $id$ and returns it to $A$.

**Challenge:** When $A$ decides that Phase 1 is complete, it chooses two equal-length plaintexts $m_0, m_1$ and two identities $id_0, id_1$ under the constraint that they have not been asked for the private keys. The challenger chooses uniformly at random two bits $b \in \{0,1\}, \gamma \in \{0,1\}$ and sends a ciphertext $c^*$ of $m_b$ as the challenge ciphertext under $id_{\gamma}$ to $A$.

**Phase 2:** The adversary $A$ can also make queries just like Phase 1 except that it cannot make a key-extraction query of either $id_0$ or $id_1$.

**Guess:** $A$ outputs a guess $(b', \gamma')$ of $(b, \gamma)$.

We define the advantage of the adversary $A$ as $\text{Adv}_A = |Pr[b = b' \land \gamma = \gamma'] - \frac{1}{2}|$. 
2.3 Testable Identity-Based Encryption

Definition 2 An Identity-Based Encryption is testable if there exists an algorithm Test(.¸) which takes as input c and an identity id and returns 1 if c is a part of a valid ciphertext under id and 0 otherwise.

Remark 1 In our construction, we need the testable IBE to satisfy an additional property that the ciphertext c can be partitioned into two parts c₀ and c₁ where c₀ contains information of the identity but no information of the message while c₁ contains information of the message but no information of the identity. And the test algorithm takes c₀ other than c as input. Our construction works if the testable IBE without this property. But if it is satisfied, our construction is more efficient because encrypting the part containing information of plaintext is sufficient. Moreover, to our knowledge, all of the existing testable IBEs satisfy it.

Some realizations of IBE from bilinear maps such as [BB04a, Wat05] satisfy the definition of testable IBE. We will prove that the scheme in [Wat05] is a testable IBE.

Let G be a group of prime order, p, for which there exists an efficiently computable bilinear map into G₁. Additionally, let e : G × G → G₁ denote the bilinear map and g be the corresponding generator. The size of the group is determined by the security parameter. Identities will be represented as bit strings of length n, a separate parameter unrelated to p. The construction follows.

Setup. The system parameters are generated as follows. We choose a random generator, g ∈ G and g₂ randomly in G. We choose a secret α ∈ Zp and set g₁ = gα. Further, choose a random value u' ∈ G and a random n-length vector U = (ui), whose elements are chosen at random from G. The published public parameters are g, g₁, g₂, u', and U. The master secret key is g₂α.

Key Generation. Let v be a n-bit string representing an identity, vᵢ denote the ith bit of v, and V ⊆ {1,...,n} be the set of all i for which vᵢ = 1. (That is V is the set of indices for which the bit string v is set to 1.) A private key for identity v is generated as follows. First, a random r ∈ Zp is chosen. Then the private key is constructed as:

d_v = (g₂²(u' ∏ i ∈ V uᵢ)ʳ, gʳ)

Encryption. A message M ∈ G₁ is encrypted for an identity v as follows. A value t ∈ Zp is chosen at random. The ciphertext is then constructed as:

C = (e(g₁,g₂)ᵗ M, gᵗ, (u' ∏ i ∈ V uᵢ)ᵗ)

Decryption. Let C = (C₁, C₂, C₃) be a valid encryption of M under the identity v. Then C can be decrypted by d_v = (d₁, d₂) as:
Anonymous Identity-Based Encryption with Identity Recovery

\[ C_1 \in \mathbb{G}_2 \times \mathbb{G}_2 = (e(g_1, g_2)^{t-M}, e((g_1, g_2)^{t-M} \prod_{i \in V} u_i)) = e(g_1, g_2)^{t-M} \]

\[ \Perp \]

We can also define a Test algorithm as follows:

**Test.** Let \( C = (C_1, C_2, C_3) \) be a valid encryption under the identity \( v \). Let \( v' \) be a \( n \)-bit string representing an identity, \( v'_i \) denote the \( i \)th bit of \( v' \), and \( V' \subseteq \{1, \ldots, n\} \) be the set of all \( i \) for which \( v'_i = 1 \). Output 1 if \( e(g, C_3) = e(C_2, (\prod_{i \in V'} u_i)) \) and \( \Perp \) otherwise. In fact, \( (C_1, C_2) \) contain the information of the message and no information of the identity. \( C_3 \) contains information of the identity but no information of the message. So it is a testable IBE.

3 Anonymous Identity-Based Encryption with Identity Recovery

Compared to identity based encryption, there is an additional algorithm Recover that takes recovery secret key and a ciphertext as inputs and output the corresponding identity or \( \Perp \) if the ciphertext is not valid. Let \( \lambda \) be a security parameter. An anonymous identity-based encryption with recovery is a tuple of algorithms \( \Pi_{AIBEIR} = (AIBEIR.Setup, AIBEIR.Extract, AIBEIR.Encrypt, AIBEIR.Decrypt, AIBEIR.Recover) \) with the following properties:

- **Setup(1^\lambda):** This is a polynomial time algorithm which takes as input \( 1^\lambda \) and outputs the system parameter \( mpk \), a master secret key \( msk \) and secret key of the identity recovery manager \( sk_{IRM} \). Then PKG sends \( sk_{IRM} \) to the identity recovery manager in a secret channel. It is operated by PKG.

- **Extract(id, msk):** This is a polynomial time algorithm which takes as input a user’s identity \( id \) and \( msk \), outputs the user’s corresponding private key \( sk_{id} \).

- **Encrypt(m, mpk, id):** This is a polynomial time algorithm which takes as input a message \( m \) in a specified message space, system parameter \( mpk \), the receiver’s identity \( id \) and outputs a ciphertext \( c \) in the ciphertext space. It is operated by the sender.

- **Decrypt(mpk, c, sk_{id}):** This is a polynomial time algorithm which takes as input system parameter \( mpk \), ciphertext \( c \), user’s private key \( sk_{id} \) and outputs the message \( m \) in the message space. It is operated by the receiver.

- **Recover(c, sk_{IRM}):** The identity recovery manager outputs an identity \( id \) if \( c \) is a valid ciphertext under \( id \) and \( \Perp \) otherwise. It is operated by the identity recovery manager.

**Correctness.** We say that \( \Pi_{AIBEIR} \) is correct if it satisfies the following two properties:
• **Decryption correctness:** For any \(id\) in identity space and \(m\) in a specified message space, \(\Pr[AIBEIR.\text{Decrypt}(sk_{id}, AIBEIR.\text{Encrypt}(m, id, mpk)) = m] = 1 - \text{negl}(\lambda)\).

• **Recovery correctness:** For any valid ciphertext \(c = AIBEIR.\text{Encrypt}(m, id, mpk)\), \(\Pr[\text{Recover}(sk_{IRM}, c) = id] = 1 - \text{negl}(\lambda)\).

**Anonymity.** The anonymity of AIBEIR is the same as that of anonymous IBE. Note that the recovery manager can not be the adversary.

**Stronger semantic security.** In the semantic security model of IBE, adversary has no information about the master secret key \(msk\). But in the definition of our AIBEIR scheme, the identity recovery manager holds \(sk_{IRM}\) which makes it more powerful. So if the identity recovery manager is the adversary, the semantic security model of IBE is not feasible. We define a stronger semantic security as follows:

**Definition 3** An AIBEIR scheme is strongly semantic secure against chosen-identity and chosen-plaintext attacks if there does not exist any polynomial adversary \(A\) who have non-negligible advantage in the game below:

**Setup:** The challenger takes as input a security parameter \(\lambda\) (in unary) and runs the \(\text{Setup}\) algorithm of the AIBEIR. It provides \(A\) with the system public parameters \(mpk\) and identity recovery secret key \(sk_{IRM}\) while keeping the master secret key \(msk\) to itself.

**Phase 1:** The adversary \(A\) can make any polynomial key-extraction queries defined as follows: key-extraction query \((id)\): \(A\) can choose an identity \(id\) and send it to the challenger. The challenger generates secret key \(sk_{id}\) and returns it to \(A\).

**Challenge:** When \(A\) decides that Phase 1 is complete, it chooses two equal-length plaintexts \(m_0, m_1\) and an identity \(id^*\) under the constraint that it has not asked for the private key and sends them to the challenger. The challenger chooses uniformly at random a bit \(b \in \{0, 1\}\) and sends a ciphertext \(c^* = \text{Encrypt}(m_b, id^*, mpk)\) as the challenge ciphertext to \(A\).

**Phase 2:** \(A\) can also make queries just like Phase 1 except that it cannot make a key-extraction query of \(id^*\).

**Guess:** \(A\) outputs a guess \(b'\) of \(b\).

We define the advantage of adversary \(A\) as \(\text{Adv}_A = |\Pr[b = b'] - \frac{1}{2}|\).

**Recovery.** An AIBEIR scheme is recoverable if \(\text{Recover}\) algorithm can always extract the right identity from a valid ciphertext and output \(\bot\) when the input is an invalid ciphertext.

**Definition 4** An AIBEIR scheme is recoverable if there does not exist any PPT adversary \(A\) who wins the following game with non-negligible probability.
Setup: The challenger takes as input a security parameter $\lambda$ (in unary) and runs the Setup algorithm of the AIBEIR. It provides $A$ with the system parameters $mpk$ while keeping the master secret key $msk$ and $sk_{IRM}$ to itself.

Monitor Phase: The adversary $A$ can query recover oracle and key-extraction oracle.

Challenge: When $A$ decides that Monitor Phase is complete, the adversary sends $e^{*}$ to the challenger. The challenger sends the output of Recover algorithm to $A$.

Output: $A$ wins the game if the output of Recover($e^{*}, sk_{IRM}$) is $\bot$ or $id$ while $e^{*}$ is a valid ciphertext under $id'$ where $id \neq id'$ or the output of Recover($e^{*}, sk_{IRM}$) is $id$ while $e^{*}$ is not a valid ciphertext. Here we require $id$ has not been asked as a key-extraction query for the need to prove the security.

4 A Construction from Anonymous IBE and Testable IBE

In this section, we present our construction of AIBEIR from anonymous IBE and testable IBE. Let $H_1 = (A$-IBE.Setup, $A$-IBE.Enc, $A$-IBE.Dec, $A$-IBE.Extract) be an anonymous IBE scheme, $H_2 = (T$-IBE.Setup, $T$-IBE.Enc, $T$-IBE.Dec, $T$-IBE.Extract, $T$-IBE.Test) be a testable IBE scheme. Let $id_{x}$ denote the identity of the identity recovery manager in scheme $H_2$. Then, we can construct an AIBEIR scheme $\Pi$ as follows:

4.1 The Construction

We describe our AIBEIR scheme ($\text{AIBEIR.Setup, AIBEIR.Extract, AIBEIR.Encrypt, AIBEIR.Decrypt, AIBEIR.Recover}$) as follows:

- Setup($1^{\lambda}$): Run the Setup algorithms of $A$-IBE and $T$-IBE and obtain $(MPK_{A}, MSK_{A}) \leftarrow A$-IBE.Setup($1^{\lambda}$), $(MPK_{T}, MSK_{T}) \leftarrow T$-IBE.Setup($1^{\lambda}$), respectively. Compute $SK_{T, id} = T$-IBE.Extract($MSK_{T}, id$), $(mpk, msk) = ((MPK_{A}, MPK_{T}),(MSK_{A}, MSK_{T}))$, $sk_{IRM} = (MSK_{A}, SK_{T, id})$.
- Extract($id, msk$): Run the Extract algorithms of $A$-IBE and $T$-IBE and obtain $SK_{A, id} = A$-IBE.Extract($id, MSK_{A}$) and $SK_{T, id} = T$-IBE.Extract($id, MSK_{T}$), respectively. Output $sk_{id} = (SK_{A, id}, SK_{T, id})$.
- Encrypt($m, id, mpk$): Run the Encrypt algorithms of $A$-IBE and $T$-IBE and obtain $(c_0, c_1) = T$-IBE.Enc($m, id, MPK_{T}$), $c_2 = A$-IBE.Enc($c_0, id, MPK_{A}$) and $c_3 = T$-IBE.Enc($id, id_{x}, MPK_{T}$). Output $c = (c_1, c_2, c_3)$.
- Decrypt($mpk, c, sk_{id}$): Parse $c$ as $c_1, c_2$ and $c_3$. Then compute $c_0 = A$-IBE.Dec($c_2, SK_{A, id}$), $m = T$-IBE.Dec($c_0|c_1$, $SK_{T, id}$).
- Recover($e, sk_{IRM}$): Parse $e$ as $c_1, c_2$ and $c_3$. Parse $sk_{IRM}$ as $MSK_{A}$ and $SK_{T, id}$. Then compute $id = T$-IBE.Dec($c_3, SK_{T, id}$) and $SK_{A, id} = A$-IBE.Extract($id, MSK_{A}$). Take as input $SK_{A, id}$ and $c_2$, obtain the ciphertext $c_0$ by running the Decrypt algorithm of $A$-IBE.Dec($SK_{A, id}, c_2$). Finally, output $id$ if $T$-IBE.Test($id, c_0$) = 1, and $\bot$ otherwise.
Remark 2 Here the message space of $\Pi_1$ includes the ciphertext space of $\Pi_2$. We set the intersection of identity space of $\Pi_1$ and $\Pi_2$ as the identity space of $\Pi$.

4.2 Correctness

Theorem 1 If $\Pi_1$ is a correct anonymous IBE scheme and $\Pi_2$ is a correct testable IBE scheme then $\Pi$ is a correct AIBEIR scheme.

- **Decryption correctness:** The decryption correctness is guaranteed by the decryption correctness of $\Pi_1$ and $\Pi_2$.
- **Recovery correctness:** The recovery correctness is guaranteed by the decryption correctness of $\Pi_1$, $\Pi_2$ and test correctness of $\Pi_2$.

4.3 Anonymity

Theorem 2 If $\Pi_1$ is an IBE scheme which is anonymous against adaptively chosen-identity and chosen-plaintext attacks and $\Pi_2$ is a testable IBE scheme which is fully secure against chosen-identity and chosen-plaintext attacks, then $\Pi$ is an AIBEIR scheme which is anonymous against adaptively chosen-identity and chosen-plaintext attacks.

Proof. We prove the above theorem by hybrid arguments.

$H_0$: This hybrid is the real experiment in the Definition 1. The logic of the challenger is shown as follows:

- **Initialization:**
  
  $$(MPK_A, MSK_A) \leftarrow A-IBE.Setup(1^\lambda), (MPK_T, MSK_T) \leftarrow T-IBE.Setup(1^\lambda)$$
  
  $$(mpk, msk) = ((MPK_A, MPK_T), (MSK_A, MSK_T))$$
  
  $SK_{T, id} = T-IBE.Extract(MSK_T, id), sk_{IRM} = (MSK_A, SK_{T, id})$$
  
  send $mpk$ to $A$

- **Upon receiving a secret key query$(id)$:**
  
  $SK_{A, id} = A-IBE.Extract(id, MSK_A)$ and $SK_{T, id} = T-IBE.Extract(id, MSK_T)$
  
  send $sk_{id} = (SK_{A, id}, SK_{T, id})$ to $A$

- **Upon receiving the challenge query$(m_0, m_1, id_0, id_1)$:**
  
  $b \leftarrow \{0, 1\}, \gamma \leftarrow \{0, 1\}$
  
  (1) $(c_0, c_1) = T-IBE.Enc(m_0, id_0, MPK_T)$
  
  (2) $c_2 = A-IBE.Enc(c_0, id_0, MPK_A)$
  
  (3) $c_3 = T-IBE.Enc(id_1, MPK_T)$
  
  send $c = (c_1, c_2, c_3)$ to $A$

\footnote{Here the adversary can not be the identity recovery manager and has PPT power. If AIBE and TIBE are both selective secure, our AIBEIR scheme is also selective secure.}
$H_1$: In this hybrid, it is identical to $H_0$ except that we just change how the challenge ciphertext is generated. We replace the lines marked (1) in $H_0$ as follows:
\[ c_0, c_1 = \text{T-IBE.Enc}(0^{\|m_0\|}, id_\gamma, MPK_T). \]

$H_2$: Compared to $H_1$, we replace the lines marked (2) in $H_0$ as follows:
\[ c_2 = \text{A-IBE.Enc}(0^{\|c_0\|}, id_\gamma, MPK_A). \]

$H_3$: Same as $H_2$, except we replace the lines marked (2) in $H_0$ as follows:
We just randomly choose $id$ from identity space except $id_0$ and $id_1$. We then set $c_2 = \text{A-IBE.Enc}(0^{\|c_0\|}, id, MPK_A)$.

$H_4$: Identical to $H_3$, except we replace the lines marked (3) in $H_0$ as follows:
We just set $c_3$ as $\text{T-IBE.Enc}(0^{\|id\|}, id_\epsilon, MPK_T)$.

It is easy to know that the challenge ciphertext in $H_4$ contains no information about $b$ and $\gamma$ (except their length). So the advantage of $A$ in $H_4$ is 0. We prove the above theorem by showing that $H_0 \approx H_1 \approx H_2 \approx H_3 \approx H_4$ through the following lemmas.

**Lemma 1** Any PPT adversary cannot distinguish $H_0$ and $H_1$, if scheme $\Pi_2$ is fully secure against adaptively chosen-identity and chosen-plaintext attacks.

**Proof.** We can construct a simulator $B$ to break the full security against chosen-identity and chosen-plaintext attacks of scheme $\Pi_2$, if there is an adversary $A$ who can distinguish $H_0$ and $H_1$.

**Setup:** The challenger takes as input a security parameter $\lambda$ (in unary) and runs the Setup algorithm of $\Pi_2$. It provides $B$ with the system parameters $MPK_T$ while keeping the master secret key $MSK_T$ to itself. $B$ computes $(MPK_A, MSK_A) \leftarrow \text{A-IBE.Setup}(1^\lambda)$, and sends $MPK = (MPK_A, MPK_T)$ to $A$.

**Phase 1:** When the adversary $A$ makes key-extraction query and sends an identity $id$ to $B$, $B$ just forwards it as the key-extraction query to the challenger. The challenger sends $SK_{T, id}$ to $B$. $B$ computes $SK_{A, id} = \text{A-IBE.Extract}(id, MSK_A)$ and sends $sk_{id} = (SK_{A, id}, SK_{T, id})$ to $A$.

**Challenge:** $A$ chooses $id_0$ and $id_1$ under the constraint that they have not been asked for the private keys and two equal-length messages $m_0, m_1$ and sends them to $B$. $B$ just chooses randomly two bits $b$ and $\gamma$ and sends $(m_b, 0, id_\gamma)$ to the challenger. The challenger chooses uniformly at random a bit $b'$ and sends $c_0, c_1 = \text{T-IBE.Enc}(m, id_\gamma, MPK_T)$ to $B$. If $b' = 0$, $m = m_0$. If $b' = 1, m = 0$. $B$ obtains $c_2, c_3$ by running $\text{A-IBE.Enc}(c_0, id_\gamma, MPK_A)$ and $\text{T-IBE.Enc}(id_\gamma, id_\epsilon, MPK_T)$ respectively. $B$ just sends $c' = (c_1, c_2, c_3)$ to $A$. 

Phase 2: $A$ makes key-extraction queries except $id_0, id_1$. $B$ answers queries just like Phase 1.

Guess $A$ sends a bit $\tilde{b}$ as a guess of $H_{\tilde{b}+1}$ to $B$. $B$ just forwards it to the challenger.

The view of $A$ is identical to $H_0$ if $\gamma' = 0$ and to $H_1$ if $\gamma' = 1$. Thus, by the semantic security of scheme $\Pi_2$, we can conclude that $H_0 \approx H_1$.

Lemma 2 Any PPT adversary cannot distinguish $H_1$ and $H_2$, if scheme $\Pi_1$ is anonymous against adaptive-identity, chosen-plaintext attacks.

Proof. Given a PPT adversary $A$ who can distinguish $H_1$ and $H_2$, we can construct a simulator $B$ attacking the anonymous security of $\Pi_1$ against adaptive-identity, chosen-plaintext attacks.

Setup: The challenger takes as input a security parameter $\lambda$ (in unary) and runs the Setup algorithm of $\Pi_1$. It provides $B$ with the system parameters $MPK_A$ while keeping the master secret key $MSK_A$ to itself. $B$ computes $(MPK_T, MSK_T) \leftarrow T-IBE.Setup(\lambda^3)$, and sends $MPK = (MPK_A, MPK_T)$ to $A$.

Phase 1: When $A$ makes key-extraction query and sends an identity $id$ to $B$, $B$ just forwards $id$ as the key-extraction query to the challenger. The challenger sends $SK_{id}$ to $B$. $B$ runs $SK_{T.id} = T-IBE.Extract(id, MSK_T)$ and sends $sk_{id} = (SK_{A.id}, SK_{T.id})$ to $A$.

Challenge: $A$ chooses two equal-length plaintexts $m_0, m_1$ and two identities $id_0, id_1$ under the constraint that they have not been asked for the private keys and sends them to $B$. $B$ chooses uniformly at random a bit $\gamma' \in \{0, 1\}$ and computes $c_0, c_1 = T-IBE.Enc(0, id_{\gamma'}, MPK_T)$, $c_3 = T-IBE.Enc(id_{\gamma'}, id_{\gamma}, MPK_T)$. $B$ sends $(c_0, 0, id_{\gamma'}, id_{\gamma'})$ to the challenger. The challenger chooses uniformly at random a bit $\gamma$ and a bit $b$. If $b = 0$, the challenger sends $c_2 = A-IBE.Enc(c_0, id_{\gamma'}, MPK_A)$ to $B$. If $b = 1$, the challenger sends $c_2 = A-IBE.Enc(0, id_{\gamma'}, MPK_A)$ to $B$. $B$ sends $(c_1, c_2, c_3)$ to $A$.

Phase 2: $B$ answers queries just like Phase 1, but $id_0$ and $id_1$ cannot be queried.

Guess: $A$ sends a bit $\tilde{b}$ as a guess of $H_{\tilde{b}+1}$ to $B$. $B$ randomly choose a bit $\gamma$ and sends $\tilde{b}$ and $\gamma$ to the challenger.

If $b = 0$, the view of $A$ is identical to $H_1$. If $b = 1$, the view of $A$ is identical to $H_2$. We can see that $H_1 \approx H_2$ by the anonymity of $\Pi_1$.

Lemma 3 Any PPT adversary cannot distinguish $H_2$ and $H_3$, if scheme $\Pi_1$ is anonymous secure against adaptively chosen-identity, chosen-plaintext attacks.
Proof. Given a PPT adversary $A$ who can distinguish $\mathcal{H}_2$ and $\mathcal{H}_3$, we can construct a simulator $B$ attacking the anonymous security of $\Pi_1$ against adaptively chosen-identity, chosen-plaintext attacks.

**Setup:** The challenger takes as input a security parameter $\lambda$ (in unary) and runs the $\text{Setup}$ algorithm of $\Pi_1$. It provides $B$ with the system parameters $MPK_A$ while keeping the master secret key $MSK_A$ to itself. $B$ computes $(MPK_T, MSK_T) \leftarrow T-\text{IBE.Setup}(1^\lambda)$, and sends $mpk = (MPK_A, MPK_T)$ to $A$.

**Phase 1:** When the adversary $A$ makes key-extraction query and sends an identity $id$ to $B$, $B$ just forwards $id$ as the key-extraction query to the challenger. The challenger sends $SK_{A, id}$ to $B$. $B$ obtains $SK_{T, id} = T-\text{IBE.Extract}(id, MSK_T)$ and sends $skid = (SK_{A, id}, SK_{T, id})$ to $A$.

**Challenge:** $A$ chooses two equal-length plaintexts $m_0, m_1$ and two identities $id_0, id_1$ under the constraint that they have not been asked for the private keys and sends them to $B$. $B$ chooses uniformly at random a bit $\gamma' \in \{0, 1\}$ and computes $c_0, c_1 = T-\text{IBE.Enc}(0, id', MPK_T)$, $c_3 = T-\text{IBE.Enc}(id, id', MPK_T)$. $B$ randomly chooses an identity $id$ from identity space except $id_0, id_1$ and sends $(0, 0, id', id)$ to the challenger. The challenger chooses uniformly at random a bit $\gamma$ and a bit $b$. If $\gamma = 0$, the challenger sends $c_2 = A-\text{IBE.Enc}(0, id, MPK_A)$ to $B$. If $\gamma = 1$, the challenger sends $c_2 = A-\text{IBE.Enc}(0, id, MPK_A)$ to $B$. $B$ sends $(c_1, c_2, c_3)$ to $A$.

**Phase 2:** $B$ answers queries just like Phase 1, but $id_0$ and $id_1$ cannot be asked.

**Guess:** $A$ sends a bit $\bar{\gamma}$ as a guess of $\mathcal{H}_{\gamma+2}$ to $B$. $B$ randomly choose a bit $\bar{b}$ and sends $\bar{\gamma}$ and $\bar{b}$ to the challenger.

If $\gamma = 0$, the view of $A$ is identical in $\mathcal{H}_2$. If $\gamma = 1$, the view of $A$ is identical in $\mathcal{H}_3$. The probability that $A$ can distinguish $\mathcal{H}_2$ and $\mathcal{H}_3$ equals $\Pr[\gamma = \gamma'] = \frac{1}{2}$, $[|2(\gamma + \text{neg}(n)) - \gamma'] = \text{neg}(n)$ because of the anonymity of $\Pi_1$. So the conclusion is that $\mathcal{H}_2 \approx \mathcal{H}_3$.

**Lemma 4** Any PPT adversary cannot distinguish $\mathcal{H}_3$ and $\mathcal{H}_4$, if scheme $\Pi_2$ is secure against chosen-identity and chosen-plaintext attacks.

Proof. Given a PPT adversary $A$ which can distinguish $\mathcal{H}_3$ and $\mathcal{H}_4$, we can construct a simulator $B$ attacking the semantic security of $\Pi_2$ against chosen-identity and chosen-plaintext attacks.

**Setup:** The challenger takes as input a security parameter $\lambda$ (in unary) and runs the $\text{Setup}$ algorithm of $\Pi_2$ and obtains $(MPK_T, MSK_T)$. It sends $MPK_T$ to $B$ and keeps $MSK_T$ to itself. $B$ computes $(MPK_A, MSK_A) \leftarrow A-\text{IBE.Setup}(1^\lambda)$ and sends $mpk = (MPK_A, MPK_T)$ to $A$. 

Anonymous Identity-Based Encryption with Identity Recovery 13
Phase 1: When the adversary $A$ makes key-extraction query and sends an identity $id$ to $B$, $B$ just forwards it as the key-extraction query to the challenger. The challenger sends $MSK_{T,id}$ to $B$. $B$ computes $SK_{A,id} = A$-IBE.Extract($id, MSK_A$) and sends $sk_{id} = (SK_{A,id}, SK_{T,id})$ to $A$.

Challenge: $A$ chooses two equal-length plaintexts $m_0, m_1$ and two identities $id_0, id_1$ under the constraint that they have not been asked for the private keys and sends them to $B$. $B$ chooses uniformly at random a bit $\gamma \in \{0, 1\}$ and computes $c_0, c_1 = T$-IBE.Enc($0, id_0, MPK_T$). $B$ randomly chooses an identity $id$ from the identity space except $id_0, id_1$ and computes $c_2 = A$-IBE.Enc($0, id, MPK_A$). $B$ sends $(id_0, 0, id_1)$ to the challenger. The challenger chooses uniformly at random a bit $b$ and sends $c_3$ to $B$. $c_3 = T$-IBE.Enc($id_3, id_3, MPK_T$), if $b = 0$. $c_3 = T$-IBE.Enc($0, id_3, MPK_T$), if $b = 1$. $B$ just sends $c^* = (c_1, c_2, c_3)$ to $A$.

Phase 2: $A$ makes key-extraction queries except $id_0, id_1$. $B$ answers queries just like Phase 1.

The view of $A$ is identical to $\mathcal{H}_3$ if $b = 0$, and $\mathcal{H}_4$ otherwise. The probability that the adversary can distinguish $\mathcal{H}_3$ and $\mathcal{H}_4$ equals the advantage of $B$ breaking the semantic security of $\Pi_2$. So we can draw the conclusion that $\mathcal{H}_3 \approx \mathcal{H}_4$.

Having proved the above lemmas, we have completed the proof of Theorem 2.

4.4 Stronger Semantic Security

Theorem 3 The AIBEIR scheme $\Pi$ is strongly semantic secure if $\Pi_2$ is semantic secure against chosen-identity and chosen-plaintext attack.

Proof. We can construct a simulator $B$ breaking semantic security of $\Pi_2$ if there exists an adversary $A$ breaking the stronger semantic security of $\Pi$.

Setup: The challenger takes as input a security parameter $\lambda$ (in unary) and runs the Setup algorithm of $\Pi_2$ and obtains $(MPK_T, MSK_T)$. It sends $MPK_T$ to $B$ and keeps $MSK_T$ to itself. $B$ computes $(MPK_A, MSK_A) \leftarrow A$-IBE.Setup$(1^\lambda)$. $B$ obtains $SK_{T,id}$ by making the secret key query of $id$ to the challenger and sends $mpk = (MPK_A, MPK_T)$ and $sk_{IRM} = (MSK_A, SK_{T,id})$ to $A$.

Phase 1: When the adversary $A$ makes key-extraction query and sends an identity $id$ to $B$, $B$ just forwards it as the key-extraction query to the challenger. The challenger sends $MSK_{T,id}$ to $B$. $B$ computes $SK_{A,id} = A$-IBE.Extract($id, MSK_A$) and sends $sk_{id} = (SK_{A,id}, SK_{T,id})$ to $A$.

Challenge: $A$ chooses two equal-length plaintexts $m_0, m_1$ and an identity $id^*$ under the constraint that it has not been asked for the private key and sends them to $B$. $B$ just forwards $(m_0, m_1, id^*)$ to the challenger. The challenger randomly chooses a bit $b$ and sends $(c_0^*, c_1^*) = T$-IBE.Enc($m_b, id^*, MPK_T$). $B$ computes $c_2^* = A$-IBE.Enc($c_0^*, id^*, MPK_A$), $c_3^* = T$-IBE.Enc($id^*, id^*, MPK_T$) and
sends $c^* = (c_1^*, c_2^*, c_3^*)$ to $A$.

**Phase 2:** $A$ makes key-extraction queries except $id^*$. $B$ answers queries just like Phase 1.

**Guess:** $B$ just forwards the output of $A$ to the challenger.

If $A$ wins, we can see $A$ as a distinguish oracle. When $B$ obtains the challenge ciphertext from challenger, $B$ just encrypts it by the $Encrypt$ algorithm of $A$-IBE and sends it to $A$. We can see that the probability that $A$ breaks the stronger semantic security equals the probability that $B$ breaks the semantic security of $Π_2$.

### 4.5 Recovery

**Theorem 4** If the testable IBE scheme $Π_2$ is secure against adaptive-identity and chosen ciphertext attack, then the AIBEIR scheme $Π$ satisfies recovery.

**Proof.** If the adversary wins in the recovery experiment, there are two cases: (1) the adversary outputs a valid AIBEIR ciphertext but the challenger output $\bot$ or a wrong identity. This will not happen, which is guaranteed by the correctness of $Recover$ algorithm. (2) the adversary outputs an invalid AIBEIR ciphertext but the challenger does not output $\bot$. We just consider the case where $(c_1, c_2, c_3)$ is a valid ciphertext. In fact, if $(c_1, c_2)$ is not a valid ciphertext, the receiver cannot decrypt correctly using its secret key. And if $c_3$ is not a valid T-IBE ciphertext under $id$, challenger will output $\bot$.

If $(c_1, c_2)$ is a valid ciphertext under $id$ and $c_3$ is a testable IBE ciphertext of a different identity $\hat{id}$ under $id$, we can show that the identity recovery manager will return $\bot$ with overwhelming probability. In fact, if there exists a PPT adversary $A$ who can fool the identity recovery manager in the recovery game, we can construct a simulator $S$ attacking $Π_2$ in adaptive-identity, chosen-plaintext attack.

**Setup:** The challenger takes as input a security parameter $λ$ (in unary) and runs the $Setup$ algorithm of $Π_2$. It provides $B$ with the system parameters $MPK_T$ while keeping the master secret key $MSK_T$ to itself. $B$ computes $(MPK_A, MSK_A) ← A$-IBE.$Setup(1^λ)$ and sends $mpk = (MPK_A, MPK_T)$ to $A$.

**Phase 1:** When the adversary $A$ makes the key-extraction queries, $B$ just forwards the identity queried by $A$ to the challenger and obtains $SK_{T, id}$ from the challenger. $B$ obtains $SK_{A, id} = A$-IBE.$Extract(id, MSK_A)$ and sends $sk_{id} = (SK_{A, id}, SK_{T, id})$ to $A$. When $A$ makes recover query, $B$ gets $SK_{T, id}$ by making secret key query of $id$ to the challenger and obtains $id$ by decrypting $c_3$ using

---

5 Although $c_1, c_2, c_3$ are all valid ciphertext, it may not be a valid AIBEIR ciphertext. Note that an AIBEIR ciphertext $(c_1, c_2, c_3)$ is valid where $c_1, c_2, c_3$ are valid ciphertexts under the same identity.
SK_{T, id}. B computes SK_{A, id} = A-IBE.Extract(id, MSK_A) and then obtains c_0 by running Dec algorithm of A-IBE. B computes h = T-IBE.Test(c_0, id), and sends id to A if h = 1, and ⊥ otherwise. We say A wins if it outputs a valid “double-encrypt” IBE ciphertext (c_1, c_2) under id_1 and a valid testable IBE ciphertext c_3 of id_2 which pass the recover algorithm (A can output the randomness used in the encrypt algorithm to show it ). Here we constrain that id_1 has not been queried the private key before. B obtains SK_{T, id_2} by making the secret key query of id_2.

Challenge: B randomly chooses two equal-length message m_0, m_1 and sends m_0, m_1 and id_1 to challenger. Challenger randomly chooses a bit b \in \{0, 1\} and obtains (c_0, c_1) = T-IBE.Enc(m_b, id_1, MPK_T).

Phase 2: B makes some queries to key-extraction oracle. In fact, B does not need to query now.

Guess: B computes c_2 = A-IBE.Enc(c_0, id_1, MPK_A) and obtains c'_0 which is a part of ciphertext under id_2 by decrypting c_2 using SK_{A, id_2}. Then B obtains m by decrypting c'_0, c_1 using SK_{T, id_2}. B outputs 0 if m = m_0 and 1 otherwise.

5 Conclusion

We define a new primitive called AIBEIR and construct it using double encryption with an anonymous IBE and a testable IBE. AIBEIR is anonymous for all users except the identity recovery manager who can recover the identity from the ciphertext. But the identity recovery manager can not obtain information about plaintext from ciphertext even holding an identity recover secret key. To our knowledge, [BB04a, Wat05] and their variations satisfy our testable IBE definition. We leave as an open problem the question of constructing testable IBE from other standard assumptions, such as lattice. Another interesting area of research is to construct more practical AIBEIR schemes.

Acknowledgements.

We would like to thank the anonymous reviewers of ACISP 2018 for their advice. Xuecheng Ma and Dongdai Lin are supported by the National Natural Science Foundation of China under Grant No. 61379139.

References

ABB10. Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In Advances in Cryptology - EUROCRYPT 2010. 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings, pages 553–572, 2010.

\[\] This means we can obtain a T-IBE ciphertext under id_2 by decrypting the “double-encrypt” ciphertext under id_1 using SK_{A, id_2}
Anonymous Identity-Based Encryption with Identity Recovery

AG09. Giuseppe Ateniese and Paolo Gasti. Universally anonymous IBE based on the quadratic residuosity assumption. In Topics in Cryptology - CT-RSA 2009, The Cryptographers' Track at the RSA Conference 2009, San Francisco, CA, USA, April 20-24, 2009. Proceedings, pages 32–47, 2009.

BB04a. Dan Boneh and Xavier Boyen. Efficient selective-id secure identity-based encryption without random oracles. In Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings, pages 223–238, 2004.

BB04b. Dan Boneh and Xavier Boyen. Secure identity based encryption without random oracles. In Advances in Cryptology - CRYPTO 2004, 24th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings, pages 443–459, 2004.

BBDP01. Mihir Bellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval. Key-privacy in public-key encryption. In Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings, pages 566–582, 2001.

BF01. Dan Boneh and Matthew K Franklin. Identity-based encryption from the weil pairing. international cryptology conference, 2001:213–229, 2001.

BGH07. Dan Boneh, Craig Gentry, and Michael Hamburg. Space-efficient identity based encryption without pairings. IACR Cryptology ePrint Archive, 2007:177, 2007.

BLS17. Zvika Brakerski, Alex Lombardi, Gil Segev, and Vinod Vaikuntanathan. Anonymous ibe, leakage resilience and circular security from new assumptions. IACR Cryptology ePrint Archive, 2017:967, 2017.

Boy03. Xavier Boyen. Multipurpose identity-based signcryption (A swiss army knife for identity-based cryptography). In Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings, pages 383–399, 2003.

Boy10. Xavier Boyen. Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more. In Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010. Proceedings, pages 499–517, 2010.

BW06. Xavier Boyen and Brent Waters. Anonymous hierarchical identity-based encryption (without random oracles). In Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings, pages 290–307, 2006.

CHKP10. David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. In Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings, pages 523–552, 2010.

Coc01. Clifford Cocks. An identity based encryption scheme based on quadratic residues. In Bahram Honary, editor, Cryptography and Coding, pages 360–363, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

DG17. Nico Döttling and Sanjam Garg. Identity-based encryption from the diffie-hellman assumption. In Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017. Proceedings, Part I, pages 537-569, 2017.
DH76. Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

Gen06. Craig Gentry. Practical identity-based encryption without random oracles. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006*, pages 445–464, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

GPV08. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, Victoria, British Columbia, Canada, May 17-20, 2008, pages 197–206, 2008.

GSRD17. Kanika Gupta, S. Sharmila Deva Selvi, C. Pandu Rangan, and Shubham Sopan Dighe. Identity-based group encryption revisited. 2017.

LRL+16. Xiling Luo, Yili Ren, Jingwen Liu, Jiankun Hu, Weiran Liu, Zhen Wang, Wei Xu, and Qianhong Wu. Identity-based group encryption. In *Information Security and Privacy - 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part II*, pages 87–102, 2016.

Sha84. Adi Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, pages 47–53, 1984.

SOK00. R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystem based on pairings. 01 2000.

Wat05. Brent Waters. Efficient identity-based encryption without random oracles. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, pages 114–127, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

Wat09. Brent Waters. Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions. In Shai Halevi, editor, *Advances in Cryptology – CRYPTO 2009*, pages 619–636, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.