Practical Identity-Based Encryption (IBE) in Multiple PKG Environments and Its Applications

Shengbao Wang, Zhenfu Cao

Department of Computer Science and Engineering,
Shanghai Jiao Tong University
800 Dongchuan Road, Shanghai 200240, China
{shengbao-wang,cao-zf}@cs.sjtu.edu.cn

Abstract. In this paper, we present a new identity-based encryption (IBE) scheme using bilinear pairings. Our IBE scheme enjoys the same Key-Extraction and Decryption algorithms with the famous IBE scheme of Boneh and Franklin (BF-IBE for short), while differs from the latter in that it has modified Setup and Encryption algorithms.
Compared with BF-IBE, we show that ours are more practical in a multiple private key generator (PKG) environment, mainly due to that the session secret g_{ID} could be pre-computed *before* any interaction, and the sender could encrypt a message using g_{ID} prior to negotiating with the intended recipient(s). As an application of our IBE scheme, we also derive an escrowed ElGamal scheme which possesses certain good properties in practice. We prove that our scheme meets chosen ciphertext security in the random oracle model, assuming the intractability of a modified version of the Bilinear Diffie-Hellman (BDH) problem.

Keywords: identity-based encryption (IBE), public key encryption (PKE), escrowed ElGamal, bilinear pairings, provable security

1 Introduction

The concept of *identity(ID)-based cryptography* was first introduced by Shamir in 1984 [15]. The basic idea behind an ID-based cryptosystem is that end users can choose an arbitrary string, for example their email addresses or other online identifiers, as their public key. The corresponding private keys are created by binding the identity with a master secret of a trusted authority (called private key generation, or PKG for short). This eliminates much of the overhead associated with key management.

In 2001, Boneh and Franklin [4] gave the first fully functional solution for ID-based encryption (IBE) using the bilinear pairing over elliptic curves. Based on pairings, Sakai and Kasahara presented another IBE (SK-IBE for short) scheme by using another Key Extraction algorithm in 2003 [16]. However, the Boneh-Franklin scheme (BF-IBE for short) has received much more attention in recent years.

In this paper, we give a new IBE scheme based on bilinear pairings. Our scheme has the same Key-Extraction and Decryption algorithms with BF-IBE, while differs from the latter in that it has different Setup and Encryption algorithms. We show that ours are more practical in a multiple private key generator (PKG) environment. Parallel to [4], we also derive an escrowed ElGamal [9] encryption scheme from our IBE scheme.

Furthermore, we show how the derived ElGamal encryption enables a dual decrptor public key encryption (PKE) scheme.

We note that SK-IBE due to Sakai and Kasahara [16] has a better performance than BF-IBE and ours. Especially, SK-IBE are also very practical in multiple PKG environments. However, its applicability to some circumstance (e.g., hierarchical IBE and threshold decryption) are not comparable to BF-IBE. In particular, unlike the BF-IBE and our new IBE, it seems very hard to derive from it an escrowed ElGamal encryption scheme. In this regard, we do not compare the new IBE with SK-IBE for now.

Paper Organization. The rest of this paper is structured as follows. In the next section, we give the necessary definition for bilinear pairings and the related complexity assumption. Section 3 describes our IBE scheme. Security results are given in Section 4, we present a new escrowed ElGamal encryption scheme in Section 5 and finally Section 6 contains a brief conclusion.

2 Preliminaries

2.1 Pairings and mBDH Assumption

In this section, we describe in a more general format the basic definition and properties of the pairing: more details can be found in [4].

Let $\mathbb{G}_1$ be a cyclic additive group generated by an element P, whose order is a prime p, and $\mathbb{G}_2$ be a cyclic multiplicative group of the same prime order p. We assume that the discrete logarithm problem (DLP) in both $\mathbb{G}_1$ and $\mathbb{G}_2$ are hard.

Definition 1 (Pairing). *An admissible pairing e is a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, which satisfies the following three properties:*

1. Bilinear*: If $P, Q \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_p^*$, then $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$;*
2. Non-degenerate*: $\hat{e}(P, P) \neq 1$;*
3. Computable*: If $P, Q \in \mathbb{G}_1$, one can compute $\hat{e}(P, Q) \in \mathbb{G}_2$ in polynomial time.*

Typically, the map e will be derived from either the Weil or Tate pairing on an elliptic curve over a finite field. We refer to [2, 4, 5, 13] for a more comprehensive description of how these groups, pairings and other parameters should be selected in practice for efficiency and security.

Definition 2 (Bilinear Diffie-Hellman (BDH) Parameter Generator). *As in [4], we say that a randomized algorithm $\mathcal{IG}$ is a* BDH *parameter generator if $\mathcal{IG}$ takes a security parameter $k > 0$, runs in time polynomial in k, and outputs the description of two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of the same prime order q and the description of an admissible pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$.*

Definition 3 (Bilinear Diffie-Hellman (BDH) Problem). *Let $\mathbb{G}_1$, $\mathbb{G}_2$, P and e be as above. The* BDH *problem in $\langle \mathbb{G}_1, \mathbb{G}_2, e \rangle$ is as follows: Given $\langle P, aP, bP, cP \rangle$ with uniformly random choices of a, b, $c \in \mathbb{Z}_q^*$, compute $\hat{e}(P, P)^{abc} \in \mathbb{G}_2$.*

The security of our new pairing-based IBE scheme is based on the difficulty of the following *modified* BDH problem. Note that this is nearly the standard BDH problem with the only difference that $a^{-1}P$ (which is hard to compute from aP) is also given as input.

Definition 4 (Modified Bilinear Diffie-Hellman (mBDH Problem) [8]). *Let $\mathbb{G}_1$, $\mathbb{G}_2$, P and e be as above. The* mBDH *problem in $\langle \mathbb{G}_1, \mathbb{G}_2, e\rangle$ is as follows: Given $\langle P, aP, a^{-1}P, bP, cP\rangle$ with uniformly random choices of a, b, $c \in \mathbb{Z}_q^*$, compute $\hat{e}(P,P)^{abc} \in \mathbb{G}_2$.*

A real-valued function $f(l)$ is *negligible* if for any integer k, $|f(l)| < l^{-k}$ for sufficiently large l. The following mBDH assumption states that, roughly, this problem is computational infeasible.

Definition 5 (Modified Bilinear Diffie-Hellman (mBDH) Assumption). *As in [4], if $\mathcal{IG}$ is a* BDH *parameter generator, the advantage $Adv_{\mathcal{IG}}(\mathcal{B})$ that an algorithm $\mathcal{B}$ has in solving the* mBDH *problem is defined to be the probability that the algorithm $\mathcal{B}$ outputs $\hat{e}(P,P)^{abc} \in \mathbb{G}_2$ when the inputs to the algorithm are $\mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, aP, a^{-1}P, bP, cP$ where $\langle \mathbb{G}_1, \mathbb{G}_2, e\rangle$ is $\mathcal{IG}'s$ output for large enough security parameter k, P is a random generator of $\mathbb{G}_1$, and $a, b, c \in \mathbb{Z}_q^*$. The* mBDH *assumption is that $Adv_{\mathcal{IG}}(\mathcal{B})$ is negligible for all efficient algorithms $\mathcal{B}$.*

Here the probability is measured over the random choices of $a, b, c \in \mathbb{Z}_q^*$ and the random bits of $\mathcal{B}$.

In Appendix A, we relate the hardness of the mBDH assumption to well-known pairing-based "standard assumptions". In particular we show that the mBDH assumption is at least as weak as 2-BDHI. The BDHI (Bilinear Diffie-Hellman Inversion) assumption was introduced by Boneh and Boyen [3] and its stronger variants (q-BDHI for some polynomial q) already found numerous applications.

2.2 Definitions for Identity-Based Encryption

We start by fixing some notation and recalling basic concepts.

Definition 6 (Identity-Based Encryption (IBE)). *An identity-based encryption scheme handling identities of length (where is a polynomially-bounded function) is specified by four probabilistic polynomial time (PPT) algorithms:*

- **Setup:** *is a probabilistic algorithm run by a private key generator (PKG) that takes as input a security parameter to output a public/private key pair (P_{Pub}, msk) for the PKG (P_{Pub} is its public key and msk is its master key that is kept secret).*
- **Key-Extraction:** *is a key generation algorithm run by the PKG on input of a master key msk and a user's identity ID to return the user's private key d_{ID}.*
- **Encrypt:** *is a probabilistic algorithm which takes as input a plaintext M, a recipient's identity ID and the PKG's public key P_{Pub} to output a ciphertext C.*
- **Decrypt:** *is a deterministic decryption algorithm which takes as input a ciphertext C and the private decryption key d_{ID} to return a plaintext M or a distinguished symbol $\perp$ if C is not a valid ciphertext.*

The security of an IBE scheme is defined by the following game between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ as first formalized in [4].

- **Setup**. $\mathcal{C}$ takes a security parameter k and runs the Setup algorithm. It gives $\mathcal{A}$ the domain-wide parameters and keeps msk to itself.
- **Find Stage**. $\mathcal{A}$ issues queries as one of follows:
  - Extraction query on ID_i. $\mathcal{C}$ runs the Extract algorithm to generate d_{ID_i} and passes it to $\mathcal{A}$.
  - Decryption query on (ID_i, C_i). $\mathcal{C}$ decrypts the ciphertext by finding d_{ID_i} first (through running Extract if necessary), and then running the Decrypt algorithm. It responds with the resulting plaintext M_i.
- **Challenge**. Once $\mathcal{A}$ decides that Phase 1 is over, it outputs two equal length plaintexts M_0, M_1, and an identity ID^* (called the challenge identity) on which it wishes to be challenged. The only constraint is that $\mathcal{A}$ must not have queried the extraction oracle on ID^* in Phase 1. $\mathcal{C}$ picks a random bit $b \in \{0, 1\}$ and sets $C^* = Encrypt(ID^*, M_b)$. It sends C^* as the challenge to $\mathcal{A}$.
- **Guess Stage**. $\mathcal{A}$ issues more queries as in Phase 1 but with two restrictions: (1) Extraction queries cannot be issued on ID^*; (2) Decryption queries cannot be issued on (ID^*, C^*).
- **Output**. Finally, $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$ and wins the game if $b' = b$.

We refer to this type of adversary as an IND-ID-CCA adversary [4, 5]. If $\mathcal{A}$ cannot ask decryption queries, we call it an IND-ID-CPA adversary. The advantage of an adversary $\mathcal{A}$ against an IBE scheme is the function of security parameter k defined as:

$$Adv_{\mathcal{A}}(k) = |\Pr[b' = b] - 1/2|.$$

Definition 7 (IBE Security). *An identity-based encryption (IBE) scheme is IND-ID-CCA secure (resp. IND-ID-CPA) if for any IND-ID-CCA (resp. IND-ID-CPA) adversary, $Adv_{\mathcal{A}}(k)$ is negligible.*

3 Proposed IBE Scheme

For the problem of inherent key escrow, the difficulty of establishing secure channels for private key distribution, and to avoid the single point of failure of using only one PKG, it is well-known that (single-PKG) IBE is only well suitable for use in relatively small and close organizations, i.e. with each organization has its own private key generator, generating private keys for the principal within its domain.

For an IBE to be used in a multiple PKG environment (namely, cross domains), all that is needed is the availability of *standard* pairing-friendly curves and a common group generator point P. We note that this is a reasonable requirement. In fact, elliptic curves, suitable group generator points and other cryptographic tools have been standardized for non-IBE applications, for example in the NIST FIPS standards [14]. Once these group generator points and curves have been agreed upon, each PKG can generate its own random master secret.

Now we describe our new IBE scheme — a "multiple PKG variant" of BF-IBE (hereafter referred to as M-IBE). Following the exploration as in [5], we first give a basic version of our scheme which is only chosen plaintext attack (CPA) secure. We then extend the basic scheme to get security against adaptive chosen ciphertext attack (CCA) in the random oracle model [6], using the second Fujisaki-Okamoto transformation [10].

3.1 Basic M-IBE Scheme with CPA Security

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be groups of prime order p, and let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be the bilinear pairing. P is a generator points of $\mathbb{G}_1$. The basic M-IBE system works as follows.

Setup. Given a security parameter k, the PKG does the following:

1. Chooses a random $s \in \mathbb{Z}_p$, calculates $P_{Pub} = s^{-1}P \in \mathbb{G}_1$ [1].
2. Picks a cryptographic hash functions $H_1 : \{0,1\}^* \to \mathbb{G}_1^*$, a cryptographic hash function $H_2 : \mathbb{G}_2 \to \{0,1\}^n$ for some n.

The message space is $\mathcal{M} = \{0,1\}^n$. The ciphertext space is $C = \mathbb{G}_1^* \times \{0,1\}^n$. The public *params* are $\langle q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{Pub}, n, H_1, H_2 \rangle$ and the *master key* is s.

Key-Extraction. This algorithm is identical to that of BF-IBE. To generate a private key for identity $ID \in \{0,1\}^*$, the PKG first computes $Q_{ID} = H_1(ID) \in \mathbb{G}_1^*$, and then sets the private key d_{ID} to be $d_{ID} = sQ_{ID}$ where s is the master key.

Encryption. To encrypt message $m \in \mathcal{M}$, the sender picks randomly a $r \in \mathbb{Z}_p$, using the receiver's identity ID to compute $Q_{ID} = H_1(ID) \in \mathbb{G}_1^*$, sets the ciphertext to be

$$C = \langle rP_{Pub},\ m \oplus H_2(g_{ID}^r) \rangle, \text{ where } g_{ID} = \hat{e}(P, Q_{ID}) \in \mathbb{G}_2^*.$$

Decryption. This algorithm is identical to that of BF-IBE. To decrypt a ciphertext $C = \langle U,\ V \rangle \in \mathcal{C}$, using the private key d_{ID} of the identity ID computes

$$m = V \oplus H_2(\hat{e}(U,\ d_{ID})).$$

Consistence: The recipient can correctly decrypt C to get m since

$$\begin{aligned} & \hat{e}(U,\ d_{ID}) \\ = & \hat{e}(rs^{-1}P,\ sQ_{ID}) \\ = & \hat{e}(P, Q_{ID})^r. \end{aligned}$$

3.2 Full M-IBE Scheme with CCA Security

In this subsection we extend the above basic M-IBE scheme to a full scheme with adaptive chosen ciphertext security using the general transformation due to Fujisaki and Okamoto (FO transformation) [10].

We borrow the description of the FO transformation from [11]. This conversion starts from an IND-CPA encryption scheme and builds an IND-CCA scheme in the random oracle model. If we denote by $E_{pk}(M, r)$ the encryption of M using the random bits r under the public key pk, with set of messages $M = \{0,1\}^n$, set of coins R and set of ciphertexts C, the new transformation is the scheme

$$E_{pk}^{hy}(M) = E_{pk}(M||r, H(M||r)),$$

[1] Note that in BF-IBE [4, 5], the public key of PKG is $P_{Pub} = sP \in \mathbb{G}_1$ instead.

where $M||r \in \{0,1\}^{n-k_0} \times \{0,1\}^{k_0}$ and $H : \{0,1\}^* \to R$ is a hash function. To decrypt a ciphertext C, one first obtains $M'||r'$ using the original decryption algorithm, and next checks if $E_{pk}(M'||r', H(M'||r')) = C$. If this is so, outputs M; otherwise outputs reject symbol.

Now we describe the full M-IBE system thereby obtained.

Setup. Given a security parameter k, the PKG does the following:

1. Chooses a random $s \in \mathbb{Z}_p$, calculates $P_{Pub} = s^{-1}P \in \mathbb{G}_1$.
2. Picks three cryptographic hash functions $H_1 : \{0,1\}^* \to \mathbb{G}_1^*$, $H_2 : \mathbb{G}_2 \to \{0,1\}^n$ for some n and $H_3 : \{0,1\}^* \to \mathbb{Z}_p^*$.

The message space is $\mathcal{M} = \{0,1\}^{n-k_0}$. The ciphertext space is $C = \mathbb{G}_1^* \times \{0,1\}^n$. The public *params* are $\langle q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{Pub}, n, H_1, H_2, H_3 \rangle$ and the *master key* is s.

Key-Extraction. This algorithm is identical to that of the basic M-IBE scheme.

Encryption. To encrypt message $m \in \mathcal{M}$, the sender picks randomly a $\sigma \in \{0,1\}^{k_0}$, using the receiver's identity ID to compute $Q_{ID} = H_1(ID) \in \mathbb{G}_1^*$, sets $r = H_3(m, \sigma) \in \mathbb{Z}_p^*$ and finally sets the ciphertext to be

$$C = \langle rP_{Pub},\ (m||\sigma) \oplus H_2(g_{ID}^r) \rangle,\ \text{where } g_{ID} = \hat{e}(P, Q_{ID}) \in \mathbb{G}_2^*.$$

Decryption. This algorithm is identical to that of Galindo's BF-IBE variant [11]. To decrypt a ciphertext $C = \langle U,\ V \rangle \in \mathcal{C}$, using the private key d_{ID} of the identity ID do

1. Compute $m = V \oplus H_2(\hat{e}(U,\ d_{ID})) = m||\sigma$.
2. Parse $m||\sigma$ and compute $r = H_3(m, \sigma)$. Check that $U = r\underline{P_{Pub}}$. If not, reject the ciphertext.
3. Output m.

Consistence: The consistence of this scheme directly follows that of the basic scheme.

3.3 Its Fitness for Multiple PKG Environments

As mentioned above, an IBE scheme is often used across multiple PKGs, namely for each organization (e.g., a company), it has its own PKG. In many cases, a principal may need to encrypt messages to principals from different domains. For example, for a salesman of company A, he may need to encrypt messages to Bob from company B, Carol from company C, or Emmy who he does not know which company she is belonging to by now.

Now we compare our M-IBE with BF-IBE [4] in such an environment. The Setup algorithm in M-IBE requires one more fast inverse operation in $\mathbb{Z}_p$ than BF-IBE, and the Key-Extraction and Decryption algorithms in the two IBE schemes are the same. In the following, we discuss what significance our different Encryption algorithm could bring in practice.

In BF-IBE [4], the session secret, i.e. the term g_{ID} is computed as $g_{ID} = \hat{e}(P_{Pub}, Q_{ID})$, in which P_{Pub} is the public key of the intended receiver's PKG. We emphasize that in a multiple PKG environment, before computing the second part of the ciphertext, i.e. V, and especially, the term g_{ID} (requires a relatively expensive pairing evaluation) which are the main operations of the overall encryption, BF-IBE requires the sender to first get to know the following two things:

- which organization the receiver is from, *and*
- the public key associated with the corresponding PKG.

Compared with BF-IBE, the biggest difference of M-IBE is that in the Encryption algorithm, the terms V and especially, $g_{ID} = \hat{e}(P, Q_{ID})$ are computed independently from *any* PKG's public key. Consequently, in M-IBE, the sender can compute the pairing (and V) *before* getting the public key of the receiver's PKG, in the case that (s)he knows which organization the receiver is from. Interestingly, the sender can even pre-compute g_{ID} and V *before* (s)he knows which organization the receiver is from!

Therefore, our scheme enables a type of efficient "on the move" IBE in a multiple PKG environment, which requires very small on-online work for the sender (i.e. encryptor).

We emphasize that this feature is particularly useful in (ID-based) broadcasting (or *multiple-recipient*) encryption scenario, namely with most of the expensive computation pre-computed, the overall performance will be upgraded to a large extent.

4 Security Results

Now we evaluate the security of our full M-IBE scheme. We prove that the security of it can reduce to the hardness of the mBDH problem. The reduction is similar to the proof of BF-IBE [5]. However, we will take into account the reduction error found by Galindo [11].

We prove the security of M-IBE scheme along the similar lines to that in [5, 11]. The proof is completed in three steps that can be sketched as follow. 1) First we prove that if there exists an IND-ID-CCA adversary, who is able to break the full M-IBE scheme by launching the adaptive chosen ciphertext attacks as defined in the security model, then there exists an IND-CCA adversary to break the $\mathbf{BasicPub}^{hy}$ scheme defined in **Lemma 1** with the adaptive chosen ciphertext attacks. 2) Second, if such IND-CCA adversary exists, then we show (in **Lemma 2**) that there must be an IND-CPA adversary that breaks the corresponding **BasicPub** scheme (defined below). 3) Finally, in **Lemma 3** we prove that if the **BasicPub** scheme is not secure against an IND-CPA adversary, then the mBDH assumption is flawed.

We first define the related non-ID-based public key encryption scheme **BasicPub**. It is described by three algorithms: keygen, encrypt, decrypt.

keygen: Given a security parameter k, the PKG does the following:

1. Chooses a random $s \in \mathbb{Z}_p$, calculates $P_{Pub} = s^{-1}P \in \mathbb{G}_1$ and $P'_{Pub} = sP \in \mathbb{G}_1$.
2. Picks a random $Q_{ID} \in \mathbb{G}_2^*$.
3. Picks a cryptographic hash functions $H_2 : \mathbb{G}_2 \to \{0,1\}^n$ for some n.

The message space is $\mathcal{M} = \{0,1\}^n$. The ciphertext space is $C = \mathbb{G}_1^* \times \{0,1\}^n$. The public key is $\langle q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{Pub}, P'_{Pub}, n, Q_{ID}, H_2 \rangle$ and the *private key* is $d_{ID} = sQ_{ID} \in \mathbb{G}_1^*$.

encrypt: To encrypt message $m \in \mathcal{M}$, the sender picks randomly a $r \in \mathbb{Z}_p$ and sets the ciphertext to be

$$C = \langle rP_{Pub},\ m \oplus H_2(g_{ID}^r) \rangle,\ \text{where } g_{ID} = \hat{e}(P, Q_{ID}) \in \mathbb{G}_2^*.$$

decrypt: To decrypt a ciphertext $C = \langle U,\ V \rangle \in \mathcal{C}$, using the private key d_{ID} computes

$$m = V \oplus H_2(\hat{e}(U,\ d_{ID})).$$

The correctness of the above public key encryption scheme can be easily verified. We refer to the full scheme of applying the Fujisaki-Okamoto transformation to **BasicPub** as $\mathbf{BasicPub}^{hy}$.

The following lemma shows that an IND-ID-CCA attack on the full M-IBE scheme can be converted to a IND-CCA attack on $\mathbf{BasicPub}^{hy}$. This means that private key extraction queries do not help the adversary.

Lemma 1. *Let $\mathcal{A}$ be an IND-ID-CCA adversary with advantage ϵ against the full* M-IBE *scheme making at most q_E private key extraction queries, q_D decryption queries and q_1 hash queries. Then there is an IND-CCA adversary $\mathcal{B}$ that has advantage at least $\frac{\epsilon}{q_1}(1 - \frac{q_1}{q_E}) \approx \frac{\epsilon}{q_1}$ against $\mathbf{BasicPub}^{hy}$. Its running time is $t_{\mathcal{B}} \leq t_{\mathcal{A}} + c_{\mathbb{G}_1}(q_D + q_E + q_1)$, where $c_{\mathbb{G}_1}$ denotes the time of computing a random multiple in $\mathbb{G}_1$.*

Proof. Use the same reduction as for Result 5 from [11], and the detailed proof will be given in the full version of the paper. □

Lemma 2. *Let $\mathcal{A}$ be an IND-CCA adversary with advantage ϵ against $\mathbf{BasicPub}^{hy}$ making at most q_D decryption queries and q_2 hash queries. Then there is an IND-CPA adversary $\mathcal{B}$ that has advantage at least $(\epsilon - q_2 2^{-(k_0-1)})(1-1/p)^{q_D} \approx \epsilon$ against $\mathbf{BasicPub}^{hy}$. Its running time is $t_{\mathcal{B}} \leq t_{\mathcal{A}} + q_2(T_{\mathbf{BasicPub}} + \log p)$, where $T_{BasicPub}$ is the running time of Encrypt algorithm in $\mathbf{BasicPub}$.*

Proof. This result is obtained applying the Fujisaki-Okamoto transformation, and the proof can be found in [10]. □

We then show that **BasicPub** is IND-CPA secure if the mBDH assumption holds.

Lemma 3. *Let $\mathcal{A}$ be an IND-CPA adversary with advantage ϵ against $\mathbf{BasicPub}$ making at most q_2 queries to H_2. Then there is an algorithm $\mathcal{B}$ that has advantage at least $2\epsilon/q_2$ in solving the mBDH problem. Its running time is $t_{\mathcal{B}} = O(t_{\mathcal{A}})$.*

Proof. See Appendix B. □

As in [11], in order to come up with the total concrete security, we bound any q_i with a single q_H, and assume that $q_E = q_D$, since extraction and decryption operations have roughly the same computational complexity. Composing the above reductions, we are now ready to state the security of our full M-IBE scheme.

Theorem 1. *The proposed full* M-IBE *scheme is (t, q_H, q_D, ϵ)-secure if the mBDH problem on $(\mathbb{G}_1, \mathbb{G}_2, \hat{e})$ is*

$$(t + c_{\mathbb{G}_1}(2q_D + q_H) + q_H O(\log^3 p + \log p), \epsilon/q_H^2)) - \textit{secure}.$$

Proof. This follows directly from **Lemma 1, 2** and **3**. □

5 Applications of M-IBE Scheme

5.1 Escrowed ElGamal Encryption

Parallel to [4], in this section we introduce a new ElGamal encryption system in which a single escrow key enables the decryption of ciphertexts encrypted under any public key.

Our escrowed ElGamal encryption scheme works as follows:

Setup. Given a security parameter k, the *escrow authority* (EA) does the following:

1. Chooses a random $s \in \mathbb{Z}_p$, calculates two points $Q_1 = sP$ and $Q_2 = s^{-1}P \in \mathbb{G}_1$ [2].
2. Chooses a cryptographic hash functions $H : \mathbb{G}_2 \to \{0,1\}^n$ for some n.

The message space is $\mathcal{M} = \{0,1\}^n$. The ciphertext space is $C = \mathbb{G}_1^* \times \{0,1\}^n$. The public *params* are $\langle q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, n, P, Q_1, Q_2, H\rangle$ and the *escrow key* is s.

Key Generation. Same as in [4], a user generates a public/private key pair for herself by picking a random $x \in \mathbb{Z}_q$ and computing $P_{Pub} = xP \in \mathbb{G}_1$. Her private key is x, her public key is P_{Pub}.

Encryption. To encrypt message $m \in \mathcal{M}$, the sender picks randomly a $r \in \mathbb{Z}_p$, sets the ciphertext to be

$$C = \langle rQ_2,\ m \oplus H_2(g^r)\rangle,\ \text{where } g = \hat{e}(P, P_{Pub}) \in \mathbb{G}_2^*.$$

Decryption. To decrypt a ciphertext $C = \langle U,\ V\rangle \in \mathcal{C}$, using the private key x of the identity ID computes

$$m = V \oplus H_2(\hat{e}(U,\ xQ_1)).$$

Escrow Decryption. To decrypt a ciphertext $C = \langle U,\ V\rangle$, using the escrow key s of the EA computes

$$m = V \oplus H_2(\hat{e}(U,\ P_{Pub})^s).$$

Consistence: The two recipients can correctly decrypt C to get m since

$$\begin{aligned}
&\hat{e}(U,\ xQ_1)\\
&= \hat{e}(rQ_2,\ xQ_1)\\
&= \hat{e}(rs^{-1}P,\ xsP)\\
&= \hat{e}(rP,\ xP)\\
&= \hat{e}(P,\ P_{Pub})^r\\
&= g^r
\end{aligned}$$

and

$$\begin{aligned}
&\hat{e}(U,\ P_{Pub})^s\\
&= \hat{e}(rs^{-1}P,\ P_{Pub})^s\\
&= \hat{e}(rP,\ P_{Pub})\\
&= \hat{e}(P,\ P_{Pub})^r\\
&= g^r.
\end{aligned}$$

[2] Note that in [5], the public key of the EA is one point $Q = sP \in \mathbb{G}_1$ instead.

Compared with the scheme in [4], our escrowed ElGamal requires the EA to publish one more point as its public key. An advantage of our scheme is that the sender can choose a designated EA (from multiple EAs) after (s)he finished most of the operations of encrypting a message. This provides the sender with more flexibility in practice.

A Variant. If we look the escrow authority (EA) in the above escrowed ElGamal scheme as an ordinary principal (who has his/her own private and public key pair), it can be then used as a *dual decryptor PKE scheme*, i.e., a single ciphertext can be decrypted *independently* by two different principals. However, unlike in conventional setting, we require at least one of the recipient to publish two points (e.g. $Y_1,\ Y_2$) as his/her public key, in the form of $Y_1 = \alpha P$ and $Y_2 = \alpha^{-1} P$ (assuming α is the private key of the recipient).

A good property of this scheme is that the sender can encrypt the message before (s)he picks up the second recipient. In other words, after the encryption has been done, the sender can change his/her mind on who the second recipient will be.

More interestingly, the sender can efficiently add more such "second recipient", each time (s)he adds one, only one scalar multiplication is needed, without any expensive pairing computation. However, we note that the size of the ciphertext will grow linearly.

5.2 Efficient Across-Domain Multi-Receiver IBE

We now look at the multi-receiver setting, i.e., a sender wants to send a message to n receivers. In 2004, Baek *et al.* [7] proposed a construction based on BF-IBE. We note that their scheme only works well in a single PKG environment, namely with all the n receivers getting their private keys from the same one PKG. However, in the cross-domain context, the sender has to compute l pairings (assuming the n receivers are from l domains) instead of 1 pairing.

In [17], based on the new IBE scheme, we present an efficient MR-IBE scheme which works efficiently across domains. Notably, the new MR-IBE scheme requires only 1 pairing computation for the sender when no matter how many domains the n receivers are from.

6 Conclusions

In this paper, we gave a new IBE scheme (which we call M-IBE) that is provably secure in the random oracle model. The security is based on a slightly stronger variant of the Bilinear Diffie-Hellman assumption. We showed that the new scheme is more practical than the famous IBE scheme due to Boneh and Franklin in multiple PKG environment. As applications, we aslo proposed a related escrowed ElGamal encryption scheme which has its distinct advantages over that in [4, 5]. Compared with the Boneh-Franklin scheme, M-IBE scheme is even more practical in the multiple-receiver setting [17].

Future work includes exploring the merits of our new IBE scheme in constructing Certificate-Based Encryption (CBE) [12] and Certificateless Public Key Encryption (CL-PKE) schemes [1].

Acknowledgment

The authors would like to thank Xiaohui Liang, Hongbing Wang, Liuquan Qin and Peng Zeng for many constructive discussions. This work was supported in part by the National High Technology Development Program of China under Grant No. 2006AA01Z424 and the National Natural Science Foundation of China under Grant Nos. 60673079 and 60572155.

References

1. S.S. Al-Riyami and K.G. Paterson. Certificateless public key cryptography. In *Proc. of ASIACRYPT 2003*, LNCS vol. 2894, pp. 452-473, 2003. [10]
2. P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairing-based cryptosystems. In *Proc. CRYPTO 2002*, LNCS vol. 2442, pp. 354-368. Springer, 2002. [2]
3. D. Boneh and X. Boyen. Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In *Proc. of EUROCRYPT 2004*, LNCS vol. 3027, pp. 223-238. Springer-Verlag, 2004. [3, 12]
4. D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In *Proc. of CRYPTO 2001*, LNCS vol. 2139, pp. 213-229. Springer-Verlag, 2001. [1, 2, 3, 4, 5, 6, 7, 9, 10]
5. D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. SIAM J. Computing, 32(3):586-615, 2003. [2, 4, 5, 7, 9, 10, 12]
6. M. Bellare and P. Rogaway, Random oracles are practical: a paradigm for designing effiient protocols, In *Proc. of First ACM Conference on Computer and Communications Security*, pp.62-73, ACM press, 1993. [4]
7. J. Baek, R. Safavi-Naini, and W. Susilo. Efficient multi-receiver identity-based encryption and its application to broadcast encryption. In *Proc. of PKC'05*, LNCS vol. 3386, pp. 380-397. Springer-Verlag, 2005. [10]
8. S. S. M. Chow, S. M. Yiu, L. C. K. Hui, and K. P. Chow. Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity. In *Proc. of ICISC'03*, LNCS vol. 2971, pp. 352-369. Springer-Verlag, 2003. [3]
9. T. ElGamal. A public key cryptosystem and signature scheme based on discrete logarithms. *IEEE Trans. Info. Theory*, 31(4), pp. 469-472, 1985. [1]
10. E. Fujisaki and T. Okamoto. How to enhance the security of public-key encryption at minimum cost. *IEICE Trans. Fundamentals*, E83-9(1):24-32, 2000. [4, 5, 8]
11. D. Galindo. Boneh-Franklin identity based encryption revisited. In *Proc. of ICALP 2005*, LNCS vol. 3580, pp. 791-802. Springer-Verlag, 2003. [5, 6, 7, 8]
12. C. Gentry. Certificate-based encryption and the certificate revocation problem. In *Proc. of Eurorypt'03*, volume 2656 of LNCS, pages 272-293. Springer, 2003. [10]
13. S.D. Galbraith, K. Harrison, and D. Soldera. Implementing the Tate pairing. In *Proc. of ANTS-V*, LNCS vol. 2369, pp. 324-337. Springer-Verlag, 2002. [2]
14. N. McCullagh and P.S.L.M. Barreto. A new two-party identity-based authenticated key agreement. In *Proc. of CT-RSA 2005*, LNCS vol. 3376, pp. 262-274. Springer-Verlag, 2005. [4]
15. A. Shamir. Identity-based cryptosystems and signature schemes. In *Proc. of CRYPTO 1984*, LNCS vol. 196, pp. 47-53. Springer-Verlag, 1984. [1]
16. R. Sakai and M. Kasahara. ID based cryptosystems with pairing on elliptic curve. Cryptology ePrint Archive, Report 2003/054. [1, 2]
17. H. Wang, S. Wang and Z. Cao. Efficient multi-receiver ID-based encryption scheme from pairings. Preprint, 2007. [10]

A mBDH Assumption Is Weaker Than 2-BDHI Assumption

Informally, the 2-BDHI problem [3] is as follows.

- Input: P, aP, a^2P.
- Output: $\hat{e}(P,P)^{1/a}$.

Assume there exists a polynomial-time adversary A that breaks the mBDH assumption. We show that then there exists a polynomial-time adversary B with oracle access to A that breaks the 2-BDHI assumption. Let $\langle P, aP, a^2P\rangle$ be an input instance of the 2-BDHI problem given to B. B's goal is to output $\hat{e}(P,P)^{1/a}$. B picks two random values b, c and defines its output as $U = V^{1/(bc)}$, where V is output from A as

$$V \leftarrow A(aP, P, a^2P, bP, cP).$$

We now show the correctness. Defining $Q = aP,\ xQ = P,\ a = 1/x,\ x^{-1}Q = a^2P,\ yQ = bP,\ zQ = cP$, then we have $y = b/a$ ($yQ = yaP = bP$) and $z = c/a$ ($zQ = zaP = cP$).

Consequently, we have $\langle aP,\ P,\ a^2P,\ bP,\ cP\rangle = \langle Q,\ xQ,\ x^{-1}Q,\ yQ,\ zQ\rangle$. Then

$$V = \hat{e}(Q,Q)^{xyz} = \hat{e}(aP, aP)^{\frac{1}{a}\cdot\frac{b}{a}\cdot\frac{c}{a}} = \hat{e}(P,P)^{\frac{bc}{a}}.$$

Therefore, $U = V^{\frac{1}{bc}} = \hat{e}(P,P)^{1/a}$.

B Proof of Lemma 3

The proof idea is largely based on that of Lemma 4.3 in [5]. Let $\mathcal{A}$ be an IND-CPA adversary against **BasicPub** who makes at most q_2 queries to random oracle H_2 and who has advantage ϵ. We show how to construct an algorithm $\mathcal{B}$ which interacts with $\mathcal{A}$ to solve the mBDH problem.

Suppose $\mathcal{B}$ has an input $\langle \mathbb{G}_1, \mathbb{G}_2, \hat{e}\rangle$ and $\langle P, a^{-1}P, aP, bP, cP\rangle$ (where $a, b, c \in \mathbb{Z}_q^*$ are unknown to $\mathcal{B}$). Let $D = \hat{e}(P,P)^{abc} \in \mathbb{G}_2$ denote the solution to the mBDH problem on these inputs.

Setup: Algorithm $\mathcal{B}$ creates the public key of **BasicPub** $\langle q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{Pub}, P'_{Pub}, n, Q_{ID}, H_2\rangle$ by setting $P_{Pub} = a^{-1}P$, $P'_{Pub} = aP$ and $Q_{ID} = bP$. Here H_2 is a random oracle controlled by $\mathcal{B}$ as described bellow. $\mathcal{A}$ is given the public key. Observe that the unknown private key associated to the public key is $d_{ID} = aQ_{ID} = abP$.

H_2-queries: To simulate H_2-queries by $\mathcal{A}$, $\mathcal{B}$ maintains a list (H_2-list) of pairs $\langle X_j, H_j\rangle$. To respond to an H_2-query on X, $\mathcal{B}$ checks first if $X = X_j$ for some X_j already on the list. If it is, then $\mathcal{B}$ responds with H_j. Otherwise, $\mathcal{B}$ chooses H uniformly at random from $\{0,1\}^m$ and places $\langle X, H\rangle$ on the H_2-list.

Challenge: $\mathcal{A}$ outputs two messages M_0, M_1 on which it wishes to be challenged. $\mathcal{B}$ picks randomly a bit $b \in \{0,1\}$, a string $S \in \{0,1\}^m$ and defines C to be the ciphertext of M_b, where $C = \langle U, V\rangle$, with $U = cP$ and $V = M_b \oplus S$. It then gives C to $\mathcal{A}$ as the challenge.

Notice that, by definition, the decryption of C is $V \oplus H(\hat{e}(cP, abP))=V \oplus H(D)$. (Recall that abP is unknown and D is the solution to the above mBDH problem.)

Guess: $\mathcal{A}$ outputs its guess $b' \in \{0, 1\}$.

Output: At this point, $\mathcal{B}$ picks a random tuple $\langle X_j, H_j \rangle$ from the H_2-list and outputs X_j as the solution to the given instance of mBDH problem.

It is easy to see that $\mathcal{A}$'s view in $\mathcal{B}$'s simulation is the same as in a real attack, in other words, the simulation is perfect. So $\mathcal{A}$'s advantage in this simulation will be ϵ. We let $\mathcal{H}$ be the event that D is queried to H_2 oracle during $\mathcal{B}$'s simulation.

Notice that $H_2(D)$ is independent of $\mathcal{A}$'s view, so if $\mathcal{A}$ never queries D to the H_2 oracle in the above simulation, then the decryption of C is also independent of its view. Therefore, in the simulation we have $\Pr[b = b'|\neg\mathcal{H}] = 1/2$. By the definition of $\mathcal{A}$, we know that in the real attack (and also in the simulation) $| \Pr[b = b'] - 1/2 | \geq \epsilon$. We have the following bounds on $\Pr[b = b']$:

$$\begin{aligned}
\Pr[b = b'] &= \Pr[b = b'|\neg\mathcal{H}]\Pr[\neg\mathcal{H}] + \Pr[b = b'|\mathcal{H}]\Pr[\mathcal{H}] \\
&\leq \Pr[b = b'|\neg\mathcal{H}]\Pr[\neg\mathcal{H}] + \Pr[\mathcal{H}] \\
&= \frac{1}{2}\Pr[\neg\mathcal{H}] + \Pr[\mathcal{H}] \\
&= \frac{1}{2} + \frac{1}{2}\Pr[\mathcal{H}],
\end{aligned}$$

$$\begin{aligned}
\Pr[b = b'] &\geq \Pr[b = b'|\neg\mathcal{H}]\Pr[\neg\mathcal{H}] \\
&= \frac{1}{2}\Pr[\neg\mathcal{H}] \\
&= \frac{1}{2}(1 - \Pr[\mathcal{H}]) \\
&= \frac{1}{2} - \frac{1}{2}\Pr[\mathcal{H}]).
\end{aligned}$$

Hence we have $| \Pr[b = b'] - 1/2 | \leq \frac{1}{2}\Pr[\mathcal{H}]$. By $| \Pr[b = b'] - 1/2 | \geq \epsilon$ we know that $\Pr[\mathcal{H}] \geq 2\epsilon$. Furthermore, by the definition of the event $\mathcal{H}$, we know that D appears in some tuple on the H_2-list with probability at least 2ϵ. It follows that $\mathcal{B}$ outputs the correct answer to the mBDH problem instance with probability at least $2\epsilon/q_2$ as required. □