Identity-Based Online/Offline Encryption

Fuchun Guo[1], Yi Mu[1], and Zhide Chen[2]

[1] Centre for Computer and Information Security Research
School of Computer Science and Software Engineering
University of Wollongong, Wollongong NSW 2522, Australia
{fuchun,ymu}@uow.edu.au

[2] Key Lab of Network Security and Cryptology
School of Mathematics and Computer Science
Fujian Normal University, Fuzhou, China
zhidechen@fjnu.edu.cn

Abstract. We consider a scenario of identity-based encryption (IBE) where the encryption device (such as a smartcard) has low power. To improve the computation efficiency, it is desirable that part of computation can be done prior to knowing the message and the recipient (its identity or public key). The real encryption can be conducted efficiently once the message and the recipient's identity become available. We borrow the notion of online/offline signatures introduced by Even, Goldreich and Micali in 1990 and call this kind of encryption *identity-based online/offline encryption* (IBOOE), in the sense that the pre-computation is referred to as *offline phase* and the real encryption is considered as *online phase*. We found that this new notion is not trivial, since all previously proposed IBE schemes cannot be separated into online and offline phases so that the online phase is very efficient. However, we also found that with a proper transformation, some existing identity-based encryption schemes can be converted into IBOOE schemes with or without random oracles. We look into two schemes in our study: Boneh-Boyen IBE (Eurocrypt 2004), and Gentry IBE (Eurocrypt 2006).

1 Introduction

The notion of online/offline digital signature was introduced by Even, Goldreich and Micali [7, 8]. With this notion, a signing process can be divided into two phases, the first phase is performed *offline* prior to the arrival of a message to be signed and the second phase is performed *online* after knowing the message. The online phase is typically very fast. Online/offline signatures are particularly useful for low-power devices such as smartcard applications. There exist several online/offline digital signatures in the literature [14, 12, 5]. Amongst those works, Shamir and Tauman [14] used a new paradigm, named "hash-sign-switch" to design an efficient online/offline signature schemes. A much more efficient scheme was proposed in [5] with the same idea.

We notice that there exists no a parallel notion for public-key encryption. It could be due to the reason that the encryption scheme is not separable, i.e., RSA encryption, or it is trivial to separate it into online/offline parts, i.e., ElGamal encryption. The latter is suitable for the situation where the sender knows who will be the recipient of the encrypted message, since the offline phase requires the knowledge of the public key of the recipient. We are not interested in this scenario; instead, we consider a novel notion that is motivated by the following situation.

Suppose there are some sensitive data stored in a smartcard, which has limited computation power. In order to send a sensitive data item to a recipient in a secure way, it should be encrypted using the recipient's public key, based on a standard IBE system [1], for instance. To ensure timely delivery, it would be desirable that part of the encryption process could be performed prior to knowing the data item to be delivered and the public key (ID) of the recipient, so that the real encryption process is very quick once the data item and the ID are known. Suppose that recipients are much more powerful, so that they do not care about a reasonable increase of decryption overhead. Unfortunately, all previously published IBE schemes do not accommodate this feature, because the recipient's ID must be known for pre-computation.

We refer to such pre-computation based approach as *identity-based online/ offline encryption* (IBOOE). In this paper, we describe how to construct IBOOE schemes where the public key is an arbitrary sting of user's identity. Our work is based on the two well-known IBE schemes: (1) Boneh-Boyen IBE [1], which was introduced by Boneh and Boyen in 2004 and is based on the selective-ID model, and (2) Gentry IBE [10], which shows an improvement over Waters' IBE scheme without random oracles [15] in terms of the size of public master parameters and security reduction. The Gentry IBE scheme is based on Cramer-Shoup's work [6]. In this paper, we show how to transform these two IBE schemes into online/offline encryption such that the online phase has a very low computational overhead. We prove that the proposed IBOOE schemes hold the same level of security as their original schemes.

Road Map: In Section 2, we will provide the definitions of IBE, including security requirements. In Sections 3 and 4, we present our IBOOE schemes from the Boneh-Boyen IBE and the Gentry IBE scheme. We give a comparison in Section 5 and conclude our paper in Section 6.

2 Definitions

2.1 Security models

An IBE system consists of four algorithms : Setup, KeyGen, Encrypt, Decrypt for master *params* and master secret key generation, private key generation, encryption and decryption, respectively. In this section, we review two security models that will be applied to our schemes.

IND-sID-CCA Model.

Initialization: The adversary outputs an identity ID^* to be challenged.

Setup: The challenger takes as input a security parameter 1^k, and then runs the algorithm Setup. It gives the adversary the resulting master public parameters denoted by *params* and keeps the master secret key for itself.

Phase 1: The adversary makes queries $q_1, q_2, \cdots, q_m$, where q_i is one of the following:

- Key generation query on ID_i. The challenger responds by running algorithm KeyGen to generate the private key d_{ID_i} and sending it to the adversary.
- Decryption query $\langle ID_i, C_i \rangle$. The challenger responds by running algorithm KeyGen to generate the private key d_{ID_i}, running algorithm Decrypt to decrypt the ciphertext $\langle ID_i, C_i \rangle$ and sending the result to the adversary.

These queries may be asked adaptively according to the replies of queries.

Challenge: Once the adversary decides that **Phase 1** is over, it outputs two plaintexts m_0, m_1 on which it wishes to be challenged. The challenger picks a random bit $c_r \in \{0,1\}$ and sets $C_{ch} = \mathsf{Encrypt}(params, ID^*, m_{c_r})$. It sends C_{ch} as the challenge to the adversary.

Phase 2: It is the same as **Phase 1** but with a constraint that the adversary cannot make a key generation query on ID^* or decryption query on (ID^*, C_{ch}).

Guess: The adversary outputs a guess $c_g \in \{0,1\}$ and wins the game if $c_g = c_r$.

We refer to such an adversary $\mathcal{A}$ as an IND-sID-CCA adversary. We define the advantage of adversary $\mathcal{A}$ in attacking the scheme $\mathcal{E}$ as

$$Adv_{\mathcal{E},\mathcal{A}}^{IND-sID-CCA} = \left| \mathsf{Pr}[c_g = c_r] - \frac{1}{2} \right|.$$

The probability is over the random bits used by the challenger and the adversary.

Definition 1 [1] *We say that an IBE system $\mathcal{E}$ is $(t, q_{ID}, q_C, \epsilon)$-adaptively chosen ciphertext secure if for any t-time IND-sID-CCA adversary $\mathcal{A}$ making at most q_{ID} chosen private key queries and at most q_C chosen decryption queries has advantage at most ϵ. As shorthand, we say that $\mathcal{E}$ is $(t, q_{ID}, q_C, \epsilon)$ IND-sID-CCA secure.*

ANON-IND-ID-CCA Model.

Setup: as IND-sID-CCA.

Phase 1: as IND-sID-CCA.

Challenge: Once the adversary decides that **Phase 1** is over it outputs two plaintexts m_0, m_1 and two identities ID_0, ID_1 on which it wishes to be challenged. The challenger picks two random bits $b_r, c_r \in \{0, 1\}$ and sets $C_{ch} = \mathsf{Encrypt}(params, ID_{b_r}, m_{c_r})$. It sends C_{ch} as the challenge to the adversary.

Phase 2: It is the same as **Phase 1**, except the constraint that the adversary cannot make key generation queries on ID_0, ID_1 or decryption C_{ch} under either identity.

Guess: The adversary outputs two bits $b_g, c_g \in \{0, 1\}$ as the guess and wins the game if $b_g = b_r$ and $c_g = c_r$.

We refer to such an adversary $\mathcal{A}$ as an ANON-IND-ID-CCA adversary. We define the advantage of adversary $\mathcal{A}$ in attacking the scheme $\mathcal{E}$ as

$$Adv_{\mathcal{E},\mathcal{A}}^{ANON-IND-ID-CCA} = \left| \mathsf{Pr}[b_g = b_r, c_g = c_r] - \frac{1}{4} \right|.$$

The probability is over the random bits used by the challenger and the adversary.

Definition 2 [10] *We say that an IBE system $\mathcal{E}$ is $(t, q_{ID}, q_C, \epsilon)$-adaptively chosen ciphertext secure if for any t-time ANON-IND-ID-CCA adversary $\mathcal{A}$ making at most q_{ID} chosen private key queries and at most q_C chosen decryption queries has advantage at most ϵ. As shorthand, we say that $\mathcal{E}$ is $(t, q_{ID}, q_C, \epsilon)$ ANON-IND-ID-CCA secure.*

2.2 Bilinear Pairing

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two cyclic groups of prime order p. Let g be a generator of $\mathbb{G}$. A map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is called a bilinear pairing (map) if this map satisfies the following properties:

- Bilinear: for all $u, v \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p$, we have $e(u^a, v^b) = e(u, v)^{ab}$.
- Non-degeneracy: $e(g, g) \neq 1$. In other words, if g be a generator of $\mathbb{G}$, then $e(g, g)$ generates $\mathbb{G}_T$.
- Computability: It is efficient to compute $e(u, v)$ for all $u, v \in \mathbb{G}$.

2.3 Complexity Assumption

We review the Decisional Bilinear Diffie-Hellamn (DBDH) problem and truncated q-Decisional Augmented Bilinear Diffie-Hellman Exponent (q-DABDHE) problem [1, 10].

Definition 3 *Given the group $\mathbb{G}$ of prime order p with generator g and elements $g, g^a, g^b, g^c \in \mathbb{G}^4$ where a, b, c are selected uniformly at random from $\mathbb{Z}_p$, the DBDH problem in $(\mathbb{G}, \mathbb{G}_T)$ is to decide whether a random value $Z \in \mathbb{G}_T$ is equal to $e(g, g)^{abc}$ or not.*

Definition 4 *We say that the (t, ϵ)-DBDH assumption holds in $(\mathbb{G}, \mathbb{G}_T)$ if no t-time algorithm has advantage at least ϵ in solving the DBDH problem in $(\mathbb{G}, \mathbb{G}_T)$.*

Definition 5 *Given the group $\mathbb{G}$ of prime order p with generators g, g' and a vector of $q+3$ elements $g', g'^{a^{q+2}}, g, g^a, g^{a^2}, \cdots, g^{a^q} \in \mathbb{G}^{q+3}$ where a is selected uniformly at random from $\mathbb{Z}_p$, the q-DABDHE problem in $(\mathbb{G}, \mathbb{G}_T)$ is to decide whether a random value $Z \in \mathbb{G}_T$ is equal to $e(g, g')^{a^{q+1}}$ or not.*

Definition 6 *We say that the (t, ϵ) q-DABDHE assumption holds in $(\mathbb{G}, \mathbb{G}_T)$ if no t-time algorithm has advantage at least ϵ in solving the q-DABDHE problem in $(\mathbb{G}, \mathbb{G}_T)$.*

3 IBOOE from the Boneh-Boyen IBE

3.1 Construction

Let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be the bilinear map, $\mathbb{G}, \mathbb{G}_T$ be two cyclic groups of order p and g be the corresponding generator in $\mathbb{G}$. Let $(\mathcal{G}, \mathcal{S}, \mathcal{V})$ be the three algorithms of a one-time strong signature scheme for key generation, signing, and signature verification, respectively. The verification key space is $\mathbb{Z}_p$ (or we can hash it into $\mathbb{Z}_p$). The signature σ can be naturally divided into online and offline phases. We denote by σ_{of} the offline signature and σ_{on} the online signature.

Setup:
The system parameters are generated as follow. Choose at random a secret $a \in \mathbb{Z}_p$, choose g, g_2, h_1, h_2 randomly from $\mathbb{G}$, and set the value $g_1 = g^a$. The master public *params* and master secret key K are, respectively,

$$params = \Big(g, g_1, g_2, h_1, h_2, \mathcal{G}, \mathcal{S}, \mathcal{V}\Big), \qquad K = g_2^a.$$

KeyGen:
To generate a private key for $ID \in \mathbb{Z}_p$, pick a random $r \in \mathbb{Z}_p$ and output

$$d_{ID} = (d_1, d_2) = \Big(g_2^a (h_1 g_1^{ID})^r, g^r\Big).$$

Encrypt:

General Encryption: We refer to the original Boneh-Boyen IBE as *general encryption.* It is not required in our IBOOE, but since our IBOOE decryption is associated the Boneh-Boyen IBE, we outline the scheme as follows.

Given a message $m \in \mathbb{G}_T$ and the public key $ID \in \mathbb{Z}_p$, randomly choose $s \in \mathbb{Z}_p$, and generate one pair of signing/verification key (sk, vk) from $\mathcal{G}$ and output the ciphertext

$$C_\mu = \Big((h_1 g_1^{ID})^s, (h_2 g_1^{vk})^s, g^s, e(g_1, g_2)^s \cdot m, \sigma, vk\Big) = (c_1, c_2, c_3, c_4, c_5, c_6),$$

where $\sigma = \mathcal{S}_{sk}(c_1, c_2, c_3, c_4)$ is the signature on c_1, c_2, c_3, c_4, and $\mathcal{S}_{sk}$ denotes a one-time signature created using sk.

Online/offline Encryption: We now describe our IBOOE, which is divided into two phases:

- Offline encryption: randomly choose $\alpha, \beta, s \in \mathbb{Z}_p$ and (sk, vk) as the above, and output

$$C_{of} = \Big((h_1 g_1^{\alpha})^s, g_1^{s\beta}, (h_2 g_1^{vk})^s, g^s, e(g_1, g_2)^s, \sigma_{of}\Big) = (c_1, c_2, c_4, c_5, c_6', c_7).$$

  Store the offline parameters $C_{of}, \alpha, \beta^{-1}, sk, vk$ for the online phase.

- Online encryption: given a message $m \in \mathbb{G}_T$ and the public key $ID \in \mathbb{Z}_p$, and output

$$C_{on} = \Big(\beta^{-1}(ID - \alpha), c_6' \cdot m, \sigma_{on}\Big) = (c_3, c_6, c_8),$$

  where $\sigma_{on} = \mathcal{S}_{sk}(c_1, c_2, c_3, c_4, c_5, c_6)$.
  The ciphertext for ID is set as

$$C_\nu = (c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8, c_9)$$

$$= \Big((h_1 g_1^{\alpha})^s, g_1^{s\beta}, \beta^{-1}(ID - \alpha), (h_2 g_1^{vk})^s, g^s, e(g_1, g_2)^s \cdot m, \sigma_{of}, \sigma_{on}, vk\Big).$$

Observe that the online phase has a very low computational complexity and the offline phase does not require the knowledge of the message and the public key (ID) of a recipient.

Decrypt:

IBOOE Decryption: Let $C_\nu = (c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8, c_9)$ be a valid encryption for $ID \in \mathbb{Z}_p$. To decrypt C_ν with d_{ID}, test whether

$$\mathcal{V}_{c_9}(c_7, c_8) = TRUE,$$

where $\mathcal{V}_{c_9}$ denotes the verification function wrt vk. If the verification fails, reject. Otherwise, it outputs

$$c_0 = c_1 \cdot c_2^{c_3} = (h_1 g_1^{\alpha})^s \cdot (g_1^{s\beta})^{\beta^{-1}(ID-\alpha)} = (h_1 g_1^{ID})^s.$$

We then have $(c_0, c_4, c_5, c_6) = \Big((h_1 g_1^{ID})^s, (h_2 g_1^{vk})^s, g^s, e(g_1, g_2)^s \cdot m\Big)$, which is the same as the output of the general encryption described earlier in this section and the message can be recovered with the general decryption procedure described below.

General Decryption: We refer to the decryption process of the original Boneh-Boyen IBE as *general decryption*, which is outlined as follows.

Let $C_\mu = (c_1, c_2, c_3, c_4, c_5, c_6)$ be a valid encryption tuple for $ID \in \mathbb{Z}_p$. To decrypt C_μ with d_{ID}, test whether

$$\mathcal{V}_{c_6}(c_5) = TRUE.$$

Then[3], test whether the ciphertext is indeed for ID using vk by

$$e(c_1, g) = e\Big((h_1 g_1^{ID})^s, g\Big) = e(h_1 g_1^{ID}, g^s) = e(h_1 g_1^{ID}, c_3)$$
$$e(c_2, g) = e\Big((h_2 g_1^{vk})^s, g\Big) = e(h_2 g_1^{vk}, g^s) = e(h_2 g_1^{vk}, c_3)$$

If it fails, reject. Otherwise, the ciphertext to be decrypted is

$$C_\mu' = \Big((h_1 g_1^{ID})^s, (h_2 g_1^{vk})^s, g^s, e(g_1, g_2)^s \cdot m\Big),$$

and the decryption is as follows:

- Compute the 2-level private key of $d_{ID|vk}$ using a random value $r' \in \mathbb{Z}_p$ as

$$d_{ID|vk} = (d_1', d_2', d_3') = \Big(g_2^a (h_1 g_1^{ID})^r (h_2 g_1^{vk})^{r'}, g^r, g^{r'}\Big);$$

[3] The IBOOE continues the decryption from here.

– Output the message by

$$\begin{aligned} c_4 \cdot \frac{e(d'_2, c_1)e(d'_3, c_2)}{e(d'_1, c_3)} &= (e(g_1, g_2)^s m) \cdot \frac{e\Big(g^r, (h_1 g_1^{ID})^s\Big) e\Big(g^{r'}, (h_2 g_1^{vk})^s\Big)}{e\Big(g_2^a (h_1 g_1^{ID})^r (h_2 g_1^{vk})^{r'}, g^s\Big)} \\ &= (e(g_1, g_2)^s m) \cdot \frac{1}{e(g_1, g_2)^s} \\ &= m. \end{aligned}$$

3.2 Security

Theorem 1 *The IBOOE scheme from the Boneh-Boyen IBE construction is still IND-sID-CCA secure assuming the DBDH assumption holds.*

Proof. Suppose there exists a $(t, q_{ID}, q_C, \epsilon)$-adversary $\mathcal{A}$ against the BB-IBE scheme, Boneh and Boyen constructed an algorithm $\mathcal{B}_\mu$ that solves the DBDH problem, which is given as input a random tuple (g, g^a, g^b, g^c, Z) that Z is either $e(g, g)^{abc}$ or just a random value in $\mathbb{G}_T$. Suppose there exists the same $(t, q_{ID}, q_C, \epsilon)$-adversary $\mathcal{A}$ against the our IBOOE scheme, we construct an algorithm $\mathcal{B}_\nu$ that solves the DBDH problem with the same challenge tuple. To avoid repeating the simulation, we only show that $\mathcal{B}_\nu$ can be construed from $\mathcal{B}_\mu$ without any additional requirements.

Initialization. The adversary outputs an identity $ID^* \in \mathbb{Z}_p$ to be challenged.

Setup: To generate the master public *params*, $\mathcal{B}_\nu$ simulates the master public *params* as $\mathcal{B}_\mu$ completely, using the same public *params* in both BB-IBE and IBOOE schemes.

Phase 1: The adversary makes the following queries:

- The adversary makes key generation query on ID_i and $\mathcal{B}_\nu$ simulates the private key d_{ID_i} as $\mathcal{B}_\mu$ completely, using the same private key construction in both BB-IBE and IBOOE schemes.
- The adversary makes key generation query on $\langle ID_i, C_i \rangle$. To respond the decryption query, $\mathcal{B}_\nu$ first tests the correctness of signature according to the Decryption algorithm of IBOOE, and then simulates the following decryption as $\mathcal{B}_\mu$, using the same decryption algorithm in both BB-IBE and IBOOE schemes.

Challenge: When $\mathcal{A}$ decides that phase 1 is over, it outputs two messages $m_0, m_1 \in \mathbb{G}_T$ on which it wishes to be challenged. $\mathcal{B}_\mu$ picks a random bit $c_r \in \{0, 1\}$ and generates its challenge ciphertext $C_{\mu,ch}$ for the BB-IBE scheme, where

$$C_{\mu,ch} = \Big((h_1 g_1^{ID^*})^s, (h_2 g_1^{vk^*})^s, g^s, e(g_1, g_2)^s \cdot m_{c_r}, \sigma^*, vk^*\Big),$$

and $\mathcal{B}_\mu$ still holds the signing key sk^* of vk^*. Using the challenge ciphertext $C_{\mu,ch}$ and sk^* without any additional simulation, $\mathcal{B}_\nu$ generates the challenge ciphertext as follows:

- Draw the elements $(h_1 g_1^{ID^*})^s, (h_2 g_1^{vk^*})^s, g^s, e(g_1, g_2)^s \cdot m_{c_r}$ from $C_{\mu,ch}$;
- Randomly choose k_1, k_2, and output

$$C' = \Big((h_1 g_1^{ID^*})^s g^{-k_1 k_2}, g^{k_1}, k_2, (h_2 g_1^{vk^*})^s, g^s, e(g_1, g_2)^s \cdot m_{c_r}\Big);$$

- Sign the above ciphertext using sk^* and output $\sigma = \langle \sigma_{of}, \sigma_{on} \rangle$.

The challenge ciphertext for IBOOE is

$$C_{ch} = \Big((h_1 g_1^{ID^*})^s g^{-k_1 k_2}, g^{k_1}, k_2, (h_2 g_1^{vk^*})^s, g^s, e(g_1, g_2)^s \cdot m_{c_r}, \sigma_{of}, \sigma_{on}, vk^* \Big).$$

Let $\alpha = ID^* - \frac{k_1 k_2}{as}, \beta = \frac{k_1}{as}$, we have

$$\begin{aligned} (h_1 g_1^{ID^*})^s g^{-k_1 k_2} &= (h_1 g_1^{\alpha})^s \\ g^{k_1} &= g_1^{s\beta} \\ k_2 &= \beta^{-1}(ID^* - \alpha). \end{aligned}$$

Then, it has that

$$C_{ch} = \Big((h_1 g_1^{\alpha})^s, g_1^{s\beta}, \beta^{-1}(ID^* - \alpha), (h_2 g_1^{vk^*})^s, g^s, e(g_1, g_2)^s \cdot m_{c_r}, \sigma_{of}, \sigma_{on}, vk^* \Big)$$

is a valid online/offline challenge ciphertext for ID^*.

Phase 2: As phase 1.

Guess: Finally, $\mathcal{A}$ outputs c_g and $\mathcal{B}_\nu$ outputs 1 if $c_g = c_r$; outputs 0, otherwise.

This completes the description of $\mathcal{B}_\nu$ in the simulation. From the above, we know that both $\mathcal{B}_\nu$ and $\mathcal{B}_\mu$ will reject all invalid ciphertext queries in a similar way and then the private key simulation and decryption simulation are identical. The challenge ciphertext in both BB-IBE simulation and IBOOE simulation appear to be the same to the adversary; therefore, what the adversary outputs are the same guess. Therefore, the IBOOE scheme from the BB-IBE construction is still IND-sID-CCA secure. □

4 IBOOE from the Gentry IBE

The Gentry IBE [10] proposed an IBE without random oracles. In comparison to Waters' encryption scheme [15], the Gentry IBE has much shorter public master parameters and offers a tighter reduction in security proofs.

4.1 Construction

Let $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ be the bilinear map, $\mathbb{G}, \mathbb{G}_T$ be two cyclic groups of order p and g be the corresponding generator in $\mathbb{G}$.

Setup:
The system parameters are generated as follows. Choose at random a secret $a \in \mathbb{Z}_p$, choose g, h_1, h_2, h_3 randomly from $\mathbb{G}$, and set the value $g_1 = g^a \in \mathbb{G}$. Choose a hash function $H : \{0,1\}^* \rightarrow \mathbb{Z}_p$ from a family of universal one-way hash function. The master public *params* and the master secret key K are

$$params = \Big(g, g_1, h_1, h_2, h_3, H \Big), \qquad K = a.$$

KeyGen:
To generate a private key for $ID \in \mathbb{Z}_p$, pick random $r_{ID,i} \in \mathbb{Z}_p$ for $i = 1, 2, 3$, and output

$$d_{ID} = \Big\{ (r_{ID,i}, h_{ID,i}) : i = 1, 2, 3 \Big\}, \text{ where } h_{ID,i} = (h_i g^{-r_{ID,i}})^{\frac{1}{a - ID}}.$$

If $ID = a$, abort. It requires the same random values $r_{ID,i}$ for ID.

Encrypt:

General Encryption. Again, we refer to the original Gentry IBE as *general encryption*, which is not required in our IBOOE. Since it is related to our IBOOE decryption procedure, we outline it as follows.

Given a message $m \in \mathbb{G}_T$ and the public key $ID \in \mathbb{Z}_p$, randomly choose $s \in \mathbb{Z}_p$ and output the ciphertext

$$C_\mu = \Big(g_1^s g^{-sID}, e(g,g)^s, e(g,h_1)^{-s} \cdot m, e(g,h_2)^s e(g,h_3)^{sH_c}\Big) = (c_1, c_2, c_3, c_4),$$

where $H_c = H(c_1, c_2, c_3) \in \mathbb{Z}_p$.

Online/Offline Encryption.

- Offline Encryption: Choose at random $\alpha, \beta, \gamma, \theta, s \in \mathbb{Z}_p$, and output

$$\begin{aligned} C_{of} &= \Big(g_1^s g^{-s\alpha}, g^{s\beta}, e(g,g)^s, e(g,h_1)^{-s}, e(g,h_2)^s e(g,h_3)^{s\gamma}, e(g,h_3)^{s\theta}\Big) \\ &= (c_1, c_2, c_4, c_5', c_6, c_7). \end{aligned}$$

  Store $C_{of}, \alpha, \beta^{-1}, \gamma, \theta^{-1}$ for the online computation.
- Online Encryption: Given a message $m \in \mathbb{G}_T$ and the public key $ID \in \mathbb{Z}_p$, output

$$C_{on} = \Big(\beta^{-1}(\alpha - ID), c_5' \cdot m, \theta^{-1}(H_c - \gamma)\Big) = (c_3, c_5, c_8),$$

  where $H_c = H(c_1, c_2, c_3, c_4, c_5, c_6, c_7) \in \mathbb{Z}_p$.
  The ciphertext for ID is $C_\nu = (c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8)$, and

$$\begin{aligned} C_\nu = \Big(& g_1^s g^{-s\alpha}, g^{s\beta}, \beta^{-1}(\alpha - ID), e(g,g)^s, e(g,h_1)^{-s} \cdot m, \\ & e(g,h_2)^s e(g,h_3)^{s\gamma}, e(g,h_3)^{s\theta}, \theta^{-1}(H_c - \gamma)\Big). \end{aligned}$$

Decrypt:

Online/Offline Decryption: Let $C_\nu = (c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8)$ be a valid encryption for $ID \in \mathbb{Z}_p$. To decrypt C_ν with d_{ID}, set $H_c = H(c_1, c_2, c_3, c_4, c_5, c_6, c_7)$ and compute

$$\begin{aligned} c_0 &= c_1 c_2^{c_3} = g_1^s g^{-s\alpha} \cdot (g^{s\beta})^{\beta^{-1}(\alpha - ID)} = g_1^s g^{-sID}, \\ c_9 &= c_6 c_7^{c_8} \\ &= e(g,h_2)^s e(g,h_3)^{s\gamma} \cdot \Big(e(g,h_3)^{s\theta}\Big)^{\theta^{-1}(H_c - \gamma)} \\ &= e(g,h_2)^s e(g,h_3)^{sH_c}. \end{aligned}$$

Then, check whether

$$c_9 = e\Big(c_0, h_{ID,2} {h_{ID,3}}^{H_c}\Big) c_4^{r_{ID,2} + r_{ID,3} H_c}.$$

If it fails, reject. Otherwise, we have

$$(c_0, c_3, c_4) = \Big(g_1^s g^{-sID}, e(g,g)^s, e(g,h_1)^{-s} \cdot m\Big),$$

which is te same as the output from a general encryption whose decryption process is referred to as *general decryption*, described below.

General Decryption: Let $C_\mu = (c_1, c_2, c_3, c_4)$ be a valid encryption tuple for $ID \in \mathbb{Z}_p$. To decrypt C_μ with d_{ID}, set $H_c = H(c_1, c_2, c_3)$ and check whether

$$c_4 = e\Big(c_1, h_{ID,2}h_{ID,3}{}^{H_c}\Big)c_2^{r_{ID,2}+r_{ID,3}H_c}.$$

If it fails, reject. Otherwise, output the ciphertext:

$$C'_\mu = \Big(g_1^s g^{-sID}, e(g,g)^s, e(g,h_1)^{-s} \cdot m\Big),$$

and the decryption is conducted by computing

$$m = c_3 \cdot e(c_1, h_{ID,1})c_2^{r_{ID,1}}.$$

The correctness of the scheme can be easily verified:

$$\begin{aligned}
& e\Big(c_1, h_{ID,2}h_{ID,3}{}^{H_c}\Big)c_2^{r_{ID,2}+r_{ID,3}H_c} \\
&= e\Big(g^{s(a-ID)}, (h_2h_3^{H_c})^{\frac{1}{a-ID}} g^{\frac{-(r_{ID,2}+r_{ID,3}H_c)}{a-ID}}\Big) \cdot e\Big(g,g\Big)^{s(r_{ID,2}+r_{ID,3}H_c)} \\
&= e\Big(g^{s(a-ID)}, (h_2h_3^{H_c})^{\frac{1}{a-ID}}\Big) \\
&= e(g,h_2)^s e(g,h_3)^{sH_c}.
\end{aligned}$$

$$\begin{aligned}
& e(c_1, h_{ID,1})c_2^{r_{ID,1}} \\
&= e\Big(g^{s(a-ID)}, h_1^{\frac{1}{a-ID}} g^{\frac{-r_{ID,1}}{a-ID}}\Big)e(g,g)^{sr_{ID,1}} = e(g,h_1)^s.
\end{aligned}$$

4.2 Security

Theorem 2 *The IBOOE scheme from the Gentry IBE construction is still ANON-IND-ID-CCA secure assuming the q-DABDHE assumption holds.*

Proof. Suppose there exists a $(t, q_{ID}, q_C, \epsilon)$-adversary $\mathcal{A}$ against the Gentry IBE scheme, Gentry constructed an algorithm $\mathcal{B}_\mu$ that solves the q-DABDHE problem, where it is given as input a random tuple $(g', g'^{a^{q+2}}, g, g^a, g^{a^2}, \cdots, g^{a^q}, Z)$ that Z is either $e(g,g)^{a^{q+1}}$ or a random value in $\mathbb{G}_T$. Suppose there exists the same $(t, q_{ID}, q_C, \epsilon)$-adversary $\mathcal{A}$ against the our IBOOE scheme; we construct an algorithm $\mathcal{B}_\nu$ that solves the q-DABDHE problem with the same challenge tuple. To avoid repeating the simulation, we also only show that $\mathcal{B}_\nu$ can be construed from $\mathcal{B}_\mu$ without any additional requirements.

Setup: To generate the master public *params*, $\mathcal{B}_\nu$ simulates the master public *params* as $\mathcal{B}_\mu$ completely, due to same public *params* in both Gentry IBE and IBOOE scheme.

Phase 1: The adversary makes the following queries:

- The adversary makes key generation query on ID_i and $\mathcal{B}_\nu$ simulates the private key d_{ID_i} as $\mathcal{B}_\mu$ completely, using the same private key construction in both Gentry IBE and IBOOE schemes.
- The adversary makes key generation query on $\langle ID_i, C_i \rangle$. To respond the decryption query, $\mathcal{B}_\nu$ first tests the correctness of the ciphertext according to the Decryption algorithm of IBOOE, and then simulates the following decryption as $\mathcal{B}_\mu$, using the same decryption algorithm in both Gentry IBE and IBOOE schemes.

Challenge: When $\mathcal{A}$ decides that phase 1 is over, it outputs and identities ID_1, ID_2 and two messages $m_0, m_1 \in \mathbb{G}_T$ on which it wishes to be challenged. $\mathcal{B}_\mu$ picks random bits $b_r, c_r \in \{0,1\}$ and generates its challenge ciphertext $C_{\mu,ch}$ for Gentry IBE scheme, where

$$C_{\mu,ch} = \Big(g_1^s g^{-sID_{b_r}}, e(g,g)^s, e(g,h_1)^{-s} \cdot m_{c_r}, e(g,h_2)^s e(g,h_3)^{sH_c}\Big),$$

and $\mathcal{B}_\mu$ still holds the elements of $e(g,h_2)^s$ and $e(g,h_3)^s$. Using the challenge ciphertext $C_{\mu,ch}$ and $e(g,h_2)^s, e(g,h_3)^s$ without any additional simulation, $\mathcal{B}_\nu$ generates the challenge ciphertext as follows:

- Draw the elements $g_1^s g^{-sID_{b_r}}, e(g,g)^s, e(g,h_1)^{-s} \cdot m_{c_r}$ from $C_{\mu,ch}$;
- Randomly choose $k_1, k_2 \in \mathbb{Z}_p$ and output

$$C' = \Big((g_1^s g^{-sID_{b_r}})^{\frac{k_1}{k_1+k_2}}, (g_1^s g^{-sID_{b_r}})^{\frac{1}{k_1+k_2}}, k_2, e(g,g)^s, e(g,h_1)^{-s} \cdot m_{c_r}\Big);$$

- Randomly choose $\gamma, \theta \in \mathbb{Z}_p$ and output

$$\Big(e(g,h_2)^s e(g,h_3)^{s\gamma}, e(g,h_3)^{s\theta}, \theta^{-1}(H_c - \gamma)\Big),$$

where H_c is the hash value of C' and $e(g,h_2)^s e(g,h_3)^{s\gamma}, e(g,h_3)^{s\theta}$.

The challenge ciphertext for IBOOE is

$$C_{ch} = \Big((g_1^s g^{-sID_{b_r}})^{\frac{k_1}{k_1+k_2}}, (g_1^s g^{-sID_{b_r}})^{\frac{1}{k_1+k_2}}, k_2, e(g,g)^s, e(g,h_1)^{-s} \cdot m_{c_r}, \\ e(g,h_2)^s e(g,h_3)^{s\gamma}, e(g,h_3)^{s\theta}, \theta^{-1}(H_c - \gamma)\Big).$$

Let $\alpha = \frac{k_1 ID_{b_r} + k_2 a}{k_1+k_2}, \beta = \frac{a - ID_{b_r}}{k_1+k_2}$, we have

$$\begin{aligned}(g_1^s g^{-sID_{b_r}})^{\frac{k_1}{k_1+k_2}} &= g_1^s g^{-s\alpha} \\ (g_1^s g^{-sID_{b_r}})^{\frac{1}{k_1+k_2}} &= g^{s\beta} \\ k_2 &= \beta^{-1}(\alpha - ID_{b_r}).\end{aligned}$$

Then, it has that

$$C_{ch} = \Big(g_1^s g^{-s\alpha}, g^{s\beta}, \beta^{-1}(\alpha - ID_{b_r}), e(g,g)^s, e(g,h_1)^{-s} \cdot m_{c_r}, \\ e(g,h_2)^s e(g,h_3)^{s\gamma}, e(g,h_3)^{s\theta}, \theta^{-1}(H_c - \gamma)\Big)$$

is a valid online/offline challenge ciphertext for ID_{b_r}.

Phase 2: as phase 1.

Guess: Finally, $\mathcal{A}$ outputs b_g, c_g and $\mathcal{B}_\nu$ outputs 1 if $b_g = b_r$ and $c_g = c_r$; outputs 0, otherwise.

This completes the description of $\mathcal{B}_\nu$ in the simulation. We know that both $\mathcal{B}_\nu$ and $\mathcal{B}_\mu$ will reject all invalid ciphertext queries in a similar way and then the private key simulation and decryption simulation are identical. The challenge ciphertext in both the Gentry IBE simulation and the IBOOE simulation appear to be the same to the adversary; therefore what the adversary outputs is the same guess. Therefore, the IBOOE scheme from the Gentry IBE construction is still ANON-IND-ID-CCA secure. □

5 Comparison

We now justify our schemes by comparing them with the online/offline scheme based on *natural splitting*. In the following, we will utilize the keyword “natural” to denote natural splitting.

5.1 Natural IBOOE

It is not hard to “naturally” divide the encryption procedure into online/offline phases. Because the schemes are only different in algorithm **Encrypt**, we omit other algorithms.

Encrypt:
Natural Online/offline Encryption from BB-IBE:

- Offline encryption: randomly choose $s \in \mathbb{Z}_p$ and one pair of signing/verification key (sk, vk) from $\mathcal{G}$, and output

$$C_{of} = \Big(h_1^s, g_1^s, (h_2 g_1^{vk})^s, g^s, e(g_1, g_2)^s, \sigma_{of}\Big) = (c_1, c_2, c_4, c_5, c_6', c_7).$$

  Store the offline parameters C_{of}, sk, vk for the online phase.
- Online encryption: given a message $m \in \mathbb{G}_T$ and the public key $ID \in \mathbb{Z}_p$, and output

$$C_{on} = \Big(c_1 \cdot c_2^{ID}, c_6' \cdot m, \sigma_{on}\Big) = (c_3, c_6, c_8),$$

  where $\sigma_{on} = \mathcal{S}_{sk}(c_3, c_4, c_5, c_6)$ is the signature signed with sk.
  The ciphertext for ID is $C_\nu = (c_3, c_4, c_5, c_6, c_7, c_8, c_9)$, and

$$C_\nu = \Big((h_1 g_1^{ID})^s, (h_2 g_1^{vk})^s, g^s, e(g_1, g_2)^s \cdot m, \sigma_{of}, \sigma_{on}, vk\Big).$$

Natural Online/offline Encryption from Gentry IBE:

- Offline encryption: randomly choose $s \in \mathbb{Z}_p$, and output

$$C_{of} = \Big(g_1^s, g^{-s}, e(g, g)^s, e(g, h_1)^{-s}, e(g, h_2)^s, e(g, h_3)^s\Big) = (c_1, c_2, c_4, c_5', c_6, c_7).$$

  Store the offline parameters C_{of} for the online phase.
- Online encryption: given a message $m \in \mathbb{G}_T$ and the public key $ID \in \mathbb{Z}_p$, and output

$$C_{on} = \Big(c_1 \cdot c_2^{ID}, c_5' \cdot m, c_6 \cdot c_7^{H_c}\Big) = (c_3, c_5, c_8),$$

  where $H_c = H(c_3, c_4, c_5)$.
  The ciphertext for ID is $C_\nu = (c_3, c_4, c_5, c_8)$, and

$$C_\nu = \Big(g_1^s g^{-sID}, e(g, g)^s, e(g, h_1)^{-s} \cdot m, e(g, h_2)^s e(g, h_3)^{sH_c}\Big).$$

5.2 Comparison

We provide a comparison of computational cost in Table 1. We denote, in the table, by “natural” a “natural split” and by “ours” our IBOOE scheme. We denote by E the exponentiation in $\mathbb{G}$, ME the multi-exponentiation in $\mathbb{G}$, M the multiplication in $\mathbb{G}$, m_c the modular computation in $\mathbb{Z}_p$, G the time in generating the pair of (sk, vk), and S the time in offline signing.

Scheme	Boneh-Boyen IBE[1]	Gentry IBE[10]
Security Model	Selective-ID model	Standard model
Assumption	DBDH	q-DABDHE
Reduction	Tight	Tight
Offline phase (natural)	4E+1ME+1G+1S	6E
Online phase (natural)	1E+2M+1m$_c$	2E+3M
Store in offline (natural)	5+1vk+1sk+1σ_{of}	6
Offline phase (ours)	3E+2ME+1G+1S	4E+2ME
Online phase (ours)	1M+2m$_c$	1M+2m$_c$
Store in offline (ours)	7+1vk+1sk+1σ_{of}	10

Table 1. This table presents a comparison of the related IBE schemes. The cost of an efficient online/offline signature [14] to achieve CCA secure in Boneh-Boyen IBE scheme is about $1G + 1S$ in offline phase result of $1\sigma_{of}$ length offline signature and $1m_c$ in online phase.

6 Conclusion

In this paper, we introduced a new notion of *identity-based online/offline encryption* (IBOOE). There is no doubt that IBOOE schemes are useful where the computational power of a device is limited. We presented two IBOOE schemes based on two existing IBE schemes: the Boneh-Boyen IBE [1] and the Gentry IBE [10]. The merits of the proposed schemes lie in the following two aspects. (1) The online encryption is extremely efficient. (2) The offline phase can be implemented without the need of the message to be encrypted and the public key (or ID) of a recipient.

Acknowledgement. The authors would like to thank the anonymous reviewers for their helpful comments on this work.

References

1. D. Boneh and X. Boyen: Efficient selective-id secure identity based encryption without random oracles. In Advances in Cryptology-Eurocrypt'04,Vol.3027 of LNCS, pages 223-238, Springer-Verlag,2004
2. D. Boneh and M. Franklin: Identity-Based Encryption from the Weil Pairing. In J. Kilian, editor,Advances in Cryptology-Crypto'01, vol.2139 of LNCS, pages 213-229, Springer-Verlag, 2001
3. D. Boneh and J. Katz. Improved efficiency for cca-secure cryptosystems built using identity based encryption. In Proceedings of RSA-CT 2005, 2005.
4. R. Canetti, S. Halevi, and J. Katz. Chosen-ciphertext security from identity-based encryption. In Proceedings of Eurocrypt 2004. Springer-Verlag, 2004.
5. X. Chen, F. Zhang, W. Susilo, and Y. Mu, Efficient Generic online/offline Signatures Without Key Exposure. Advances in ACNS 2007, LNCS 4521, pp. 18-30,Springer-Verlag, 2007.
6. R. Cramer and V. Shoup. A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attacks. In Advances in Cryptology C Crypto 1998, volume 1462 of LNCS, pages 13-25. Springer-Verlag, 1998.
7. S. Even, O. Goldreich, and S. Micali, online/offline digital signatures, Advances in Cryptology-Crypto 1989, LNCS 2442, pp.263-277, Springer-Verlag, 1989.
8. S. Even, O. Goldreich, and S. Micali, online/offline digital signatures, Journal of Cryptology, 9(1), pp.35-67, Springer-Verlag, 1996.
9. J. Horwitz and B. Lynn. Toward hierarchical identity-based encryption. In Advances in Cryptology: EUROCRYPT 2002, pages 466-481, 2002.
10. C. Gentry: Practical Identity-Based Encryption Without Random Oracles. In Advance of Eurocrypt'06, vol.4004 of LNCS, pages 445-464, Springer-Verlag, 2006
11. C. Gentry and A. Silverberg. Hierarchical id-based cryptography. In Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security, pages 548-566. Springer-Verlag, 2002.
12. K. Kurosawa and K. Schmidt-Samoa, New online/offline signature schemes without random oracles, Advances in Public-Key Cryptography-PKC 2006, LNCS 3958, pp.330-346, Springer-Verlag, 2006.

13. A. Shamir: Identity-based cryptosystems and signature schemes. In Advances in Cryptology-Crypto'84, Vol. 196 of LNCS, pages 47-53, Springer-Verlag, 1984
14. A. Shamir and Y. Tauman, Improved online/offline signature schemes, Advances in Cryptology-Crypto 2001, LNCS 2139, pp.355-367, Springer-Verlag, 2001.
15. B.Waters: Efficient Identity-Based Encryption without Random Oracles. In advance in Cryptology-Eurocrypt'05,vol.3494 of LNCS, pages 114-127, Springer-Verlag, 2005