2015

Improved identity-based online/offline encryption

Jianchang Lai
University of Wollongong, jl967@uowmail.edu.au

Yi Mu
University of Wollongong, ymu@uow.edu.au

Fuchun Guo
University of Wollongong, fuchun@uow.edu.au

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Publication Details

Lai, J., Mu, Y., Guo, F. & Susilo, W. (2015). Improved identity-based online/offline encryption. Lecture Notes in Computer Science, 9144 160-173.

Improved identity-based online/offline encryption

Abstract
The notion of online/offline encryption was put forth by Guo, Mu and Chen (FC 2008), where they proposed an identity-based scheme called identity-based online/offline encryption (IBOOE). An online/offline encryption separates an encryption into two stages: offline and online. The offline phase carries much more computational load than the online phase, where the offline phase does not require the information of the message to be encrypted and the identity of the receiver. Subsequently, many applications of IBOOE have been proposed in the literature. As an example, Hobenberger and Waters (PKC 2014) have recently applied it to attribute-based encryption. In this paper, we move one step further and explore a much more efficient variant.We propose an efficient semi-generic transformation to obtain an online/offline encryption from a tradition identity-based encryption (IBE). Our transformation provides a new method to separate the computation of receiver's identity into offline and online phases. The IBOOE schemes using our transformation saves one group element in both offline and online phases compared to other IBOOE schemes in identity computing. The transformed scheme still maintains the same level of security as in the original IBE scheme.

Disciplines
Engineering | Science and Technology Studies

Publication Details
Lai, J., Mu, Y., Guo, F. & Susilo, W. (2015). Improved identity-based online/offline encryption. Lecture Notes in Computer Science, 9144 160-173.

Improved Identity-Based Online/Offline Encryption

Jianchang Lai(✉), Yi Mu, Fuchun Guo, and Willy Susilo

Centre for Computer and Information Security Research,
School of Computing and Information Technology, University of Wollongong,
Wollongong, NSW 2522, Australia
{jl967,ymu,fuchun,wsusilo}@uow.edu.au

Abstract. The notion of online/offline encryption was put forth by Guo, Mu and Chen (FC 2008), where they proposed an identity-based scheme called *identity-based online/offline encryption* (IBOOE). An online/offline encryption separates an encryption into two stages: offline and online. The offline phase carries much more computational load than the online phase, where the offline phase does not require the information of the message to be encrypted and the identity of the receiver. Subsequently, many applications of IBOOE have been proposed in the literature. As an example, Hobenberger and Waters (PKC 2014) have recently applied it to attribute-based encryption. In this paper, we move one step further and explore a much more efficient variant. We propose an efficient semi-generic transformation to obtain an online/offline encryption from a tradition identity-based encryption (IBE). Our transformation provides a new method to separate the computation of receiver's identity into offline and online phases. The IBOOE schemes using our transformation saves one group element in both offline and online phases compared to other IBOOE schemes in identity computing. The transformed scheme still maintains the same level of security as in the original IBE scheme.

Keywords: Identity-based encryption · Online/offline encryption

1 Introduction

Identity based encryption (IBE) was first introduced by Shamir in 1984 [14]. In an IBE system, each user's public key can be an arbitrary string binding the user's identity, such as an email address or a telephone number. IBE removes the necessity of complex certificate management that exists in traditional public key cryptography. The need to incorporate certificates has been elimiated, and hence, it removes complicated and costly certificate verification processes. If a new user wants to join the network in a network system based on IBE, there is no need for other users in the network to verify its certificate in order to communicate securely.

One of the main concerns in cryptography is the efficiency of computation. However, most IBE schemes [2,7,17] in cryptography involve computations

E. Foo and D. Stebila (Eds.): ACISP 2015, LNCS 9144, pp. 160–173, 2015.
DOI: 10.1007/978-3-319-19962-7_10

including pairings over points on elliptic cure and exponentiations (point multiplications) in groups. These operations are regarded as the most costly computations in cryptography, which might be too costly to be applied in lightweight devices. One elegant way to solve the problem was proposed to reduce the computational overhead of digital signature schemes by Even, Goldreich and Micali [6], where a signing process is split into two phases. The first phase is called the offline phase and is performed prior to obtaining the message to be signed. The second phase is called the online phase and is executed when the message becomes available. All the heavy computations in signing phase are pre-computed in the offline phase. In the online phase, it only performs the light computations such as modular multiplication.

The notion of online/offline encryption was first introduced by Guo, Mu and Chen [8] in 2008, where they proposed an identity-based construction. The motivation of online/offline encryption is to improve the efficiency of encryption. In the offline phase, most of the heavy computations are conducted without the need to know the recipient's identity and the message to be encrypted. When the recipient's identity and the message become available, the online phase can be accomplished with great efficiency. This seminal work has attracted a lot of attention.

Guo, Mu and Chen [8] constructed the first two identity-based IBOOE schemes based on the IBE schemes of Boneh and Boyen [2] and Gentry [7]. Both IBOOE schemes were proven to be secure against chosen ciphertext attack (CCA) without random oracle. Subsequently, a more efficient IBOOE scheme than Guo et al.'s scheme [8] was proposed by Liu and Zhou [10]. They proved that their proposed scheme was CCA-secure in the random oracle model. However, Selvi, Vivek and Rangan [12,13] found that the scheme proposed by Liu and Zhou [10] actually was not CCA secure and gave a concrete example of an attack on confidentiality. The adversary could easily forge a ciphertext and distinguish the challenge message in the security proof. The authors also proposed a possible fix for the weakness in [10]. This notion has been extended to various areas such as attribute based encryption [9] and signcryption [18].

In an IBE system, the message space is quite limited such as in a cyclic group. To optimize the encryption system for any arbitrary message, one can make use of hybrid encryption. A useful tool called key encapsulation mechanism (KEM) was proposed by Cramer and Shoup [5] to build a hybrid encryption scheme. A KEM is similar to a public key encryption scheme, except that it encrypts a session key K instead of a message. The message is encrypted using the session key with a symmetry encryption system. Identity-based online/offline key encapsulation mechanism (IBOOKEM) is sufficient for practical applications. Therefore, with IBOOKEM, the main work is how to split the encryption into offline phase and online phase, where the identity of receiver only appears in the online phase.

The IBOOKEM was first proposed by Chow, Liu and Zhou [3]. It naturally requires that the KEM is able to divide into online phase and offline phase. Based on their IBOOKEM, they presented a CCA secure IBOOE scheme in the random oracle model and gave the general transformation from a one-way

IBOOKEM scheme into a CCA IBOOE scheme. However, Selvi, Vivek and Rangan [13] showed that there was one weakness in the proof of CCA security in [3], and hence, the scheme is insecure. Selvi, Vivek and Rangan [12,13] proposed a new provably CCA secure and efficient IBOOE scheme in the random oracle model. Subsequently, they revisited their IBOOE and constructed signcryption schemes [13]. A practical IBOOE scheme for wireless sensor network in the selective ID model was proposed by Chu et al. [4]. Recently, Hohenberger and Waters [9] proposed the first online/offline attribute based encryption (OOABE) scheme. Both schemes in their paper were selective chosen plaintext attack (CPA) secure.

A more efficient way to complete encryption and signature at the same time is signcryption. An, Dodis and Rabin [1] proposed online/offline signcryption. But they only gave the general security proof notions and did not give their constructions. Sun et al. [15] provided the definition of the identity-based online/offline signcryption and the corresponding security model. Based on the work by Sun et al., several online/offline signcryption schemes have been proposed in the literature [13,16,18,19].

1.1 Our Contribution

In this paper, we introduce a new semi-generic transformation to split the computation of identity into online and offline. Our transformation is *more efficient* than the previous transformation through the comparison in encryption computation and the ciphertext size. All the previous IBOOE schemes [3,10,12,13] applied the technique introduced by Guo, Mu and Chen [8]. To deal with identity, they require at least two group elements in $\mathbb{G}$ and one element in $\mathbb{Z}_p^*$ while we only need one group element in $\mathbb{G}$ and one element in $\mathbb{Z}_p^*$. We reduce one exponentiation operation in offline computation and save one group element in $\mathbb{G}$ both in offline storage and ciphertext length. We provide the security proof of our semi-generic transformation. We claim that the IBOOE schemes using our semi-generic transformation hold the same security level as in the original IBE schemes. Then we show a natural extension of IBE of Sakai and Kasahara [11], Boneh and Boyen [2], Gentry [7] and Waters [17] applying our transformation.

Organization of the Paper. In Section 2, we review some preliminaries including the definition of bilinear, identity-based online/offline encryption and the security model of IBOOE. Our semi-generic transformation, its security proof and a comparison are provided in Section 3. Four examples of IBOOE schemes converted by our transformation from the classical IBE schemes and our conclusion are presented in Section 4 and Section 5, respectively.

2 Preliminaries

In this section, we define bilinear pairing and identity-based online/offline encryption and then review the definition of security model for an IBOOE system. For simplicity, in this paper, we define an IBOOE as an IBOOKEM.

2.1 Bilinear Pairing

Let $\mathbb{G}$ be a cyclic group of prime order p and $\mathbb{G}_T$ be a multiplicative cyclic group of the same prime order p. Let g be a generator of $\mathbb{G}$. A bilinear pairing is a map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ with the following properties:

1. Bilinear: For all $u, v \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p^*$, we have $e\left(u^a, v^b\right) = e(u, v)^{ab}$.
2. Non-degeneracy: $e\left(g, g\right) \neq 1$.
3. Computability: It is efficient to compute $e\left(u, v\right)$ for all $u, v \in \mathbb{G}$.

2.2 Identity-Based Online/Offline Encryption

An identity-based online/offline encryption scheme consists of the following five algorithms:

Setup(λ): Taking a security parameter λ as input and returns the system parameters mpk and the master key msk. The system parameters mpk includes the descriptions of a finite key space $\mathcal{K}$, a finite message space $\mathcal{M}$ and a finite ciphertext space $\mathcal{CT}$. The system parameters are publicly known, while the master key is kept secretly and known to generator (PKG) only.

KeyGen(mpk, msk, ID): Taking mpk, msk and an arbitrary $ID \in \{0,1\}^*$ as input, returns a private key d_{ID} for ID. Here ID is an arbitrary string which will be used as a public key.

Off-Encrypt(mpk): Taking the system parameter mpk as input, outputs a pair $\left(C_{\text{off}}, K\right)$ where C_{off} is called offline ciphertext and K as the message encryption key.

On-Encrypt(mpk, C_{off}, ID): Taking the system parameters mpk, offline ciphertext C_{off} and an identity $ID \in \{0,1\}^*$ as input, returns a ciphertext CT for K.

Decrypt(mpk, CT, d_{ID}): Taking the system parameters mpk, ciphertext CT and the private key d_{ID} as input, outputs the session key K or a reject symbol $\perp$.

For correctness we require that if for every $(\mathsf{mpk}, \mathsf{msk})$ returned by **Setup(λ)**, every d_{ID} returned by **KeyGen(mpk, msk, ID)**, every $\left(C_{\text{off}}, K\right)$ returned by **Off-Encrypt(mpk)** and every CT returned by **On-Encrypt(mpk, C_{off}, ID)**, then **Decrypt(mpk, CT, d_{ID})** $= K$.

2.3 Security for IBOOE

The semantic security between a challenger and an adversary is defined as follows.

Setup: The challenger takes as input a secure parameter λ and runs the **Setup** algorithm. It gives the adversary $\mathcal{A}$ the system public parameters mpk.

Phase 1: $\mathcal{A}$ issues polynomially private key queries $q_1, \ldots, q_m$. The challenger responds by running key generation algorithm **KeyGen** to generate the private key d_{ID_i} corresponding to ID_i. It sends d_{ID_i} to $\mathcal{A}$. These queries may be asked adaptively, that is, each query q_i may depend on the replies to $q_1, \ldots, q_{i-1}$.

Challenge: Once $\mathcal{A}$ decides that Phase 1 is over, it outputs an identity ID^* on which it wishes to be challenged. $\mathcal{A}$ did not request a private key for ID^* in Phase 1. The challenger chooses a random bit $b \in \{0, 1\}$ and computes a challenge ciphertext CT^* and a session key K_0^* corresponding to ID^*. If $b = 0$, the challenger sends (CT^*, K_0^*) to $\mathcal{A}$. Otherwise, the challenger sends (CT^*, K_1^*) to $\mathcal{A}$, where K_1^* is a random section key from key space.

Phase 2: $\mathcal{A}$ issues more private key queries $q_{m+1}, \ldots, q_n$ on one restriction that $ID_i \neq ID^*$. The challenger responds the same as in Phase 1.

Guess: Finally, $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$ of b and wins the game if $b' = b$

We define adversary $\mathcal{A}$'s advantage in attacking the above game is

$$Adv_A(\lambda) = \left| \Pr[b = b'] - \frac{1}{2} \right|.$$

Definition 1. *An IBOOE system is semantically secure if for any polynomial time adversary $\mathcal{A}$, the function $Adv_A(\lambda)$ is negligible.*

3 Semi-Generic Transformation

In IBE system, the identity in ciphertext is embedded in some group elements. We refer to those group elements containing identity as ID header. Therefore, the ciphertext of IBE can be written as $CT = (\mathsf{Hdr}, C)$ where Hdr is called ID header and C is the other components of ciphertext excluding ID header.

The IBE schemes in the literature [2,7,11,17] have the same ID headers in the ciphertext, if we do not consider the group which the ID headers belong to. Their ID headers are defined as

$$\left(g_1 g^{ID}\right)^s,$$

where g_1, g are group elements of mpk and $s \in \mathbb{Z}_p^*$ is the random number chosen by the encryptor.

Without loss of generality, the encryption algorithm in IBE system can be written as follow:

$$\mathsf{Hdr} = \left(g_1 g^{ID}\right)^s, \qquad (C, K) \leftarrow \mathcal{E}(\mathsf{mpk}, s),$$

$$CT = (\mathsf{Hdr}, C) = \left(\left(g_1 g^{ID}\right)^s, C\right),$$

where K is the message encryption key and $\mathcal{E}$ is the encryption algorithm without the computation of ID header.

Based on the above scheme, we have the main task of IBOOE is to achieve the online/offline computation on the ID header. Obviously, there is a trivial method to achieve online/offline from IBE. We can compute $C_1 = g_1^s$, $C_2 = g^s$ in the offline phase and perform $C_3 = C_1 \cdot {C_2}^{ID}$ after one has obtained the identity in the online phase. However, one exponentiation operation is required in the online phase to achieve the online/offline encryption, which is still inefficient.

In the following parts of this session, we first revisit the online/offline computation on the ID header with structure $\mathsf{Hdr} = \left(g_1 g^{ID}\right)^s$. Then we give our improved semi-generic transformation that only needs two elements to deal with the ID header to achieve online/offline.

3.1 Previous Method of Transformation

We review how the authors dealt with the online/offline computation of the ID header in previous IBOOE schemes [3,8,12,13].

Off-Encrypt: Randomly choose $\alpha, \beta, s \in \mathbb{Z}_p^*$ and compute

$$C_1 = (g_1 g^{\alpha})^s, \quad C_2 = g^{s\beta},$$

$$(C, K) \leftarrow \mathcal{E}\left(\mathsf{mpk}, s\right).$$

Then output the offline ciphertext $C_{\text{off}} = \left(C_1, C_2, \alpha, \beta^{-1}, C\right)$ and the message encryption key K.

On-Encrypt: Upon receiving $ID \in \mathbb{Z}_p^*$, compute

$$C_3 = \beta^{-1}\left(ID - \alpha\right) \bmod p.$$

The ID header is $\mathsf{Hdr}_{\text{on}} = (C_1, C_2, C_3)$. Then output the ciphertext

$$CT = (\mathsf{Hdr}_{\text{on}}, C) = (C_1, C_2, C_3, C).$$

In the decryption algorithm, the receiver first recoves the general ID header in the traditional IBE scheme from the ID header as below:

$$C_1 \cdot {C_2}^{C_3} = (g_1 g^{\alpha})^s \cdot \left(g^{s\beta}\right)^{\beta^{-1}(ID-\alpha)} = \left(g_1 g^{ID}\right)^s.$$

It is the same as the ID header in IBE. Then, the receiver follows the general decryption procedures using its private key as in the traditional encryption scheme to obtain the key K. It needs three elements to handle the ID header.

3.2 Our Method of Transformation

We describe our method to achieve the online/offline encryption, where only two elements are required to deal with the ID header. It saves one group element compared to the previous method.

Off-Encrypt: Randomly choose $s, w \in \mathbb{Z}_p^*$ and compute

$$C_1 = (g_1 g^w)^s,$$

$$(C, K) \leftarrow \mathcal{E}(\mathsf{mpk}, s).$$

Then output the offline ciphertext $C_{\text{off}} = (C_1, w, s, C)$ and the message encryption key K.

On-Encrypt: Upon receiving $ID \in \mathbb{Z}_p^*$, compute

$$C_2 = s(ID - w) \bmod p.$$

The ID header is $\mathsf{Hdr}_{\text{on}} = (C_1, C_2)$. Then output the ciphertext

$$CT = (\mathsf{Hdr}_{\text{on}}, C) = (C_1, C_2, C).$$

Correctness: Given the ID header $\mathsf{Hdr}_{\text{on}} = (C_1, C_2)$, compute

$$C_1 g^{C_2} = (g_1 g^w)^s \cdot g^{s(ID-w)} = \left(g_1 g^{ID}\right)^s.$$

After recovering the original ID header, the recipient follows the general decryption procedures using its private key as in traditional identity-based encryption schemes to obtain the key K.

3.3 Security

Theorem 1. *The identity-based online/offline encryption scheme converted with our transformation is secure if the original identity-based encryption scheme is secure.*

Proof. Let $\mathcal{A}$ be an adversary that has advantage $\varepsilon(\lambda)$ against the IBOOE scheme converted using our transformation. Then, there is a simulator $\mathcal{B}$ that has advantage $\varepsilon(\lambda)$ against the original IBE.

We show how to construct a simulator $\mathcal{B}$ that uses $\mathcal{A}$ to gain advantage $\varepsilon(\lambda)$ against IBE in Fig.1. Here, we refer the IBE as the oracle. The IBE and the simulator $\mathcal{B}$ start the game with the IBE first running the **Setup** algorithm of IBE to generate the system public key mpk. As usual, $\mathbb{G}$ is a cyclic groups of prime order p, and g is the generator of $\mathbb{G}$. Random secret $a \in \mathbb{Z}_p^*$ is the master key and $g_1 = g^a$. The IBE gives mpk to simulator $\mathcal{B}$. Simulator $\mathcal{B}$ is supposed to output an identity ID^* and expects to receive back the IBE challenge ciphertext CT^* and the challenger session key K^* under mpk. Simulator $\mathcal{B}$ outputs its guess $b \in \{0, 1\}$ on K^*.

Simulator $\mathcal{B}$ works by interacting with adversary $\mathcal{A}$ as follows ($\mathcal{B}$ simulates the challenger for $\mathcal{A}$):

Setup: Simulator $\mathcal{B}$ gives mpk to $\mathcal{A}$ as the IBOOE system parameter.

Phase 1: The adversary $\mathcal{A}$ issues polynomially private key queries $q_1, \ldots, q_m$. For the query on ID_i from $\mathcal{A}$, $\mathcal{B}$ queries its private key to IBE, then forwards the results from IBE to $\mathcal{A}$. These queries may be asked adaptively.

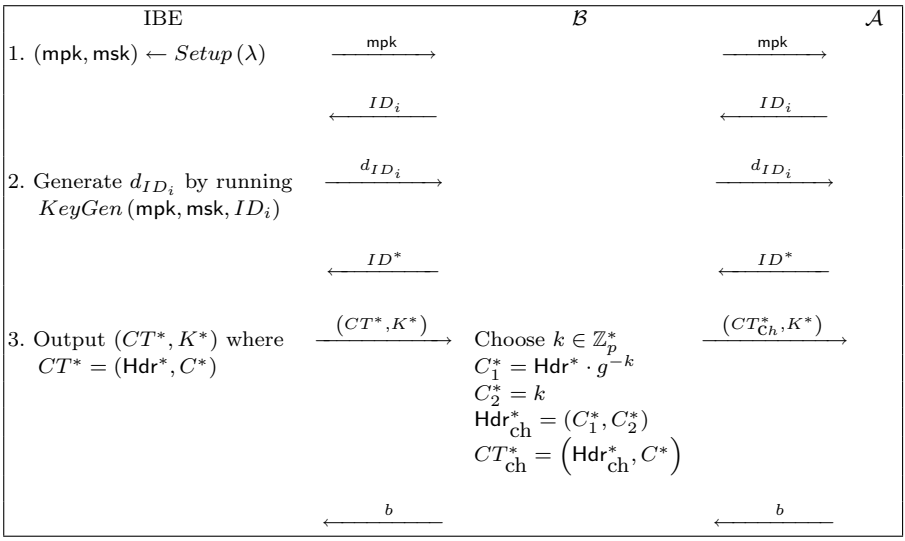

Fig. 1. Security Proof

Challenge: Once adversary $\mathcal{A}$ decides that Phase 1 is over, it outputs an ID^* on which it wishes to be challenged. Simulator $\mathcal{B}$ responds as follows:

1. $\mathcal{B}$ gives IBE the challenge identity ID^*. IBE responds with challenge ciphertext CT^* and the corresponding message encryption key K^* where

$$CT^* = (\mathsf{Hdr}^*, C^*) = \left(\left(g_1 g^{ID^*}\right)^s, C^*\right).$$

2. Next, $\mathcal{B}$ randomly chooses $k \in \mathbb{Z}_p^*$ and computes the challenge ID header:

$$\mathsf{Hdr}^*_{\mathrm{ch}} = (C_1^*, C_2^*) = \left(\mathsf{Hdr}^* \cdot g^{-k}, k\right) = \left(\left(g_1 g^{ID^*}\right)^s g^{-k}, k\right).$$

   Then, set the online/offline challenge ciphertext as $CT^*_{\mathrm{ch}} = \left(\mathsf{Hdr}^*_{\mathrm{ch}}, C^*\right)$. $\mathcal{B}$ responds to $\mathcal{A}$ with the online/offline challenge ciphertext $\left(CT^*_{\mathrm{ch}}, K^*\right)$.

Note that CT^*_{ch} is a valid IBOOE ciphertext under the identity ID^*. To see this, let $w = ID^* - \frac{k}{s}$, we have

$$C_1^* = \left(g_1 g^{ID^*}\right)^s g^{-k} = (g_1 g^w)^s, \quad C_2^* = k = s\,(ID^* - w).$$

Therefore,

$$\mathsf{Hdr}^*_{\mathrm{ch}} = (C_1^*, C_2^*) = \left((g_1 g^w)^s, s\,(ID^* - w)\right)$$

is a valid online/offline challenge ID header for the challenge identity ID^*.

Phase 2: $\mathcal{A}$ issues more private key queries $q_{m+1}, \ldots, q_n$ on one restriction that $ID_i \neq ID^*$. $\mathcal{B}$ responds as in Phase 1.

Guess: Finally, $\mathcal{A}$ outputs a guess $b \in \{0,1\}$ on K^*. Simulator $\mathcal{B}$ outputs b as its guess.

It is obvious that if the adversary $\mathcal{A}$ has advantage $\varepsilon(\lambda)$ to break the IBOOE scheme converted by our transformation, simulator $\mathcal{B}$ has advantage $\varepsilon(\lambda)$ to break the original IBE scheme.

3.4 Comparison

In an IBOOKEM system, there is no message to be encrypted. Therefore, it is important that how to efficiently compute ID header from KEM system to achieve IBOOKEM, which greatly affects the efficiency of IBOOKEM system. Here, we provide a comparison of computation cost of computing ID header and the ID header size among the traditional IBE, previous transformation and our transformation. We denote by E the exponentiation in group $\mathbb{G}$ and m_c the modular multiplication in $\mathbb{Z}_p^*$.

Table 1. Comparison of Computing ID header for IBOOE

	Traditional IBE	[8],[3],[12],[13]	[10]	Ours
Offline computation	/	3E	5E	2E
Online computation	2E	$1m_c$	$2m_c$	$1m_c$
Offline storage	/	$2\mathbb{G} + 2\mathbb{Z}_p$	$3\mathbb{G} + 4\mathbb{Z}_p$	$1\mathbb{G} + 2\mathbb{Z}_p$
Ciphertext size	$1\mathbb{G}$	$2\mathbb{G} + 1\mathbb{Z}_p$	$3\mathbb{G} + 2\mathbb{Z}_p$	$1\mathbb{G} + 1\mathbb{Z}_p$

From Table 1, it is clear that the online/offline encryption has a larger size of ID header than traditional IBE. However, the online/offline method can greatly reduce the online computation which is the motivation to use the online/offline encryption. Our semi-generic transformation of computing the ID deader is more efficient than the previous transformation to achieve identity-based online/offline encryption. The previous transformation requires two group elements in $\mathbb{G}$ and one element in $\mathbb{Z}_p^*$ to deal with identity while we only need one group element in $\mathbb{G}$ and one element in $\mathbb{Z}_p^*$. We reduce one exponentiation operation in the offline computation and save one group element in $\mathbb{G}$ both in offline storage and ciphertext length. We claim that the identity-based encryption schemes with this kind of ID header can be efficiently converted to online/offline encryption schemes by our method.

4 Identity Based Online/Offline Encryption Schemes

In this section, we give four examples applying our transformation to achieve the online/offline encryption from the classical identity-based encryption schemes

[2,7,11,17]. Four IBOOE schemes are given in the form of key encapsulation. Their security are easy to prove according to the original schemes. We omit their security proofs here. We also claim that the first example is a CPA-secure identity-based online/offline key encapsulation mechanism scheme with the shortest ciphertext.

4.1 IBOOE from Sakai-Kasahara IBE [11]

Setup: The system parameters are generated as follow. The PKG randomly chooses $\alpha \in \mathbb{Z}_p^*$ and sets $g_1 = g^\alpha$. Let $H_1 : \{0,1\}^* \to \mathbb{Z}_p^*$ be the cryptographic hash function. The public parameters mpk and msk are given by

$$\mathsf{mpk} = (\mathbb{G}, \mathbb{G}_T, q, g, g_1, H_1), \quad \mathsf{msk} = \alpha.$$

KeyGen: To generate the private key for $ID \in \{0,1\}^*$, PKG computes

$$d_{ID} = g^{\frac{1}{H_1(ID)+\alpha}}.$$

Off-Encrypt: Randomly choose $x, y \in \mathbb{Z}_p^*$ and compute

$$K = e(g,g)^x, \quad C_1 = (g_1 g^y)^x.$$

Output the offline ciphertext $C_{\text{off}} = (C_1, x, y)$ and the session key K. Note that $e(g,g)$ can be pre-computed by the PKG in **Setup** phase as part of the public parameters mpk. Thus, there is no pairing to be computed in the offline phase.

On-Encrypt: To generate a ciphertext for ID, compute

$$C_2 = x\left(H_1(ID) - y\right) \bmod p.$$

Output the ciphertext $CT = (C_1, C_2)$ corresponding to the session key K.

Decrypt: Upon receiving the ciphertext $CT = (C_1, C_2)$, to recover the session key, the recipient decrypts the ciphertext using the private key d_{ID} and computes

$$K = e\left(C_1 \cdot g^{C_2}, d_{ID}\right).$$

According to our transformation, it is easy to check its correctness

$$e\left(C_1 \cdot g^{C_2}, d_{ID}\right) = e\left(\left(g_1 g^{H_1(ID)}\right)^x, g^{\frac{1}{H_1(ID)+\alpha}}\right) = e(g,g)^x = K.$$

4.2 IBOOE from Boneh-Boyen IBE [2]

Setup: PKG randomly chooses a secret $a \in \mathbb{Z}_p$, generators $g, g_2, h_1 \in \mathbb{G}$ and sets $g_1 = g^a$. The system public parameters mpk and master key msk are

$$\mathsf{mpk} = (g, g_1, g_2, h_1), \quad \mathsf{msk} = g_2^a.$$

KeyGen: To generate the private key for $ID \in \mathbb{Z}_p$, PKG picks a random $r \in \mathbb{Z}_p$ and computes

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

Off-Encrypt: Randomly chooses $w, s \in \mathbb{Z}_p$, compute

$$K = e(g_1, g_2)^s, \quad C_1 = (h_1 g_1^w)^s, \quad C_2 = g^s.$$

Output the offline ciphertext $C_{\text{off}} = (C_1, C_2, w, s)$ and session key K.

On-Encrypt: To generate a ciphertext for an identity $ID \in \mathbb{Z}_p$, compute

$$C_3 = s\,(ID - w) \bmod p.$$

Then output the ciphertext $CT = (C_1, C_2, C_3)$ corresponding to the session key K.

Decrypt: To decrypt the ciphertext $CT = (C_1, C_2, C_3)$ for $ID \in \mathbb{Z}_p$ and recover the session key, the receiver uses its private key d_{ID} and computes

$$C_0 = C_1 \cdot g_1^{C_3} = \left(h_1 g_1^{ID}\right)^s, \quad K = \frac{e\,(d_1, C_2)}{e\,(C_0, d_2)}.$$

For a valid ciphertext, we have

$$\frac{e\,(d_1, C_2)}{e\,(C_0, d_2)} = \frac{e\left(g_2^a \left(h_1 g_1^{ID}\right)^r, g^s\right)}{e\left(\left(h_1 g_1^{ID}\right)^s, g^r\right)} = e(g_1, g_2)^s = K.$$

4.3 IBOOE from Gentry IBE [7]

Setup: PKG randomly chooses $a \in \mathbb{Z}_p$ and generators $g, h \in \mathbb{G}$ and sets $g_1 = g^a$. The system parameters mpk and the master key msk are

$$\mathsf{mpk} = (g, g_1, h), \quad \mathsf{msk} = a.$$

KeyGen: To generate the private key for $ID \in \mathbb{Z}_p$, PKG picks a random $r \in \mathbb{Z}_p$ and outputs

$$d_{ID} = (d_1, d_2) = \left(r, \left(h g^{-r}\right)^{\frac{1}{a - ID}}\right).$$

Off-Encrypt: Randomly choose $w, s \in \mathbb{Z}_p$ and compute

$$K = e(g, h)^{-s}, \quad C_1 = \left(g_1 g^{-w}\right)^s, \quad C_2 = e(g, g)^s.$$

Then output the offline ciphertext $C_{\text{off}} = (C_1, C_2, w, s)$ and session key K.

On-Encrypt: To generate a ciphertext for an identity $ID \in \mathbb{Z}_p$, the sender computes

$$C_3 = s\,(w - ID) \bmod p.$$

Then output the ciphertext $CT = (C_1, C_2, C_3)$ corresponding to the session key K.

Decrypt: To decrypt the ciphertext $CT = (C_1, C_2, C_3)$ with ID and recover the session key, the recipient computes

$$C_0 = C_1 \cdot g^{C_3} = \left(g_1 g^{-w}\right)^s \cdot g^{s(w-ID)} = \left(g_1 g^{-ID}\right)^s,$$

$$K = \frac{1}{e\left(C_0, d_2\right) \cdot {C_2}^{d_1}}.$$

4.4 IBOOE from Waters' Dual System IBE [17]

Setup: Let $\mathbb{G}$ be a group of prime order p. The PKG chooses generators $g, v, v_1, v_2, w, u, h \in \mathbb{G}$ and $a_1, a_2, b, \alpha \in \mathbb{Z}_p$. Let $\tau_1 = v v_1^{a_1}$, $\tau_2 = v v_2^{a_2}$. The system public parameters mpk and the master key msk are

$$\mathsf{mpk} = \left\{g^b, g^{a_1}, g^{a_2}, g^{b \cdot a_1}, g^{b \cdot a_2}, \tau_1, \tau_2, \tau_1^b, \tau_2^b, w, u, h, e(g,g)^{\alpha \cdot a_1 \cdot b}\right\},$$

$$\mathsf{msk} = \left\{g, g^{\alpha}, g^{\alpha \cdot a_1}, v, v_1, v_2\right\}.$$

KeyGen: To generate the private key for identity $ID \in \mathbb{Z}_p$, the PKG randomly chooses $r_1, r_2, z_1, z_2, tag_k \in \mathbb{Z}_p$. Let $r = r_1 + r$ and computes

$$D_1 = g^{\alpha \cdot a_1} v^r, \quad D_2 = g^{-\alpha} v_1^r g^{z_1}, \quad D_3 = \left(g^b\right)^{-z_1}, \quad D_4 = v_2^r g^{z_2}, \quad D_5 = \left(g^b\right)^{-z_2},$$

$$D_6 = g^{r_2 \cdot b}, \quad D_7 = g^{r_1}, \quad R = \left(u^{ID} w^{tag_k} h\right)^{r_1}.$$

The private key is

$$d_{ID} = \left(D_1, \ldots, D_7, R, tag_k\right).$$

Off-Encrypt: Choose random $s_1, s_2, t, x, tag_c \in \mathbb{Z}_p$ and let $s = s_1 + s_2$ and compute:

$$K = \left(e(g,g)^{\alpha \cdot a_1 \cdot b}\right)^{s_2}, \quad C_1 = \left(g^b\right)^{s_1 + s_2}, \quad C_2 = \left(g^{b \cdot a_1}\right)^{s_1}, \quad C_3 = \left(g^{a_1}\right)^{s_1},$$

$$C_4 = \left(g^{b \cdot a_2}\right)^{s_2}, C_5 = \left(g^{a_2}\right)^{s_2}, \quad C_6 = \tau_1^{s_1} \tau_2^{s_2},$$

$$C_7 = \left(\tau_1^b\right)^{s_1} \left(\tau_2^b\right)^{s_2} w^{-t}, \quad E_1 = \left(u^x w^{tag_c} h\right)^t, \quad E_2 = g^t.$$

Then output the offline ciphertext

$$C_{\text{off}} = \left(C_1, \ldots, C_7, E_1, E_2, tag_c\right)$$

and the session key K.

On-Encrypt: To generate a ciphertext for an identity $ID \in \mathbb{Z}_p$, compute

$$C_8 = t\left(ID - x\right) \bmod p.$$

Then output the ciphertext $CT = (C_1, \ldots, C_8, E_1, E_2, tag_c)$ corresponding to the session key K.

Decrypt: To decrypt the ciphertext $CT = (C_1, \ldots, C_8, E_1, E_2, tag_c)$ with ID, the receiver first checks tag_c, if $tag_c = tag_k$, outputs invalid. Otherwise, the receiver computes

$$E_3 = E_1 \cdot u^{C_8} = \left(u^x w^{tag_c} h\right)^t \cdot u^{t(ID-x)} = \left(u^{ID} w^{tag_c} h\right)^t,$$

$$\begin{aligned} A_1 &= e\left(C_1, D_1\right) \cdot e\left(C_1, D_1\right) \cdot e\left(C_1, D_1\right) \cdot e\left(C_1, D_1\right) \cdot e\left(C_1, D_1\right) \\ &= e(g,g)^{\alpha \cdot a_1 \cdot b \cdot s_2} e(v,g)^{b(s_1+s_2)r} e(v_1,g)^{a_1 b s_1 r} e(v_2,g)^{a_2 b s_2 r} \end{aligned}$$

Since $r = r_1 + r_2$, we have

$$A_2 = e\left(C_6, D_6\right) \cdot e\left(C_7, D_7\right) = e(v,g)^{b(s_1+s_2)r} e(v_1,g)^{a_1 b s_1 r} e(v_2,g)^{a_2 b s_2 r} e(g,w)^{-r_1 t},$$

$$A_3 = \frac{A_1}{A_2} = e(g,g)^{\alpha \cdot a_1 \cdot b \cdot s_2} e(g,w)^{r_1 t},$$

$$A_4 = \left(\frac{e\left(E_3, D_7\right)}{e\left(E_2, R\right)}\right)^{\frac{1}{tag_c - tag_k}} = e(g,w)^{r_1 t}.$$

Finally, the receiver can recover the session key by computing

$$K = \frac{A_3}{A_4}.$$

5 Conclusion

We proposed a semi-generic transformation to transform IBE into IBOOE. Our transformation is applicable to those IBE schemes whose ID header is $\left(g_1 g^{ID}\right)^s$. In comparison with traditional IBOOE schemes, our transformation saves one group element in both offline storage and ciphertext length and reduces one exponentiation operation in offline computation. We proved that our transformation is secure if the IBE scheme is secure. We presented four examples of IBE of Sakai and Kasahara [11], Boneh and Boyen [2], Gentry [7] and Waters [17] by applying our transformation.

References

1. An, J.H., Dodis, Y., Rabin, T.: On the security of joint signature and encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 83–107. Springer, Heidelberg (2002)
2. Boneh, D., Boyen, X.: Efficient selective-id secure identity-based encryption without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)

3. Chow, S.S.M., Liu, J.K., Zhou, J.: Identity-based online/offline key encapsulation and encryption. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2011, pp. 52–60 (2011)
4. Chu, C., Liu, J.K., Zhou, J., Bao, F., Deng, R.H.: Practical id-based encryption for wireless sensor network. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ASIACCS, pp. 337–340 (2010)
5. Cramer, R., Shoup, V.: Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM J. Comput. **33**(1), 167–226 (2003)
6. Even, S., Goldreich, O., Micali, S.: On-line/off-line digital signatures. J. Cryptology **9**(1), 35–67 (1996)
7. Gentry, C.: Practical identity-based encryption without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (2006)
8. Guo, F., Mu, Y., Chen, Z.: Identity-based online/offline encryption. In: Tsudik, G. (ed.) FC 2008. LNCS, vol. 5143, pp. 247–261. Springer, Heidelberg (2008)
9. Hohenberger, S., Waters, B.: Online/offline attribute-based encryption. In: Krawczyk, H. (ed.) PKC 2014. LNCS, vol. 8383, pp. 293–310. Springer, Heidelberg (2014)
10. Liu, J.K., Zhou, J.: An efficient identity-based online/offline encryption scheme. In: Abdalla, M., Pointcheval, D., Fouque, P.-A., Vergnaud, D. (eds.) ACNS 2009. LNCS, vol. 5536, pp. 156–167. Springer, Heidelberg (2009)
11. Sakai, R., Kasahara, M.: ID based cryptosystems with pairing on elliptic curve. IACR Cryptology ePrint Archive 2003, 54 (2003)
12. Selvi, S.S.D., Vivek, S.S., Rangan, C.P.: Identity based online/offline encryption scheme. IACR Cryptology ePrint Archive 2010, 178 (2010)
13. Selvi, S.S.D., Vivek, S.S., Rangan, C.P.: Identity based online/offline encryption and signcryption schemes revisited. In: Joye, M., Mukhopadhyay, D., Tunstall, M. (eds.) InfoSecHiComNet 2011. LNCS, vol. 7011, pp. 111–127. Springer, Heidelberg (2011)
14. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
15. Sun, D., Huang, X., Mu, Y., Susilo, W.: Identity-based on-line/off-line signcryption. In: IFIP International Conference on Network and Parallel Computing, NPC, pp. 34–41 (2008)
16. Sun, D., Mu, Y., Susilo, W.: A generic construction of identity-based online/offline signcryption. In: IEEE International Symposium on Parallel and Distributed Processing with Applications, ISPA, pp. 707–712 (2008)
17. Waters, B.: Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer, Heidelberg (2009)
18. Yan, F., Chen, X., Zhang, Y.: Efficient online/offline signcryption without key exposure. IJGUC **4**(1), 85–93 (2013)
19. Zhao, J., Zhao, X., Shi, Y.: Certificateless signcryption with online/offline technique. Journal of Computer Applications **34**, 2659–2663 (2014)