# Identity-Based Online/Offline Key Encapsulation and Encryption

Sherman S.M. Chow[1], Joseph K. Liu[2], and Jianying Zhou[2]

[1] Department of Computer Science
Courant Institute of Mathematical Sciences
New York University, NY 10012, USA
schow@cs.nyu.edu
[2] Institute for Infocomm Research
Singapore
{ksliu,jyzhou}@i2r.a-star.edu.sg

**Abstract.** An identity-based online/offline encryption (IBOOE) scheme splits the encryption process into two phases. The first phase performs most of the heavy computations, such as modular exponentiation or pairing over points on elliptic curve. The knowledge of the plaintext or the receiver's identity is not required until the second phase, where the ciphertext is produced by only light computations, such as integer addition/multiplication or hashing. This division of computations makes encryption affordable by devices with limited computation power since the preparation works can be executed "offline" or possibly by some powerful devices.
Since efficiency is the main concern, smaller ciphertext size and less burden in the computation requirements of all phases (i.e., both phases of encryption and the decryption phase) are desirable. In this paper, we proposed new schemes with improved efficiency over previous schemes by assuming random oracles. Our first construction is a very efficient scheme which is secure against chosen-plaintext attack (CPA), This scheme is slightly modified from an existing scheme. In particular, the setup and the user private key remain the same. We then proceed to propose the notion of *ID-based Online/Offline KEM* (IBOOKEM) that allows the key encapsulation process to be split into offline and online stages, in the same way as IBOOE does. We also present a generic transformation to get security against chosen-ciphertext attack (CCA) for IBOOE from any IBOOKEM scheme with one-wayness only. Our schemes (both CPA and CCA) are the most efficient one in the state-of-the-art, in terms of online computation and ciphertext size, which are the two main focuses of online/offline schemes. Our schemes are very suitable to be deployed on embedded devices such as smartcard or wireless sensor which have very limited computation powers and the communication bandwidth is very expensive.

## 1 Introduction

The notion of online/offline cryptographic algorithm was first introduced by Even, Goldreich and Micali [EGM], in the context of digital signature. With this notion, the signing process can be divided into two phases. The first phase is called *offline* phase which is executed prior to knowing the message to be signed and the second phase is called *online* phase which is performed after knowing the message. The online phase should be very fast and require only very light computation, such as integer multiplication or hashing. Other heavier computations such as modular exponentiation should be avoided in the online phase. Online/offline cryptographic schemes are thus particularly useful for low-power devices such as smartcards or wireless sensors. It may take a very long time, if not impossible, for these devices to execute heavy cryptographic computation. With this notion, these heavy computations can be done in the offline phase which can be carried out by other powerful devices instead.

### 1.1 Related Work

Several online/offline signature schemes [ST01,KSS06,CZSM07,Joy08] were proposed since the work of Even *et al.* in 1989. However, the first online/offline encryption scheme was proposed

by Guo, Mu and Chen [GMC08] nearly after two decades. One possible reason for this gap lies in how the public key is associated with the cryptographic object. A signature is bound to the signer's public key, which is obviously known to the signer; while there are many possibilities for the recipient's public key in encryption. It seems challenging to bundle the ciphertext with a public key by only "cheap" operations. Guo *et al.* did not directly tackle this challenge since their scheme were proposed in the context of identity-based encryption. The difference is that the ciphertext is addressed to an identity but not a public key. The offline phase of their schemes can be carried out *without* knowing the identity of the recipient.

### 1.2 Motivations

Nevertheless, we believe that identity-based (ID-based) online/offline encryption is worthy to be studied, from both the practical perspective and the cryptographic design perspective.

**Application.** First, ID-based system is particularly suitable for power-constrained devices. In an ID-based cryptosystem, encryption is done with respect to an arbitrary string corresponding to an identity (e.g., an email address, a device identifier). Only the entity who is "certified" by a trusted key generation center (KGC) will receive a private key for an identity string. This property gives the original motivation of ID-based cryptosystem [Sha84], which is to eliminate the necessity for checking the validity of certificates in traditional public key infrastructure (PKI). One only needs to know the recipient's identity in order to encrypt a message. It avoids the complicated and costly certificate (chain) verification for the authentication purpose, which is equivalent to at least *two* signature verifications in PKI-based encryption[3].

Consider a wireless sensor network (WSN) scenario, in which the sensors are collecting sensitive data, and is necessary to be encrypted before sending back to the base stations. To ensure timely and efficient delivery of sensitive information, online/offline encryption is a handy tool. Similar to the offline phase of the signature, it would be much better if part of the encryption process could be done *prior* to knowing the data to be encrypted *and* the recipient's public key or identity. The offline part (containing all heavy computations) can be done by a powerful device at the setup or manufacturing stage, which fits exactly with the offline stage of the online/offline encryption paradigm since (obviously) no data is collected and the identity of the base station maybe still unknown to the wireless sensor at this stage. Using an ID-based system, when there is a new node added to the network, other nodes do not need to have its certificate verified in order to communicate in a secure way. This can greatly reduce communication overhead and computation cost.

**Cryptographic Challenge.** The *de facto* standard of encryption scheme is indistinguishability against adaptive chosen-ciphertext attack (CCA), which the adversary can ask for the decryption of many ciphertexts except the one it is challenged with. When it comes to online/offline encryption, the division of the encryption algorithm into two stages may introduce extra vulnerability in its design. Indeed, we found out that [Cho09] the scheme recently proposed in [LZ09] is actually vulnerable to CCA attack[4].

While there exists generic transformations such as [FO99] which can build a CCA-secure scheme from a weaker one (e.g., with one-wayness). Due to the assumption of random oracle, these CCA-transformations are actually very efficient, in the sense that not much computational overhead is introduced in additional to the underlying scheme. However, they are not "online/offline"-aware,

[3] It may cost less than two signature verification for certified encryption [BFPW07], but the specific construction provided in [BFPW07] does not support offline preprocessing, specifically, all the exponentiations involved require the knowledge of the message to be encrypted and the identity and the public key of the recipient.

[4] Indeed, the authors of [LZ09] have reported the CCA attack discovered in [Cho09] and the corresponding fix in the presentation in ACNS 2009. The weakness of [LZ09] is recently made explicit in [SSC10].

i.e., the most expensive part of the encryption can only be done with the knowledge of the recipient and the message.

One may also consider using hybrid encryption to get an ID-based online/offline encryption scheme. Specifically, a key encapsulation mechanism (KEM) is firstly used to derive a session key, then a data encapsulation mechanism (DEM) is used to encrypt the message using the session key produced by the KEM. An obvious requirement that it is possible to divide the KEM into offline stage and inexpensive online stage, which is not formally studied in the ID-based setting. Moreover, a generic transformation borrowing a similar concept for getting CCA security [OP01] requires the underlying building block to support plaintext-check, which possibly translates to a strengthening of the underlying assumption. Specifically, the security reduction requires that a certain class of computational problem remains hard even given the access of the corresponding decisional oracle. This may render the security proof unfalsifiable, and possibly one may want to deploy the resulting online/offline system with a larger security parameter which leads to a lower operational efficiency. Ideally, it is desirable to enjoy the online/offline feature without affecting the underlying scheme.

Finally, we remark that one can transform an $\ell$-level semantic secure hierarchical IBE (HIBE) to an $(\ell - 1)$-level CCA-secure HIBE using a strong one-time signature (OTS) with the technique in [BCHK07]. However, our concern here is efficiency, and the involvement of an "extra" level in HIBE certainly degrades it, not to mention that the signing algorithm of the OTS scheme can only be done in the online stage, and possibly we need to use an online/offline OTS instead. To conclude, an efficient way to get CCA security which preserves the online/offline property of the underlying scheme is lacking.

### 1.3 Contribution

Our contribution is in two folds. First, we propose two efficient identity-based online/offline encryption (IBOOE) schemes. One is very efficient with CPA security while the another one achieves the *de facto* CCA security. Both our schemes can be proven secure in the random oracle model. As far as the authors know, there are only 4 IBOOE schemes in the literature. The first two were proposed by Guo *et al.* in [GMC08]. Although they satisfy the basic requirements, they are not very efficient. The first scheme (denoted by $\mathcal{GMC}^{\mathcal{BB}}$) requires 7 pairings to decrypt and the second scheme (denoted by $\mathcal{GMC}^{\mathcal{G}}$) produces very large (more than 6400 bits) ciphertext. Liu and Zhou [LZ09] proposed another IBOOE scheme (denoted by $\mathcal{LZ}$) in the random oracle model. Although the authors claimed that the scheme provides CCA security, it is later found that the scheme is actually CPA secure only [SSC10]. Recently Chu *et al.* [CLZ+10] also proposed another IBOOE scheme (denoted by $\mathcal{CLZBD}$) in the selective-ID model, in contrast to the standard adaptive-ID model.

When compared to all previous schemes, our schemes outperform in terms of efficiency. The online computation is the critical factor for any IBOOE scheme. Both our schemes only require 1 modular computation in the online stage, which are at least 50% faster than other schemes. The ciphertexts of our schemes are very small. The ciphertext of our CPA scheme is only 640 bits and that of our CCA scheme is just 800 bits, which is 30% smaller than $\mathcal{CLZBD}$, 3 times small than $\mathcal{GMC}^{\mathcal{BB}}$ or 8 times smaller than $\mathcal{GMC}^{\mathcal{G}}$. Moreover, both our schemes require only 1 pairings in decryption, which is the minimum among all (non-online/offline) efficient identity-based encryption schemes. Another desirable feature of our schemes is that they work with the setup of the non-online/offline version (in contrast to $\mathcal{LZ}$). The administrator and the users of a deployed system are free from the trouble of setting up the whole system again and arranging new user private keys for using our online/offline algorithms.

Second, we propose a new notion called *Identity-Based Online/Offline KEM* (IBOOKEM) which parallelizes the concept of IBOOE in a way that it splits the process of key encapsulation into offline and online stage. Similar to IBOOE, the receiver identity is not required in the offline stage. We provide an efficient instantiation of IBOOKEM and present a generic transformation from any IBOOKEM with one-wayness to CCA-secure IBOOE. Our CCA-secure IBOOE scheme is the result of this efficient transformation.

### 1.4 Organization

The rest of our paper is organized as follow. Some definitions will be given in Section 2. We present our CPA scheme in Section 3. Next we introduce the new notion of IBOOKEM and give an instantiation and generic transformation to CCA-secure IBOOE in Section 4. It is followed by the detail comparison between our schemes and other schemes in Section 5. Finally we conclude the paper in Section 6.

## 2 Definitions

### 2.1 Pairings and Related Intractability Assumption

Let $\mathbb{G}$ and $\mathbb{G}_T$ be an additive and a multiplicative cyclic group of prime order $q$. Let $P$ be a generator of $\mathbb{G}$. We define $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ to be a bilinear pairing if it has the following properties:

1. *Bilinearity*: For all $U, V \in \mathbb{G}$, and $a, b \in \mathbb{Z}$, $\hat{e}(aU, bV) = \hat{e}(U, V)^{ab}$.
2. *Non-degeneracy*: $\hat{e}(P, P) \neq 1$.
3. *Computability*: It is efficient to compute $\hat{e}(U, V)$ for all $U, V \in \mathbb{G}$.

**Definition 1 ($\ell$-Bilinear Diffie-Hellman Inversion ($\ell$-BDHI)).** *[BB04] The $\ell$-BDHI problem in $(\mathbb{G}, \mathbb{G}_T)$ is defined as follow: On input an $(\ell+1)$-tuple $(P, \alpha P, \alpha^2 P, \cdots, \alpha^\ell P) \in \mathbb{G}^{\ell+1}$, output $\hat{e}(P, P)^{\frac{1}{\alpha}} \in \mathbb{G}_T$. We say that the $(t, \epsilon, \ell)$-BDHI assumption holds in $(\mathbb{G}, \mathbb{G}_T)$ if no $t$-time algorithm has advantage at least $\epsilon$ in solving the $\ell$-BDHI problem in $(\mathbb{G}, \mathbb{G}_T)$.*

### 2.2 Framework and Security of ID-based Online/Offline Encryption

An ID-based online/offline encryption (IBOOE) scheme consists of the following five probabilistic polynomial time (PPT) algorithms:

- $(\mathsf{param}, \mathsf{msk}) \leftarrow \mathsf{Set}(1^k)$ takes a security parameter $k \in \mathbb{N}$ and generates $\mathsf{param}$, the global public parameters and $\mathsf{msk}$, the master secret key of the KGC.
- $D_{\mathsf{ID}} \leftarrow \mathsf{Ext}(1^k, \mathsf{param}, \mathsf{msk}, \mathsf{ID})$ takes a security parameter $k$, the global parameters $\mathsf{param}$, a master secret key $\mathsf{msk}$ and an identity $\mathsf{ID}$ to generate a secret key $D_{\mathsf{ID}}$ corresponding to this identity.
- $\bar{\mathfrak{C}} \leftarrow \mathsf{Enc}^{\mathsf{Off}}(1^k, \mathsf{param})$ takes a security parameter $k$ and the global parameters $\mathsf{param}$ to generate an offline ciphertext $\bar{\mathfrak{C}}$.
- $\mathfrak{C} \leftarrow \mathsf{Enc}^{\mathsf{On}}(1^k, \mathsf{param}, m, \bar{\mathfrak{C}}, \mathsf{ID})$ takes a security parameter $k$, the global parameters $\mathsf{param}$, a message $m$, an offline ciphertext $\bar{\mathfrak{C}}$, an identity $\mathsf{ID}$ to generate a ciphertext $\mathfrak{C}$.
- $(m / \perp) \leftarrow \mathsf{Dec}(1^k, \mathsf{param}, \mathfrak{C}, D_{\mathsf{ID}})$ takes a security parameter $k$, the global parameters $\mathsf{param}$, a ciphertext $\mathfrak{C}$, a secret key of the receiver $D_{\mathsf{ID}}$ to generate a message $m$, or a symbol $\perp$ which indicates the failure of decryption.

For simplicity, we omit the notation of $1^k$ and $\mathsf{param}$ from the input arguments of the above algorithms in the rest of this paper.

**Definition 2 (Chosen Plaintext Security (CPA)).** *An ID-based online/offline encryption scheme is semantically secure against chosen plaintext insider attack (IND-IOE-CPA) if no PPT adversary has a non-negligible advantage in the following game:*

1. *The challenger $\mathcal{C}$ runs $\mathsf{Set}$ and gives the resulting $\mathsf{param}$ to adversary $\mathcal{A}$. It keeps $\mathsf{msk}$ secret.*
2. *In the first stage, $\mathcal{A}$ makes a number of queries to the extraction oracle $\mathsf{OExt}(\cdot)$ simulated by $\mathcal{C}$. $\mathcal{A}$ submits an identity $\mathsf{ID}$ and gets the result of $\mathsf{Ext}(\mathsf{msk}, \mathsf{ID})$. These queries can be asked adaptively. That is, each query may depend on the answers of previous ones.*
3. *$\mathcal{A}$ produces two messages $m_0, m_1$ and an identity $\mathsf{ID}^*$. $\mathcal{C}$ chooses a random bit $b \in \{0, 1\}$ and computes an encrypted ciphertext $\mathfrak{C}^* = \mathsf{Enc}^{\mathsf{On}}(m_b, \mathsf{Enc}^{\mathsf{Off}}(), \mathsf{ID}^*)$. $\mathfrak{C}^*$ is sent to $\mathcal{A}$.*

4. *$\mathcal{A}$ makes a number of new queries as in the first stage with the restriction that it cannot query the extraction oracle with* $\mathsf{ID}^*$.
5. *At the end of the game, $\mathcal{A}$ outputs a bit $b'$ and wins if $b' = b$.*

*$\mathcal{A}$'s advantage is defined as* $\boldsymbol{Adv}^{\mathsf{IndIOE-CPA}}(\mathcal{A}) = |\Pr[b' = b] - \frac{1}{2}|$.

Next we give the definition of a higher security standard: chosen ciphertext security. The main difference is the additional decryption oracle query. The complete definition is given as follow:

**Definition 3 (Chosen Ciphertext Security (CCA)).** *An ID-based online/offline encryption scheme is semantically secure against chosen ciphertext insider attack (IND-IOE-CCA) if no PPT adversary has a non-negligible advantage in the following game:*

1. *The challenger $\mathcal{C}$ runs* $\mathsf{Set}$ *and gives the resulting* $\mathsf{param}$ *to adversary $\mathcal{A}$. It keeps* $\mathsf{msk}$ *secret.*
2. *In the first stage, $\mathcal{A}$ makes a number of queries to the following oracles simulated by $\mathcal{C}$:*
   (a) $\mathsf{OExt}(\cdot)$*: $\mathcal{A}$ submits an identity* $\mathsf{ID}$ *to the extraction oracle for the result of* $\mathsf{Ext}(\mathsf{msk}, \mathsf{ID})$.
   (b) $\mathsf{ODec}(\cdot,\cdot)$*: $\mathcal{A}$ submits a ciphertext $\mathfrak{C}$ and a receiver identity* $\mathsf{ID}$ *to the oracle for the result of* $\mathsf{Dec}(\mathfrak{C}, D_{\mathsf{ID}})$*. The result is made of a message if the decryption is successful. Otherwise, a symbol $\perp$ is returned for rejection.*

   *These queries can be asked adaptively. That is, each query may depend on the answers of previous ones.*
3. *$\mathcal{A}$ produces two messages $m_0, m_1$ and an identity* $\mathsf{ID}^*$*. $\mathcal{C}$ chooses a random bit $b \in \{0,1\}$ and computes an encrypted ciphertext* $\mathfrak{C}^* = \mathsf{Enc}^{\mathsf{On}}(m_b, \mathsf{Enc}^{\mathsf{Off}}(), \mathsf{ID}^*)$*. $\mathfrak{C}^*$ is sent to $\mathcal{A}$.*
4. *$\mathcal{A}$ makes a number of new queries as in the first stage with the restriction that it cannot query the decryption oracle with* $(\mathfrak{C}^*, \mathsf{ID}^*)$ *and the extraction oracle with* $\mathsf{ID}^*$.
5. *At the end of the game, $\mathcal{A}$ outputs a bit $b'$ and wins if $b' = b$.*

*$\mathcal{A}$'s advantage is defined as* $\boldsymbol{Adv}^{\mathsf{IndIOE-CCA}}(\mathcal{A}) = |\Pr[b' = b] - \frac{1}{2}|$.

### 2.3 Framework and Security of ID-based Online/Offline KEM

An ID-based online/offline KEM (IBOOKEM) consists of the following five probabilistic polynomial time (PPT) algorithms:

- $\mathsf{Set}$: same as IBOOE.
- $\mathsf{Ext}$: same as IBOOE.
- $\{\bar{\mathfrak{C}}, K\} \leftarrow \mathsf{KEM}^{\mathsf{Off}}(1^k, \mathsf{param}, r)$ takes a security parameter $k$, the global parameters $\mathsf{param}$ and a randomness $r$ from an appropriate space implicitly defined by the global public parameters, to generate an offline ciphertext $\bar{\mathfrak{C}}$ and a session key $K$.
  We require that for the same randomness $r$, the same session key $K$ should be generated. We make $r$ to be an explicit input of the algorithm for a more readable presentation of our transformation.
- $\mathfrak{C} \leftarrow \mathsf{KEM}^{\mathsf{On}}(1^k, \mathsf{param}, \bar{\mathfrak{C}}, \mathsf{ID})$ takes a security parameter $k$, the global parameters $\mathsf{param}$, an offline ciphertext $\bar{\mathfrak{C}}$, an identity $\mathsf{ID}$ to generate a ciphertext $\mathfrak{C}$.
- $(K/\perp) \leftarrow \mathsf{DeKEM}(1^k, \mathsf{param}, \mathfrak{C}, D_{\mathsf{ID}})$ takes a security parameter $k$, the global parameters $\mathsf{param}$, a ciphertext $\mathfrak{C}$, a secret key of the receiver $D_{\mathsf{ID}}$ to generate a key $K$ or $\perp$ which indicates failure of the process.

For simplicity, we omit the notation of $1^k$ and $\mathsf{param}$ from the input arguments of the above algorithms in the rest of this paper.

**Security of IBOOKEM.** The notions of CPA and CCA of IBOOKEM are similar to that for IBOOE, except that there are no challenge messages to encrypt. Instead, in the challenge phase the challenger chooses a random bit $b \in \{0,1\}$ and the adversary is given a ciphertext $\mathfrak{C}^*$ and a string $K^*$, which will be the session key encapsulated by the ciphertext if $b = 1$, or a random string from the key space if $b = 0$. The adversary makes adaptive decapsulation queries (for CCA security, except on $\mathfrak{C}^*$, once revealed), and eventually outputs a guess $b'$ for $b$.

We also define another lower level of security: one-wayness. For one-wayness, the adversary $\mathcal{A}$ is asked to output an identity $\mathsf{ID}^*$ after making extraction oracle queries. Then it is given a ciphertext $\mathfrak{C}^*$ and is asked to output a session key $K^*$. The adversary wins if the decapsulation of $\mathfrak{C}^*$ under the secret key of $\mathsf{ID}^*$ is equal to $K^*$ and $\mathsf{ID}^*$ is not submitted to the extraction oracle. Note that no decapsulation query is allowed in one-wayness. Schemes that are CPA or CCA secure are also one-wayness. $\mathcal{A}$'s advantage in breaking the one-wayness is defined as $\mathbf{Adv}^{\mathsf{IOKEM-OW}}(\mathcal{A}) = \Pr[\mathcal{A} \text{ wins }]$.

## 3 New CPA-Secure ID-Based Online/Offline Encryption

We first explain the intuition behind the design of our scheme. The ID-based private key of our scheme uses the exponent-inversion key of the IBE proposed by Sakai and Kasahara [SK03,CC05] ($\mathcal{SK} - \mathit{IBE}$ scheme). Since the identity string is mapped to a $\mathbb{Z}^q$ element, the offline stage essentially picks a random element as the identity, and stores a little additional information such that the online stage can be done by giving a value in $\mathbb{Z}^q$ which "converts" the random identity to the desired one.

### 3.1 Construction

Set: The KGC selects a generator $P \in \mathbb{G}$ and randomly chooses $s \in_R \mathbb{Z}_q^*$. It sets $P_{pub} = sP$. Define $\mathcal{M}$ to be the message space. Let $n_M = |\mathcal{M}|$. Also let $H_1 : \{0,1\}^* \to \mathbb{Z}_q^*$ and $H_2 : \{0,1\}^* \to \{0,1\}^{n_M}$ be some cryptographic hash functions. The public parameters $\mathsf{param}$ and master secret key $\mathsf{msk}$ are given by

$$\mathsf{param} = (\mathbb{G}, \mathbb{G}_T, q, P, P_{pub}, \mathcal{M}, H_1, H_2) \qquad \mathsf{msk} = s$$

Ext: To generate a secret key for a user with identity $\mathsf{ID} \in \{0,1\}^*$, the KGC computes:

$$D_{\mathsf{ID}} = (H_1(\mathsf{ID}) + s)^{-1} P$$

$\mathsf{Enc}^{\mathsf{Off}}$: Randomly generates $x, \alpha, \beta \in_R \mathbb{Z}_q^*$ and computes:

$$R \leftarrow \hat{e}(P,P)^x$$

$$T_0 \leftarrow x\Big(\alpha P + P_{pub}\Big)$$

$$T_1 \leftarrow x\beta P$$

$$c' \leftarrow H_2(R, T_1)$$

Outputs the offline ciphertext $\bar{\mathfrak{C}} = (T_0, T_1, (c', \alpha, \beta))$. Note that $\hat{e}(P,P)$ can be pre-computed by the KGC as part of the $\mathsf{param}$ so that no pairing is needed in this phase.

$\mathsf{Enc}^{\mathsf{On}}$: To encrypt a message $m \in \mathcal{M}$ to $\mathsf{ID}$, at the online stage, computes:

$$t_1' \leftarrow \beta^{-1}\Big(H_1(\mathsf{ID}) - \alpha\Big) \bmod q$$

$$c \leftarrow c' \oplus m$$

Outputs the ciphertext $\mathfrak{C} = (T_0, T_1, t_1', c)$.

Dec: To decrypt using secret key $D_{\mathsf{ID}}$, computes

$$R \leftarrow \hat{e}(T_0 + t_1' T_1,\ D_{\mathsf{ID}}) \qquad m \leftarrow c \oplus H_2(R, T_1)$$

and outputs $m$.

### 3.2 Security Analysis

**Theorem 1.** *Our IBOOE scheme is CPA-secure, assuming the $\mathcal{SK} - \mathcal{IBE}$ is also CPA-secure in the random oracle model.*

*Proof.* Assume there is an adversary $\mathcal{A}$ who can break the CPA-security of our scheme, we construct another adversary $\mathcal{B}$ to break the CPA-security of $\mathcal{SK} - \mathcal{IBE}$ scheme as described in [CC05].

The setup and the extraction oracle are the same as $\mathcal{SK} - \mathcal{IBE}$ scheme. Thus the challenger can forward the parameters from $\mathcal{SK} - \mathcal{IBE}$ to $\mathcal{A}$. It also forwards any extraction oracle request to the extraction oracle from $\mathcal{SK} - \mathcal{IBE}$.

We just need to show how to construct a challenge ciphertext of our scheme, from the challenge ciphertext of $\mathcal{SK} - \mathcal{IBE}$. Given a challenge ciphertext of $\mathcal{SK} - \mathcal{IBE}$ $\mathfrak{C}^* = \{X, C\}$, where

$$X = x(H_1(\mathsf{ID})P + P_{pub}), \qquad C = m^* \oplus H_4(\hat{e}(P,P)^x)$$

for a challenge message $m^*$ and some $x \in \mathbb{Z}_q^*$, we generate $\mathfrak{C}' = (T_0^*, T_1^*, t_1^*, c^*)$ as follows.

1. Pick a random $R \in \mathbb{G}$.
2. Pick a random $s \in \mathbb{Z}_q$.
3. Set $T_0^* = X - R$.
4. Set $T_1^* = sR$.
5. Set $t_1^* = 1/s$.
6. Set $c^* = C$.

It is a perfect simulation, as we can see from the following facts:

1. We express $R = rP$.

$$\begin{aligned} T_0^* &= X - R \\ &= x(H_1(\mathsf{ID})P + P_{pub}) - rP \\ &= x((H_1(\mathsf{ID}) - r/x)P + P_{pub}) \\ &= x(\alpha P + P_{pub}) \end{aligned}$$

   when we define $\alpha = H_1(\mathsf{ID}) - r/x$. Since $R$ is random, so does $\alpha$.
2.

$$\begin{aligned} T_1^* &= sR \\ &= srP \\ &= s(xH_1(\mathsf{ID}) - x\alpha)P \\ &= x\beta P \end{aligned}$$

   when we define $\beta = s(H_1(\mathsf{ID}) - \alpha)$. Such $\beta$ always exists since we are working in $\mathbb{Z}_q$. Moreover, since $\alpha$ is random, so does $\beta$.
3.

$$\begin{aligned} t_1^* &= 1/s \\ &= (H_1(\mathsf{ID}) - \alpha)/(\beta) \end{aligned}$$

4. $H_2(\hat{e}(P,P)^x, T_1^*) = H_4(\hat{e}(P,P)^x)$, which we can implicitly define in the random oracle model.

□

## 4 Online/Offline KEM with Generic Transformation to CCA

In this section, we propose a generic transformation from any IBOOKEM with one-wayness to IBOOE with CCA-security. We first give a generic transformation, then we give an efficient instantiation of the IBOOKEM.

### 4.1 Generic Transformation from IBOOKEM to IBOOE

Set: Same as the underlying IBOOKEM, except the system parameter also contains the descriptions of two additional hash functions $H$ and $H'$ which map any arbitrary string to some appropriate domains.[5]

Ext: Same as the underlying IBOOKEM.

$\mathsf{Enc}^{\mathsf{Off}}$: To generate an offline ciphertext, generate a randomness $r$ and computes:

$$(\bar{\mathfrak{C}}_{KEM}, K) \leftarrow \mathsf{KEM}^{\mathsf{Off}}(r)$$

Outputs the offline ciphertext $\bar{\mathfrak{C}} = \{\bar{\mathfrak{C}}_{KEM}, K, r\}$.

$\mathsf{Enc}^{\mathsf{On}}$: To encrypt a message $m \in \mathcal{M}$ to $\mathsf{ID}$, at the online stage, computes:

$$\mathfrak{C}_1 \leftarrow \mathsf{KEM}^{\mathsf{On}}(\bar{\mathfrak{C}}_{KEM}, \mathsf{ID})$$

$$\mathfrak{C}_2 \leftarrow H(K, \mathfrak{C}_1, m) \oplus r$$

$$\mathfrak{C}_3 \leftarrow H'(K, \mathfrak{C}_1) \oplus m$$

Outputs the ciphertext $\mathfrak{C} = \{\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3\}$.

Dec: To decrypt using secret key $D_{\mathsf{ID}}$, split $\{\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3\} \leftarrow \mathfrak{C}$ and computes:

$$(K/\perp) \leftarrow \mathsf{DeKEM}(\mathfrak{C}_1, D_{\mathsf{ID}})$$

If $\perp$ is the output, outputs $\perp$. Otherwise computes

$$m \leftarrow H'(K, \mathfrak{C}_1) \oplus \mathfrak{C}_3$$

Let $K' \leftarrow \mathsf{KEM}^{\mathsf{Off}}(\mathfrak{C}_2 \oplus H(K, \mathfrak{C}_1, m))$. If $K' = K$, outputs $m$. Otherwise outputs $\perp$.

**Security Analysis.**

**Theorem 2.** *Our IBOOE is CCA-secure in the random oracle model, assuming the underlying IBOOKEM is one-wayness.*

*Proof.* Setup: Assume there is an adversary $\mathcal{A}$ who can break the CCA-security of the IBOOE, we construct another adversary $\mathcal{B}$ to break the one-wayness of the underlying IBOOKEM.

The setup and the extraction oracle are the same as IBOOKEM scheme. Thus the challenger can forward the parameters from IBOOKEM to $\mathcal{A}$. It also forwards any extraction oracle request to the extraction oracle from IBOOKEM. In additional, the challenger $\mathcal{C}$ also simulates two random oracles $H$ and $H'$ as the normal way.

Decryption Oracle: Upon received a decryption request for a ciphertext $\{\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3\}$, the challenger does the following:

1. Retrieve $\{h_i\}$ from the table recording the input/output of random oracle $H$ such that
   - $h_i = H(K_i, \mathfrak{C}_1, m_i)$ and $m_i = \mathfrak{C}_3 \oplus H'(K_i, \mathfrak{C}_1)$,
   - the $K_i$ from $H$ random oracle is the same as the $K_i$ from $H'$ random oracle.
2. For every $\{h_i\}$ from the last step, check if $K_i = \mathsf{KEM}^{\mathsf{Off}}(\mathfrak{C}_2 \oplus h_i)$. If no such $K_i$ is found, output $\perp$. Otherwise output $H'(K_i, \mathfrak{C}_1) \oplus \mathfrak{C}_3$.

[5] We may also use some padding or encoding mechanism to make the bit length of $r$ as the same as the output of the hash function $H$.

Output: The challenger $\mathcal{C}$ received a challenged ciphertext $\mathfrak{C}'$ from IBOOKEM. $\mathcal{C}$ returns $\mathfrak{C}^* = \{\mathfrak{C}', \mathfrak{C}_2^*, \mathfrak{C}_3^*\}$ for some randomly picked $\mathfrak{C}_2^*$ and $\mathfrak{C}_3^*$ as the challenged ciphertext to $\mathcal{A}$. If $\mathcal{A}$ is able to win the game with non-negligible probability, it should query $H(K^*, \mathfrak{C}', m^*)$ and $H'(K^*, \mathfrak{C}')$ before outputting the bit $b'$. $\mathcal{C}$ randomly chooses a random oracle query and outputs the first component as the output to the game IBOOKEM.

Probability Analysis: If $\mathcal{A}$ does not make any query with $K^*$, it does not gain any advantage for the random guess. If it does, $\mathcal{C}$ succeeds with probability $1/q_H$. So the overall successful probability of $\mathcal{C}$ should be $\Pr[\mathcal{A}]/q_H$. □

### 4.2 Our IBOOKEM with One-Wayness

Set: The KGC selects a generator $P \in \mathbb{G}$ and randomly chooses $s \in_R \mathbb{Z}_q^*$. It sets $P_{pub} = sP$. Also let $H_1 : \{0,1\}^* \to \mathbb{Z}_q^*$ be a cryptographic hash function. The public parameters $\mathsf{param}$ and master secret key $\mathsf{msk}$ are given by

$$\mathsf{param} = (\mathbb{G}, \mathbb{G}_T, q, P, P_{pub}, H_1) \qquad \mathsf{msk} = s$$

Ext: To generate a secret key for a user with identity $\mathsf{ID} \in \{0,1\}^*$, the KGC computes:

$$D_{\mathsf{ID}} = (H_1(\mathsf{ID}) + s)^{-1} P$$

$\mathsf{KEM}^{\mathsf{Off}}$: For a random number $r \in \mathbb{Z}_q^*$, computes the session key as:

$$K \leftarrow \hat{e}(P, P)^r$$

To generate the offline ciphertext, first randomly generates $\alpha, \beta \in_R \mathbb{Z}_q^*$ and computes:

$$T_0 \leftarrow r\Big(\alpha P + P_{pub}\Big)$$

$$T_1 \leftarrow r\beta P$$

Outputs the offline ciphertext $\bar{\mathfrak{C}} = \{T_0, T_1, \alpha, \beta\}$ and the session key $K$.

$\mathsf{KEM}^{\mathsf{On}}$: To generate a ciphertext for $\mathsf{ID}$, at the online stage, computes:

$$t_1' \leftarrow \beta^{-1}\Big(H_1(\mathsf{ID}) - \alpha\Big) \bmod q$$

Outputs the ciphertext $\mathfrak{C} = (T_0, T_1, t_1')$.

DeKEM: To recover the session key using secret key $D_{\mathsf{ID}}$, computes

$$K \leftarrow \hat{e}(T_0 + t_1' T_1,\ D_{\mathsf{ID}})$$

**Security Analysis.** For completeness, we give a direct proof resembling that of [CC05] here, instead of reducing the one-wayness of our scheme to that of the underlying $\mathcal{SK} - \mathit{IBE}$ [SK03].

**Theorem 3.** *If there is an IOKEM-OW adversary $\mathcal{A}$ of the proposed scheme that succeeds with probability $\epsilon$, then there is a simulator $\mathcal{B}$ running in polynomial time that solves the $(\ell+1)$-BDHI problem with probability at least*

$$\epsilon \cdot \frac{1}{q_1}$$

*where $q_1$ is the number of queries allowed to the random oracle $H_1$ and we assume $q_1 = \ell$.*

*Proof.* Setup: Suppose $\mathcal{B}$ is given a random instance of the $(\ell+1)$-BDHI problem $(\hat{P}, \alpha\hat{P}, \alpha^2\hat{P}, \ldots, \alpha^{\ell}\hat{P}, \alpha^{\ell+1}\hat{P})$, $\mathcal{B}$ runs $\mathcal{A}$ as a subroutine to output $e(\hat{P},\hat{P})^{\frac{1}{\alpha}}$. $\mathcal{B}$ sets up a simulated environment for $\mathcal{A}$ as follow.

$\mathcal{B}$ first randomly selects $\pi \in_R \{1,\ldots,q_1\}$, $I_\pi \in_R \mathbb{Z}_q^*$ and $w_1, \ldots, w_{\pi-1}, w_{\pi+1}, \ldots, w_\ell \in_R \mathbb{Z}_q^*$. For $i \in \{1,\ldots,\ell\} \setminus \{\pi\}$, it computes $I_i = I_\pi - w_i$. Construct a polynomial with degree $\ell - 1$ as

$$f(z) = \prod_{i=1, i\neq\pi}^{\ell} (z + w_i)$$

to obtain $c_0, \ldots, c_{\ell-1} \in \mathbb{Z}_q^*$ such that $f(z) = \sum_{i=0}^{\ell-1} c_i z^i$. Then it sets generator $G = \sum_{i=0}^{\ell-1} c_i(\alpha^i\hat{P}) = f(\alpha)\hat{P}$.

For $i \in \{1,\ldots,\ell\}\backslash\{\pi\}$, $\mathcal{B}$ expands $f_i(z) = f(z)/(z+w_i) = \sum_{j=0}^{\ell-2} d_{i,j} z^j$ to obtain $d_{i,1}, \ldots, d_{i,\ell-2} \in \mathbb{Z}_q^*$ and sets

$$\tilde{H}_i = \sum_{j=0}^{\ell-2} d_{i,j}(\alpha^j\hat{P}) = f_i(\alpha)\hat{P} = \frac{f(\alpha)}{\alpha + w_i}\hat{P} = \frac{1}{\alpha + w_i}G$$

It randomly chooses $\hat{w} \in \{1,\ldots,\ell\} \setminus \{\pi\}$, and computes the public key $P_{pub}$ as

$$P_{pub} = -\alpha G - I_\pi G = (-\alpha - I_\pi)G$$

where $\alpha G = \sum_{i=0}^{\ell-1} c_i(\alpha^{i+1}\hat{P})$ so that its unknown master secret key $msk$ is implicitly set to $x = -\alpha - I_\pi \in \mathbb{Z}_q^*$, while public parameter $param$ are set to $(G, P_{pub})$ which are given to the adversary. For all $i \in \{1,\ldots,\ell\} \setminus \{\pi\}$, we have $(I_i, -\tilde{H}_i) = (I_i, \frac{1}{I_i+x}G)$.

Oracle Simulation: $\mathcal{B}$ first initializes a counter $\nu$ to 1 and starts $\mathcal{A}$. Throughout the game, we assume that $H_1$-queries are distinct, that the target identity $ID^*$ is submitted to $H_1$ at some point.

1. *Random Oracle:* For $H_1$-queries (we denote $ID_\nu$ the input of the $\nu^{th}$ one of such queries), $\mathcal{B}$ answers $I_\nu$ and increments $\nu$.
2. *Extraction Oracle:* On input $ID_\nu$, if $\nu = \pi$, $\mathcal{B}$ aborts. Otherwise, it knows that $H_1(ID_\nu) = I_\nu$ and returns $-\tilde{H}_\nu = (1/(I_\nu + x))G$.

Challenge: $\mathcal{A}$ outputs an identity $ID^*$ for which it never obtained $ID^*$'s private key. If $ID^* \neq ID_\pi$, $\mathcal{B}$ aborts. Otherwise it randomly selects $t'_1, \tilde{t}_0, \tilde{t}_1 \in_R \mathbb{Z}_q^*$ and computes $T_0 = \tilde{t}_0 G, T_1 = \tilde{t}_1 G$ to return the challenge ciphertext $\phi^* = (T_0, T_1, t'_1)$. Let $\xi = \tilde{t}_0 + t'_1\tilde{t}_1$ and $T = -\xi G$. Since $x = -\alpha - I_\pi$, we let $\rho = \frac{\xi}{\alpha}$, we can check that

$$\begin{aligned} T &= -\xi G \\ &= -\alpha\rho G \\ &= \rho(I_\pi + x)G \end{aligned}$$

which is a perfectly simulated ciphertext.

Output Calculation: $\mathcal{A}$ outputs a session key $K^*$, with probability $\epsilon$ it is in the right form, that is,

$$K^* = e(G,G)^\rho = e(G,G)^{-\xi/(I_\pi+x)} = e(\hat{P},\hat{P})^{f(\alpha)^2\xi/\alpha}$$

where $f(z) = \sum^* \ell - 1_{i=0} c_i z^i$ is the polynomial for which $G = f(\alpha)P$. The $(\ell+1)$-BDHI solution can be extracted by computing

$$\left(\frac{R^{1/\xi}}{e\Big(\sum_{i=0}^{\ell-2} c_{i+1}(\alpha^i\hat{P}), c_0\hat{P}\Big)e\Big(\sum_{j=0}^{\ell-2} c_{j+1}(\alpha^j)\hat{P}, G\Big)}\right)^{1/c_0^2}$$

$$= \left( \frac{e(\hat{P},\hat{P})^{f(\alpha)^2/\alpha}}{e(\hat{P},\hat{P})^{c_0(c_1+c_2\alpha+c_3\alpha^2+\ldots c_{\ell-1}\alpha^{\ell-2})} e(\hat{P},\hat{P})^{f(\alpha)(c_1+c_2\alpha+c_3\alpha^2+\ldots c_{\ell-1}\alpha^{\ell-2})}} \right)^{1/c_0^2}$$

$$= \left( \frac{e(\hat{P},\hat{P})^{f(\alpha)^2/\alpha}}{e(\hat{P},\hat{P})^{\frac{c_0(c_1\alpha+c_2\alpha^2+\ldots c_{\ell-1}\alpha^{\ell-1})+f(\alpha)(c_1\alpha+c_2\alpha^2+\ldots c_{\ell-1}\alpha^{\ell-1})}{\alpha}}} \right)^{1/c_0^2}$$

$$= e(\hat{P},\hat{P})^{\frac{f(\alpha)^2-(c_1\alpha+c_2\alpha^2+\ldots c_{\ell-1}\alpha^{\ell-1})(c_0+f(\alpha))}{{c_0}^2\alpha}}$$

$$= e(\hat{P},\hat{P})^{\frac{{c_0}^2}{{c_0}^2\alpha}}$$

$$= e(\hat{P},\hat{P})^{1/\alpha}$$

Probability Analysis: $\mathcal{B}$ only fails in providing a consistent simulation because one of the following independent events happen:

- $E_1$ : $\mathcal{A}$ does not choose to be challenged on $ID_\pi$.
- $E_2$ : A key extraction query is made on $ID_\pi$.

We have $\Pr[\neg E_1] = 1/q_1$ and $\neg E_1$ implies $\neg E_2$. Combining together, the overall successful probability $\Pr[\neg E_1]$ is at least

$$\frac{1}{q_1}$$

□

## 5 Comparison

We use $\mathcal{GMC}^{\mathcal{BB}}$ and $\mathcal{GMC}^{\mathcal{G}}$ to denote the schemes proposed in [GMC08], $\mathcal{LZ}$ and $\mathcal{CLZBD}$ to denote the schemes proposed in [LZ09] and [CLZ+10] respectively. We assume that $|\mathbb{G}| = 160$ bits, $|q| = 160$ bits, $|\mathbb{G}_T| = 1024$ bits and $|\mathcal{M}| = |q| = 160$ bits for the following comparison. We denote by $E$ the point multiplication in $\mathbb{G}$ or $\mathbb{G}_T$, $ME$ the multi-point multiplication in $\mathbb{G}$ or $\mathbb{G}_T$ (which costs about 1.3 times more than a single point multiplication), $M$ the multiplication in $\mathbb{G}$ or $\mathbb{G}_T$, $m_c$ the modular computation in $\mathbb{Z}_q$ and $SE$ the CCA secure symmetric key encryption.

| | $\mathcal{GMC}^{\mathcal{BB}}$ | $\mathcal{GMC}^{\mathcal{G}}$ | $\mathcal{LZ}$ | $\mathcal{CLZBD}$ | Our CPA scheme | Our CCA scheme |
|---|---|---|---|---|---|---|
| Offline computation | $5E + 2ME$ | $4E + 2ME$ | $4E + 1ME$ | $3E + 2ME$ | $3E + 1ME$ | $3E + 1ME$ |
| Online computation | $1M + 2m_c$ | $1M + 2m_c$ | $3m_c$ | $2m_c + SE$ | $1m_c$ | $1m_c$ |
| Offline storage (bits) | 2624 | 5056 | 2624 | 1248 | 800 | 1824 |
| Ciphertext length (bits) | 2144 | 6464 | 1280 | 1168 | 640 | 800 |
| Pairing in decryption | 7 | 2 | 2 | 4 | 1 | 1 |
| Security model | selective-ID | standard | random oracle | selective-ID | random oracle | random oracle |
| Security level | CCA | CCA | CPA | CCA | CPA | CCA |

**Table 1.** Comparison of computation cost and size

$\mathcal{GMC}^{\mathcal{BB}}$ requires an online/offline signature for encryption. For a fair comparison, we take a very efficient instantiation in [BB08]. The costs involved by [BB08] – 320 bits for offline storage

and for signature length, and 1 $E$ operation for the key generation and for the offline signing, have been added to the table.

Table 1 shows that our scheme achieves the best operational performance across all dimensions – the least computation and the smallest size in both offline storage and final ciphertext. Specifically, there are a number of significant improvements:

1. Online computation is the main focus of online/offline encryption. Our schemes (both CPA and CCA) only require 1 modular computation in the online stage. Our schemes do not require any multiplication ($M$ operation) or symmetric encryption in the online encryption stage. Modular computation ($m_c$ operation) is much faster than $M$ operation. Thus our online encryption stage is the fastest among all other schemes.
2. The offline storage is very small. For the CPA version, it is the smallest among all other schemes. It just requires 800 bits. For the CCA version, it is also smaller than $\mathcal{GMC}^{\mathcal{BB}}$ by 30% and about 3 times smaller than $\mathcal{GMC}^{\mathcal{G}}$. This result is important for embedded devices with very limited storage.
3. The ciphertexts of our schemes (both CPA and CCA) are the smallest among all other schemes. For the CPA scheme, it is about 50% smaller than $\mathcal{LZ}$, while for the CCA scheme, it is also 30% smaller than $\mathcal{CLZBD}$. When compared to $\mathcal{GMC}^{\mathcal{BB}}$ and $\mathcal{GMC}^{\mathcal{G}}$, the improvement is even greater. It is almost 3 times smaller than $\mathcal{GMC}^{\mathcal{BB}}$ and 8 times smaller than $\mathcal{GMC}^{\mathcal{G}}$. This improvement is very significant when the communication bandwidth is very limited, which is typical in the environment where computationally-limited devices are deployed.
4. Both our schemes only require 1 pairing operation in the decryption stage, which is the minimum requirement for any *efficient* identity-based encryption scheme in the state-of-the-art[6]. It is about 4 times less than $\mathcal{CLZBD}$. Although decryption is usually done in the server side with more computation power, this improvement will be significant for decryption of a huge number of ciphertexts as pairing is the most time and power consuming algorithm.

We remark that our security proof is given in the random oracle model. Theoretically speaking, schemes in the random oracle model is not as secure as those in the standard model; however, they still achieve an acceptable level of security. There are many applications that put efficiency as the most important factor. In these scenarios, schemes that are efficient but can be only proven secure in the random oracle model maybe a better choice.

In addition, we provide an optimized CPA version, for scenarios where CPA security is enough and CCA security maybe an overkill. The size of the ciphertext is just 640 bits and the offline storage is just 800 bits. It provides an excellent environment for those very lower power devices to carry out *secure enough* encryption.

## 6 Conclusion and Future Directions

We have proposed a new efficient identity-based online/offline encryption scheme. We provided two versions: a very efficient CPA version and the CCA version that achieves the highest security level. When compared to previous schemes, our scheme (both versions) enjoys a number of significant improvements in efficiency. These improvements allow our scheme to be used in many practical scenarios such as smart card and wireless sensor networks. Our scheme can be proven secure in the random oracle model.

Our study of the notion of identity-based online/offline key encapsulation mechanism, and the online/offline preserving CCA-transformation, may be of independent interests. Future research effort can be made in devising a very efficient KEM that is only one-way secure. Since our scheme is based on the widely used Sakai and Kasahara IBE [SK03,CC05],or more generally, the exponent-inversion framework [Boy07], applications are numerous. We leave the details of an online/offline ID-based signcryption scheme based on [BLMQ05], and an online/offline attribute-based encryption scheme based on [Boy07] as our future work.

[6] All *efficient* IBE schemes require pairing in the decryption stage. IBE schemes that do not require any pairing are still relatively inefficient.

## References


[BB04] Dan Boneh and Xavier Boyen. Efficient selective-ID secure identity-based encryption without random oracles. In *Proc. EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 223–238. Springer-Verlag, 2004.

[BB08] Dan Boneh and Xavier Boyen. Short signatures without random oracles the SDH assumption in bilinear groups. *Journal of Cryptology*, 2:149–177, 2008.

[BCHK07] Dan Boneh, Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. *SIAM J. Comput.*, 36(5):1301–1328, 2007.

[BFPW07] Alexandra Boldyreva, Marc Fischlin, Adriana Palacio, and Bogdan Warinschi. A closer look at PKI: Security and efficiency. In *Proc. PKC 2007*, volume 4450 of *Lecture Notes in Computer Science*, pages 458–475. Springer-Verlag, 2007.

[BLMQ05] Paulo S. L. M. Barreto, Benoît Libert, Noel McCullagh, and Jean-Jacques Quisquater. Efficient and provabley-secure identity-based signature and signcryption from bilinear maps. In *AsiaCrypt 2005*, volume 3788 of *Lecture Notes in Computer Science*, pages 515–532. Springer-Verlag, 2005.

[Boy07] Xavier Boyen. General *ad hoc* encryption from exponent inversion IBE. In *Proc. EUROCRYPT 2007*, volume 4507 of *Lecture Notes in Computer Science*, pages 394–411. Springer-Verlag, 2007.

[CC05] Liqun Chen and Zhaohui Cheng. Security proof of Sakai-Kasahara's identity-based encryption scheme. In *IMA Int. Conf.*, volume 3796 of *Lecture Notes in Computer Science*, pages 442–459. Springer, 2005.

[Cho09] Sherman S.M. Chow. Private communication happened before ACNS 2009, 2009.

[CLZ+10] Cheng-Kang Chu, Joseph K. Liu, Jianying Zhou, Feng Bao, and Robert H. Deng. Practical ID-based encryption for wireless sensor network. To appear in ASIACCS 2010, 2010. Also available at http://eprint.iacr.org/2010/002.

[CZSM07] Xiaofeng Chen, Fangguo Zhang, Willy Susilo, and Yi Mu. Efficient generic online/offline signatures without key exposure. In *ACNS 2007*, volume 4521 of *Lecture Notes in Computer Science*, pages 18–30. Springer-Verlag, 2007.

[EGM] Shimon Even, Oded Goldreich, and Silvio Micali.

[FO99] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *Proc. CRYPTO 99*, pages 537–554. Springer-Verlag, 1999. Lecture Notes in Computer Science.

[GMC08] Fuchun Guo, Yi Mu, and Zhide Chen. Identity-based online/offline encryption. In *Financial Cryptography and Data Security 2008*, volume 5143 of *Lecture Notes in Computer Science*, pages 247–261. Springer-Verlag, 2008.

[Joy08] Marc Joye. An efficient on-line/off-line signature scheme without random oracles. In *CANS 2008*, volume 5339 of *Lecture Notes in Computer Science*, pages 98–107. Springer, 2008.

[KSS06] Kaoru Kurosawa and Katja Schmidt-Samoa. New online/offline signature schemes without random oracles. In *PKC 2006*, volume 3958 of *Lecture Notes in Computer Science*, pages 330–346. Springer-Verlag, 2006.

[LZ09] Joseph K. Liu and Jianying Zhou. An efficient identity-based online/offline encryption scheme. In *ACNS*, volume 5536 of *Lecture Notes in Computer Science*, pages 156–167. Springer, 2009.

[OP01] Tatsuaki Okamoto and David Pointcheval. REACT: Rapid enhanced-security asymmetric cryptosystem transform. In *CT-RSA 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 159–175, 2001.

[Sha84] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Proc. CRYPTO 84*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer-Verlag, 1984.

[SK03] Ryuichi Sakai and Masao Kasahara. ID based cryptosystems with pairing on elliptic curve. Cryptology ePrint Archive, Report 2003/054, 2003. http://eprint.iacr.org/.

[SSC10] Sharmila Deva Selvi S, Sree Vivek S, and Pandu Rangan C. A note on the security identity based online/offline encryption scheme, 2010. Available at http://eprint.iacr.org/2010/178.

[ST01] Adi Shamir and Yael Tauman. Improved online/offline signature schemes. In *Proc. CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 355–367. Springer-Verlag, 2001.