Hierarchical Identity-Based Online/Offline Encryption

Zhongren Liu  
*Fujian Normal University*

Li Xu  
*Fujian Normal University*

Zhide Chen  
*Fujian Normal University*

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

Fuchun Guo  
*Fujian Normal University, fuchun@uow.edu.au*

Publication Details
Hierarchical Identity-Based Online/Offline Encryption

Abstract
The notion of identity-based online/offline encryption (IBOOE) was recently introduced by Guo, Mu and Chen in FC 2008. In an IBOOE system, the encryption is split into online and offline phases. The offline phase is performed prior to the arrival of a message and the recipient's public key (or, identity). The online phase is performed very efficiently after knowing the message and public key. The IBOOE scheme is particularly useful for devices that have very low computation power since part of computation is conducted while the device is not busy. In this paper, we extend the notion of IBOOE to the hierarchical identity-based online/offline encryption (HIBOOE), and propose a "selective-ID" secure HIBOOE scheme from Boneh, Boyen and Goh's HIBE, where the online phase in HIBOOE is very efficient.

Disciplines
Physical Sciences and Mathematics

Publication Details

This conference paper is available at Research Online: http://ro.uow.edu.au/infopapers/3191
Hierarchical Identity-Based Online/Offline Encryption

Zhongren Liu¹, Li Xu¹, Zhide Chen¹, Yi Mu² and Fuchun Guo¹

¹ School of Mathematics and Computer Science
Fujian Normal University, Fuzhou, China
zhongren88@163.com

² School of Computer Science and Software Engineering
University of Wollongong, Wollongong NSW 2522, Australia
ymu@uow.edu.au

Abstract

The notion of Identity-Based Online/Offline Encryption (IBOOE) was recently introduced by Guo, Mu and Chen in FC 2008. In an IBOOE system, the encryption is split into online and offline phases. The offline phase is performed prior to the arrival of a message and the recipient’s public key (or, identity). The online phase is performed very efficiently after knowing the message and public key. The IBOOE scheme is particularly useful for devices that have very low computation power since part of computation is conducted while the device is not busy. In this paper, we extend the notion of IBOOE to the Hierarchical Identity-Based Online/Offline Encryption (HIBOOE), and propose a “selective-ID” secure HIBOOE scheme from Boneh, Boyen and Goh’s HIBE, where the online phase in HIBOOE is very efficient.

Keywords: Identity based, encryption, online, offline.

1 Introduction

Identity Based Encryption (IBE) is a public key cryptosystem where any arbitrary string such as an email address or a telephone number can be utilized as a valid public key. The corresponding user private keys can only be computed by a trusted third party called the Private Key Generator (PKG) (who possesses a master secret key). The notion of identity based cryptography was first proposed by Shamir in 1984 [10]. This notion was later extended to IBE (e.g., [1, 3, 6, 12]). In a traditional IBE scheme, there is only one PKG that distributes private keys for users. To improve the efficiency of key generation, Horwitz and Lynn first introduced the notion of Hierarchical Identity-Based Encryption (HIBE) in [9]. HIBE is a generalization of IBE that mirrors an organizational hierarchy. In an HIBE system, there is a root PKG who has a master secret key, some domain PKGs, and users. The domain PKGs and users are all associated with their ID which are arbitrary strings. Root PKG generates a private key for the top-level domain PKG. The lower-level PKG requests a private key form their parent domain PKGs. Users ask for their private keys from their domain PKGs. It is noticed that several efficient HIBE schemes were proposed in [1, 2, 8, 11] with or without random oracles.

Recently, Guo, Mu and Chen [7] introduced the notion of identity-based online/offline encryption (IBOOE). The basic concept of online/offline encryption lies in splitting the encryption algorithm into two phases, the first phase is performed offline prior to the arrival of a message to be encrypted and a public key (identity ID). The second phase is performed online after knowing the message and ID. The online phase is typically very fast and the offline phase is designed to handle the most costly computation. This scheme is particularly useful for weak devices that do not have sufficient computation capacity.

In this paper, we extend the IBOOE to the Hierarchical Identity-Based Online/Offline Encryption (HIBOOE) and describe how to construct an HIBOOE scheme where the public key is a multi-tuple vector of domain identities. Although the IBOOE [7] scheme from Boneh-Boyen IBE can be extended to HIBOOE in a trivial way, the construction unfortunately results in a longer ciphertext and multiple modular computations in the online phase. In this paper, we construct a much more efficient HIBOOE from another HIBE [2], which was proposed by Boneh, Boyen and Goh in 2005 to construct the constant ciphertext of HIBE. Our HIBOOE scheme performs very efficiently in the online phase which requires two modular computations only and has a shorter ciphertext with $k + 4$ elements (where $k$ is the
Non-degeneracy: The adversary makes queries be two cyclic groups of prime order is one of the following: $G$ or any prefix of $ID$. 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 equal length plaintexts $M_0, M_1$ on which it wishes to be challenged. The challenger picks a random bit $b \in \{0, 1\}$ and sets $C = \text{Encrypt}(\text{params}, ID^*, M_b)$. It sends $C$ as the challenge to the adversary.

**Phase 2:** It is the same as **Phase 1** but with a constraint that the adversary makes a decryption query on $\langle C_i \rangle \neq \langle C \rangle$ for $ID^*$ or any prefix of $ID^*$.

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

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

$$Adv_{E,A} = \left| \Pr[b' = b] - \frac{1}{2} \right|.$$ 

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

**Definition 2** [1] We say that an HIBE system $E$ is $(t, q_{ID}, \epsilon)$-adaptively chosen plaintext secure if $E$ is $(t, q_{ID}, 0, \epsilon)$ adaptively chosen ciphertext secure. As shorthand, we say that $E$ is $(t, q_{ID}, \epsilon)$ IND-sID-CPA secure.

### 2.2 Bilinear Map

Let $G$ and $G_1$ be two cyclic groups of prime order $p$. Let $g$ be a generator of $G$. A map $e : G \times G \to G_1$ is called a bilinear map if this map satisfies the following properties:

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

### 2.3 Complexity Assumption

We briefly review the $\ell$-Decisional Bilinear Diffie-Hellman Inversion ($\ell$-DBDHI) problem and $\ell$-Weak Decisional Bilinear Diffie-Hellman Inversion ($\ell$-wDBDHI) problem [1, 2].
Definition 3 Let \( G \) and \( G_1 \) be two multiplicative groups of prime order \( p \). Let \( w \in G \) be a generator and \( \beta \in \mathbb{Z}_p^* \). Given elements \( w, w^{\beta}, w^{\beta^2}, \ldots, w^{\beta^s} \in G \), the \( \ell \)-wDBDH problem in \((G, G_1)\) is to decide whether a random value \( Z \in G_1 \) is equal to \( e(w, w)^{\beta} \) or not.

Definition 4 We say that the \((t, \epsilon, \ell)\)-wDBDH assumption holds in \((G, G_1)\) if no \( t \)-time algorithm has advantage at least \( \epsilon \) in solving the \( \ell \)-wDBDH problem in \((G, G_1)\).

Definition 5 Let \( G \) and \( G_1 \) be two multiplicative groups of prime order \( p \). Let \( g, h \in G \) be two generators and \( \alpha \in \mathbb{Z}_p^* \).

1. Given elements \( g, h, g^\alpha, g^{\alpha^2}, \ldots, g^{\alpha^s} \in G \), the \( \ell \)-wDBDH problem in \((G, G_1)\) is to decide whether a random value \( Z \in G_1 \) is equal to \( e(g, h)^{(\alpha^{s+1})} \) or not.

2. Given elements \( g, h, g^\alpha, g^{\alpha^2}, \ldots, g^{\alpha^s}, g^{\alpha^{s+2}}, \ldots, g^{\alpha^{2s}} \in G \), the \( \ell \)-wDBDH* problem in \((G, G_1)\) is to decide whether a random value \( Z \in G_1 \) is equal to \( e(g, h)^{(\alpha^{s+1})} \) or not.

Definition 6 We say that the \((t, \epsilon, \ell)\)-wDBDH* assumption holds in \((G, G_1)\) if no \( t \)-time algorithm has advantage at least \( \epsilon \) in solving the \( \ell \)-wDBDH* problem in \((G, G_1)\).

Definition 7 Let \( y_i = g^{\alpha_i} \in G^* \) and \( \overline{y}_{g,a,t} = (y_1, \ldots, y_t, y_{t+2}, \ldots, y_{2t}) \). An algorithm \( B \) has advantage \( \epsilon \) in solving \( \ell \)-wDBDH* in \( G \) if

\[
\left| Pr[B(g, h, \overline{y}_{g,a,t}, e(g, h)^{(\alpha^{s+1})}) = 0] - Pr[B(g, h, \overline{y}_{g,a,t}, e(g, h)^{(\alpha^{s+1})}) = 0] \right| \geq \epsilon,
\]

where the probability is over the random choice of generators \( g, h \in G^* \), the random choice of \( \alpha \) in \( \mathbb{Z}_p^* \), the random choice of \( T \in G^* \), and the random bits consumed by \( B \). We refer to the distribution on the left as \( \mathcal{P}_wDBDH^* \) and the distribution on the right as \( \mathcal{P}_wDBDH^* \).

3 HIBOOE from BBG-HIBE

3.1 Construction

Let \( G \) be a bilinear group of prime order \( p \) and let \( e : G \times G \rightarrow G_1 \) be a bilinear map. We assume that public keys (that is, identities \( ID \)) at level \( k \) are vectors of elements in \((\mathbb{Z}_p^*)^k \). We write \( ID = (I_1, \ldots, I_k) \in (\mathbb{Z}_p^*)^k \). The \( j \)-th component corresponds to the identity at level \( j \). If necessary, we extend the construction to public keys over \( \{0, 1\}^* \) by first hashing some components \( \{I_j \mid 1 \leq j \leq k\} \) using a collision resistant hash \( H : \{0, 1\}^* \rightarrow \mathbb{Z}_p^* \). We also assume that the messages to be encrypted are elements in \( G_1 \). The HIBE system works as follows:

Setup: To generate system parameters for an HIBE of maximum level \( \ell \), select a random generator \( g \in G^* \), a random \( a \in \mathbb{Z}_p \), and set \( g_1 = a^g \). Next, pick random elements \( g_2, g_3, h_1, \ldots, h_\ell \in G \). The public parameters and secret master-key are

\[
\text{params} = (g, g_1, g_2, g_3, h_1, \ldots, h_\ell),
\]

\[
\text{master-key} = g_2^a.
\]

KeyGen(\( ID_s, ID \)): To generate a private key \( d_{ID} \) for an identity \( ID = (I_1, \ldots, I_k) \in (\mathbb{Z}_p^*)^k \) of depth \( k \leq \ell \), using the master secret, pick a random \( r \in \mathbb{Z}_p \) and output

\[
d_{ID} = \left( g_2^r \cdot (h_1^{I_1} \cdots h_k^{I_k} \cdots g_3)^r \cdot g_\ell^{r+1}, \cdots, h_\ell^{r} \right)
\]

Note that \( d_{ID} \) becomes shorter as the depth of \( ID \) increases. The private key for \( ID \) can be generated incrementally, given a private key for the parent identity \( ID_{k-1} = (I_1, \ldots, I_{k-1}) \in (\mathbb{Z}_p^*)^{k-1} \), as required. Indeed, let

\[
d_{ID_{k-1}} = \left( g_2^r \cdot (h_1^{I_1} \cdots h_{k-1}^{I_{k-1}} \cdot g_3)^r \cdot g_\ell^{r+1}, \cdots, h_\ell^{r} \right)
\]

be the private key for \( ID_{k-1} \). To generate \( d_{ID} \), pick a random \( t \in \mathbb{Z}_p \) and output

\[
d_{ID} = \left( a_0^t \cdot b_k^{I_k} \cdot (h_1^{I_1} \cdots h_k^{I_k} \cdot g_3)^t \cdot a_1^t g_3^s, \right.
\]

\[
\left. b_{k+1}^{I_{k+1}}, \ldots, b_\ell^{I_\ell} \right).
\]

The private key is a properly distributed private key for \( ID = (I_1, \ldots, I_k) \) for \( r = r' + t \in \mathbb{Z}_p \).

Encrypt(\( \text{params}, ID, M \) ): We refer to the original BBG-HIBE as general encryption. It is not required in our HIBOOE, but since our HIBOOE decryption is associated with the BBG-HIBE, we outline the scheme as follows:

General Encryption: To encrypt a message \( M \in G_1 \) under the public key \( ID = (I_1, \ldots, I_k) \in (\mathbb{Z}_p^*)^k \), pick a random \( s \in \mathbb{Z}_p \) and output

\[
C_\mu = \left( e(g_1, g_2)^s \cdot M, g_3^s, (h_1^{I_1} \cdots h_k^{I_k} \cdot g_3)^s \right)
\]

\[
= (c_0, c_1, c_2).
\]

Online/Offline Encryption: We now describe our HI-
BOOEs, which is divided into two phases:

- Offline Encryption: Choose random \( s, \beta, \alpha_1, \cdots, \alpha_{\ell} \in \mathbb{Z}_p \), and output

\[
C_{o_f} = (e(g_1, g_2)^s, (g_3^{\alpha_1} h_1)^s, \cdots, (g_3^{\alpha_k} h_k)^s), \quad (g_3^{\beta}, g^s, g^s)
\]

Store the offline parameters \( C_{o_f}, \beta, \alpha_1, \cdots, \alpha_{\ell} \) for the online phase.

- Online Encryption: Given a message \( M \in \mathbb{G}_1 \) and the public key \( ID = (I_1, \cdots, I_k) \in (\mathbb{Z}_p^*)^k \), and output

\[
C_{o_n} = \left(c_0 \cdot M \cdot \beta^{-1}(1 - \sum_{i=1}^{k} \alpha_i I_i) \right) = (c_0, \nu_3).
\]

The ciphertext for \( ID \) is \( C = (c_0, c_1, \cdots, c_k, \nu_1, \nu_2, \nu_3) \), where

\[
C = \left(e(g_1, g_2)^s \cdot M, (g_3^{\alpha_1} h_1)^s, \cdots, (g_3^{\alpha_k} h_k)^s, \right)
\]

\[
(g_3^{\beta}, g^s, \beta^{-1}(1 - \sum_{i=1}^{k} \alpha_i I_i)).
\]

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. The length of ciphertext is \( k + 4(k \leq \ell) \), which is acceptable since the parameter \( \ell \) is limited.

Decryption\((d_{ID}, C)\): We describe our HIBOOE decryption and general decryption in this phase.

**HIBOOE Decryption:** Let \( C = (c_0, c_1, \cdots, c_k, \nu_1, \nu_2, \nu_3) \) to be a valid ciphertext for \( ID = (I_1, \cdots, I_k) \in (\mathbb{Z}_p)^k \). To decrypt \( C \) with \( d_{ID} \), compute

\[
c = (c_1)^{I_1} \cdots (c_k)^{I_k} \cdot (\nu_1)^{\nu_1}
\]

\[
= ((g_3^{\alpha_1} h_1)^s)^{I_1} \cdots ((g_3^{\alpha_k} h_k)^s)^{I_k} \cdot
\]

\[
(g_3^{\beta})^{\beta^{-1}(1 - \sum_{i=1}^{k} \alpha_i I_i)} = (g_3^{\alpha_1 h_1^{I_1} \cdots h_k^{I_k}} \cdot g_3^{1(1 - \sum_{i=1}^{k} \alpha_i I_i)})
\]

\[
= (h_1^{I_1} \cdots h_k^{I_k} \cdot g_3)^s.
\]

We then have \( (c_0, \nu_2, c) = (e(g_1, g_2)^s \cdot M, g^s, (h_1^{I_1} \cdots h_k^{I_k} \cdot g_3)^s) \), 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 as below.

**General Decryption:** We refer to the decryption process of the original BBG-HIBE as general decryption. Consider an identity \( ID = (I_1, \cdots, I_k) \). To decrypt a given ciphertext \( C_{o_n} = (c_0, c_1, c_2) \) using the private key \( d_{ID} = (a_0, a_1, b_{k+1}, \cdots, b_{\ell}) \), output

\[
c_0 \cdot e(a_1, c_2) / e(c_1, a_0) = M.
\]

Indeed, for a valid ciphertext, we have

\[
e(a_1, c_2) = \frac{e(g^s, (h_1^{I_1} \cdots h_k^{I_k} \cdot g_3)^s)}{e(c_1, a_0)} = \frac{1}{e(g_1, g_2)^s}.
\]

**3.2 Security**

We show that our HIBOOE scheme is selective identity secure (IND-sID-CPA) under the Decisional Bilinear Diffie-Hellman Inversion assumption. As mentioned in Section 2.3, we use a slightly weaker assumption called the Weak BDHI*.

**Theorem 3.1** Let \( \mathbb{G} \) be a bilinear group of prime order \( p \). Suppose the \((t, \epsilon, \ell)\)-wBDHI* assumption holds in \( \mathbb{G} \). Then the previously defined \( \ell \)-HIBOOE system is \((t', q_s, \epsilon)*\)-selective identity, chosen plaintext (IND-sID-CPA) secure for arbitrary \( \ell, q_s \), and \( t' < t - \Theta(\ell q_s) \), where \( \tau \) is the maximum time for an exponentiation in \( \mathbb{G} \).

**Proof Sketch.** Suppose \( A \) has advantage \( \epsilon \) in attacking the \( \ell \)-HIBOOE system. Using \( A \), we build an algorithm \( B \) that solve the \( \ell \)-wDBDHI* problem in \( \mathbb{G} \).

For a generator \( g \in \mathbb{G} \) and \( a \in \mathbb{Z}_p \), let \( y_i = g^{(a^i)} \) in \( \mathbb{G} \). Algorithm \( B \) is given as input a random tuple \((g, h, y_1, \cdots, y_\ell, y_{\ell+2}, \cdots, y_{2\ell}, T)\) that is either sampled from \( P_{wBDHI} \) (where \( T = e(g, h)^{(\alpha^s)} \)) or from \( R_{wBDHI} \) (where \( T \) is uniform and independent in \( \mathbb{G} \)). Algorithm \( B \)'s goal is to output 1 when the input tuple is sampled from \( P_{wBDHI} \) and 0 otherwise. We do not give the proof in detail here, due to the limitation of the length of the paper. Contact the authors if needed.

**Chosen Ciphertext Security.** Canetti [5] provided a general method of building an IND-sID-CCA secure \( \ell \)-HIBE from an IND-sID-CPA secure (\( \ell + 1 \))-HIBE. A more efficient construction is given by Boneh and Katz [4]. Applying these methods to our HIBOOE construction results in IND-sID-CCA secure \( \ell \)-HIBOOE for arbitrary \( \ell \).
4 Comparison

In a conventional HIBE, some components of ciphertext could also be pre-computed (naturally split an encryption into online/offline phases), but it is inefficient. Our HIBOOE scheme is much more efficient. We provide a comparison of computational cost in Table 1. Let “E” denote the exponentiation in $G$, “ME” denote the multie-exponentiation in $G$, “M” denote the modular computation. It’s clear that the algorithm “M” is much faster than “E”. We also assume that the message is encrypted under the public key $ID = (I_1, \cdots, I_\ell) \in (\mathbb{Z}_p^*)^\ell$.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>BBG-HIBE</th>
<th>Our HIBOOE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline phase</td>
<td>$(\ell + 3)E$</td>
<td>$\ell ME + 3E$</td>
</tr>
<tr>
<td>Store in offline</td>
<td>$\ell + 3$</td>
<td>$2\ell + 4$</td>
</tr>
<tr>
<td>Online phase</td>
<td>$\ell E$</td>
<td>$2M$</td>
</tr>
</tbody>
</table>

Table 1. This table presents a comparison of the related HIBE schemes under the IND-sID-CPA secure model. It shows that the online phase of our scheme is much more efficient than the conventional scheme.

5 Conclusion

In this paper, we extended the notion of Identity-based Online/offline Encryption to Hierarchical Identity-Based Online/Offline Encryption (HIBOOE) and proposed an efficient scheme, which is useful for devices with limited computational power. Our HIBOOE construction from BBG-HIBE [2] is provably secure without random oracles. In the encryption phase, the offline phase encryption can be run without the message to be encrypted and the public key (or ID) of a recipient and the online phase encryption is extremely efficient with only two modular computations.

Acknowledgement

This work is supported by National Natural Science Foundation of China (60502047), Education Bureau of Fujian Province (JA07030), Natural Science Foundation of Fujian Province (2008J0014) and Science and Technology of Fujian Province (2006F5036).

References


