Identity-Based Online/Offline Encryption

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

[1]University of Wollongong, Australia
ymu@uow.edu.au

[2]Fujian Normal University, Fuzhou, China
fuchunguo1982@gmail.com

Outline

Identity-based Encryption Review

Identity-based Encryption (IBE)

The notion was first proposed in 1984 by Shamir and there have been many efficient schemes since 2001, e.g.,

Boneh-Franklin IBE in 2001; Boneh-Boyen IBE in 2004;
Waters IBE in 2005; Gentry IBE in 2006;

- Simply the certificate management
- The public key is a piece of public information such as email address, ID number or telephone number
- The private key is computed by the (private key generator) PKG

Encryption

When Alice wants to send some sensitive data m to Bob, for secure, she must encrypt it first in a secure encryption system.

E.g.: A secure Identity-based Encryption system.

$$Alice \quad \overset{C(m)=E_{\text{``}Bob\text{''}}(m)}{- - - - - - - - - - - - \longrightarrow} \quad Bob$$

Encryption in a untrusted environment

- When Alice is home, she may just store the data in her secure PC.
- When Alice is outside, she may store her data in a convenient device with a limited computation power, such as a smartcard.
- The encryption must be achieved in the smartcard which is not powerful enough for efficient encryption

Need a better IBE

A more suitable identity-based encryption system for smartcard application should satisfy the property:

Part of the encryption process can be performed prior to knowing the data item and the public key of the recipient.

The real encryption process is very quick once the data item and the ID are known.

Identity-based Online/offline Encryption (IBOOE)

The encryption can be divided into two phases:

Offline Phase: Pre-computation *before* the data item and the public key are known.

Online Phase: Very efficient encryption *after* the data item and the public key are presented.

Identity-based Online/offline Encryption

Unfortunately ......

All previously published IBE schemes do not accommodate this feature

- Computation depends on the public key
- Cannot be naturally slitted into efficient online/offline phases

Our Contribution

1. We propose two IBOOE schemes from the two previous IBE schemes.

   Boneh-Boyen IBE: secure in the selective-ID model
   Gentry IBE: secure in the standard model

2. The computation in the *online* phase of our IBOOE is very efficient

Boneh-Boyen IBE

We only show its CPA construction for simplicity.
Let $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ be the bilinear map, $\mathbb{G}, \mathbb{G}_T$ be two cyclic groups of order p and g be the corresponding generator in $\mathbb{G}$.

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

$$params = \Big(g, g_1, g_2, h_1\Big), \qquad K = g_2^a.$$

Boneh-Boyen IBE

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

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

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

$$C_\mu = \left((h_1 g_1^{ID})^s, g^s, e(g_1, g_2)^s \cdot m\right) = (c_1, c_2, c_3)$$

“Natural" Online/offline Encryption

Let’s try to separate it into online and offline phases “naturally":

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

  $$C_{of} = \left(h_1^s, g_1^s, g^s, e(g_1, g_2)^s\right).$$

  Store the offline parameters C_{of} for the online phase.

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

  $$C_{on} = \left(h_1^s \cdot (g_1^s)^{ID}, e(g_1, g_2)^s \cdot m\right).$$

  The ciphertext for ID is C_ν and

  $$C_\nu = \left((h_1 g_1^{ID})^s, g^s, e(g_1, g_2)^s \cdot m\right).$$

Our Online/offline Encryption

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

$$C_{of} = \Big((h_1 g_1^{\alpha})^s, g_1^{s\beta}, g^s, e(g_1, g_2)^s \Big).$$

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

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

$$C_{on} = \Big(\beta^{-1}(ID - \alpha), e(g_1, g_2)^s \cdot m \Big).$$

The ciphertext for ID is C_ν, and

$$C_\nu = \Big((h_1 g_1^{\alpha})^s, g_1^{s\beta}, \beta^{-1}(ID - \alpha), g^s, e(g_1, g_2)^s \cdot m \Big)$$

Decryption

From Original Encryption:

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

From “Natural" Online/offline Encryption:

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

Decryption

Our Online/offline Encryption

$$C_\nu = \Big((h_1 g_1^{\alpha})^s,\ \ g_1^{s\beta},\ \ \beta^{-1}(ID-\alpha),\ \ g^s,\ \ e(g_1,g_2)^s \cdot m \Big).$$

$$(h_1 g_1^{\alpha})^s \cdot (g_1^{s\beta})^{\beta^{-1}(ID-\alpha)} = (h_1 g_1^{ID})^s$$

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

Therefore, the decryption of these three schemes is the same.

Analysis

“Natural" Online/offline Encryption

Online Phase:

$$C_{on} = \Big(h_1^s \cdot (g_1^s)^{ID}, e(g_1,g_2)^s \cdot m \Big).$$

The cost is one exponentiation + two multiplications

Our Online/offline Encryption

Online Phase:

$$C_{on} = \Big(\beta^{-1}(ID-\alpha), e(g_1,g_2)^s \cdot m \Big).$$

The cost is one modular computation + one multiplication

CCA secure

- The Boneh-Boyen IBE uses one-time strong signature scheme to achieve CCA secure.
- We can choose a proper signature scheme, such as Boneh-Boyen short signature, so that we can divide it into online/offline signature and the cost on *online* phase is only one modular computation.

Analysis (CCA)

“Natural" Online/offline Encryption

Online Phase:

$$C_{on} = \left(h_1^s \cdot (g_1^s)^{ID}, e(g_1, g_2)^s \cdot m, \sigma_{on}\right)$$

The cost is one exponentiation + two multiplications +one modular computation

Our Online/offline Encryption

Online Phase:

$$C_{on} = \left(\beta^{-1}(ID - \alpha), e(g_1, g_2)^s \cdot m, \sigma_{on}\right)$$

The cost is two modular computations + one multiplication

Gentry IBE

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

Setup:
Choose at random a secret $a \in \mathbb{Z}_p$, choose g, h_1, h_2, h_3 randomly from $\mathbb{G}$, and set the value $g_1 = g^a \in \mathbb{G}$. Choose a secure hash function $H : \{0, 1\}^* \rightarrow \mathbb{Z}_p$. The master public *params* and the master secret key K are

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

KeyGen

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

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

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

Encryption

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

$$\begin{aligned} C_\mu &= \left(g_1^s g^{-sID},\ e(g,g)^s,\ e(g,h_1)^{-s}\cdot m,\ e(g,h_2)^s e(g,h_3)^{sH_c}\right) \\ &= (c_1, c_2, c_3, c_4) \end{aligned}$$

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

Motivation
Identity-based Online/offline Encryption
Security
Conclusion

“Natural" Online/offline Encryption

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

$$C_{of} = \left(g_1^s, g^{-s}, e(g,g)^s, e(g,h_1)^{-s}, e(g,h_2)^s, e(g,h_3)^s\right).$$

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

$$C_{on} = \left(g_1^s \cdot (g^{-s})^{ID}, e(g,h_1)^{-s} \cdot m, e(g,h_2)^s \cdot (e(g,h_3)^s)^{H_c}\right),$$

  where the computation of H_c is the same as the general encryption and the ciphertext for ID is

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

Our Online/offline Encryption

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

$$C_{of} = \Big(g_1^s g^{-s\alpha}, g^{s\beta}, e(g,g)^s, e(g,h_1)^{-s}, e(g,h_2)^s e(g,h_3)^{s\gamma}, e(g,h_3)^{s\theta} \Big)$$

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

$$C_{on} = \Big(\beta^{-1}(\alpha - ID), e(g,h_1)^{-s} \cdot m, \theta^{-1}(H_c - \gamma) \Big),$$

  where H_c is the hash value of all elements and C_ν is

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

Decryption

General Encryption:

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

Natural Online/offline Encryption

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

Decryption

Our Online/offline Encryption

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

$$g_1^s g^{-s\alpha} \cdot (g^{s\beta})^{\beta^{-1}(\alpha - ID)} = g_1^s g^{-sID}$$

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

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

Therefore, the decryptions for all three are the same.

Motivation
Identity-based Online/offline Encryption
Security
Conclusion

Analysis

Natural Online/offline Encryption

Online Phase:

$$C_{on} = \Big(g_1^s \cdot (g^{-s})^{ID}, e(g,h_1)^{-s} \cdot m, e(g,h_2)^s \cdot (e(g,h_3)^s)^{H_c}\Big).$$

The cost is two exponentiations + three multiplications

Our Online/offline Encryption

Online Phase:

$$C_{on} = \Big(\beta^{-1}(\alpha - ID), e(g,h_1)^{-s} \cdot m, \theta^{-1}(H_c - \gamma)\Big).$$

The cost is two modular computations + one multiplication

Fuchun Guo, Yi Mu, Zhide Chen Identity-Based Online/Offline Encryption

Security

The proof for the two schemes are similar, we just take the IBOOE based on Gentry IBE as the example.

	Gentry IBE & IBOOE
Private Key	same
Encryption	different
Decryption	actually same

Therefore, we just show that the simulator can simulate

the challenge ciphertext C_ν for IBOOE
from
the challenge ciphertext C_μ for Gentry IBE.

Ciphertext

Gentry IBE

$$C_\mu = \left(g_1^s g^{-sID},\ e(g,g)^s,\ e(g,h_1)^{-s} \cdot m,\ e(g,h_2)^s e(g,h_3)^{sH_c}\right)$$

Our Online/offline Encryption

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

Simulation

Gentry IBE   *IBOOE*

$$g_1^s g^{-sID} \quad \Rightarrow \quad g_1^s g^{-s\alpha}, g^{s\beta}, \beta^{-1}(\alpha - ID)$$

Given $g_1^s g^{-sID}$, randomly choose $k_1, k_2 \in \mathbb{Z}_p$ and output

$$g_1^s g^{-s\alpha} = \left(g_1^s g^{-sID}\right)^{\frac{k_1}{k_1+k_2}} \qquad g^{s\beta} = \left(g_1^s g^{-sID}\right)^{\frac{1}{k_1+k_2}} \qquad \beta^{-1}(\alpha - ID) = k_2$$

Motivation
Identity-based Online/offline Encryption
Security
Conclusion

Analysis

$$\left(g_1^s g^{-sID}\right)^{\frac{k_1}{k_1+k_2}} \qquad \left(g_1^s g^{-sID}\right)^{\frac{1}{k_1+k_2}} \qquad k_2$$

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

$$\left(g_1^s g^{-sID}\right)^{\frac{k_1}{k_1+k_2}} = g_1^s g^{-s\alpha} \qquad \left(g_1^s g^{-sID}\right)^{\frac{1}{k_1+k_2}} = g^{s\beta} \qquad k_2 = \beta^{-1}(\alpha - ID)$$

Fuchun Guo, Yi Mu, Zhide Chen Identity-Based Online/Offline Encryption

Simulation

Gentry IBE *IBOOE*

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

In Gentry IBE, the simulator can simulate $e(g,h_2)^s e(g,h_3)^{sH_c}$ because it can simulate $e(g,h_2)^s$, $e(g,h_3)^s$ and H_c.

Therefore, randomly choose $\gamma, \theta \in \mathbb{Z}_p$, we can simulate $e(g,h_2)^s e(g,h_3)^{s\gamma}, e(g,h_3)^{s\theta}, \theta^{-1}(H_c-\gamma)$ from $e(g,h_2)^s$, $e(g,h_3)^s$ and H_c too.

Analysis

Gentry IBE

$$C_\mu = \left(g_1^s g^{-sID},\ e(g,g)^s,\ e(g,h_1)^{-s}\cdot m,\ e(g,h_2)^s e(g,h_3)^{sH_c}\right)$$

Our Online/offline Encryption

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

1. We can simulate IBOOE based on the simulation of Gentry IBE without any additional requirements.
2. Therefore, IBOOE achieve the same leave of security to Gentry IBE.

Comparison

E: the exponentiation in $\mathbb{G}$;
M: the multiplication in $\mathbb{G}$;
m: the modular computation in $\mathbb{Z}_p$.

Scheme	Boneh-Boyen IBOOE	Gentry IBOOE
Online (natural)	1E+2M+1m	2E+3M
Online (ours)	1M+2m	1M+2m

When the data is pre-encrypted in the *offline* phase, the *online* phase can be much more efficient and requires only one modular computation.

Conclusion

1. We introduced a new notion of Identity-Based Online/offline Encryption (IBOOE).
2. IBOOE schemes are useful where the computational power of a device is limited.
3. We presented two IBOOE schemes based on two existing IBE schemes, such that online encryption is extremely efficient.