An Efficient Identity Based Online/Offline Encryption Scheme

Sharmila Deva Selvi S, Sree Vivek S, Pandu Rangan C

Theoretical Computer Science Lab,
Department of Computer Science and Engineering,
Indian Institute of Technology Madras,
Chennai, India-600036

Abstract. Consider the situation where a low power device with limited computational power has to perform cryptographic operation in order to do secure communication to the base station where the computational power is not limited. The most obvious way is to split each and every cryptographic operations into resource consuming, heavy operations (which are performed when the device is idle) and the fast light weight operations (which are executed on the fly). This concept is called online/offline cryptography. In this paper, we show the security weakness of an identity based online offline encryption scheme proposed in ACNS 09 by Liu et al. [7]. The scheme in [7] is the first identity based online offline encryption scheme in the random oracle model, in which the message and recipient are not known during the offline phase. We have shown that this scheme is not CCA secure. We have also proposed a new identity based online offline encryption scheme in which the message and receiver are not known during the offline phase and is efficient than the scheme in [7]

Keywords: Identity Based Cryptography, Encryption, Online/Offline, Cryptanalysis, Random Oracle Model.

1 Introduction

Seperating the process of signing or encrypting into two phases namely, online phase and offline phase is the concept of "Online/Offline" cryptography. This notion was first introduced in the context of digital signatures by Even, Goldreich and Micali [4]. Their construction is inefficient as it increases the size of each signature by a quadratic factor. Shamir and Tauman [9] proposed an improved version which makes use of a new paradigm called "hash-sign-switch" to design more efficient online/offline signature schemes. During the offline phase most of the heavy computations like exponentiation and bilinear pairing are done and in the online phase in-order to make the execution faster, only light weight integer operations (multiplication and addition) and hashing are performed. In an online/offline signature scheme the message is not known in the offline phase and in an online/offline encryption scheme both the message and receiver are not known in the offline phase. Thus, online/offline schemes find use in low power devices such as PDA's, sensor networks, hand held devices including mobile phones and smart-cards.

Adi Shamir [8] introduced the concept of identity based cryptography and proposed the first identity based signature scheme. The idea of identity based cryptography is to enable an user to use any arbitrary string that uniquely identifies him as his public key. Identity based cryptography serves as an efficient alternative to Public Key Infrastructure (PKI) based systems. Most of the identity based encryption (IBE) schemes use the costly bilinear pairing operation and the concept of online/offline computation is an important area of research with respect to IBE. The first identity based online/offline encryption scheme was proposed by Guo et al.[6]. It should be noted that, the major difference between online/offline signature and encryption schemes is that, the receiver is not known during the offline phase in encryption schemes. This makes it subtle and interesting to explore for new directions in constructing efficient and elegant online/offline encryption schemes. Few motivating examples for online/offline encryption schemes can be found in [6] and [7].

Guo et al. [6] have shown natural extension of the IBE of Boneh and Boyen [1] and Gentry [5]. They have also given constructions which efficiently divide the IBE schemes in [1] and [5]. All the schemes are in the standard model. In 2009, Joseph. K. Liu et al. [7] have proposed an identity based online/offline encryption scheme. It was proved to be chosen ciphertext (CCA) secure in the random oracle model and was claimed to be much efficient that the scheme in [6] (obviously true due to random oracle assumption). Recently, Chow et al. in [2] proposed a CPA secure identity based online/offline encryption scheme and have given a KEM (Key Encapsulation Mechanism) based CCA construction. Although they are giving a generic transformation from identity based online/offline KEM (IBOOKEM) to CCA secure identity based online/offline encryption, there is no concrete IBOOKEM scheme discussed in the paper. Hence, we do not compare our results with the results reported in [2].

Our Contribution: In this paper, we show that the scheme in [7] is not CCA secure, i.e. an adversary can distinguish the challenge ciphertext with accessing the decryption oracle. We provide a fix for the bug in the scheme and also propose a new efficient construction for identity based online/offline encryption. We prove the new scheme in the random oracle model and claim that ours is the only existing identity based online/offline encryption scheme secure in the random oracle model.

2 Preliminaries

2.1 Bilinear Pairing

Let $\mathbb{G}_1$ be an additive cyclic group generated by P, with prime order q, and $\mathbb{G}_2$ be a multiplicative cyclic group of the same order q. Let $\hat{e}$ be a bilinear pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$.

2.2 Computational Assumptions

In this section, we recall the computational assumptions related to bilinear maps[3] that are relevant to the security of our scheme.
Modified BDHI for k values (k-mBDHIP) :k-mBDHIP is the bilinear variant of the k-CAA problem. Given $(P, aP, (x_1 + a)^{-1}P, ..., (x_k + a)^{-1}P) \in \mathbb{G}_1^{k+2}$ for unknown $a \in Z_q{}^*$ and known $x_1, ..., x_k \in Z_q{}^*$, the k-mBDHIP problem is to compute $\hat{e}(P, P)^{(a+x^*)^{-1}}$ for some $x^* \notin \{x_1, ..., x_k\}$.

Definition 1. *The advantage of any probabilistic polynomial time algorithm $\mathcal{A}$ in solving the k-mBDHIP problem in $\mathbb{G}_1$ is defined as*

$$\begin{aligned} Adv_{\mathcal{A}}{}^{k-mBDHIP} &= Pr[\mathcal{A}(P, aP, (x_1 + a)^{-1}P, ..., (x_k + a)^{-1}P, x_1, ..., x^k) \\ &= \hat{e}(P, P)^{(a+x^*)^{-1}} | a, x^* \in_R Z_q{}^*, \ x^* \notin \{x_1, ..., x_k\}]. \end{aligned}$$

We say that the k-mBDHIP problem is (t, ϵ) hard if for any t time probabilistic algorithm $\mathcal{A}$, the advantage $Adv_{\mathcal{A}}{}^{k-mBDHIP} < \epsilon$.

3 Identity Based Online/Offline Encryption Schemes(IBOOE)

3.1 Generic Model

An identity based online/offline encryption scheme consists of the following algorithms.

- ***Setup***(1^κ) *:* Given a security parameter κ, the Private Key Generator(PKG) generates a master private key msk and public parameters $Params$. $Params$ is made public while msk is kept secret by the PKG.
- ***Extract***(ID) *:* Given an identity ID, the PKG executes this algorithm to generate the private key D_{ID} corresponding to ID and transmits D_{ID} to the user with identity ID via. secure channel.
- ***Off-Encrypt*** $(Params)$ *:* To generate the offline share of the encryption, this algorithm is executed without the knowledge of message to be encrypted and the receiver of the encryption. The offline ciphertext is represented as ϕ.
- ***On-Encrypt*** (m, ID_A, ϕ) *:* For encrypting a message m to user with identity ID_A, any sender can run this algorithm to generate the encryption σ of message m. This algorithm uses a new offline ciphertext ϕ and generates the full encryption σ.
- ***Decrypt***(σ, ID_A, D_A) *:* For decryption of σ, the receiver ID_A uses his private key D_A and run this algorithm to get back the message m.

3.2 Security Model

Definition 2. *An ID-Based online/offline encryption scheme is said to be indistinguishable against adaptive chosen ciphertext attacks (IND-IBOOE-CCA2) if no polynomially bounded adversary has a non-negligible advantage in the following game.*

1. ***Setup :*** The challenger $\mathcal{C}$ runs the *Setup* algorithm with a security parameter κ and obtains public parameters $Params$ and the master private key *msk*. $\mathcal{C}$ sends $Params$ to the adversary $\mathcal{A}$ and keeps *msk* secret.
2. ***Phase I :*** The adversary $\mathcal{A}$ performs a polynomially bounded number of queries. These queries may be adaptive, i.e. current query may depend on the answers to the previous queries.
   - ***Key extraction queries(Oracle*** $\mathcal{O}_{Extract}(ID)$***) :*** $\mathcal{A}$ produces an identity ID and receives the private key D_{ID}.
   - ***Decryption queries(Oracle*** $\mathcal{O}_{Decrypt}(\sigma, ID_A)$***) :*** $\mathcal{A}$ produces the receiver identity $ID_{\mathbb{A}}$ and the ciphertext σ. $\mathcal{C}$ generates the private key D_A and sends the result of $Decrypt(\sigma,\ ID_A,\ D_A)$ to $\mathcal{A}$. This result will be "$Invalid''$ if σ is not a valid ciphertext or the message m if σ is a valid encryption of message m to ID_A.
3. ***Challenge :*** $\mathcal{A}$ chooses two plaintexts, m_0 and m_1 and the receiver identity $ID_{\mathbb{R}}$, on which $\mathcal{A}$ wishes to be challenged. $\mathcal{A}$ should not have queried for the private key corresponding to $ID_{\mathbb{R}}$ in Phase I. $\mathcal{C}$ chooses randomly a bit $b \in \{0, 1\}$, computes $\sigma = Encrypt(m_b,\ ID_{\mathbb{R}})$ and sends it to $\mathcal{A}$.
4. ***Phase II :*** $\mathcal{A}$ is now allowed to get training as in $Phase-I$. During this interaction, $\mathcal{A}$ is not allowed to extract the private key corresponding to $ID_{\mathbb{R}}$. Also, $\mathcal{A}$ cannot query the decryption oracle with $\sigma, ID_{\mathbb{R}}$ as input, i.e. $\mathcal{O}_{Decrypt}(\sigma,\ ID_{\mathbb{R}})$.
5. ***Guess :*** Finally, $\mathcal{A}$ produces a bit $b^{'}$ and wins the game if $b^{'} = b$.

$\mathcal{A}^{'}\ s$ advantage is defined as Adv($\mathcal{A}$) $= 2\left|Pr\left[b^{'} = b\right] - 1\right|$ *where* $Pr\left[b^{'} = b\right]$ denotes the probability that $b^{'}$ $= b$.

4 Review and Attack of Liu et al. Identity Based Online/Offline Encryption Scheme(L-IBOOE) [7]

In this section we review the identity based online/offline encryption scheme proposed in [7].

4.1 Review of L-IBOOE Scheme [7]

Let $\mathbb{G}$ and $\mathbb{G}_T$ be groups of prime order q , and let $\hat{e}$:$\mathbb{G}\ \times\ \mathbb{G}_T\ \rightarrow\ \mathbb{G}_T$ be the bilinear pairing. We use a multiplicative notation for the operation in $\mathbb{G}$ and $\mathbb{G}_T$.
Setup: The PKG selects a generator $P \in \mathbb{G}$ and randomly chooses $s,\ w \in \mathbb{Z}_q^*$. It sets $P_{pub} = sP$, $P_{pub}^{'} = s^2P$ and $W = (w+s)^{-1}P$. Define $\mathcal{M}$ to be the message space. Let $n_M = \mid \mathcal{M} \mid$. Let H_2:{0,1}* $\times\ \mathbb{G}_T \rightarrow \mathbb{Z}_q^*$ and H_3:{0,1}* $\rightarrow$ {0,1}^{n_M} be two hash functions. The public parameters $Params$ and master private key msk are given by,

$$Params = \langle \mathbb{G},\ \mathbb{G}_T,\ q,\ P_{pub},\ P_{pub}^{'},\ W,\ w,\ \mathcal{M},\ H_1,\ H_2,\ H_3\rangle\ msk = s.$$

Extract(ID):
- $q_{ID} = H_1(ID)$
- $D_{ID} = \dfrac{1}{q_{ID}+s}P$.

Off-Encrypt($Params$**):**
- $u,\ x,\ \alpha,\ \beta,\ \gamma,\ \delta \in_R \mathbb{Z}_q^*$
- $U = W$- uP
- $R = \hat{e}(wP+\ P_{pub}, P)^x$
- $T_0 = x(w\ \alpha P\ +\ (w+\ \gamma)P_{pub} + P_{pub}^{'})$
- $T_1 = xw\beta P$.
- $T_2 = x\delta P_{pub}$.
- Output the offline ciphertext $\phi = \langle u, x, \alpha, \beta, \gamma, \delta, U, R, T_0, T_1, T_2\rangle$.

On-Encrypt(m, ID_A, ϕ**):**
- $t_1 = \beta^{-1}(H_1(ID_A)$- $\alpha)$ mod q
- $t_2 = \beta^{-1}(H_1(ID_A)$- $\gamma)$ mod q
- $t = H_2(m,\ R)x+u$ mod q
- $c = H_3(R)\oplus\ m$
- Output the ciphertext $\sigma = \langle U, T_0, T_1, T_2, t, t_1, t_2, c\rangle$

Decrypt(σ,ID_A, D_A):
- $R = \hat{e}(T_0 + t_1 T_1 + t_2 T_2,\ D_A)$
- $m = c \oplus H_3(R)$
- and checks for $R^{H_2(m,R)} \stackrel{?}{=} \hat{e}(tP + U,\ wP + P_{pub})\ \hat{e}(P,P)^{-1}$
- outputs m if equal. Otherwise outputs $\perp$

4.2 Attack on confidentiality

During the confidentiality game, after the completion of Phase-1 of training, the adversary $\mathcal{A}$ picks two messages, (m_0, m_1) of equal length and an identity $ID_{\mathbb{R}}$($D_{\mathbb{R}}$ is not known to $\mathcal{A}$), and submits THEM to $\mathcal{C}$. $\mathcal{C}$ chooses a bit $b \in_R \{0,1\}$, generates the challenge ciphertext $\sigma^* = \langle U,\ T_0, T_1,\ T_2,\ t_1^{'}, t_2^{'}, t, \ c\rangle$ of message m_b and gives σ^* to $\mathcal{A}$. Now, we show that $\mathcal{A}$ can cook up another valid ciphertext δ= (U^*, T_0^*, T_1^*, T_2^*, t_1^*, t_2^*, t^*, c^*) as given below:

- Chooses r^*, t_1^*, $t_2^* \in_R \mathbb{Z}_q^*$.
- Computes $U^* = U$ - $r^* P$ = W- (u+ r^*)P.
- Chooses T_1^*, $T_2^* \in_R \mathbb{G}$.
- Computes $T_0^* = T_0$ - $(t_1^* T_1^* + t_2^* T_2^*)$ +$(t_1 T_1 + t_2 T_2) = x(w+s)(q_A+s)$P-$(t_1^* T_1^* + t_2^* T_2^*)$
  (since $T_0 + t_1 T_1 + t_2 T_2 = x(w+s)(q_A+s)$P).
- Computes $t^* = t + r^* \bmod q$
- Sets $c^* = c$
- Now, $\mathcal{A}$ queries the decrypt oracle with δ as input during $Phase-2$ of training. Here, the relations between σ^* and δ are $R = R^* = \hat{e}(P,P)^{(w+s)x}$ and $c = c^*$. Hence, the decryption of δ will give the message $m_b = c \oplus H_3(R) = c^* \oplus H_3(R^*)$. So, $\mathcal{A}$ can obtain m_b by constructing δ from σ^* and querying the decrypt oracle with δ as input (which is allowed in the security model of [7], i.e. δ is totally different from the challenge ciphertext). The only restriction for $\mathcal{A}$ during Phase - 2 is that $\mathcal{A}$ should not query the decryption of the challenge ciphertext σ^* and the extract of $ID_{\mathbb{R}}$. Also, it should be noted that the check ${R^*}^{H_2(m_b,R^*)} \stackrel{?}{=} \hat{e}(t^*P + U^*,\ wP + P_{pub})\ \hat{e}(P,P)^{-1}$ should hold.

  Proof of Correctness: The equality of R and R^* can be shown by,

$$\begin{aligned}
R^* &= \hat{e}(T_0^* + t_1^*T_1^* + t_2^*T_2^*, D_R) \\
&= \hat{e}(x(w+s)(q_R+s)P - (t_1^*T_1^* + t_2^*T_2^*) + t_1^*T_1^* + t_2^*T_2^*, D_R) \\
&= \hat{e}(x(w+s)(q_R+s)P, D_R) \\
&= \hat{e}(x(w+s)(q_R+s)P, \frac{1}{q_R+s}P) \\
&= \hat{e}(x(w+s)P, P) \\
&= \hat{e}((w+s)P, xP) \\
&= \hat{e}(wP + P_{pub}, P)^x \\
&= R
\end{aligned}$$

  Also, the derived ciphertext δ will pass the verification test, which can be shown as,

$$\begin{aligned}
\hat{e}(t^*P + U^*, wP + P_{pub})\hat{e}(P,P)^{-1} &= \hat{e}((t+r^*)P + U - r^*P, wP + P_{pub})\hat{e}(P,P)^{-1} \\
&= \hat{e}((xH_2(m_b, R^*) + u + r^*)P, wP + P_{pub}) \\
&\qquad \hat{e}(W - (u+r^*)P, wP + P_{pub})\hat{e}(P,P)^{-1} \\
&= \hat{e}(xH_2(m_b, R)P + W, wP + P_{pub})\hat{e}(P,P)^{-1} \text{ (Since } R^* = R) \\
&= \hat{e}(xH_2(m_b, R)P, wP + P_{pub})\hat{e}(W, wP + P_{pub})\hat{e}(P,P)^{-1} \\
&= \hat{e}(xH_2(m_b, R)P, wP + P_{pub})\hat{e}(P,P)\hat{e}(P,P)^{-1} \\
&= \hat{e}(wP + P_{pub}, P)^{xH_2(m_b,R)} \\
&= R^{H_2(m_b,R)} \\
&= {R^*}^{H_2(m_b,R^*)}
\end{aligned}$$

4.3 A possible Fix for the Weakness in [7]

The security weakness of [7] shown in section 4.2 can be fixed by providing the modifications to the $On-Encrypt$ algorithm and the definition of the hash function H_2 allowing all other algorithms unaltered. The improved On-Encrypt protocol can be given by,

On-Encrypt(m, ID_A, ϕ):

- $t_1 = \beta^{-1}(H_1(ID_A)\text{- } \alpha) \bmod q$
- $t_2 = \beta^{-1}(H_1(ID_A)\text{- } \gamma) \bmod q$
- $t = H_2(m, U, R, T_0, T_1, T_2, t_1, t_2)x{+}u \bmod q$
- $c = H_3(R)\oplus\ m$
- Output the ciphertext $\sigma = \langle U, T_0, T_1, T_2, t, t_1, t_2, c\rangle$

The hash function H_2 is redefined as $H_2 : \{0,1\}^* \times \mathbb{G}_T\mathbb{G}^3 \times \mathbb{Z}_q^* \times \mathbb{Z}_q^* \rightarrow \mathbb{Z}_q^*$

5 New Identity Based Online/Offline Encryption Scheme (New-IBOOE)

In this section we provide a new identity based online/offline encryption scheme, which is more efficent than the fixed version of [7]. Let $\mathbb{G}$ be a cyclic additive group and $\mathbb{G}_T$ be a cyclic multiplicative group. Both the groups have prime order, q and let $\hat{e}$:$\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ be the bilinear pairing. The algorithms in the scheme are described below:

Setup: The PKG selects a generator $P \in_R \mathbb{G}$ and randomly chooses $s \in \mathbb{Z}_q^*$. It computes $P_{pub} = sP$ and $\alpha = \hat{e}(P,P)$. Let $\mathcal{M}$ denotes the message space and $n_M = \mid \mathcal{M} \mid$. Let $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $H_2 : \{0,1\}^* \times \mathbb{G}_T \times \mathbb{G}^4 \rightarrow \mathbb{Z}_q^*$ and $H_3 : \{0,1\}^* \rightarrow \{0,1\}^{n_M}$ be three cryptographic hash functions. The public parameters $Params$ and master private key msk are given as:

$$Params{=}\ \langle \mathbb{G},\ \mathbb{G}_T,\ q,\ P_{pub},\ P'_{pub},\ \alpha,\ \mathcal{M},\ H_1,\ H_2,\ H_3\rangle,\ msk{=}\ s.$$

Extract(ID_A):
- $q_A = H_1(ID_A)$
- $D_A = \dfrac{1}{q_A + s}P.$

Off-Encrypt($Params$):
- $u,\ x,\ a,\ \hat{b} \in_R \mathbb{Z}_q^*$
- $U = uP$
- $R = \alpha^x$
- $\beta = H_3(R)$
- $T_1 = a^{-1}xP$
- $T_2 = x(\hat{b} + s)P.$
- Outputs the offline ciphertext $\phi = \langle u, x, a, \hat{b}, U, R, T_1, T_2, \beta\rangle$.

On-Encrypt(m, ID_A, ϕ):
- $t_1 = a(q_A - \hat{b}) \, mod \, q$
- $t_2 = H_2(m, R, U, T_1, T_2, t_1)x + u \, mod \, q$
- $c = \beta \oplus m$
- Outputs the ciphertext $\sigma = \langle U, T_1, T_2, t_1, t_2, c\rangle$

Decrypt(σ, ID_A, D_A):
- $R = \hat{e}(T_2 + t_1T_1, D_A)$
- $m = c \oplus H_3(R)$
- $h = H_2(m, R, U, T_1, T_2, t_1)$
- Checks $R^h \stackrel{?}{=} \hat{e}(t_2P - U, P)$
- Outputs m if equal. Otherwise, $\perp$

It should be noted that the offline encryption process is carried out before knowing the message m as well as the receiver identity ID_A. These are the attracing features of our scheme.

6 Security Results

6.1 Proof of Confidentiality of New-IBOOE(IND-IBOOE-CCA2)

Theorem 1. *Assume that an adversary $\mathcal{A}$ making q_e key extraction queries, q_{H_i} queries to hash oracles H_i (i=1, 2, 3), and q_d decryption queries, has an advantage ϵ against the IND-IBOOE-CCA2 security of the New-IBOOE scheme. Then, there exists an algorithm $\mathcal{C}$ to solve the k-modified Bilinear Diffie Hellman Inversion Problem (k-mBDHIP) for $k = q_{H_1}$ with an advantage $\epsilon' \geq \epsilon\left(\dfrac{1}{q_{H_1}q_{H_3}}\right)$.*

Proof: The challenger algorithm $\mathcal{C}$ takes an instance $(P, sP, l^*, \dfrac{1}{l_1 + s}P, ..., \dfrac{1}{l_k + s}P)$ of k-mBDHIP problem, and aims to find $\hat{e}(P,P)^{\dfrac{1}{l^* + s}}$, for random $l^* \notin \{l_1, ..., l_k\}$. $\mathcal{C}$ simulates the system with the various oracles $\mathcal{O}_{H_1}$, $\mathcal{O}_{H_2}$, $\mathcal{O}_{H_3}$, $\mathcal{O}_{Decrypt}$. The adversary $\mathcal{A}$ is allowed to make polynomially bounded number of adaptive queries to these oracles provided by $\mathcal{C}$. The game between $\mathcal{C}$ and $\mathcal{A}$ can be demonstrated as follows:

- ***Setup***: $\mathcal{C}$ *generates the public parameters by setting* $P_{pub} = sP$, $\alpha = \hat{e}(P,P)$ *and sends the system parameters* $\langle \mathbb{G}, \mathbb{G}_T, P,, P_{pub}, \alpha, \hat{e}(.,.)\rangle$ *to* $\mathcal{A}$.
- ***Phase-I***: *For maintaining the consistency of the oracle query responses,* $\mathcal{C}$ *maintains three lists* $\mathcal{L}_{H_i}$ *, (i = 1, 2, 3) which keeps track of the responses given by* $\mathcal{C}$ *to the corresponding oracle (*$\mathcal{O}_{H_1}$, $\mathcal{O}_{H_2}$, $\mathcal{O}_{H_3}$*) queries respectively.* $\mathcal{C}$ *simulates* $\mathcal{A}$*'s queries as follows:*
  - $\mathcal{O}_{H_1}$ ***oracle query***: *Without loss of generality, we assume that queries to* $\mathcal{O}_{H_1}$ *are distinct and that any query involving an identity* ID *is preceded by the random oracle query* $H_1(ID)$. $\mathcal{C}$ *selects a random index* γ*, where* $1 \leq \gamma \geq q_{H_1}$. *When* $\mathcal{A}$ *generates the* γ^{th} *query on* ID_γ, $\mathcal{C}$ *decides to fix* ID_γ *as target identity for the challenge phase. Moreover,* $\mathcal{C}$ *responds to* $\mathcal{A}$ *as follows:*
    - ∗ *If it is the* γ^{th} *query, then* $\mathcal{C}$ *sets* $q_\gamma = l^*$*, returns* q_γ *as the response to the query and stores* (ID_γ, q_γ) *in the list* $\mathcal{L}_{H_1}$.
    - ∗ *For all other queries,* $\mathcal{C}$ *sets* $q_i = l_i$ *where* l_i *is the value given in the instance of k-mDBHIP. The tuple* (ID_i, q_i) *is stored in the list* $\mathcal{L}_{H_1}$.
  - $\mathcal{O}_{H_2}$ ***oracle query***: *When* $\mathcal{A}$ *makes a query to this oracle with* (m, R, U, T_1, T_2, t_1) *as input,* $\mathcal{C}$ *does the following:*
    - ∗ *Searches for the tuple* $(m, R, U, T_1, T_2, t_1, h_{2_i})$ *in the list* $\mathcal{L}_{H_2}$ *and if found,* $\mathcal{C}$ *responds with* h_{2_i}.
    - ∗ *Otherwise,* $\mathcal{C}$ *responds to* $\mathcal{A}$ *by choosing a random* $h_{2_i} \leftarrow \mathbb{Z}_q{}^*$ *such that no other entry* h_{2_i} *exist in* $\mathcal{L}_{H_2}$ *and adds the tuple* $(m, R, U, T_1, T_2, t_1, h_{2_i})$ *into* $\mathcal{L}_{H_2}$.
  - $\mathcal{O}_{H_3}$ ***oracle query***: *When* $\mathcal{A}$ *makes a query to this oracle with* R *as input,* $\mathcal{C}$ *does the following:*
    - ∗ *Searches for the tuple* (R, h_{3_i}) *in the list* $\mathcal{L}_{H_3}$ *and if found,* $\mathcal{C}$ *responds with* h_{3_i}.
    - ∗ *Otherwise,* $\mathcal{C}$ *responds to* $\mathcal{A}$ *by choosing a random* $h_{3_i} \leftarrow \mathbb{Z}_q{}^*$ *such that no entry* $(.,h_{3_i})$ *exists in the list* $\mathcal{L}_{H_3}$ *and adds the tuple* (R, h_{3_i}) *into the list* $\mathcal{L}_{H_3}$.

  - $\mathcal{O}_{Extract}$ *query: On getting a request for private key of user* $\mathcal{U}_i$ *with identity* ID_i, $\mathcal{C}$ *aborts if* $ID_i = ID_\gamma$. *Else,* $\mathcal{C}$ *recovers the corresponding pair* (ID_i, l_i) *from the list* $\mathcal{L}_{H_1}$ *and responds to* $\mathcal{A}$ *with* $\dfrac{1}{l_i + s}P$ *which is given in the instance of k-mBDHIP.*
  - $\mathcal{O}_{\boldsymbol{Decrypt}}$ ***query***: *Upon receiving an decryption query of ciphertext* $\sigma = \langle U, T_1, T_2, t_1, t_2, c\rangle$ *with* ID_A *as receiver,* $\mathcal{C}$ *proceeds as follows:*
    If $ID_A \neq ID_\gamma$*, then* $\mathcal{C}$ *can directly decrypt the ciphertext, since* $\mathcal{C}$ *knows the private key* D_A *corresponding to* ID_A. *If the receiver identity* $ID_A = ID_\gamma$ *(i.e.* $\mathcal{C}$ *does not know the private key corresponding to* ID_A*),* $\mathcal{C}$ *generates the response as explained below:*
    1. *Let* $L_3{}^*$ *be the set of all* R, h_{3_i} *available in list* $\mathcal{L}_{H_3}$.
    2. *For each* $R \in L^*$*, perform the following:*
       (a) *Retrieve* (R, h_{2_i}) *from list* $\mathcal{L}_{H_2}$ *and let this set be* $L_2{}^*$.
          - ∗ *Check* $R \stackrel{?}{=} \hat{e}(t_2P - U, P)^{h_{2_i}{}^{-1}}$ *and* $\hat{e}(T_2 + t_1T_1, P) \stackrel{?}{=} \hat{e}(t_2P - U, q_AP + P_{pub})^{h_{2_i}{}^{-1}}$
          - ∗ *If the tests in the above step hold, output the* m *in the tuple containing* R, h_{2_i} *in list* $\mathcal{L}_{H_2}$
    3. *If none of the tuples obtained in step(1) passes the checks, then returns "Invalid".*

- ***Challenge Phase***: *In the challenge phase* $\mathcal{A}$ *chooses two equal length plain texts* $m_0, m_1 \in \mathcal{M}$*, a receiver identity* $ID_\mathbb{R}$ *on which* $\mathcal{A}$ *wishes to be challenged.* $\mathcal{A}$ *sends* (m_0, m_1), $ID_\mathbb{R}$ *to* $\mathcal{C}$. *It should be noted that* $\mathcal{A}$ *should not have queried the private key corresponding to* $ID_\mathbb{R}$ *in Phase-I.* $\mathcal{C}$ *aborts, if* $ID_\mathbb{R} \neq ID_\gamma$*; else,* $\mathcal{C}$ *chooses a bit* $b \in \{0,1\}$ *and computes the challenge ciphertext* σ^* *of* m_b *as follows :*
  - Picks $x_1, x_2 \in_R \mathbb{Z}_q^*$
  - Selects $U \in_R \mathbb{G}$
  - Chooses $t_2, t_1 \in_R \mathbb{Z}_q^*$
  - Computes $T_1 = t_1{}^{-1}x_1P$
  - Computes $T_2 = x_2P$.
  - *Randomly picks a c of the size defined in the scheme.*
  - $\mathcal{C}$ *Outputs the challenge ciphertext* $\sigma^* = \langle U, T_1, T_2, t_1, t_2, c\rangle$

- ***Phase-II***: *After receiving the challenge ciphertext,* $\mathcal{A}$ *gets training as in Phase-I, except that* $\mathcal{A}$ *is not allowed to ask decryption query on* σ^* *and extract query for* $ID_\mathbb{R}$.
  Here, as per the decryption algorithm $R = \hat{e}(T_2 + t_1T_1, D_\mathcal{R}) = \hat{e}(x_2P + t_1(t_1^{-1}x_1P), D_\mathbb{R}) = \hat{e}((x_2 + x_1)P), D_\mathbb{R})$. *Hence,* $R^{(x_1+x_2)^{-1}}$ *will be equal to* $\hat{e}(P, D_\mathbb{R}) = \hat{e}(P, D_\gamma)$*, if* R *is queried by* $\mathcal{A}$ *to oracle* $\mathcal{O}_{H_2}$.

– ***Guess:*** *At the end of the Phase-II,* $\mathcal{A}$ *returns a bit* b'*.* $\mathcal{C}$ *ignores the response by* $\mathcal{C}$*.* $\mathcal{C}$ *fetches a random entry* (R, h_{3_i}) *from the list* $\mathcal{L}_{H_3}$ *and computes* $\eta = R^{(x_1+x_2)^{-1}}$*. With probability* $\frac{1}{q_{H_3}}$, $\eta^* = \hat{e}(P, (q_\gamma + s)^{-1}P)$ *and this should have been queried by* $\mathcal{A}$*, since the simulation given by* $\mathcal{C}$ *is indistinguishable from the real protocol.*

$$\hat{e}(P,P)^{(q_\gamma+s)^{-1}} = \hat{e}(P,P)^{\frac{1}{l^* + s}}.$$

Now, $\mathcal{C}$ *returns* (l^*, $\hat{e}(P,P)^{(l^*+s)^{-1}}$) *as the output.*
The probability of success of $\mathcal{C}$ *can be measured by analyzing the various events that happen during the simulation :*
The events in which $\mathcal{C}$ *aborts the IND-IBOOE-CCA2 game are,*

1. E_1 *- when* $\mathcal{A}$ *queries the private key of the target identity* ID_γ *and* $Pr[E_1] = \frac{q_e}{q_{H_1}}$.
2. E_2 *- when* $\mathcal{A}$ *does not choose the target identity* ID_γ *as the receiver during the challenge and* $Pr[E_2] = 1 - \frac{1}{q_{H_1} - q_e}$.

The probability that $\mathcal{C}$ *does not abort in the IND-IBOOE-CCA2 game is given by,*

$$Pr[\neg E_1 \wedge \neg E_2] = \left(1 - \frac{q_e}{q_{H_1}}\right)\left(\frac{1}{q_{H_1} - q_e}\right) = \frac{1}{q_{H_1}}.$$

The probability that the random entry chosen by $\mathcal{C}$ *from the list* $\mathcal{L}_{H_3}$ *becoming the solution to the k-mBDHIP is* $\left(\frac{1}{q_{H_3}}\right)$*. Therefore the probability of* $\mathcal{C}$ *solving the k-mBDHIP is given by,*

$$\Pr[\mathcal{A}(P, aP, (x_1+a)^{-1}P, ..., (x_k+a)^{-1}P, x_1, ..., x^k) = \hat{e}(P,P)^{(a+x^*)^{-1}} | a, x^* \in_R \mathbb{Z}_q{}^*, x^* \notin \{x_1, ..., x_k\}] = \epsilon\left(\frac{1}{q_{H_1} q_{H_3}}\right)$$

As ϵ *is non-negligible, the probability of* $\mathcal{C}$ *solving k-mBDHIP is also non-negligible. This clearly shows that no adversary exists who can solve the IND-IBOOE-CCA2 security of New-IBOOE scheme* □

Conclusion

Identity based encryption schemes wherein the encryption is carried out in two phases namely, offline and online phase according to the complexity of the operations performed is known to be identity based online/offline encryption scheme. The subtle issue in designing an identity based online/offline encryption scheme is to split the operations into heavy weight (for offline phase) and light weight (for online phase) without knowing the message and receiver. [7] gives a solution for this problem in the random oracle model. In this paper, we have pointed out that the scheme in [7] is not CCA secure. We have proposed a possible fix for the same and have also given a more efficient identity based online/offline encryption scheme. We have formally proved the security of the new scheme in the random oracle model. The complexity figure of our scheme is given below:

Scheme	Encrypt					Decrypt				
	Offline			Online						
	BP	SPM	EXP	M	Ex	BP	SPM	EXP	M	Ex
Improved L-IBOOE (Sec. 4.3)	1	7	1	3	1	3	4	1	-	1
New-IBOOE	-	4	1	2	1	2	2	1	-	1

Table-1: Comparison of Complexity

SPM - Scalar Point Multiplication, BP - Bilinear Pairing, Exp - Exponentiation in $\mathbb{G}_T$, M - Modular Computation in $\mathbb{Z}_q^*$, Ex - Exclusive OR

References

1. Dan Boneh and Xavier Boyen. Efficient selective-id secure identity-based encryption without random oracles. In *Advances in Cryptology - EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 223–238. Springer, 2004.
2. Sherman S.M. Chow, Joseph K. Liu, and Jianying Zhou. Identity-based online/offline key encapsulation and encryption. Cryptology ePrint Archive, Report 2010/194, 2010.
3. Ratna Dutta, Rana Barua, and Palash Sarkar. Pairing-based cryptographic protocols: A survey. In *In Cryptology ePrint Archive, Report 2004/064*, 2004.
4. Shimon Even, Oded Goldreich, and Silvio Micali. On-line/off-line digital signatures. *Journal of Cryptology*, Volume 9(Number 1), 1996.
5. Craig Gentry. Practical identity-based encryption without random oracles. In *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 445–464. Springer, 2006.
6. Fuchun Guo, Yi Mu, and Zhide Chen. Identity-based online/offline encryption. In *Financial Cryptography and Data Security, FC - 2008*, volume 5143 of *Lecture Notes in Computer Science*, pages 247–261. Springer, 2008.
7. Joseph K. Liu and Jianying Zhou. An efficient identity-based online/offline encryption scheme. In *Applied Cryptography and Network Security, 7th International Conference, ACNS 2009, Paris-Rocquencourt, France, June 2-5, 2009. Proceedings*, volume 5536 of *Lecture Notes in Computer Science*, pages 156–167, 2009.
8. Adi Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology, CRYPTO - 1984*, Lecture Notes in Computer Science, pages 47–53. Springer, 1984.
9. Adi Shamir and Yael Tauman. Improved online/offline signature schemes. In *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 355–367. Springer, 2001.