A Note on the Security 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. In this paper, we show the security weakness of an identity based online offline encryption scheme proposed in ACNS 09 by Liu et al. [1]. The scheme in [1] 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.

Keywords: Identity Based, encryption, online/offline, cryptanalysis.

1 Identity Based Online/Offline Encryption Schemes(IBOOE)

1.1 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.

1.2 Security Model

Definition 1. *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 $Decrypt(\sigma,\ ID_A,\ D_B)$ 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 $\mathrm{Adv}(\mathcal{A}) = 2\left|Pr\left[b^{'} = b\right] - 1\right|$ $where\, Pr\left[b^{'} = b\right]$ denotes the probability that $b^{'} = b$.

2 Review and Attack of Liu et al. Identity Based Online/Offline Encryption Scheme(L-IBOOE)[1]

2.1 Review of L-IBOOE Scheme [1]

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 $n_M = |\mathcal{M}|$. Also Let H_2:$\{0,1\}^* \times \mathbb{G}_T \rightarrow \mathbb{Z}_q^*$ and H_3:$\{0,1\}^* \rightarrow \{0,1\}^{n_M}$ be some cryptographic 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, α, β, γ, $\delta \in_R \mathbb{Z}_q^*$
- $U = W\text{-}\ uP$
- $R = \hat{e}(wP + P_{pub}, P)^x$
- $T_0 = x(w\ \alpha P + (w+\gamma)P_{pub} + P'_{pub})$
- $T_1 = xw\beta P.$
- $T_2 = x\delta P_{pub}.$
- 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) **:**
- $t_1 = \beta^{-1}(H_1(ID_A)\text{-}\ \alpha) \bmod q$
- $t_2 = \beta^{-1}(H_1(ID_A)\text{-}\ \gamma) \bmod q$
- $t = H_2(m, R)x + u \bmod q$
- $c = H_3(R) \oplus m$
- Output the ciphertext $\sigma = \langle U, T_0, T_1, T_2, t, t_1, t_2, c \rangle$

Decrypt(σ,ID_A, D_A) **:**
- $R = \hat{e}(T_0 + t_1T_1 + t_2T_2,\ D_A\ )$
- $m = c \oplus H_3(R)$
- 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 $\perp$

2.2 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_R(D_R is not known to $\mathcal{A}$), and submits 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, $\mathcal{A}$ can cook up another ciphertext $\delta = (U^*,\ T_0^*,\ T_1^*,\ T_2^*,\ t_1^*,\ t_2^*,\ t^*,\ c^*\ )$ as given below:

- Chooses r^*, t_1^*, $t_2^* \in_R \mathbb{Z}_q^*$.
- Computes $U^* = U\ \text{-}\ r^*P = W\text{-}\ (u+\ r^*)\mathrm{P}$.
- Chooses T_1^*, $T_2^* \in_R G$.
- Computes $T_0^* = T_0\ \text{-}\ (t_1^*T_1^* + t_2^*T_2^*\ ) + (t_1T_1 + t_2T_2) = x(w+\ s)(q_A+\ s)\mathrm{P}\text{-}(t_1^*T_1^* + t_2^*T_2^*)$
  (since $T_0 + t_1T_1 + t_2T_2 = x(w+\ s)(q_A+\ s)\mathrm{P}$).
- 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 for both σ^* and δ, $R = R^* = \hat{e}(P,P)^{(w+s)x}$ 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 model). Also, it should be noted that the check $R^{*H_2(m_b,R^*)} \stackrel{?}{=} \hat{e}(t^*P + U^*, wP + P_{pub}) \hat{e}(P,P)^{-1}$ will 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 by,

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

Conclusion

In this paper, we have showed the scheme in [1] is not CCA secure. We have also proposed a new online/Offline IBOOE which does not require the knowledge of message and receiver during the offline phase and is efficient than [1].

Scheme	Encrypt						Decrypt		
	Offline			Online					
	BP	SPM	Exp	BP	SPM	Exp	BP	SPM	Exp
L-IBOOE	1	7	1	-	-	-	3	4	1
New-IBOOE	-	4	1	-	-	-	2	2	1

Fig. 1. Efficiency Comparison

SPM : Scalar Point Multiplication
BP : Bilinear Pairing
Exp : Exponentiation in $\mathbb{G}_T$

References

1. 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.