Security Analysis and Modification of ID-Based Encryption with Equality Test from ACISP 2017

Hyung Tae Lee[1], Huaxiong Wang[2], Kai Zhang[3, 4]

[1] Chonbuk National University, Republic of Korea

[2] Nanyang Technological University, Singapore

[3] Shanghai University of Electric Power, China

[4] Anhui University, China

July 13 2018@ ACISP 2018

PKE and IBE with Equality Test

- At CT-RSA 2010, Yang, Tan, Huang, and Wong presented a public key encryption with equality test (PKEET).
  - Their encryption algorithm: $(C_1, C_2, C_3) = (g^r, m^r, H(C_1, C_2, y^r) \oplus (m \| r))$
  - Anyone can check the equality between messages in ciphertexts: Given (C_1, C_2, C_3) and (C_1', C_2', C_3'), check whether $e(C_1, C_2') \stackrel{?}{=} e(C_1', C_2)$.
  - It achieves one-wayness against chosen ciphertext attacks only.
- PKEET has various applications, such as keyword search and efficient data managements.
- There have been proposed various types of PKEET schemes.
  - Enhance the security by introducing a tester
  - Improve efficiency
  - Provide functionality by extending to identity-based setting $\rightarrow$ IBEET

Insider Attack aginst PKEET and IBEET

- Supporting equality test allows for an adversary $\mathcal{A}$ an **insider attack**: Once the challenge ciphertext CT^* is given,
  1. $\mathcal{A}$ generates a ciphertext CT of a message chosen by himself/herself.
  2. $\mathcal{A}$ performs equality test between CT and CT^*.
  3. Repeat until the solution is found.
- Previous schemes avoids this issue by assuming that
  - the size of message space is exponential in the security parameter λ,
  - the min-entropy of message distribution is higher than λ.

IBEET against Insider Attack

- At ACISP 2017, Wu, Ma, Mu, and Zeng presented an identity-based encryption with equality test (IBEET) against insider attack.
- Main strategy for Wu et al.'s IBEET construction
  - Anyone can perform equality test publicly.
  - But, only group users who have a token for encryption can generate ciphertexts.
- Definition of IBEET
  - $\mathsf{Setup}(\lambda) \rightarrow (\mathrm{PP}, \mathrm{MSK}, \mathrm{MTK})$
  - $\mathsf{Extract}(\mathsf{ID}, \mathrm{MSK}, \mathrm{MTK}) \rightarrow (d_{\mathsf{ID}}, \mathsf{tok}_{\mathsf{ID}})$
  - $\mathsf{Enc}(\mathrm{PP}, m, \mathsf{ID}, \mathsf{tok}_{\mathsf{ID}}) \rightarrow \mathrm{CT}$
  - $\mathsf{Dec}(\mathrm{CT}, d_{\mathsf{ID}}, \mathsf{tok}_{\mathsf{ID}}) \rightarrow m$ or $\perp$
  - $\mathsf{Test}(\mathrm{CT}_A, \mathrm{CT}_B) \rightarrow 1$ or 0

Security Model for IBEET against Insider Attack

- Almost the same as IND-ID-CCA2 security model for traditional IBE schemes, but
  - An encryption oracle should be provided to the adversary $\mathcal{A}$
  - $\mathcal{A}$ cannot request encryption queries on challenge messages m_0, m_1.
- Security game between the adversary $\mathcal{A}$ and the challenger $\mathcal{C}$
  1. **Setup:** $\mathcal{C}$ runs $(\mathrm{PP}, \mathrm{MSK}, \mathrm{MTK}) \leftarrow \mathsf{Setup}(\lambda)$ and passes PP to $\mathcal{A}$.
  2. **Phase 1**: $\mathcal{A}$ may issue queries to key extraction, decryption, and encryption oracles adaptively and polynomially many times.
  3. **Challenge**: $\mathcal{A}$ passes ID^*, m_0, m_1 and then $\mathcal{C}$ runs $\mathrm{CT}^*_{\mathsf{ID}^*,b} \leftarrow \mathsf{Enc}(\mathrm{PP}, m_b, \mathsf{ID}^*, \mathsf{tok}_{\mathsf{ID}^*})$ for a random bit b, and sends $\mathrm{CT}^*_{\mathsf{ID}^*,b}$ to $\mathcal{A}$.
  4. **Phase 2:** As in **Phase 1**, $\mathcal{A}$ may issue queries to the oracles adaptively and polynomially many times.
  5. **Guess:** $\mathcal{A}$ returns a random guess b'.

  The advantage of $\mathcal{A}$ is defined to $\left|\Pr[b' = b] - \frac{1}{2}\right|$.
- We say that an IBEET scheme is **weak-IND-ID-CCA2 secure** if for any PPT adversary, its advantage is negligible in λ.

Wu et al.'s Concrete Construction

- The encryption algorithm of Wu et al.'s IBEET construction

$$\underbrace{C_1 = \mathrm{tok}_{\mathrm{ID}}^{r_1 \mathsf{H}(m)},\ C_2 = g_{\mathrm{ID}}^{r_1},}_{\text{for equality test}}$$

$$\underbrace{C_3 = g^{r_2},\ C_4 = (m \| r_1) \oplus \mathsf{H}_2(C_1 \| C_2 \| C_3 \| e(P_{pub}, g_{\mathrm{ID}})^{r_2})}_{\text{for recovering a message}}$$

  - g: a generator of a group $\mathbb{G}$ with bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$
  - $g_{\mathrm{ID}} = \mathsf{H}_1(\mathrm{ID})$, $\mathrm{tok}_{\mathrm{ID}} = g_{\mathrm{ID}}^{\beta}$ for the master token key β
  - $P_{pub} = g^{\alpha}$: a public parameter for the master secret key α
  - $\mathsf{H}, \mathsf{H}_1, \mathsf{H}_2$: hash functions

- Equality test: Given two ciphertexts (C_1, C_2, C_3, C_4) and (C_1', C_2', C_3', C_4'), check whether $e(C_1, C_2') \stackrel{?}{=} e(C_1', C_2)$

$$\because\ e(C_1, C_2') = e(\mathrm{tok}_{\mathrm{ID}}^{r_1 \mathsf{H}(m)}, g_{\mathrm{ID}'}^{r_1'}) = e(g_{\mathrm{ID}}, g_{\mathrm{ID}'})^{\beta r_1 r_1' \mathsf{H}(m)}$$

$$e(C_1', C_2) = e(\mathrm{tok}_{\mathrm{ID}'}^{r_1' \mathsf{H}(m')}, g_{\mathrm{ID}}^{r_1}) = e(g_{\mathrm{ID}'}, g_{\mathrm{ID}})^{\beta r_1 r_1' \mathsf{H}(m')}$$

Our Attack against Wu et al.'s IBEET

- Focus on that the first two parts for equality test can be modified.
  1. At **Phase** 1, $\mathcal{A}$ requests an encryption query on a message m and receives a ciphertext such that

$$\begin{aligned} C_1 &= \mathrm{tok}_{\mathrm{ID}}^{r_1 \mathrm{H}(m)}, \quad C_2 = g_{\mathrm{ID}}^{r_1}, \quad C_3 = g^{r_2}, \\ C_4 &= (m \| r_1) \oplus \mathrm{H}_2(C_1 \| C_2 \| C_3 \| e(P_{pub}, g_{\mathrm{ID}})^{r_2}) \end{aligned}$$

  2. At **Challenge** phase, $\mathcal{A}$ submits ID^* and m_0, m_1, which are different from m, and receives the challenge ciphertext CT^* such that

$$\begin{aligned} C_1^* &= \mathrm{tok}_{\mathrm{ID}^*}^{r_1^* \mathrm{H}(m_b)}, \quad C_2^* = g_{\mathrm{ID}^*}^{r_1^*}, \quad C_3^* = g^{r_2^*}, \\ C_4^* &= (m_b \| r_1^*) \oplus \mathrm{H}_2(C_1^* \| C_2^* \| C_3^* \| e(P_{pub}, g_{\mathrm{ID}^*})^{r_2^*}) \end{aligned}$$

  3. Once receiving the challenge ciphertext $\mathrm{CT}_{\mathrm{ID}^*,b}^* = (C_1^*, C_2^*, C_3^*, C_4^*)$ from $\mathcal{C}$, $\mathcal{A}$ first computes

$$C_1' = (C_1^{\mathrm{H}(m)^{-1}\mathrm{H}(m_1) \bmod p}) \tag{1}$$

     Then, $\mathcal{A}$ checks whether $e(C_1', C_2^*) \stackrel{?}{=} e(C_1^*, C_2)$ If it holds, it returns 1. Otherwise, it returns 0.

$\Rightarrow$ Cost: 1 encryption query, 1 exponentiation, and 2 bilinear map evaluations

Ideas for Our Modification

- Our observations from Wu et al.'s construction
  - Anyone can manipulate the part for equality test, i.e., (C_1, C_2).
  - This part does not need to be probabilistic, but should be hard to compute.

  $\Rightarrow$ Replace (C_1, C_2) by the keyed permutation value of the hashed message

  $$C_1 = F(K_1, \mathrm{H}(m)),\ C_2 = g^r,\ C_3 = (m \| r) \oplus \mathrm{H}_2(C_1 \| C_2 \| e(P_{pub}, g_{\mathrm{ID}})^r)$$

  where F is a (secure) keyed permutation.
  - But, the above construction is not secure yet if the adversary generates a new ciphertext using C_1 and new r.
  - Need an additional step to prevent the above attack against the provisional modification

  $\Rightarrow$ Exploit a message authentication code

Brief Description of Our Modification

- Our encryption algorithm

$$C_1 = F(K_1, \mathrm{H}(m)),\ C_2 = g^r,\ C_3 = (m \| r) \oplus \mathrm{H}_2(T \| C_2 \| e(P_{pub}, g_{\mathrm{ID}})^r)$$

  where $T \leftarrow \mathrm{S}(K_2, C_1)$ for the signing algorithm S of the employed MAC.

- Equality test: Given two ciphertexts (C_1, C_2, C_3) and (C_1', C_2', C_3'), check whether $C_1 \stackrel{?}{=} C_1'$.

Security of Our Modification

- Informally speaking, to break our scheme, the adversary should
  - distinguish whether a pre-image of the exploited keyed permutation F between two candidates,
  - generate a valid tag for the exploited MAC, or
  - generate a DDH solution $e(P_{pub}, g_{\mathrm{ID}})^r$, which is the solution of DDH instance $(g, P_{pub} = g^{\alpha}, g^r)$

Theorem

Our modification is weak-IND-ID-CCA2 secure in the random oracle model if

- *the DDH assumption holds,*
- *the exploited keyed permutation is strong pseudorandom, and*
- *the employed MAC is existentially unforgeable.*

- Refer to the full version of our paper for the details of the proof: eprint.iacr.org/2018/369.pdf

Conclusion & Discussion

- Presented an attack against Wu et al.'s IBEET construction at ACISP 2017
- Provided a modification for their scheme
- Is our modification a real identity-based encryption?
  - No, need a token for encryption!
  - IBEET for registered group users?

Thanks for your attention!

&

Question?