Insecurity of the Public Key Encryption with Filtered Equality Test Proposed by Huang et al.

Hyung Tae Lee[1], San Ling[2], Jae Hong Seo[3], and Huaxiong Wang[2]

[1] Division of Computer Science and Engineering, Jeonbuk National University, Korea
[2] Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore
[3] Department of Mathematics, Hanyang University, Korea

Abstract. Recently, Huang et al. proposed a concept of public key encryption with filtered equality test (PKE-FET) that allows a tester who has a warrant for the selected message set to check equality of messages in ciphertexts that belong to that set (Journal of Computer and System Sciences, 2017). They also presented an instantiation of the PKE-FET that was asserted to achieve the indistinguishability against adaptive chosen ciphertext attacks (IND-CCA2) in the standard model. In this note, we show that Huang et al.'s instantiation does not achieve the IND-CCA2 security by presenting a simple adaptive chosen ciphertext attack.

Keywords: Computation over ciphertext, filtered equality test, adaptive chosen ciphertext attacks

1 Introduction

Public key encryption with equality test (PKEET) is a public key encryption (PKE) scheme that allows to check whether two ciphertexts under different public keys as well as under the same public key have the same message or not. This feature enables PKEET to be applied to various practical scenarios, e.g., keyword search, database management, and spam filtering in email systems. For these reasons, since Yang et al. [13] first introduced the concept of PKEET, various PKEET schemes [4, 6–12] have been proposed to improve its efficiency or to support additional functionalities.

Recently, Huang et al. [3] proposed a variant concept of PKEET, called public key encryption with filtered equality test (PKE-FET). The main difference between the previous PKEET schemes and the PKE-FET scheme is that a receiver in the PKE-FET system can issue a warrant for equality tests for messages belonging to a set of polynomial size at the same time, whereas in the previous PKEET schemes a receiver issues a warrant for equality tests for either one specified ciphertext or all ciphertexts of user. More concretely, let us consider an email system, which is a typical example of PKEET/PKE-FET applications. In the email system, each user stores his/her encrypted emails at the server by appending keywords encrypted using PKEET or PKE-FET to the email for

supporting keyword search over encrypted emails efficiently. To maintain the security of the system, the server needs to monitor stored emails and thus to test equality among encrypted keywords using warrants for equality tests. For this purpose, the server asks each user to issue warrants for equality tests among keywords that he wants to monitor. If the system uses previous PKEET schemes, the server requests to issue a warrant for each ciphertext [4, 5, 8] or requests to issue a warrant for all ciphertexts only [9–12]. On the contrary, if PKE-FET is used, the server requests to issue warrants for a set of keywords at once. In [3], Huang et al. first introduced the system and security models for PKE-FET and then presented an instantiation of PKE-FET, which was claimed to achieve indistinguishability against adaptive chosen ciphertext attacks (IND-CCA2) regardless of whether adversaries have warrants for the filtered equality tests or not.

In this paper, we present an adaptive chosen ciphertext attack on the PKE-FET instantiation proposed by Huang et al. That is, we show that the security claim in [3] is flawed. Let us provide an intuitive reason why our attack works. Our attack is quite simple. Let $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ be a bilinear map where $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ are multiplicative groups of prime order q. Let g_1 and g_2 be the generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. A ciphertext of message m[4] in the Huang et al.'s PKE-FET scheme consists of

$$A = g_1^r,\ B = U^r \cdot m,\ C = V^r \cdot H_1(m),\ \text{and}$$
$$D = ((D_i)_{i=0}^n) = (((S_i)^{rh^i})_{i=0}^n),$$

where r is a random element in $\mathbb{Z}_q^*$, $U = g_1^u$, $V = e(g_1, g_2)^{uv}$, $S_i = g_1^{s_i}$ with $0 \le i \le n$ for secret values $u, v, s_i \in \mathbb{Z}_q^*$, $h = H_2(m)$, and $H_1 : \{0,1\}^* \to \mathbb{G}_T$ and $H_2 : \{0,1\}^* \to \mathbb{Z}_q^*$ are cryptographic hash functions. We observe that (A, B, C) in a ciphertext of Huang et al.'s PKE-FET scheme can be regarded as a combination of two ElGamal-type ciphertexts of messages m and $H_1(m)$ that share a randomness g_1^r. That is,

$$\mathsf{Enc}(pk_1, m) = (A, B)\ \text{and}$$
$$\mathsf{Enc}(pk_2, H_1(m)) = (A, C),$$

where $pk_1 = (g_1, U)$, $pk_2 = (g_1, V)$, and Enc is an ElGamal encryption algorithm [1]. However, unfortunately, ElGamal cryptosystem is not IND-CCA2 secure. So, we can obtain valid ciphertexts of $\overline{m}$ and $H_1(\overline{m})$ from (A, B) and (A, C), respectively, without changing A. Furthermore, since the order of the underlying group $\mathbb{G}_1$ is public, the adversary can change from h to $\overline{h} = H_2(\overline{m})$ in D_i's by computing $D_i^{(\overline{h}/h)^i}$.

Thus, we can obtain another ciphertext $\overline{CT}$ of message $\overline{m}$ from the challenge ciphertext CT^* in the IND-CCA2 security game for Huang et al.'s PKE-FET scheme by guessing the message in CT^* with 1/2 probability. Thereafter, the adversary can confirm the message in CT^* by checking the response of the

[4] We assume that each message m belongs to $\mathbb{G}_1$. If needed, one can first apply an appropriate encoding to a *raw* message so that it becomes a group element.

decryption oracle on the ciphertext $\overline{CT}$; the oracle returns $\overline{m}$ if the adversary has guessed the message correctly. If not, it returns $m' \neq \overline{m}$ or $\perp$.

Roadmap. Section 2 reviews Huang et al.'s PKE-FET scheme and Section 3 provides our adaptive chosen ciphertext attack on their scheme.

2 Huang et al.'s PKE-FET Scheme

In this section, we review Huang et al.'s PKE-FET scheme [3]. The description of Huang et al.'s PKE-FET scheme is as follows.

- $\mathsf{Setup}(\lambda)$: On input a security parameter λ, it first generates a Type-III pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ where $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ are (distinct) multiplicative cyclic groups of prime order $q = q(\lambda)$. It chooses random generators g_1 and g_2 of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. The message space $\mathcal{M}$ of the scheme is $\mathbb{G}_1$. It generates two cryptographic hash functions $H_1 : \mathcal{M} \to \mathbb{G}_T$ and $H_2 : \{0,1\}^* \to \mathbb{Z}_q^*$ and sets the auxiliary input n to be polynomial in λ. It outputs the public parameter

$$pp = \{\lambda, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, q, g_1, g_2, H_1, H_2, n\}.$$

- $\mathsf{KeyGen}(pp)$: It takes the public parameter pp as an input and selects $u, v, s_0, s_1, \ldots, s_n \xleftarrow{\$} \mathbb{Z}_q^*$ at random. Then, it computes $U = g_1^u$, $V = e(g_1, g_2)^{uv}$ and $S_i = g_1^{s_i}$ for all $i \in [0, n]$, and outputs a secret key sk and a public key pk,

$$sk = (pp, u, v, s_0, s_1, \ldots, s_n),$$
$$pk = (pp, U, V, S_0, S_1, \ldots, S_n).$$

- $\mathsf{Enc}(pk, m)$: Given a public key pk and a message $m \in \mathcal{M}$, it randomly chooses $r \xleftarrow{\$} \mathbb{Z}_q^*$, computes

$$A = g_1^r,\ B = m \cdot U^r,\ C = V^r \cdot H_1(m)$$

and

$$\begin{aligned} D &= (D_0, D_1, \ldots, D_n) \\ &= ((S_0)^r, (S_1)^{rh}, (S_2)^{rh^2}, \ldots, (S_n)^{rh^n}) \end{aligned}$$

where $h = H_2(m)$. It outputs $CT = (A, B, C, D)$.

- $\mathsf{Dec}(sk, CT)$: It takes a secret key sk and a ciphertext CT as inputs and first parses a ciphertext as (A, B, C, D). It computes $m' = B/A^u$ and $h' = H_2(m')$. Then, it checks whether
  1. $C = e(A, g_2)^{uv} \cdot H_1(m')$ and
  2. $D_i = A^{s_i (h')^i}$ for all $i \in [0, n]$ where $D = (D_0, \ldots, D_n)$.

  If both hold, it returns m'. Otherwise, it returns $\perp$.

– $\mathsf{Aut}(sk, M)$: Given a secret key sk and a subset of the message space, $M = \{m_1, \ldots, m_n\} \subset \mathcal{M}$, it computes a degree-$n$ polynomial

$$f(X) = \prod_{i=1}^{n}(X - H_2(m_i)) + uv = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}_q[X].$$

Then, it computes $w_i = g_2^{a_i/s_i}$ for all $i \in [0, n]$ and outputs the warrant of the set M for filtered equality tests,

$$w = (w_0, \ldots, w_n).$$

– $\mathsf{FET}((CT, w), (CT', w'))$: It takes two pairs of a ciphertext and a warrant, (CT, w) and (CT', w'), as inputs. Then, it performs as follows.

1. Parse $CT = (A, B, C, D)$, $D = (D_0, \ldots, D_n)$, and $w = (w_0, \ldots, w_n)$.
2. Compute

$$z = C / \prod_{i=0}^{n} e(D_i, w_i).$$

3. Similarly, compute z' from (CT', w') as Steps 1 and 2.

It returns 1 if $z = z'$ and 0 otherwise.

Remark 1. One may doubt whether the authors of [3] actually considered IND-CCA2 security or not because it was not clearly stated. However, they referred to the conference version [2] of their paper for the security proof of their proposed PKE-FET scheme and at the beginning of the security proof in [2] they explicitly argued that the decryption oracle was given to the adversary after the challenge phase. Thus, we conclude that their scheme was claimed to achieve IND-CCA2 security, not IND-CCA security.

3 Our Adaptive Chosen Ciphertext Attack

In this section, we present our adaptive chosen ciphertext attack against Huang et al.'s PKE-FET scheme [3].

Let $CT^* = (A^*, B^*, C^*, D^*)$ be the challenge ciphertext in the IND-CCA2 security game for Huang et al.'s PKE-FET scheme. Then, CT^* is of the form

$$\begin{aligned}
A^* &= g_1^{r^*}, \\
B^* &= m_b \cdot U^{r^*}, \\
C^* &= V^{r^*} \cdot H_1(m_b), \text{ and} \\
D^* &= (D_0^*, D_1^*, \ldots, D_n^*) \\
&= ((S_0)^{r^*}, (S_1)^{r^* h_b}, (S_2)^{r^* h_b^2}, \ldots, (S_n)^{r^* h_b^n})
\end{aligned}$$

for some $r^* \in \mathbb{Z}_q^*$ and $b \in \{0, 1\}$, chosen by the challenger in the IND-CCA2 security game, where $h_b = H_2(m_b)$.

Once receiving the challenge ciphertext CT^* from the challenger, the adversary generates another valid ciphertext $\overline{CT}$ from CT^* by the following manner.

1. The adversary chooses a random message $\overline{m} \stackrel{\$}{\leftarrow} \mathcal{M}$, which is different from m_0 and m_1 that were submitted to the challenger in the challenge phase.
2. The adversary computes $B' = \left(\frac{\overline{m}}{m_0}\right) B^*$ and $C' = \left(\frac{H_1(\overline{m})}{H_1(m_0)}\right) C^*$.
3. The adversary computes $D'_i = (D^*_i)^{(\overline{h}/h_0)^i}$ for all $i \in [0, n]$ where $\overline{h} = H_2(\overline{m})$, $h_0 = H_2(m_0)$, and sets $D' = (D'_0, D'_1, \ldots, D'_n)$.

The adversary requests a query on $\overline{CT} = (A^*, B', C', D')$ to the decryption oracle. If $m_b = m_0$, then $\overline{CT}$ is a valid ciphertext of message $\overline{m}$ since

$$B' = \left(\frac{\overline{m}}{m_0}\right) B^* = \overline{m} \cdot \left(\frac{m_b}{m_0}\right) U^{r^*},$$
$$C' = \left(\frac{H_1(\overline{m})}{H_1(m_0)}\right) C^* = H_1(\overline{m}) \cdot \left(\frac{H_1(m_b)}{H_1(m_0)}\right) U^{r^*},$$

and

$$D'_i = (D^*_i)^{(\overline{h}/h_0)^i} = (S_i)^{r^* \overline{h}^i (h_b/h_0)^i}$$

for all $i \in [0, n]$ where $h_b = H_2(m_b)$ and $h_0 = H_2(m_0)$. Thus, the decryption oracle returns $\overline{m}$ if $m_b = m_0$. Otherwise, it returns $\perp$ or m', which is not equal to $\overline{m}$. Therefore, our attack algorithm breaks the IND-CCA2 security of Huang et al.'s PKE-FET scheme described in Section 2. We note that we may reconfirm whether m_b is m_1 with repeating the above attack algorithm by substituting m_1 for m_0.

4 Conclusion

In this note, we provided an adaptive chosen ciphertext attack against Huang et al.'s PKE-FET scheme that was asserted to be IND-CCA2 secure in the standard model [3].

References

1. T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.
2. K. Huang, Y. Chen, and R. Tso. Semantic secure public key encryption with filtered equality test - PKE-FET. In M. S. Obaidat, P. Lorenz, and P. Samarati, editors, *International Conference on Security and Cryptography (SECRYPT) 2015*, pages 327–334. SciTePress, 2015.
3. K. Huang, R. Tso, and Y. Chen. Somewhat semantic secure public key encryption with filtered-equality-test in the standard model and its extension to searchable encryption. *J. Comput. Syst. Sci.*, 89:400–409, 2017.
4. K. Huang, R. Tso, Y. Chen, S. M. M. Rahman, A. Almogren, and A. Alamri. PKE-AET: Public key encryption with authorized equality test. *Comput. J.*, 58(10):2686–2697, 2015.

5. H. T. Lee, S. Ling, J. H. Seo, and H. Wang. CCA2 attack and modification of huang *et al.*'s public key encryption with authorized equality test. *Comput. J.*, 59(11):1689–1694, 2016.
6. H. T. Lee, S. Ling, J. H. Seo, and H. Wang. Semi-generic construction of public key encryption and identity-based encryption with equality test. *Information Sciences*, 373:419–440, 2016.
7. H. T. Lee, S. Ling, J. H. Seo, H. Wang, and T.-Y. Youn. Public key encryption with equality test in the standard model. Cryptology ePrint Archive, Report 2016/1182, 2016. Available at `http://eprint.iacr.org/2016/1182`.
8. S. Ma, Q. Huang, M. Zhang, and B. Yang. Efficient public key encryption with equality test supporting flexible authorization. *IEEE Transactions on Information Forensics and Security*, 10(3):458–470, 2015.
9. S. Ma, M. Zhang, Q. Huang, and B. Yang. Public key encryption with delegated equality test in a multi-user setting. *Comput. J.*, 58(4):986–1002, 2015.
10. Q. Tang. Towards public key encryption scheme supporting equality test with fine-grained authorization. In U. Parampalli and P. Hawkes, editors, *ACISP 2011*, volume 6812 of *LNCS*, pages 389–406. Springer, 2011.
11. Q. Tang. Public key encryption schemes supporting equality test with authorisation of different granularity. *IJACT*, 2(4):304–321, 2012.
12. Q. Tang. Public key encryption supporting plaintext equality test and user-specified authorization. *Security and Communication Networks*, 5(12):1351–1362, 2012.
13. G. Yang, C. H. Tan, Q. Huang, and D. S. Wong. Probabilistic public key encryption with equality test. In J. Pieprzyk, editor, *Topics in Cryptology - CT-RSA 2010*, volume 5985 of *LNCS*, pages 119–131. Springer, 2010.