SECURITY ANALYSIS OF PUBLIC KEY ENCRYPTION WITH FILTERED EQUALITY TEST

YU-CHI CHEN

Department of Computer Science and Engineering
Yuan Ze University
Taoyuan 320, Taiwan

(Communicated by Lih-Chung Wang)

Abstract. Public key encryption with equality test can provide a very simple add-on in which any one can directly perform testing over a pair of ciphertexts to check whether the underlying messages are identical or not without decryption. To restrict the such test power for different scenarios, that of delegated equality test is introduced to allow only the authenticated party to perform the test. In this paper, we focus on the security of public key encryption with filtered equality test (PKE-FET). The delegation to the party is only of a message set for designated testers in PKE-FET, which implies it cannot test any underlying message out of the set. We aim for investigating distinct security notions (static and adaptive security) with specific properties of the potential adversaries. Finally, we show the relationship between the security and complexity, and show the scheme of Huang et al. can reach adaptive security.

1. Introduction

General computation of ciphertext is regarded as a hard task, but some basic functions can be easily reached such as equality test which can verify the equivalence of ciphertext without description. Peng et al. [6] introduced a notion in public key encryption setting, which allows the server to play the role of a tester and has an ability to test the equality for two ciphertexts of the same receiver (whether the underlying messages are identical or not). To make the equality test more flexible, it unavoidably has to work in multi-user setting; for example, equality test for ciphertexts of different receivers. Yang et al. introduced the use of public key encryption with equality testing (PKE-ET [8]), and proposed the first PKE-ET scheme in multi-user setting. Many follow-up works have proposed a great amount of results of PKE-ET to satisfy distinct demands, such as authorization/delegated equality test [5, 7, 3, 4, 2]. Recently, Huang et al. [1] proposed a new notion called public key encryption with filtered-equality-test, PKE-FET. Its main functionality for equality test can be realized as that the testability is delegated for only a selected message set from the message space. This implies semantic security can be reached for the other messages in the complement of this set.

2020 Mathematics Subject Classification: Primary: 94A60; Secondary: 68P25.
Key words and phrases: Public key encryption, Filtered equality test, Security, Complexity.

Y. Chen is supported by Ministry of Science and Technology of Taiwan, under grants Nos. 109-2628-E-155-001-MY3 and 110-2218-E-004-001-MBK.
1.1. Contributions. Let us elaborate the results of this paper. Our starting point comes from a simple observation on the existing notion of PKE-FET. In the security definition of PKE-FET by Huang et al., the adversary $A$ receives a warrant at the beginning of the game, where the underlying message set of the warrant is chosen by the challenger. To release the setting about the returned warrant, we will obtain many potential security notions. A significant result is to formally state the security definitions with different power of $A$.

We temporarily call the first PKE-FET definition (by Huang et al.) as weak security in this paper. This inspires us to address different levels of security listed as follows.

- **Static security:** $A$ has an additional power to choose a message set at the beginning.
- **Adaptive security:** $A$ can choose a message set at anytime, even after the challenge phase.

Review of the proof of Huang et al.’s scheme. According to the security proof of Huang et al.’s scheme, the hardness assumption is embedded into parts of the system parameter. This induces that at the beginning of $A$’s activities, the challenger $C$ has already prepared the message set for producing the warrant. Once we consider a better security notion such as static security, the same proof cannot be straightly applied.

Our results. We do not modify the proof of Huang et al.’s scheme, but use some proof techniques to lift its security (with the original proof) to higher security. By applying the such manners, we will analyze the relationship between security and complexity. Finally, we obtain an interesting results in which Huang et al.’s scheme can reach adaptive security.

Organization. The rest of this paper is organized as follows. In the next section, we will show some security models of PKE-FET section. In section 3, we analyze the PKE-FET scheme and discuss specific parameters. Finally, the conclusions of this paper are given in section 4.

2. Security models of PKE-FET

We have to describe the syntax of PKE-FET prior to our defined security models. Notations. We briefly list some notations used in this paper. Negligible functions are denoted by $\text{negl}(\cdot)$ where for every positive polynomial $\text{poly}(\cdot)$, there exists an integer $N_{\text{poly}} > 0$ such that for all $x > N_{\text{poly}}$, $\text{negl}(x) < \frac{1}{\text{poly}(x)}$. For simplicity, we use $\text{negl} = \text{negl}(\lambda)$ where $\lambda$ is the security parameter. In addition, let $\xleftarrow{} \mathcal{S}$ be uniformly choosing from a space $\mathcal{S}$.

2.1. Syntax of PKE-FET. Formally, PKE-FET consists of the following probabilistic polynomial-time algorithms, denoted by $\Pi = (\text{Setup, KeyGen, Enc, Dec, Aut, Fet})$. Let $\mathcal{M}$ be the message space.

- **Setup($\lambda$):** Given a security parameter $\lambda$, it generates a series of public parameters $\text{pp}$.
- **KeyGen($\text{pp}$):** Given the public parameter $\text{pp}$, it returns the receiver’s key pair $(sk, pk)$.
- **Enc($\text{pp}, pk, m$):** Given a public key $pk$, a message $m \in \mathcal{M}$ with $\text{pp}$, it generates a ciphertext $c$. 


• Dec(pp, sk, c): Given a ciphertext c and the secret key sk, it outputs the message m.
• Aut(pp, sk, M): This algorithm, run by the receiver, takes the secret key sk to generates a warrant w w.r.t a message set $M = \{m_1, ..., m_n\}$ in order to delegate the equality testability to a tester. Therefore, the tester can perform filtered equality tests on those ciphertexts encrypted under the receiver’s public key.
• Fet(pp, c, c’, w, w’): This algorithm, run by the tester, takes as input two ciphertexts $c = \text{Enc}(pp, pk, m)$ and $c’ = \text{Enc}(pp, pk’, m’)$ and two warrants $w = \text{Aut}(pp, sk, M)$ and $w’ = \text{Aut}(pp, sk’, M’)$.

or returns 0 if not.

Remark. For simplicity of further discussions, we assume that the syntax fixes $n$ and sets it as part of pp.

2.2. Weak security. The definition of weak security of PKE-FET is stated by Huang et al. [1], which is modeled by an interactive game between a probability polynomial time (PPT) adversary $A$ and a challenger $C$. $A$ will receive a warrant at the beginning and it has additional power of oracle query. The game is also denoted by $w_{\text{PubK,FET}}^\Pi_A(\lambda)$.

• Setup:
  1. $C$ runs $\text{KeyGen}(pp) \to (sk, pk)$ and chooses a message set $M = \{m_1, ..., m_n\}$ to produce the warrant $w = \text{Aut}(pp, sk, M)$, and then sends $pk$ and $(M, w)$ to $A$.
  2. $A$ may also run $\text{KeyGen}(pp)$ for polynomial times to obtain its own keys $(sk’, pk’)$.  
• Dec1 Oracle: $A$ sends $c_j$ to $C$, and then $C$ runs $\text{Dec}(pp, sk, c_j)$ and returns the result of its decryption.
• Challenge:
  1. $A$ submits $m_0^*$ and $m_1^*$ to $C$, where $|m_0^*| = |m_1^*|$ and $m_0^* \notin M$ ($b \in \{0, 1\}$).
  2. $C$ selects $b \leftarrow \{0, 1\}$, and then obtains $c^* = \text{Enc}(pp, pk, m_b^*)$ and sends $c^*$ back to $A$.
• Dec2 Oracle: $A$ sends $c_j$ to $C$ with $c_j \neq c^*$, and then $C$ runs $\text{Dec}(pp, c_j, sk)$ and returns the result of its output.
• Guess:
  Finally $A$ outputs $b’$. If $b = b’$, $A$ wins the game, which is denoted by $w_{\text{PubK,FET}}^\Pi_A(\lambda) = 1$.

We say the PKE-FET scheme $\Pi$ is weakly secure if $\Pr[w_{\text{PubK,FET}}^\Pi_A(\lambda) = 1] \leq \frac{1}{2} + \text{negl}(\lambda)$.

2.3. Static security. We formally introduce another security notion of PKE-FET. Instead of $M$ determined by $C$, $A$ can choose one message set $M$ for requiring a warrant at the beginning in static security. The game is also denoted by $s_{\text{PubK,FET}}^\Pi_A(\lambda)$.

We only describe the modification as follows.
The game, denoted by $aPubK_{\Pi}$ choice of the message set.

2.5. Full security. We say the PKE-FET scheme $\Pi$ is statically secure if $\Pr[sPubK_{A,\Pi}(\lambda) = 1] \leq \frac{1}{2} + \text{negl}(\lambda)$.

2.4. Adaptive security. In adaptive security, $A$ is not required to commit its choice of the message set. $A$ can submit $M$ at anytime with some strict constraints. The game, denoted by $aPubK_{A,\Pi}(\lambda)$, is formally presented as follows.

- Setup:
  1. $C$ runs KeyGen$(pp) \rightarrow (sk,pk)$, and then sends $pk$ to $A$.
  2. $A$ may also run KeyGen$(pp)$ for polynomial times to obtain its own keys $(sk', pk')$.

- Aut1 Oracle:
  $A$ sends one message set $M = (m_1, m_2, \cdots, m_n)$ to $C$, and then $C$ runs $\text{Aut}(pp, M = (m_1, m_2, \cdots, m_n), sk)$ and returns the corresponding warrant $w_j$ to $A$.

- Dec1 Oracle:
  $A$ sends $c_j$ to $C$, and then $C$ runs $\text{Dec}(pp, sk, c_j)$ and returns the result of its decryption.

- Challenge:
  1. $A$ submits $m_0^*$ and $m_1^*$ to $C$, where $|m_0^*| = |m_1^*|$ and $m_b^* \notin M (b \in \{0, 1\})$.
     Note that the constraint is needed only if $A$ has queried Aut1 before challenge.
  2. $C$ selects $b \leftarrow \mathsf{U} \{0, 1\}$, and then obtains $c^* \rightarrow \text{Enc}(pp, pk, m_b^*)$ and sends $c^*$ back to $A$.

- Aut2 Oracle:
  If $A$ does not query Aut1, $A$ can do Aut2. $A$ sends one message set $M = (m_1, m_2, \cdots, m_n)$ to $C$ where this must follow the constraint $m_b^* \notin M (b \in \{0, 1\})$, and then $C$ runs $\text{Aut}(pp, M = (m_1, m_2, \cdots, m_n), sk)$ and returns the corresponding warrant $w_j$ to $A$.

- Dec2 Oracle:
  $A$ sends $c_j$ to $C$ with $c_j \neq c^*$, and then $C$ runs $\text{Dec}(pp, c_j, sk)$ and returns the result of its output.

- Guess:
  Finally $A$ outputs $b'$. If $b = b'$, $A$ wins the game, which is denoted by $aPubK_{A,\Pi}(\lambda) = 1$.

We say the PKE-FET scheme $\Pi$ is adaptively secure if $\Pr[aPubK_{A,\Pi}(\lambda) = 1] \leq \frac{1}{2} + \text{negl}(\lambda)$.

2.5. Full security. We can follow adaptive security to define full security. $A$ can submit at least $q$ message sets at anytime where $q = q(\lambda)$. The corresponding game is denoted by $fPubK_{A,\Pi}(\lambda)$. We only show the modification as follows.

- Aut1(2) Oracle:
  $A$ sends at most $q$ message sets, $M = (m_1, m_2, \cdots, m_n)$, to $C$, and then $C$ runs $\text{Aut}(pp, M = (m_1, m_2, \cdots, m_n), sk)$ and returns the corresponding warrant $w_j$.
to $\mathcal{A}$. However, in Aut2 oracle queries, the additional constraint is that $\mathcal{A}$ cannot submit any $M$ where the challenge message $m_i^*$ is in $M$ ($b \in \{0, 1\}$).

We say the PKE-FET scheme $\Pi$ is adaptively secure if $\Pr[fPubK_{\mathcal{A},\Pi}^{\text{FET}}(\lambda) = 1] \leq \frac{1}{2} + \negl(\lambda)$.

3. Analysis of the PKE-FET scheme

Notation. The size of message space $\mathcal{M}$ is denoted by $\ell$. The number of messages in a message set is denoted by $n$.

**Theorem 1.** Let $\Pi$ be a PKE-FET scheme with $\ell = \ell(\lambda)$ and $n = O(1)$ where $\ell$ is some polynomial. If $\Pi$ is a weakly secure PKE-FET scheme, then $\Pi$ is also a statically secure scheme.

**Proof.** Suppose there exists an adversary $\mathcal{A}$ can break static security, and then we can run $\mathcal{A}$ as a subroutine to create $\mathcal{A}'$ to break weak security. When $\mathcal{A}$ performs any query, $\mathcal{A}'$ also does the same. Here we only describe the difference between $\mathcal{A}$ and $\mathcal{A}'$.

- **Setup:** $\mathcal{A}$ submits a message set $M$, and accordingly $\mathcal{A}'$ will require a pair $(M', w')$.

However, $\mathcal{A}'$ only can responds correctly if $M' = M$. Assuming $\mathcal{A}'$ is able to answer, we provide an error factor $\epsilon$ between $\mathcal{A}$ and $\mathcal{A}'$ such that $\Pr[sPubK_{\mathcal{A},\Pi}^{\text{FET}}(\lambda) = 1] = \epsilon \Pr[wPubK_{\mathcal{A}',\Pi}^{\text{FET}}(\lambda) = 1]$. By the following lemma with $\ell = \ell(\lambda)$ (positive polynomial) and a constant $n$, the error is bounded by $O(\frac{1}{\ell^c})$ with constant $c$ where $O(\ell^c) = \left(\frac{\ell^c}{n}\right)^n$. Hence, if $\epsilon$ is $O(\frac{1}{\ell^c})$, we obtain $\Pr[sPubK_{\mathcal{A},\Pi}^{\text{FET}}(\lambda) = 1] = \frac{1}{\ell^c} \Pr[wPubK_{\mathcal{A}',\Pi}^{\text{FET}}(\lambda) = 1]$. By contradiction, the assumption is $\Pr[wPubK_{\mathcal{A}',\Pi}^{\text{FET}}(\lambda) = 1] \leq \negl(\lambda)$, which implies $\Pr[sPubK_{\mathcal{A},\Pi}^{\text{FET}}(\lambda) = 1] \leq \negl(\lambda)$, and the proof is complete.

**Lemma 1.** $C'$ chooses the message set uniformly. Thus, the error factor is less than $(\frac{\ell^c}{n})^n$ where $\epsilon$ is the natural number.

As we know, $C'$ randomly chooses $n$ messages from $\mathcal{M}$. This implies that $C'$ picks one from $\left(\frac{\ell^c}{n}\right)^n$. Quote the bound of $\left(\frac{\ell^c}{n}\right)^n$ to complete the proof of this lemma. \hfill $\square$.

With the same technique, we are able to lift security of the scheme to adaptive security.

**Theorem 2.** Let $\Pi$ be a PKE-FET scheme with $\ell = \ell(\lambda)$ and $n = O(1)$ where $\ell$ is some polynomial. If $\Pi$ is a weak secure PKE-FET scheme, then $\Pi$ is also an adaptively secure scheme.

**Corollary 1.** Huang et al.’s scheme is adaptively secure with $\ell = \ell(\lambda)$ and $n = O(1)$.

3.1. Remark on public key encryption with multiple keyword search from PKE-FET. To the best of knowledge, the work of Huang et al. indicated a new construction of public key encryption with multiple keyword search (PKE-MKS) from PKE-FET. In the following, we highlight the construction in an informal way, where in addition to PKE-FET, we also need a public key encryption $\text{PKE} = \{\text{PKE.KeyGen}, \text{PKE.Enc}, \text{PKE.Dec}\}$.

- **Setup:** It runs $\text{Setup}(\lambda)$ to obtain $pp$.
- **KeyGenUser:** It runs $\text{KeyGen}$ to obtain $(sk, pk)$. 
• KeyGenServer: It runs PKE.KeyGen to obtain \((sk_p, pk_p)\).
• BuildIndex: With a keyword \(m\), it runs \(\text{Enc}(pp, pk, m)\) to obtain \(c\), and then sends the encrypted keyword \(ct \leftarrow \text{PKE.Enc}(pk_p, c)\).
• Trapdoor: Let the keyword set be \(M = (m_1, m_2, ..., m_l)\). It runs \(\text{Aut}(pp, sk, M)\) to obtain \(w\), and sets the trapdoor \(td \leftarrow \text{PKE.Enc}(pk_p, w)\).
• Test: Recovering \(c, w\) by \(\text{PKE.Dec}(sk_p, \cdot)\), it runs \(\text{Fet}(pp, c, c', w, w')\) and checks the output, where \((c', w') = (c, w)\). If the output is 1, the underlying keyword of \(c\) is identical to one of them of \(w\).

According to the work of Huang et al., it relies on PKE-FET to build its application, PKE-MKS, where \(\ell = \ell(\lambda)\) and \(n = O(1)\). In the realistic setting of PKE-MKS, the keyword size is \(\ell\), and the keyword set is constant.

4. Conclusion

In this paper, we revisit the notion, PKE-FET. We state many security models to capture different levels of security and adversary’s power. Finally, we provide a proof to analyze the relationship between security and space complexity. In particular, Huang et al.’s scheme can be adaptively secure by our security lifting proof, but currently we do not find any flaw of their scheme in the full security model or have a simple intuition (technique) to prove its security in special parameter setting.

References

[1] K. Huang, R. Tso and Y.-C. Chen, Somewhat semantic secure public key encryption with filtered-equality-test in the standard model and its extension to searchable encryption, Journal of Computer and System Sciences, 89 (2017), 400–409.
[2] K. Huang, R. Tso, Y.-C. Chen, W. Li and H.-M. Sun, A new public key encryption with equality test, In International Conference on Network and System Security, Springer, 2015, 550–557.
[3] S. Ma, Identity-based encryption with outsourced equality test in cloud computing, Information Sciences, 328 (2016), 389–402.
[4] 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 (2015), 458–470.
[5] S. Ma, M. Zhang, Q. Huang and B. Yang, Public key encryption with delegated equality test in a multi-user setting, The Computer Journal, 58 (2015), 986–1002.
[6] K. Peng, C. Boyd, E. Dawson and B. Lee, Ciphertext comparison, a new solution to the millionaire problem, In International Conference on Information and Communications Security, Springer, 3783 (2005), 84–96.
[7] Q. Tang, Public key encryption schemes supporting equality test with authorisation of different granularity, International Journal of Applied Cryptography, 2 (2012), 304–321.
[8] G. Yang, C. H. Tan, Q. Huang and D. S. Wong, Probabilistic public key encryption with equality test, In Cryptographers’ Track at the RSA Conference, Springer, 5985 (2010), 119–131.

Received June 2021; revised August 2021; early access November 2021.

E-mail address: wycchen@saturn.yzu.edu.tw