A formal security proof of generic construction of anonymous IBE from PEKS

Hyun Sook Rhee[1] and Taek-Young Youn[2]*
[1]Samsung Electronics Co.Ltd., Suwon-si, Gyeonggi-do, Republic of Korea
[2]Dankook University, Yongin, Gyeonggi, Republic of Korea
hyunsook.rhee@gmail.com, taekyoung@dankook.ac.kr

Abstract

Abdalla et al.[1, 2] proposed a transform of an anonymous IBE (A-IBE) scheme to a PEKS(Public key encryption with keyword search) scheme. Boneh et al. proposed a transform of a PEKS scheme to an A-IBE scheme for only one-bit message. Rhee et al.[3] proposed a transform for constructing an A-IBE scheme for polynomially many-bit message by using a PEKS scheme. They firstly defined a multiple PEKS (mPEKS) scheme and showed that a mPEKS scheme can be constructed from a PEKS scheme. In this paper, we formally prove that if a PEKS scheme is confidential, so is the resulting mPEKS scheme. We then provide a transform from a mPEKS scheme to an A-IBE scheme for a polynomially many-bit message.

Keywords: Public key encryption with keyword search, Searchable encryption, Anonymous identity-based encryption, Formal Proof.

1 Introduction

An identity-based encryption (IBE) scheme is a public-key encryption scheme in which the public-key of a user is an identity of the user. Recently, there has been much interest in *anonymous* IBE (A-IBE) schemes with increasing applicability in various privacy preserving settings such as private broadcast encryption, encrypted email system and hidden credentials [4, 2, 5, 6, 7, 8, 9]. (An IBE scheme is said to be anonymous if a ciphertext does not reveal the identity of the intended recipient.) A study of identifying the relationships among cryptographic primitives greatly clarifies our understanding of the primitives themselves and is considered to be one of the promising approaches in cryptography. Once the relationship between two primitives is identified, a secure and customized primitive can be inexpensively constructed by exploiting the relationship and utilizing firm results of the other primitive.

Along the line of the approach above, an effort to identify the relation between A-IBE and PEKS has been continued. A PEKS is a variant of searchable encryption which provides a privacy of data and a retrievability on encrypted data. Prior results have shown that a PEKS scheme can be constructed from any A-IBE scheme [1, 2] and an A-IBE scheme for one-bit message can be constructed from any PEKS scheme [2]. Rhee et al. [3] proposed a transform for constructing an A-IBE scheme for polynomially many-bit message by using a PEKS scheme. They firstly defined a multiple PEKS (mPEKS) scheme and showed that a mPEKS scheme can be constructed from a PEKS scheme. This is the full version of [3]. Based on these results, the construction of an A-IBE scheme has been considered to be harder and more challenging than the construction of a PEKS scheme.

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 7, Article No. 18 (December 15, 2021)
DOI:*10.22667/ReBiCTE.2021.12.15.018*

*Corresponding author: 152, Jukjeon-ro, Suji-gu, Yongin-si, Gyeonggi-do, Republic of Korea 16890, Tel: +82-(0)31-8005-3253, Web: `https://sites.google.com/view/iislab`

The notion of PEKS firstly was suggested by Boneh et al. [2] and has received a lot of attention in the field of searchable encryption [10, 11, 12, 13]. A PEKS scheme enables an email server to correctly test whether or not a given keyword ndis present in an encrypted email without revealing any information on the email. In PEKS, a sender generates a *PEKS ciphertext* CT_w of a keyword w uer the public key of a receiver and sends the PEKS ciphertext CT_w along with an encrypted email message to a server. To retrieve from the server the email messages containing a keyword w', a receiver provides the server with a *trapdoor* $T_{w'}$ (generated under the receiver's secret key). The server then runs a test function with CT_w and $T_{w'}$ to identify whether or not $w = w'$, and forwards the corresponding email messages to the receiver.

Shamir [14] firstly introduced the concept of IBE. An IBE scheme is a public-key encryption in which a public key is a public identifier (i.e. a user's email address). In set-up, a trusted third party, called the Private Key Generator (PKG), generates master public/secret keys. To send a message, a sender encrypts the message by using the master public key and the identifier ID of a intended recipient. To decrypt the message, the recipient obtains the private key d_{ID} corresponding ID from the PKG.

1.1 Contribution

Rhee et al. [3] showed that an A-IBE scheme for a polynomially many-bit message can be constructed from any PEKS scheme. They first defined a multiple PEKS (mPEKS) scheme, which encrypts multiple keywords instead of one keyword with the same public key, and proved that a confidential mPEKS scheme can be derived from any confidential PEKS scheme. Next, they provided a transform of a confidential mPEKS scheme to an anonymous IBE scheme for a polynomially many-bit message. In this paper, we give all security proofs which were omitted in the Proceedings version [3] due to the page limitation. See Section "Security Proofs" for details. We formally prove that (1) if a PEKS scheme is IND-CPA then the resulting IBE scheme is ANO-CPA and IND-CPA (2) if a PEKS scheme provides consistency (which requires that email messages should be correctly routed) then the A-IBE scheme satisfies a correctness (which requires that the result of decrypting of any valid ciphertext should be an original message). To verify the correctness of the resulting A-IBE scheme, we newly define a computational relaxation of the notion of correctness as the same manner in [1].

1.2 Paper Organization.

The remainder of this paper is organized as follows. We review several primitives that are necessary for our transforms, such as the IBE and PEKS schemes in Section 2. In Section 3, we define a multiple PEKS (mPEKS) scheme and its security model. We then a confidential mPEKS scheme can be constructed from a confidential PEKS scheme. In Section 4, we review a transform of a confidential mPEKS scheme to a A-PEKS scheme proposed by Rhee et al. [3]. Finally, Section 5 concludes the paper.

2 Preliminaries

2.1 Identity-Based Encryption

We follow the definition of identity-based encryption (IBE) defined by Boneh and Franklin [15]. Let the message space be denoted by $\mathscr{M}$, the ciphertext space by $\mathscr{C}$, and the identity space by $\mathscr{I}\mathscr{D}$. An IBE scheme $\mathbf{IBE} = (\mathbf{Setup}, \mathbf{Extract}, \mathbf{Encrypt}, \mathbf{Decrypt})$ consists of four algorithms as follows.

- **Setup**(k) takes as input a security parameter k, and outputs public parameters PP and a master secret key msk.
- **Extract**$(\mathsf{msk},\mathsf{ID})$ takes as input a master secret key msk and an identity $\mathsf{ID} \in \mathscr{I}\mathscr{D}$. It outputs a private key d_{ID} corresponding to an identity ID.
- **Encrypt**$(\mathsf{PP},\mathsf{ID},M)$ takes as input PP, ID, and $M \in \mathscr{M}$ where $\mathscr{M}$ is a finite message space. It outputs a ciphertext C.
- **Decrypt**$(\mathsf{C},d_{\mathsf{ID}})$ takes as input $\mathsf{C} \in \mathscr{C}$ and a private key d_{ID}, where $\mathscr{C}$ is a ciphertext space. It outputs either $M \in \mathscr{M}$ or a symbol $\perp$ indicating failure.

Correctness. For all $\mathsf{ID} \in \mathscr{I}\mathscr{D}$, all $M \in \mathscr{M}$, if C is the output of **Encrypt** with input $(\mathsf{PP},\mathsf{ID},M)$ and d_{ID} is a valid private-key about ID, then M is the result of applying **Decrypt** with input $(\mathsf{C},d_{\mathsf{ID}})$. That is, for the given PP we have

$$\Pr[\mathbf{Decrypt}(\mathbf{Encrypt}(\mathsf{PP},\mathsf{ID},M),d_{\mathsf{ID}}) = M] = 1-\varepsilon(k),$$

where $\varepsilon(k)$ is a negligible function.

2.2 Security for A-IBE

Let $\mathbf{IBE} = (\mathbf{Setup},\mathbf{Extract},\mathbf{Encrypt},\mathbf{Decrypt})$ be an IBE scheme and $\mathscr{A}$ be an adversary. The confidentiality (IND-CPA-security) and anonymity (ANO-CPA-security) of IBE scheme against adaptive chosen-plaintext attacks follows [16, 1], as shown in Table 1. The oracle $\mathbf{Extract}(\cdot)$ is defined as: when ID is queried by $\mathscr{A}$

$$\mathsf{SetID} \leftarrow \mathsf{SetID} \cup \{\mathsf{ID}\}\ ; \qquad \text{Return } d_{\mathsf{ID}} \leftarrow \mathsf{KeyDer}(\mathsf{msk},\mathsf{ID}).$$

The advantage of $\mathscr{A}$ in the corresponding experiment as

$$\mathbf{Adv}^{\mathsf{ibe\text{-}ind\text{-}cpa}}_{\mathbf{IBE},\mathscr{A}}(k) = \Pr[\mathbf{Exp}^{\mathsf{ibe\text{-}ind\text{-}cpa\text{-}1}}_{\mathbf{IBE},\mathscr{A}}(k)=1] - \Pr[\mathbf{Exp}^{\mathsf{ibe\text{-}ind\text{-}cpa\text{-}0}}_{\mathbf{IBE},\mathscr{A}}(k)=1]\ ,$$
$$\mathbf{Adv}^{\mathsf{ibe\text{-}ano\text{-}cpa}}_{\mathbf{IBE},\mathscr{A}}(k) = \Pr[\mathbf{Exp}^{\mathsf{ibe\text{-}ano\text{-}cpa\text{-}1}}_{\mathbf{IBE},\mathscr{A}}(k)=1] - \Pr[\mathbf{Exp}^{\mathsf{ibe\text{-}ano\text{-}cpa\text{-}0}}_{\mathbf{IBE},\mathscr{A}}(k)=1]\ .$$

Definition 1. *We say that an* **IBE** *is IND-CPA-secure (resp., ANO-CPA-secure) if for any probabilistic polynomial-time (PTT) adversary* $\mathscr{A}$ *attacking* **IBE** *scheme the advantage* $\mathbf{Adv}^{\mathsf{ibe\text{-}ind\text{-}cpa}}_{\mathbf{IBE},\mathscr{A}}(k)$ (resp., $\mathbf{Adv}^{\mathsf{ibe\text{-}ano\text{-}cpa}}_{\mathbf{IBE},\mathscr{A}}(k)$) *is negligible.*

2.3 Public-Key encryption with Keyword Search

A public key encryption with keyword search (PEKS) scheme [2] $\mathbf{PEKS} = (\mathbf{KG}, \mathbf{PEKS}, \mathbf{Td}, \mathbf{Test})$ defined by Boneh *et al.* consists of four polynomial time randomized algorithms as follows.

- **KG**(k) takes as input a security parameter k, and outputs a pair of public and private keys (PK,SK).
- **PEKS**(PK,w) takes as input the public key PK and a keyword $w \in \mathscr{K}\mathscr{W}$, where $\mathscr{K}\mathscr{W}$ is a keyword space. It returns a ciphertext CT.

$\mathbf{Exp}^{\text{ibe-ind-cpa-b}}_{\mathbf{IBE},\mathscr{A}}(k)$	$\mathbf{Exp}^{\text{ibe-ano-cpa-b}}_{\mathbf{IBE},\mathscr{A}}(k)$
$\mathsf{SetID} \leftarrow \emptyset$; $(\mathsf{PP},\mathsf{msk}) \leftarrow \mathbf{Setup}(k)$	$\mathsf{SetID} \leftarrow \emptyset$; $(\mathsf{PP},\mathsf{msk}) \leftarrow \mathbf{Setup}(k)$
$(\mathsf{ID},M_0,M_1,s) \leftarrow \mathscr{A}^{\mathbf{Extract}(\cdot)}(\mathtt{find},\mathsf{PP})$	$(\mathsf{ID}_0,\mathsf{ID}_1,M,s) \leftarrow \mathscr{A}^{\mathbf{Extract}(\cdot)}(\mathtt{find},\mathsf{PP})$
if $\{M_0,M_1\} \nsubseteq \mathscr{M}$ then return 0	if $\{M\} \nsubseteq \mathscr{M}$ then return 0
$b \leftarrow \{0,1\}$; $\mathsf{C} \leftarrow \mathbf{Encrypt}(\mathsf{PP},\mathsf{ID},M_b)$	$b \leftarrow \{0,1\}$; $\mathsf{C} \leftarrow \mathbf{Encrypt}(\mathsf{PP},\mathsf{ID}_b,M)$
$b' \leftarrow \mathscr{A}^{\mathbf{Extract}(\cdot)}(\mathtt{guess},\mathsf{C},s)$	$b' \leftarrow \mathscr{A}^{\mathbf{Extract}(\cdot)}(\mathtt{guess},\mathsf{C},s)$
if $\mathsf{ID} \notin \mathsf{SetID}$ and $\lvert M_0\rvert = \lvert M_1\rvert$	if $\{\mathsf{ID}_0,\mathsf{ID}_1\} \cap \mathsf{SetID} = \emptyset$
then return b' else return 0	then return b' else return 0

Table 1: The confidentiality (IND-CPA) and the anonymity (ANO-CPA) of IBE

- $\mathbf{Td}(SK,w)$ takes as input the secret key SK and a keyword w. It returns a trapdoor T_w.
- $\mathbf{Test}(\mathsf{CT},T_{w'})$ takes as input a ciphertext CT and a trapdoor T_w. It outputs '1' if $w = w'$ and '0' otherwise, where $\mathsf{CT} = \mathbf{PEKS}(PK,w)$ and $T_{w'} \leftarrow \mathbf{Td}(SK,w')$.

Correctness. For all $w \in \mathscr{KW}$, $\mathsf{CT} \leftarrow \mathbf{PEKS}(PK,w)$, and $T_w \leftarrow \mathbf{Td}(SK,w)$, then $\mathbf{Test}(\mathsf{CT},T_w)$ always accepts. That is, for all $w \in \mathscr{KW}$ we have

$$\Pr[\mathbf{Test}(\mathbf{Td}(SK,w),\mathbf{PEKS}(PK,w)) = 1] = 1 - \varepsilon(k),$$

where the probability is taken over the choice of $(PK,SK) \leftarrow \mathbf{KG}(k)$ and $\varepsilon(k)$ is a negligible function.

2.4 Security for PEKS

A PEKS system [1, 2] requires a confidentiality (IND-CPA security), it should be infeasible for an adversary to decide which keyword is used in generating the ciphertext, and a consistency, email messages should be correctly routed. Let **PEKS** = (**KG**, **PEKS**, **Td**, **Test**) be a PEKS scheme and let $\mathscr{A}$ be a PPT adversary. We review a confidentiality and a computational consistency for PEKS scheme as follows.

Confidentiality of PEKS. The confidentiality (IND-CAP-secure) for a PEKS scheme was defined using an experiment in the Table 2 [1, 2].

The advantage of $\mathscr{A}$ is defined as follows.

$$\mathbf{Adv}^{\text{peks-ind-cpa}}_{\mathbf{PEKS},\ \mathscr{A}}(k) = \Pr[\mathbf{Exp}^{\text{peks-ind-cpa-1}}_{\mathbf{PEKS},\mathscr{A}}(k) = 1] - \Pr[\mathbf{Exp}^{\text{peks-ind-cpa-0}}_{\mathbf{PEKS},\mathscr{A}}(k) = 1]\ .$$

Definition 2. *We say that a* **PEKS** *is IND-CPA-secure if for any PPT adversary $\mathscr{A}$ attacking* PEKS *scheme the advantage $\mathbf{Adv}^{\text{peks-ind-cpa}}_{\mathbf{PEKS},\ \mathscr{A}}(k)$ is negligible.*

Consistency of PEKS. In [1], Abdalla *et al.* defined a computational consistency for PEKS scheme. Suppose there exists an adversary $\mathscr{A}$ that wants to make consistency fail. A computational consistency for a mPEKS scheme is defined using an experiment in the Table 3.

The advantage of $\mathscr{A}$ is defined as follows.

$$\mathbf{Adv}^{\text{peks-cons}}_{\mathbf{PEKS},\mathscr{A}}(k) = \Pr[\mathbf{Exp}^{\text{peks-cons}}_{\mathbf{PEKS},\mathscr{A}}(k) = 1],$$

```
$\mathbf{Exp}^{\textsf{peks-ind-cpa-b}}_{\mathbf{PEKS},\ \mathscr{A}}(k)$
  $\mathsf{SetTrap} \leftarrow \emptyset$
  $(PK, SK) \leftarrow \mathbf{KG}(k)$
  $(w_0, w_1, s) \leftarrow \mathscr{A}^{\mathbf{Td}(\cdot)}(PK)$
  $b \leftarrow \{0,1\}$ ; $\mathsf{CT} \leftarrow \mathbf{PEKS}(\texttt{find}, PK, w_b)$
  $b' \leftarrow \mathscr{A}^{\mathbf{Td}(\cdot)}(\texttt{guess}, \mathsf{CT}, s)$
  If $\{w_0, w_1\} \cap \mathsf{SetTrap}(k) = \emptyset$
  then return $b'$ else return 0
```

```
Oracle $\mathbf{Td}(w)$
  $\mathsf{SetTrap} \leftarrow \mathsf{SetTrap}(k) \cup \{w\}$
  $T_w \leftarrow \mathbf{Td}(SK, w)$
  Return $T_w$
```

Table 2: The security(IND-CPA) of PEKS.

```
$\mathbf{Exp}^{\textsf{peks-cons}}_{\mathbf{PEKS},\mathscr{A}}(k)$
  $(PK, SK) \leftarrow \mathbf{KG}(k)$
  $(w, w') \leftarrow \mathscr{A}(PK)$
  $\mathsf{CT} \leftarrow \mathbf{PEKS}(PK, w)$ ; $T_{w'} \leftarrow \mathbf{Td}(SK, w')$
  If $w \neq w'$ and $\mathbf{Test}(\mathsf{CT}, T_{w'}) = 1$ then return 1 else return 0
```

Table 3: Computational Consistency of PEKS.

where the probability is taken over all possible coin flips of all the algorithms involved.

Definition 3. *We say that a* ***PEKS*** *is "computationally consistent" if for any PPT adversary $\mathscr{A}$ attacking* PEKS *scheme the advantage $\boldsymbol{Adv}^{\textsf{peks-cons}}_{\boldsymbol{PEKS},\mathscr{A}}(k)$ is negligible.*

3 Multiple PEKS

In this section, we firstly define a notion of multiple PEKS (mPEKS) and the security for mPEKS. We then prove that any PEKS scheme having an IND-CPA security is secure even when used to encrypt multiple messages.

3.1 Definition of Multiple PEKS

A multiple public key encryption with keyword search (mPEKS) scheme **mPEKS** = (**KG**, **mPEKS**, **Td**, **mTest**) for encrypting multiple keywords is as follows.

- $\mathbf{KG}(k)$ takes as input a security parameter k and outputs a pair of public and private keys (PK, SK).
- $\mathbf{mPEKS}(PK, \overrightarrow{w})$ takes as input the public key PK and a vector of keywords $\overrightarrow{w} = (w_1, ..., w_t)$. For every i $(1 \leq i \leq t)$, it computes $c_i = \mathbf{PEKS}(PK, w_i)$ and returns a ciphertext $\mathsf{CT} = [c_1, ..., c_t]$ of $\overrightarrow{w}$.
- $\mathbf{Td}(SK, w_i)$ takes as inputs the secret key SK and a keyword w_i. It computes $T_{w_i} = \mathbf{Td}(PK, w_i)$.
- $\mathbf{mTest}(\mathsf{CT}, T_{\overrightarrow{w}})$ takes as inputs a ciphertext $\mathsf{CT} = [c_1, ..., c_t]$ and a vector of trapdoors $T_{\overrightarrow{w}} = [T_{w_1}, ..., T_{w_t}]$. For every i $(1 \leq i \leq t)$, it computes $res_i = \mathbf{Test}(c_i, T_{w_i})$ and outputs $[res_1, ..., res_t]$.

Correctness. For all vector of t keywords $\overrightarrow{w} = (w_1, ..., w_t) \in \mathscr{KW}^t$, $\mathsf{CT} \leftarrow \mathbf{mPEKS}(PK, \overrightarrow{w})$, $T_{w_i} \leftarrow \mathbf{Td}(PK, w_i)$, and let a vector of trapdoors $T_{\overrightarrow{w}} = [T_{w_1}, ..., T_{w_t}]$, then $\mathbf{mTest}(\mathsf{CT}, T_{\overrightarrow{w}})$ always outputs $\overrightarrow{1}$.

$\mathbf{Exp}^{\textsf{mpeks-ind-cpa-b}}_{\mathbf{mPEKS},\ \mathscr{A}}(k)$	Oracle $\mathsf{Td}(w)$
$\mathsf{SetTrap} \leftarrow \emptyset$	$\mathsf{SetTrap} \leftarrow \mathsf{SetTrap}(k) \cup \{w\}$
$(PK, SK) \leftarrow \mathbf{KG}(k)$	$T_w \leftarrow \mathbf{Td}(SK, w)$
$(\overrightarrow{w}_0, \overrightarrow{w}_1, s) \leftarrow \mathscr{A}^{\mathsf{Td}(\cdot)}(PK)\ (\lvert\overrightarrow{w}_0\rvert = \lvert\overrightarrow{w}_1\rvert = t(k))$	Return T_w
$b \leftarrow \{0,1\}$; $\mathsf{CT} \leftarrow \mathsf{mPEKS}(\texttt{find}, PK, \overrightarrow{w}_b)$	
$b' \leftarrow \mathscr{A}^{\mathsf{Td}(\cdot)}(\texttt{guess}, \mathsf{CT}, s)$	
If $\{w_0^j, w_1^j \mid j \in D\} \cap \mathsf{SetTrap}(k) = \emptyset$	
then return b' else return 0	

Table 4: IND-CPA-Security of mPEKS.

That is, for all $\overrightarrow{w} = (w_1, ..., w_t) \in (\mathscr{KW})^t$ we have

$$\Pr[\mathbf{mTest}(\mathbf{mPEKS}(PK, (w_1, ..., w_t)), [\mathbf{Td}(SK, w_1), ..., \mathbf{Td}(SK, w_t)]) = \overrightarrow{1}] = 1 - \varepsilon(k),$$

where the probability is taken over the choice of $(PK, SK) \leftarrow \mathbf{KG}(k)$ and $\varepsilon(k)$ is a negligible function.

3.2 Security for mPEKS

In this subsection, we firstly define a confidentiality and a computational consistency for mPEKS. Let **mPEKS** = (**KG**, **mPEKS**, **Td**, **mTest**) be a mPEKS scheme and $\mathscr{A}$ be a PPT adversary. We suppose that $\overrightarrow{w}_0 = (w_0^1, ..., w_0^t)$ and $\overrightarrow{w}_1 = (w_1^1, ..., w_1^t)$ are vectors of $t(k)$ keywords. We let that $D = \{j \mid w_0^j \neq w_1^j\ ,\ 1 \leq j \leq t\}$.

The definitions of securities are as follows.

Confidentiality of mPEKS. The confidentiality (IND-CAP-secure) for a mPEKS scheme is defined using an experiment in the Table 4. The advantage of $\mathscr{A}$ is defined as follows.

$$\mathbf{Adv}^{\textsf{mpeks-ind-cpa}}_{\mathbf{mPEKS},\ \mathscr{A}}(k) = \Pr[\mathbf{Exp}^{\textsf{mpeks-ind-cpa-1}}_{\mathbf{mPEKS},\mathscr{A}}(k) = 1] - \Pr[\mathbf{Exp}^{\textsf{mpeks-ind-cpa-0}}_{\mathbf{mPEKS},\mathscr{A}}(k) = 1]\ .$$

Definition 4. *We say that a mPEKS scheme* **mPEKS** *is IND-CPA-secure if for any PPT adversary $\mathscr{A}$ attacking* mPEKS *scheme the advantage $\boldsymbol{Adv}^{\textsf{mpeks-ind-cpa}}_{\mathbf{mPEKS},\ \mathscr{A}}(k)$ is negligible.*

Consistency of mPEKS. Suppose there exists an adversary $\mathscr{A}$ that wants to make consistency fail. A computational consistency for a mPEKS scheme is defined using an experiment in the Table 5.

The advantage of $\mathscr{A}$ is defined as follows.

$$\mathbf{Adv}^{\textsf{mpeks-cons}}_{\mathbf{mPEKS},\mathscr{A}}(k) = \Pr[\mathbf{Exp}^{\textsf{mpeks-cons}}_{\mathbf{mPEKS},\mathscr{A}}(k) = 1],$$

where the probability is taken over all possible coin flips of all the algorithms involved.

Definition 5. *We say that a* ***mPEKS*** *is "computationally consistent" if for any PPT adversary $\mathscr{A}$ attacking* mPEKS *scheme the advantage $\boldsymbol{Adv}^{\textsf{mpeks-cons}}_{\boldsymbol{mPEKS},\mathscr{A}}(k)$ is negligible.*

```
$\mathbf{Exp}^{\text{mpeks-cons}}_{\mathbf{mPEKS},\mathscr{A}}(k)$
  $(PK,SK) \leftarrow \mathbf{KG}(k)$
  $(\overrightarrow{w}_0 = (w_0^1,...,w_0^t), \overrightarrow{w}_1 = (w_1^1,...,w_1^t)) \leftarrow \mathscr{A}(PK)$
  $\mathsf{CT} \leftarrow \mathbf{PEKS}(PK, w_j)$ ; $T_{w'_j} \leftarrow \mathbf{Td}(SK, w'_j)$
  If there exists $j \in \{1,...,t\}$ such that $w_j \neq w'_j$ and $\mathbf{Test}(\mathsf{CT}, T_{w'_j}) = 1$
  then return 1 else return 0
```

Table 5: Computational Consistency of mPEKS.

3.3 Relation between PEKS and mPEKS

We show here that, if a PEKS scheme **PEKS** is IND-CPA-secure, then a multiple PEKS scheme **mPEKS** is IND-CPA-secure. To prove this, we consider the following hybrid games which differs on what challenge ciphertext CT_i is given by the challenger to the adversary.

$$\begin{aligned}
\mathsf{CT}_0 &= (\mathsf{PEKS}(PK,w_1^1),\mathsf{PEKS}(PK,w_1^2),...,\mathsf{PEKS}(PK,w_1^i)),...,\mathsf{PEKS}(PK,w_1^t))\\
\mathsf{CT}_1 &= (\mathsf{PEKS}(PK,w_0^1),\mathsf{PEKS}(PK,w_1^2),...,\mathsf{PEKS}(PK,w_1^i),...,\mathsf{PEKS}(PK,w_1^t))\\
&\vdots \qquad\qquad \vdots\\
\mathsf{CT}_i &= (\mathsf{PEKS}(PK,w_0^1),...,\mathsf{PEKS}(PK,w_0^i),\mathsf{PEKS}(PK,w_1^{i+1}),...,\mathsf{PEKS}(PK,w_1^t))\\
\mathsf{CT}_{i+1} &= (\mathsf{PEKS}(PK,w_0^1),...,\mathsf{PEKS}(PK,w_0^{i+1}),\mathsf{PEKS}(PK,w_0^{i+2}),...,\mathsf{PEKS}(PK,w_1^t))\\
&\vdots \qquad\qquad \vdots\\
\mathsf{CT}_t &= (\mathsf{PEKS}(PK,w_0^1),...,\mathsf{PEKS}(PK,w_0^i),...,\mathsf{PEKS}(PK,w_0^{t-1}),\mathsf{PEKS}(PK,w_0^t)).
\end{aligned}$$

CT_0 is the challenge ciphertext given to the adversary when $b = 0$ is chosen and CT_t is the challenge ciphertext given to the adversary when $b = 1$ is chosen. Since the above PEKS ciphertexts are always performed using independent random coins, and so the above one actually represents a distribution over vectors containing t PEKS ciphertexts. We show that no polynomially-bounded adversary is able to distinguish between CT_0 and CT_t by proving that CT_i and CT_{i+1} $(1 \leq i \leq t-1)$ are computationally indistinguishable. We note that the proof idea follows from the work of Katz and Lindell [17].

Theorem 1. If **PEKS** is IND-CPA-secure, then **mPEKS** is IND-CPA-secure.

Proof. Since the following theorem had been proven in [3], we will omit the detail proof. □

4 Relation between mPEKS and A-IBE

We investigate the relation between PEKS and A-IBE scheme. In [1], Abdalla *et al.* provided a transform of an A-IBE scheme for only one-bit message from a confidential and consistent PEKS scheme. The transform mpeks-2-ibe proposed by Rhee *et al.* [3] is as follows.

- $\mathsf{Setup}(k)$: This algorithm runs $\mathbf{KG}(k)$ to obtain (PK,SK). The public parameter is $\mathsf{PP} = PK$ and the master secret key is $\mathsf{mk} = SK$. It outputs $(\mathsf{PP},\mathsf{mk}) = (PK,SK)$.

- $\mathsf{Extract}(\mathsf{mk},\mathsf{ID})$: Let $\mathsf{ID} \in \mathscr{ID}$ be a set of identities. To generate a private key $d_{\mathsf{ID}} = T_{(1\|\mathsf{ID})}$ of ID, the key extraction algorithm runs $T_{(1\|\mathsf{ID})} \leftarrow \mathbf{Td}(SK, 1\|\mathsf{ID})$. The private key is $d_{\mathsf{ID}} = T_{(1\|\mathsf{ID})}$.

$\mathbf{Exp}_{\mathbf{IBE},\mathscr{A}}^{\text{ibe-correct}}(k)$
$(\mathsf{PP},\mathsf{msk}) \leftarrow \mathbf{Setup}(k)$
$(R,R',\mathsf{ID}) \leftarrow \mathscr{A}(\mathsf{PP})\ (\lvert R\rvert = \lvert R'\rvert = t(k))$
$\mathsf{C} \leftarrow \mathbf{Encrypt}(\mathsf{PP},\mathsf{ID},R)$; $d_{\mathsf{ID}} \leftarrow \mathbf{Extract}(\mathsf{msk},\mathsf{ID})$
If $R \neq R'$ and $\mathbf{Decrypt}(\mathsf{C},d_{\mathsf{ID}}) = R'$ then return 1 else return 0

Table 6: Computational Correctness of IBE. Here, $\mathscr{I}\mathscr{D}$ is a set of identities and $\mathsf{ID} \in \mathscr{I}\mathscr{D}$ and $R,R' \in \{0,1\}^{t(k)} \subseteq \mathscr{M}$ are binary messages.

- **Encrypt**$(\mathsf{PP},\mathsf{ID},M)$: To encrypt a message $M = (m_1,...,m_t) \in \{0,1\}^t$(with $t = \lvert M\rvert$) under the identity ID, this algorithm first sets $\overrightarrow{w} = (w_1,...,w_t)$ and runs $\mathsf{CT} \leftarrow \mathbf{mPEKS}(\mathsf{PP},\overrightarrow{w})$ to obtain a PEKS ciphertext CT. Here, the t-bit message $M = (m_1,...,m_t)$ is mapped to the vector of keywords $\overrightarrow{w} = (w_1,...,w_t)$ as follows. For $i \in \{1,...,t\}$, if $m_i = 1$ then sets $w_i = (1\|\mathsf{ID})$; otherwise, sets $w_i = (0\|\mathsf{ID})$.
- **Decrypt**$(\mathsf{CT},d_{\mathsf{ID}})$: To decrypt CT with a private key d_{ID}, this algorithm sets $\overrightarrow{d}_{\mathsf{ID}} = (d_{\mathsf{ID}},...,d_{\mathsf{ID}})$ and runs $(m_1,...,m_t) \leftarrow \mathbf{mTest}(\mathsf{CT},\overrightarrow{d}_{\mathsf{ID}})$ to obtain a message $(m_1,...,m_t)$.

When assuming the ciphertext is well-formed, the correctness of the resulting IBE scheme in our transform is verified in the following subsection. To verify the correctness of the resulting IBE scheme in our transform, we define a correctness of IBE scheme using an experiment in the Table 6 as follows.

Correctness of IBE. Suppose there exists an adversary $\mathscr{A}$ that wants to make correctness fail. A correctness for an IBE scheme is defined using an experiment in the Table 6.

The advantage of $\mathscr{A}$ is defined as follows.

$$\mathbf{Adv}_{\mathbf{IBE},\mathscr{A}}^{\text{ibe-correct}}(k) = \Pr[\mathbf{Exp}_{\mathbf{IBE},\mathscr{A}}^{\text{ibe-correct}}(k) = 1],$$

where the probability is taken over all possible coin flips of all the algorithms involved.

Definition 6. *We say that an **IBE** satisfies "computationally correctness" if for any PPT adversary $\mathscr{A}$ attacking* IBE *scheme the advantage $\mathbf{Adv}_{\mathbf{IBE},\mathscr{A}}^{\text{ibe-correct}}(k)$ is negligible.*

4.1 Security Proofs

Let **mPEKS** be a mPEKS scheme and let **IBE** be an IBE scheme derived from **mPEKS** via a new transform mpeks-2-ibe. We now show that (1) the confidentiality (IND-CPA) and the anonymity (ANO-CPA) of an IBE scheme can be derived from the confidentiality (IND-CPA) of the **mPEKS** scheme via our transform mpeks-2-ibe and (2) a correctness of IBE scheme is given from a consistency of mPEKS scheme.

Theorem 2. *If* **mPEKS** *is IND-CPA-secure, then* **IBE** *is ANO-CPA-secure.*

Proof. Let $\mathscr{A}$ be any PPT adversary attacking the correctness of **IBE**. We construct an algorithm $\mathscr{B}$ that uses $\mathscr{A}$ to attack the IND-CPA-security in **mPEKS**. Let $\mathscr{C}$ denote a challenger against $\mathscr{B}$. $\mathscr{C}$ begins by supplying $\mathscr{B}$ with the public key PK of **mPEKS** and $\mathscr{B}$ forwards PK (as the public parameter PP) to $\mathscr{A}$. $\mathscr{B}$ mounts an IND-CPA attack on **mPEKS** by interacting with $\mathscr{A}$ as follows.

- On an extraction query ID, $\mathscr{B}$ makes a trapdoor query with a keyword $w = (1\|\mathsf{ID})$ to $\mathscr{C}$. Upon receiving a corresponding trapdoor T_w $(= d_{\mathsf{ID}})$ from $\mathscr{C}$, $\mathscr{B}$ gives the private key T_w $(= d_{\mathsf{ID}})$ to $\mathscr{A}$.
- On a challenge query $(\mathsf{ID}_0^*, \mathsf{ID}_1^*, M^*)$, $\mathscr{B}$ computes the followings. Suppose that a message $M^* = (m_1, ..., m_t)$ is a t-bit non-zero binary string. $\mathscr{B}$ sets $\overrightarrow{w}_0 = (w_0^0, ..., w_0^t)$ and $\overrightarrow{w}_1 = (w_1^0, ..., w_1^t)$ as follows. For any $i \in \{1, ..., t\}$, if $m_i = 1$ then $\mathscr{B}$ sets $w_0^i = (1\|\mathsf{ID}_0^*)$ and $w_1^i = (1\|\mathsf{ID}_1^*)$. Otherwise, $\mathscr{B}$ sets $w_0^i = (1\|\mathsf{ID}_1^*)$ and $w_1^i = (1\|\mathsf{ID}_0^*)$. $\mathscr{B}$ gives a challenge query $(\overrightarrow{w}_0, \overrightarrow{w}_1)$ to $\mathscr{C}$. $\mathscr{B}$ receives his challenge ciphertext $\mathsf{CT}_b^* = \mathsf{PEKS}(PK, \overrightarrow{w}_b)$ from $\mathscr{C}$ and gives back CT_b^* to $\mathscr{A}$.

Eventually, $\mathscr{A}$ should make a guess b' for b. Then $\mathscr{B}$ outputs b' as its guess for b. It is easy to see that for any $b \in \{0, 1\}$,

$$\Pr[\mathbf{Exp}_{\mathbf{IBE},\mathscr{B}}^{\text{ibe-ano-cpa-b}}(k) = b] = \Pr[\mathbf{Exp}_{\mathbf{mPEKS},\mathscr{A}}^{\text{mpeks-ind-cpa-b}}(k) = b].$$

Thus, $\mathbf{Adv}_{\mathbf{mPEKS},\mathscr{A}}^{\text{mpeks-ind-cpa}}(k) \leq \mathbf{Adv}_{\mathbf{IBE},\mathscr{B}}^{\text{ibe-ano-cpa}}(k)$. □

Theorem 3. *If* **mPEKS** *is IND-CPA-secure, then* **IBE** *is IND-CPA-secure.*

Proof. Let $\mathscr{A}$ be any PPT adversary attacking the IND-CPA-security of **IBE**. We construct an algorithm $\mathscr{B}$ that uses $\mathscr{A}$ to attack the IND-CPA-security in **mPEKS**. Let $\mathscr{C}$ denote a challenger against $\mathscr{B}$. $\mathscr{C}$ begins by supplying $\mathscr{B}$ with the public key PK of **mPEKS** and $\mathscr{B}$ forwards PK (as the public parameter PP) to $\mathscr{A}$. $\mathscr{B}$ mounts an IND-CPA attack on **mPEKS** by interacting with $\mathscr{A}$ as follows.

- On an extraction query ID, $\mathscr{B}$ makes a trapdoor query with a keyword $w = (1\|\mathsf{ID})$ to $\mathscr{C}$. Upon receiving a corresponding trapdoor T_w $(= d_{\mathsf{ID}})$ from $\mathscr{C}$, $\mathscr{B}$ gives the private key T_w $(= d_{\mathsf{ID}})$ to $\mathscr{A}$.
- On a challenge query $(\mathsf{ID}^*, M_0^*, M_1^*)$, $\mathscr{B}$ computes the followings. Suppose that $M_0^* = (m_0^1, ..., m_0^t)$ and $M_1^* = (m_1^1, ..., m_1^t)$ are distinct t-bit binary messages. $\mathscr{B}$ sets $\overrightarrow{w}_0 = (w_0^1, ..., w_0^\ell)$ and $\overrightarrow{w}_1 = (w_1^1, ..., w_1^\ell)$ as follows. For every $i \in \{1, ..., t\}$, if $m_0^i = 1$ then $\mathscr{B}$ sets $w_0^i = (1\|\mathsf{ID}^*)$ and if $m_0^i = 0$, $\mathscr{B}$ sets $w_0^i = (0\|\mathsf{ID}^*)$. Also, if $m_1^i = 1$ then $\mathscr{B}$ sets $w_1^i = (1\|\mathsf{ID}^*)$ and if $m_1^i = 0$, $\mathscr{B}$ sets $w_1^i = (0\|\mathsf{ID}^*)$. $\mathscr{B}$ gives a challenge query $(\overrightarrow{w}_0, \overrightarrow{w}_1)$ to $\mathscr{C}$. $\mathscr{B}$ receives his challenge ciphertext $\mathsf{CT}_b^* = \mathsf{PEKS}(PK, \overrightarrow{w}_b)$ from $\mathscr{C}$ and gives back the challenge ciphertext CT_b^* to $\mathscr{A}$.

Eventually, $\mathscr{A}$ should make a guess b' for b. Then $\mathscr{B}$ outputs b' as its guess for b. It is easy to see that for any $b \in \{0, 1\}$,

$$\Pr[\mathbf{Exp}_{\mathbf{IBE},\mathscr{B}}^{\text{ibe-ind-cpa-b}}(k) = b] = \Pr[\mathbf{Exp}_{\mathbf{mPEKS},\mathscr{A}}^{\text{mpeks-ano-cpa-b}}(k) = b].$$

Thus, $\mathbf{Adv}_{\mathbf{mPEKS},\mathscr{A}}^{\text{mpeks-ano-cpa}}(k) \leq \mathbf{Adv}_{\mathbf{IBE},\mathscr{B}}^{\text{ibe-ind-cpa}}(k)$. □

Theorem 4. *If* **mPEKS** *is computationally consistent, then* **IBE** *satisfies the correctness.*

Proof. Suppose that there exists a PPT adversary $\mathscr{A}$ attacking the correctness of the IBE scheme. We then want to construct a PPT adversary $\mathscr{B}$ attacking the computational consistency of **mPEKS**. Let $\mathscr{C}$ denote a challenger against $\mathscr{B}$. $\mathscr{C}$ begins by supplying $\mathscr{B}$ with the public key PK of **mPEKS** and $\mathscr{B}$ forwards PK (as the public parameter PP) to $\mathscr{A}$. $\mathscr{B}$ runs $\mathscr{A}(PK)$ to obtain (R, R', ID), where $R = (r_1, ..., r_t)$ and $R' = (r_1', ..., r_t')$ are distinct t-bit messages such that $\mathbf{Decrypt}(\mathbf{Encrypt}(\mathsf{PP}, \mathsf{ID}, R), d_{\mathsf{ID}}) = R'$. Since R and R' are distinct, there should exist $1 \leq i \leq t$ such that $r_i \neq r_i'$. Without loss of generality, we let $r_i = 0$ and $r_i' = 1$.

$\mathscr{B}$ constructs a vector $\overrightarrow{v} = (w_1, \ldots, w_t)$ of keywords, where w_i corresponding to r_i becomes $w_i = 0||\mathsf{ID}$. Next, $\mathscr{B}$ generates a ciphertext $\mathsf{CT} \leftarrow \mathbf{Encrypt}(\mathsf{PP}, \mathsf{ID}, R)$ as an encryption of the message R. Let c_i be the encryption corresponding to the bit $r_i = 0$, i.e., $c_i = \mathbf{PEKS}(PK, 0||\mathsf{ID})$. By the correctness property broken, $\mathscr{B}$ knows that decryption for i-th bit yields the result of $\mathbf{Test}(c_i, d_{\mathsf{ID}}) = r'_i = 1$, where d_{ID} is a private key for ID. However, we know that $d_{\mathsf{ID}} = T_{1||\mathsf{ID}}$. As a result, c_i is associated with $r_i = 0$ whereas $d_{\mathsf{ID}} = T_{1||\mathsf{ID}}$ is associated with $r'_i = 1$. This implies that the computational consistency of **mPEKS** is broken. $\mathscr{B}$ outputs two keywords $w = 0||\mathsf{ID}$ and $w' = 1||\mathsf{ID}$ which are definitely distinct and $\mathbf{Test}(c_i, d_{\mathsf{ID}}) = 1$. Then, we can see that

$$\Pr[\mathbf{Exp}^{\mathsf{ibe\text{-}correct}}_{\mathbf{IBE},\mathscr{B}}(k)] = \Pr[\mathbf{Exp}^{\mathsf{mpeks\text{-}consist}}_{\mathbf{mPEKS},\mathscr{A}}(k)].$$

Thus, $\mathbf{Adv}^{\mathsf{mpeks\text{-}consist}}_{\mathbf{mPEKS},\mathscr{A}}(k) \leq \mathbf{Adv}^{\mathsf{ibe\text{-}correct}}_{\mathbf{IBE},\mathscr{B}}(k)$. □

5 Conclusions

We have examined the necessary properties of a PEKS and mPEKS scheme in producing secure (anonymous and confidential) A-IBE scheme for polynomially many-bit message. It turned out that both an anonymity and a confidentiality for an IBE scheme can be derived from the confidentiality for a PEKS scheme. Also, we have identified that the computational consistency of a PEKS scheme gives rise to the correctness of an IBE scheme. Our result has shown that an A-IBE scheme for polynomially many-bit message can be constructed by using a PEKS scheme.

References

[1] M. AbdallaMihir, B. Dario, C. Eike, K. Tadayoshi, K. Tanja, L. John, Malone-Lee, G. Neven, P. Paillier, and H. Shi. Searchable encryption revisited : Consistency properties, relation to anonymous ibe, and extensions. *Journal of Cryptology*, 21(3):350–391, January 2008.

[2] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano. Public key encryption with keyword search. In *Proc. of the 23th Proceedings of EUROCRYPT2004 (EURO'04), Interlaken, Switzerland*, volume 3027 of *Lecture Notes in Computer Science*, pages 506–522. Springer-Verlag, May 2004.

[3] H. S. Rhee and D. H. Lee. Anonymous ibe from peks : A generic construction. In *Proc. of the 22nd World Conference on Information Security Applications (WISA'21), Jeju Island, South Korea*, volume 13009 of *Lecture Notes in Computer Science*, pages 105–118. Springer-Verlag, August 2021.

[4] A. Barth, D. Boneh, and B. Waters. Privacy in encrypted content distribution using private broadcast encryption. In *Proc. of the 10th Financial Cryptography and Data Security (FC'06), Paradise Cove Anguilla, British West Indies*, volume 4107 of *Lecture Notes in Computer Science*, pages 52–64. Springer-Verlag, February-March 2006.

[5] D. Boneh and B. Waters. Conjunctive, subset, and range queries on encrypted data. In *Proc. of the 4th Theory of Cryptography Conference (TCC'07), Amsterdam, Netherlands*, volume 4392 of *Lecture Notes in Computer Science*, pages 535–554. Springer-Verlag, September 2007.

[6] J. E. Holt, R. W. Bradshaw, K. E. Seamons, and H. Orman. An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks. In *Proc. of the 2003 ACM workshop on Privacy in the Electronic Society (WPES'03), Washington, DC, USA*, pages 1–8. ACM, October 2003.

[7] J. K. abd Amit Sahai and B. Waters. redicate encryption supporting disjunctions, polynomial equations, and inner products. In *Proc. of the 27th Annual Eurocrypt Conference (EURO'08), Istanbul, Turkey*, volume 4965 of *Lecture Notes in Computer Science*, pages 146–162. Springer-Verlag, April 2008.

[8] J. S. Rhee, J. H. Park, W. Susilo, and D. H. Lee. Improved searchable public key encryption with designated tester. In *Proc. of the 4th International Symposium on Information, Computer, and Communications Security (ASIACCS'09), Sydney, Australia*, pages 376–?379. ACM, March 2009.

[9] H. S. Rhee, W. Susilo, and H.-J. Kim. Secure searchable public-key encrytion against keyword guessing attacks. *IEICE Electronics Express*, 6:237–243, 2009.

[10] J. Byun, H. Rhee, H. Park, and D. Lee. Off-line keyword guessing attacks on recent keyword search schemes over encrypted data. In *Proc. of the 3rd VLDB Workshop on Secure Data Management (SDM'06), Seoul, Korea*, volume 4165 of *Lecture Notes in Computer Science*, pages 75–83. Springer-Verlag, September 2006.

[11] L. Fang, W. Susilo, C. Ge, and J. Wang. Public key encryption with keyword search secure against keyword guessing attacks without random oracle. *Information Sciences*, 238:221–241, July 2013.

[12] H. Q and H. Li. An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks. *Information Sciences*, 403-404:1–14, September 2017.

[13] Y. Lu, G. Wang, and J. Li. Keyword guessing attacks on a public key encryption with keyword search scheme without random oracle and its improvement. *Information Sciences*, 479:270–276, December 2019.

[14] A. Shamir. Identity-based cryptosystems and signature schemes. In *Proc. of the 1st Workshop on the Theory and Application of Cryptographic Techniques (CRYPTO'84), Santa Barbara, CA, USA*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer-Verlag, November 1984.

[15] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. *SIAM Journal of Computing*, 32(3):586–615, January 2003.

[16] M. Bellare, A. Boldyreva, A. Desai, and D. Pointcheval. Key-privacy in public-key encryption. In *Proc. of the 7th International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt'01), Gold Coast, Australia*, volume 2248 of *Lecture Notes in Computer Science*, pages 566–582. Springer-Verlag, December 2001.

[17] J. Katz and Y. Lindell. Introduction to modern cryptography. In *Introduction to Modern Cryptography*. Chapman & Hall/CRC Press, 2007.

Author Biography

Hyun Sook Rhee received the B.S. and the M.S. degrees in Department of Mathematics from Dankook University, Korea, in 1998 and 2000, respectively. She received the Ph.D. degree in Information Security from Korea University, Korea, in 2008. In 2008, she was in a research fellow position in Wollongong University, Australia. From 2009 into 2010, she had served as a research professor in the Information Security from Korea University, Korea. Since 2011, he has been an senior professional with Samsung Electronics, South Korea. Her research areas include public-key encryption, searchable encryption, and privacy enhanced technologies.

Taek-Young Youn received the B.S., M.S., and Ph.D. degrees from Korea University, in 2003, 2005, and 2009, respectively. From 2010 to 2020, he has worked as a Senior Researcher with the Electronics and Telecommunications Research Institute (ETRI), South Korea. From 2016 to 2020, he was an Associate Professor with the University of Science and Technology (UST), South Korea. Since 2020, he has been an Assistant Professor with Dankook University, South Korea. His research interests include cryptography, information security, authentication, data privacy, and security issues in various communications.(Based on document published on 9 November 2020).