An Identity-Based Key-Insulated Encryption with Message Linkages for Peer-to-Peer Communication Network

Chien-Lung Hsu [1,2] and Han-Yu Lin [3,*]

[1] Department of Information Management, Chang Gung University
Tao-Yuan, 333, Taiwan
[e-mail: clhsu@mail.cgu.edu.tw]

[2] Department of Electrical Engineering and Computer Science, University of Central Florida,
Orlando, Florida 32816-2362, United States

[3] Department of Computer Science and Engineering, National Taiwan Ocean University
Keelung, 202, Taiwan
[e-mail: lin.hanyu@msa.hinet.net]
*Corresponding author: Han-Yu Lin

Received May 19, 2011; revised September 9, 2012; revised January 10, 2013; revised March 23, 2013; accepted September 21, 2013; published November 29, 2013

Abstract

Key exposure is a major threat to secure cryptosystems. To mitigate the impact caused by key-compromise attacks, a key-insulated cryptographic mechanism is a better alternative. For securing the large message communication in peer-to-peer networks, in this paper, we propose the first novel identity-based key-insulated encryption (IB-KIE) scheme with message linkages. Our scheme has the properties of unbounded time periods and random-access key-updates. In the proposed scheme, each client can periodically update his private key while the corresponding public one remains unchanged. The essential security assumption of our proposed scheme is based on the well-known bilinear Diffie-Hellman problem (BDHP). To ensure the practical feasibility, we also formally prove that the proposed scheme achieves the security requirement of confidentiality against indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2) in the random oracle model.

Keywords: identity-based, key-insulated, encryption, message linkages, bilinear pairing.

http://dx.doi.org/10.3837/tiis.2013.11.022

1. Introduction

The first public key cryptosystem was introduced by Diffie and Hellman [1] in 1976. In such a system, each user has a self-chosen private key and a corresponding public one. Two important techniques, the public key encryption and the digital signature scheme [2-4], are commonly adopted for ensuring the properties of integrity, confidentiality [5], authenticity [6] and non-repudiation [7]. In 1984, Shamir [8] proposed an identity-based system in which each user's public key is explicitly his own identity information (such as the name and e-mail address, etc.) while the corresponding private key is computed by a private key generation center (PKG). The derived private key is then sent to each user via a secure channel. Compared with the traditional public key system, an identity-based system is unnecessary to maintain public key certificates. Yet, in practice the key exposure is a major threat to system security and it sometimes imposes extra burdens to reset the whole system again.

To deal with the issue of key exposure, in 2002, Dodis *et al*. [9] proposed a key-insulated cryptosystem in which each user has a long-term private key and a short-term one, respectively. The former is stored in a physically-secure but computation limited device (called base or helper) while the latter is kept secret by the user. The general idea of key-insulated systems is that at different time periods each user can periodically update his short-term private key with the assistance of helper while the corresponding public key remains unchanged. The next year, they [10] further presented the notion of strongly key-insulated systems, i.e., even if the helper is corrupted by a malicious adversary, he cannot perform any operation with respect to the user's private key.

Considering identity-based systems, in 2005, Hanaoka *et al*. [11] proposed the first identity-based key-insulated system from bilinear maps. They also showed how to construct a partially collusion resistant hierarchical identity-based encryption (HIBEI) from arbitrary IBE in the random oracle model. In 2006, Zhou *et al*. [12] proposed an identity-based key-insulated signature scheme based on the computational Diffie-Hellman (CDH) problem. The formal security proof is also realized in the random oracle model. Later, Hanaoka *et al*. [13] proposed a parallel key-insulated public key encryption scheme in which two independent helpers are involved for updating user's private keys alternatively. Such a mechanism helps with reducing the possibility of helper exposure and increasing the security of helpers. In 2008, Weng *et al.* [14] addressed an identity-based (k, n) threshold key-insulated encryption scheme in which at least k out of n helpers are sufficient to update the user's short-term private key. Besides, the security of their scheme is proved in the standard model. For facilitating the delegation operation in an organization, in 2009, Wan *et al*. [15] proposed a strongly identity-based key-insulated proxy signature scheme with secure key-updates. Their scheme also supports unbounded time periods and random-access key-updates. Recently, Yu *et al*. [16] proposed a new identity-based key-insulated signature scheme and applied it to a novel application called full delegation proxy signature scheme with time restriction. Their scheme has the advantages of efficient key-update procedures and low computational costs for the verifier.

In a peer-to-peer network, each computer is served as both a server and a client. With an ad-hoc manner, communications can be directly established by two end computers. Consider the real situation that the communication message in a peer-to-peer file transmission system might be large. It therefore causes the difficulty in encrypting such a large plaintext due to

the limited system bandwidth. Furthermore, in an identity-based system, the key exposure attack is considered the most serious one, as the corresponding user identity has to be removed from the system. Although previous mentioned works [11-16] have addressed some solutions using key-insulted systems, their schemes are not suitable for large file transmission in peer-to-peer networks. It thus can be seen that extending the capability of current IB-KIE scheme for facilitating the peer-to-peer file transmission system is vital. In this paper, we propose the first identity-based key-insulated encryption (IB-KIE) scheme with message linkages. In our scheme, we first divide a large plaintext into lots of smaller message blocks and then encrypt them, respectively. Each ciphertext of message blocks is chained with its preceding one using a collision-resistant one-way hash function and the exclusive-OR operation. The bilinear computation is only employed to derive the mutual shared private key, rather than chaining all ciphertext blocks. Consequently, the number of required pairing operations remains a constant when the message blocks increase. The division of large files not only benefits the encryption process with limited system bandwidth, but also reduces the retransmission overheads in case of some erroneous blocks. In a peer-to-peer file transmission system, the division of large files enables a client to simultaneously download blocks from one peer and upload previously received blocks to another, as so to save the overall transmission time. The gains obtained through our proposed scheme include lower computational efforts (compared with previous works) and the capability of large file transmission. With our proposed scheme, the impact of key exposure can be minimized and two end computers can encrypt and transfer a large plaintext without increasing extra computational costs, i.e., only one mutual shared private key will be generated for transmitting multiple blocks in one communication session. Additionally, the formal security proof of confidentiality against indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2) is presented in the random oracle model.

The rest of this paper is organized as follows. Section 2 states some preliminaries. We introduce the proposed IB-KIE scheme with message linkages in Section 3. The security proof is detailed in Section 4. Finally, a conclusion is made in Section 5.

2. Preliminaries

In this section, we briefly review some security notions and the computational assumptions. The proposed scheme is based on the bilinear pairing from elliptic curve systems. A commonly adopted security assumption comes from the Bilinear Diffie-Hellman problem (BDHP). We state the basic operations of bilinear pairing and the BDH assumption below:

Bilinear Pairing

Let $(\boldsymbol{G}_1, +)$ and $(\boldsymbol{G}_2, \times)$ denote two groups of the same prime order q and e: $\boldsymbol{G}_1 \times \boldsymbol{G}_1 \rightarrow \boldsymbol{G}_2$ be a bilinear map which satisfies the following properties:

(i) ***Bilinearity***:

$e(P_1 + P_2, Q) = e(P_1, Q)e(P_2, Q)$;

$e(P, Q_1 + Q_2) = e(P, Q_1)e(P, Q_2)$;

(ii) ***Non-degeneracy***:

If P is a generator of $\boldsymbol{G}_1$, $e(P, P)$ is a generator of $\boldsymbol{G}_2$.

(iii) ***Computability***:

Given $P, Q \in \boldsymbol{G}_1$, the value of $e(P, Q)$ can be efficiently computed by a polynomial-time algorithm.

Bilinear Diffie-Hellman Problem; BDHP

The BDHP is, given an instance $(P, A, B, C) \in \boldsymbol{G}_1^4$ where P is a generator, $A = aP$, $B = bP$ and $C = cP$ for some $a, b, c \in Z_q$, to compute $e(P, P)^{abc} \in \boldsymbol{G}_2$.

Bilinear Diffie-Hellman (BDH) Assumption

For every probabilistic polynomial-time algorithm $\mathcal{A}$, every positive polynomial $Q(\cdot)$ and all sufficiently large k, the algorithm $\mathcal{A}$ can solve the BDHP with an advantage at most $1/Q(k)$, i.e.,

$$\Pr[\mathcal{A}(P, aP, bP, cP) = e(P, P)^{abc}; a, b, c \leftarrow Z_q, (P, aP, bP, cP) \leftarrow \boldsymbol{G}_1^4] \leq 1/Q(k).$$

The probability is taken over the uniformly and independently chosen instance and over the random choices of $\mathcal{A}$.

Definition 1. *The* (t, ε)*-BDH assumption holds if there is no polynomial-time adversary that can solve the BDHP in time at most t and with the advantage* ε.

3. Proposed IB-KIE Scheme with Message Linkages

In this section, we first address involved parties and algorithms of our proposed scheme and then give concrete constructions. Some performance analyses with previous works are also demonstrated.

3.1 Involved Parties

An IB-KIE scheme has four involved parties: a private key generation center (PKG), a helper (device) and two communication clients. Each one is a Probabilistic Polynomial-time Turing Machine (PPTM). The PKG is responsible for generating each user's initial private key and a master helper key. Each client can periodically update his i-th private key at time period i with the assistance of his helper.

3.2 Algorithms

The proposed IB-KIE scheme consists of the following algorithms:

– **Setup:** Taking as input 1^k where k is a security parameter, the PKG generates system's public parameters *params* and a master helper key.

–**KeyExtract (KE):** The KE algorithm takes as input the system parameters *params*, an identity *ID*, the master secret key of PKG. It generates an initial private key $S_{ID, 0}$ with respect to the identity *ID*.

–**KeyUpdate (KU):** The KU algorithm takes as input the system parameters *params*, a time period i, a helper key $HK_{ID, i}$ and a private key $S_{ID, i-1}$. It generates a private key $S_{ID, i}$ for the time period i.

– **Encryption (Enc):** The Enc algorithm takes as input the system parameters *params*, a time period i, a plaintext and the identity of receiver. It generates a corresponding ciphertext δ.

– **Decryption (Dec):** The Dec algorithm takes as input the system parameters *params*, a ciphertext δ and the private key of receiver. It outputs the recovered plaintext or an error symbol $\perp$.

3.3 Basic Construction of IB-KIE Scheme

Motivated by Wan *et al.*'s [15] and Yu *et al.*'s [16] schemes, in this subsection, we first give a

basic construction of our IB-KIE scheme without message linkages. Details of each algorithm are described below:

– **Setup:** Taking as input 1^k, the private key generation center (PKG) chooses a master secret key $s \in_R Z_q$ along with a master helper key $w \in_R Z_q$, and then computes the corresponding public keys $P_{TA} = sP$ and $P_{HK} = wP$, respectively. The master helper key w is sent to the helper via a secure channel. The PKG also selects two groups $(\boldsymbol{G}_1, +)$ and $(\boldsymbol{G}_2, \times)$ of the same prime order q where $|q| = k$. Let P be a generator of order q over $\boldsymbol{G}_1$, e: $\boldsymbol{G}_1 \times \boldsymbol{G}_1 \to \boldsymbol{G}_2$ a bilinear pairing, H: $\{0, 1\}^k \to \boldsymbol{G}_1$ and F: $\boldsymbol{G}_1 \times \boldsymbol{G}_2 \to Z_q$ collision resistant hash functions. The PKG announces public parameters $params = \{P_{TA}, P_{HK}, \boldsymbol{G}_1, \boldsymbol{G}_2, q, P, e, H, F\}$.

– **KeyExtract (KE):** Given an identity, say ID_A of the client Alice, the PKG computes the initial private key as

$$S_{A,0} = sH(ID_A) + wH(ID_A, 0), \tag{1}$$

and then returns it to Alice via a secure channel.

– **KeyUpdate (KU):** Given an identity ID_A and a time period $i \in \{1, \ldots, N\}$, the helper first generates a helper key as

$$HK_{A,i} = w[H(ID_A, i) - H(ID_A, i-1)] \tag{2}$$

and then sends it to Alice who can therefore update her private key by computing

$$S_{A,i} = S_{A,i-1} + HK_{A,i}. \tag{3}$$

The values $(S_{A,i-1}, HK_{A,i})$ are deleted subsequently.

– **Encryption (Enc):** At time period $i \in \{1, \ldots, N\}$, to encrypt a plaintext M for Alice, a sender first chooses $t \in_R Z_q$ and then computes

$$T = tP, \tag{4}$$

$$\sigma = e(P_{TA}, tH(ID_A))e(P_{HK}, tH(ID_A, i)), \tag{5}$$

$$C = M \cdot F(T, \sigma). \tag{6}$$

The ciphertext is $\delta = (i, T, C)$ which is then delivered to Alice.

– **Decryption (Dec):** Upon receiving the ciphertext $\delta = (i, T, C)$, Alice decrypts it with her private key $S_{A,i}$ at time period $i \in \{1, \ldots, N\}$ by computing

$$M = C \cdot F(T, e(T, S_{A,i}))^{-1}. \tag{7}$$

If the recovered redundancy in M is valid, Alice accepts the plaintext. Otherwise, an error symbol $\perp$ is returned to signal that δ is invalid. We show that Eq. (7) works correctly. From the right-hand side of Eq. (7), we have

$$\begin{aligned}
&C \cdot F(T, e(T, S_{A,i}))^{-1} \\
&= C \cdot F(T, e(T, sH(ID_A) + wH(ID_A, i)))^{-1} && \text{(by Eq. (1))} \\
&= C \cdot F(T, e(T, sH(ID_A))e(T, wH(ID_A, i))^{-1} \\
&= C \cdot F(T, e(sT, H(ID_A))e(wT, H(ID_A, i))^{-1} \\
&= C \cdot F(T, e(stP, H(ID_A))e(wtP, H(ID_A, i))^{-1} && \text{(by Eq. (4))} \\
&= C \cdot F(T, e(P_{TA}, tH(ID_A))e(P_{HK}, tH(ID_A, i)))^{-1} \\
&= C \cdot F(T, \sigma)^{-1} && \text{(by Eq. (5))}
\end{aligned}$$

$$= M \cdot F(T, \sigma) \cdot H(T, \sigma)^{-1} \quad \text{(by Eq. (6))}$$
$$= M$$

which leads to the left-hand side of Eq. (7).

3.4 Construction of IB-KIE Scheme with Message Linkages

Based on our basic IB-KIE scheme, we introduce an IB-KIE scheme with message linkages to benefit the encryption of a large plaintext by dividing it into lots of small blocks. Let F_1: $Z_q \rightarrow Z_q$ be a collision resistant hash function. The construction is similar as our basic IB-KIE scheme stated in Section 3.3. We only describe the different parts as follows:

– **Encryption (Enc):** At time period $i \in \{1, \ldots, N\}$, to encrypt a large plaintext M for Alice, a sender first divides M into l pieces, i.e., $M = M_1 \| M_2 \| \ldots \| M_l$, M_r's $\in Z_q$, and then chooses $t \in_R Z_q$ and $C_0 = 0$ to compute (T, σ) as Eqs. (4) and (5). The sender further computes

$$C_r = M_r \cdot F_1(C_{r-1} \oplus F(T, \sigma)), \text{ for } r = 1, 2, \ldots, l. \quad (6^*)$$

The ciphertext is $\delta = (i, T, C_1, C_2, \ldots, C_l)$ which is then delivered to Alice.

– **Decryption (Dec):** Upon receiving $\delta = (i, T, C_1, C_2, \ldots, C_l)$, Alice first decrypts it with her private key $S_{A,i}$ at time period $i \in \{1, \ldots, N\}$ by computing

$$M_r = C_r \cdot F_1(C_{r-1} \oplus F(T, e(T, S_{A,i})))^{-1}, \text{ for } r = 1, 2, \ldots, l, \quad (7^*)$$

and then recovers the original plaintext M as $M_1 \| M_2 \| \ldots \| M_l$. If the recovered redundancy in M is valid, Alice accepts the plaintext. Otherwise, an error symbol $\perp$ is returned to signal that δ is invalid.

We show that Alice can recover M with her private key by Eq. (7*). From the right-hand side of Eq. (7*), we have

$$C_r \cdot F_1(C_{r-1} \oplus F(T, e(T, S_{A,i})))^{-1}$$
$$= M_r \cdot F_1(C_{r-1} \oplus F(T, \sigma)) \cdot F_1(C_{r-1} \oplus F(T, e(T, S_{A,i})))^{-1} \quad \text{(by Eq. (6*))}$$
$$= M_r$$

which leads to the left-hand side of Eq. (7*).

3.5 Performance Analyses

In a pairing-based IB-KIE scheme, it will incur more computational efforts to extend such an algorithm to the scheme with message linkages when the encrypted message is tightly combined with the pairing computation. For example, the pairing computation of Hanaoka *et al.*'s scheme [11] takes as input the encrypted message. When we extend their algorithm to the scheme with message linkages by our construction, a sender has to employ the pairing operation for chaining all ciphertext blocks. That is to say, the number of bilinear pairing will be proportional to that of message blocks. Yet, in our proposed scheme, the bilinear computation is only adopted to derive the mutual shared private key. **Table 1** demonstrates the efficiency comparisons among the proposed and previous works including Hanaoka *et al.*'s [11] (HHS for short) and Weng *et al.*'s [14] (WLC for short) schemes in terms of the number of required pairing computation which is considered the most time-consuming operation. It can be seen that both HHS and WLC schemes incur more computational efforts as the message blocks increase while ours remains a constant, i.e., 3.

Table 1. Comparisons of required pairing computation

Scheme / #Message block	HHS	WLC	Ours
1	4	4	3
n	$4n$	$4n$	3

4. Security Proof

In this section, we define the crucial security requirement of our proposed IB-KIE scheme and prove it in the random oracle model. Since our IB-KIE scheme with message linkages has almost the same structures as those in the basic scheme, it is sufficient to show the security of our basic scheme. The security of the proposed IB-KIE scheme with message linkages is directly implied by it.

4.1 Security Requirement

The crucial security requirement of proposed IB-KIE scheme is confidentiality against indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2). We define the notion as follows:

Definition 2. *An IB-KIE scheme is said to achieve the security requirement of confidentiality against indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2) if there is no probabilistic polynomial-time adversary $\mathcal{A}$ with non-negligible advantage in the following game played with a challenger $\mathcal{B}$:*

Setup: $\mathcal{B}$ first runs the Setup(1^k) algorithm and sends the system's public parameters *params* to the adversary $\mathcal{A}$.

Phase 1: The adversary $\mathcal{A}$ can issue several queries adaptively, i.e., each query might be based on the result of previous queries:

– *KeyExtract (KE) queries:* $\mathcal{A}$ makes a KE query for some identity *ID*. $\mathcal{B}$ returns the initial private key $S_{ID, 0}$.

– *Helper-Keye (HK) queries:* $\mathcal{A}$ makes an HK query for some identity *ID* and the time period $i \in \{1, \ldots, N\}$. $\mathcal{B}$ returns the corresponding helper key $HK_{ID, i}$.

– *KeyUpdate (KU) queries:* $\mathcal{A}$ makes a KU query for some identity *ID* and the time period $i \in \{1, \ldots, N\}$. $\mathcal{B}$ returns the corresponding private key $S_{ID, i}$.

– *Encryption (Enc) queries:* $\mathcal{A}$ makes an Enc query for a plaintext M, a time period $i \in \{1, \ldots, N\}$ and an identity *ID*. $\mathcal{B}$ returns the corresponding ciphertext δ to $\mathcal{A}$.

– *Decryption (Dec) queries:* $\mathcal{A}$ makes a Dec query for a ciphertext δ with respect to an identity *ID*. If the decrypted plaintext has correct redundancy, $\mathcal{B}$ returns it. Otherwise, an error symbol $\perp$ is returned as a result.

Challenge: The adversary $\mathcal{A}$ produces two messages, M_0 and M_1, of the same length and chooses a fresh identity *ID** along with a time period $i^* \in \{1, \ldots, N\}$. The challenger $\mathcal{B}$ flips a coin $\lambda \leftarrow \{0, 1\}$ and generates a ciphertext δ^* in relation to (i^*, M_λ, *ID**). The ciphertext δ^* is then delivered to $\mathcal{A}$ as a target challenge.

Phase 2: The adversary $\mathcal{A}$ can issue new queries as those in Phase 1 except the KE(*ID**), HK(i^*, *ID**), KU(i^*, *ID**) and Dec(δ^*, *ID**) queries.

Guess: At the end of the game, $\mathcal{A}$ outputs a bit λ'. The adversary $\mathcal{A}$ wins this game if $\lambda' = \lambda$. We define $\mathcal{A}$'s advantage as $Adv(\mathcal{A}) = |\Pr[\lambda' = \lambda] - 1/2|$.

4.2 Security Proof

We prove that the proposed scheme achieves the IND-CCA2 security in the random oracle model as Theorem 1.

Theorem 1. *The proposed IB-KIE scheme is* $(t, q_H, q_F, q_{KE}, q_{HK}, q_{KU}, q_{Enc}, q_{Dec}, \varepsilon)$*-secure against indistinguishability under adaptive chosen-ciphertext attacks* (*IND-CCA2*) *in the random oracle model if there is no probabilistic polynomial-time adversary that can* (t', ε')*-break the BDHP, where*

$$\varepsilon' \geq (q_F{}^{-1})(2\varepsilon - \frac{N-1}{q_{KU}} - \frac{q_{Dec}}{2^k}),$$

$$t' \approx t + t_\lambda(2q_{Enc} + q_{Dec}).$$

Here N is the number of total time periods and t_λ *is the time for performing one bilinear pairing operation.*

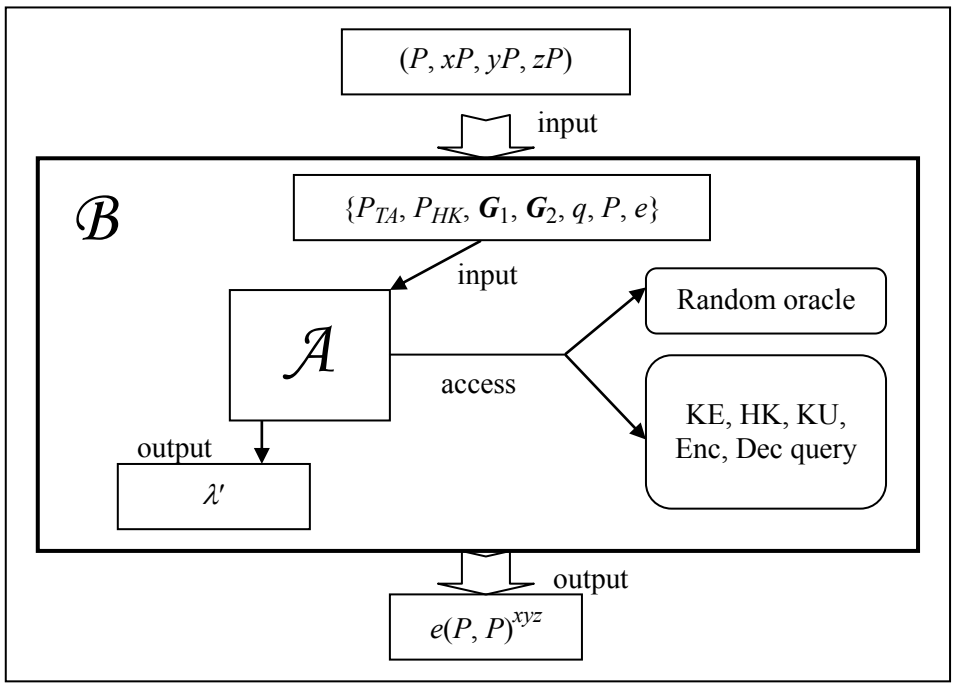

Fig. 1. The proof structure of Theorem 1

Proof: Fig. 1 depicts the proof structure of this theorem. Suppose that a probabilistic polynomial-time adversary $\mathcal{A}$ can $(t, q_H, q_F, q_{KE}, q_{HK}, q_{KU}, q_{Enc}, q_{Dec}, \varepsilon)$-break the proposed IB-KIE scheme with non-negligible advantage ε under adaptive chosen ciphertext attacks after running at most t steps and making at most q_H H, q_F F, q_{KE} KE, q_{HK} HK, q_{KU} KU, q_{Enc} Enc and q_{Dec} Dec queries. Then we can construct another algorithm $\mathcal{B}$ that

(t', ε')-breaks the BDHP by taking $\mathcal{A}$ as a subroutine. The objective of $\mathcal{B}$ is to obtain $e(P, P)^{xyz}$ by taking (P, xP, yP, zP) as inputs. In this proof, $\mathcal{B}$ simulates a challenger to $\mathcal{A}$ in the following game.

Setup: The challenger $\mathcal{B}$ runs the Setup(1^k) algorithm to obtain the system's public parameters $params = \{\boldsymbol{G}_1, \boldsymbol{G}_2, q, P, e\}$. Then $\mathcal{B}$ sets $P_{TA} = xP$ and $P_{HK} = dP$ where $d \in_R Z_q$. After that, $\mathcal{B}$ returns ($params$, P_{TA}, P_{HK}) to the adversary $\mathcal{A}$.

Phase 1: $\mathcal{A}$ makes the following queries adaptively:

– *H oracle:* When $\mathcal{A}$ queries an H oracle of $H(ID_j)$, $\mathcal{B}$ first checks H_list for a matched entry. Otherwise, $\mathcal{B}$ chooses $h_j \in_R Z_q$, adds the entry (ID_j, h_j, h_jP) to H_list, and returns h_jP as a result.

– *F oracle:* When $\mathcal{A}$ queries an F oracle of $F(T_j, \sigma_j)$, $\mathcal{B}$ first checks F_list for a matched entry. Otherwise, $\mathcal{B}$ chooses $f_j \in_R Z_q$ and adds the entry (T_j, σ_j, f_j) to F_list. Finally, $\mathcal{B}$ returns f_j as a result.

–*KE queries:* When $\mathcal{A}$ makes a KE query for ID_j, $\mathcal{B}$ returns the initial private key $S_{j,0} = h_j(xP) + d(h_{j,0}P)$ to $\mathcal{A}$.

– *HK queries:* When $\mathcal{A}$ makes an HK query for (i, ID_j) where $i \in \{1, \ldots, N\}$ is the time period, $\mathcal{B}$ returns the helper key $HK_{j,i} = d[H(ID_j, i) - H(ID_j, i-1)]$ to $\mathcal{A}$.

– *KU queries:* When $\mathcal{A}$ makes a KU query for (i, ID_j) where $i \in \{1, \ldots, N\}$ is the time period, $\mathcal{B}$ returns the corresponding private key $S_{j,i} = h_j(xP) + d(h_{j,i}P)$ to $\mathcal{A}$.

– *Enc queries:* When $\mathcal{A}$ makes an Enc query with respect to (i, M, ID) where $i \in \{1, \ldots, N\}$ is the time period, $\mathcal{B}$ follows the steps in Section 3.3 to return the ciphertext $\delta = (i, T, C)$.

– *Dec queries:* When $\mathcal{A}$ makes a Dec query for some pair (ID_j, δ) where $\delta = (i, T, C)$, $\mathcal{B}$ first derives the private key $S_{j,i} = h_j(xP) + d(h_{j,i}P)$ to run the Decryption algorithm in Section 3.3 and then returns the corresponding result.

Challenge: The adversary $\mathcal{A}$ produces two messages, M_0 and M_1, of the same length and chooses a fresh identity ID^* along with a time period $i^* \in \{1, \ldots, N\}$. The challenger $\mathcal{B}$ flips a coin $\lambda \leftarrow \{0, 1\}$ and generates a ciphertext δ^* in relation to (i^*, M_λ, ID^*) as follows:

Step 1 Add the entry (ID^*, null, yP) to H_list,
i.e., implicitly define $H(ID^*) = yP$ where y is unknown to $\mathcal{B}$.

Step 2 Set $T^* = zP$;

Step 3 Choose $f^* \in_R Z_q$ and add the entry (T^*, null, f^*) to F_list,
i.e., implicitly define $F(T^*, \sigma^*) = f^*$ where σ^* is unknown to $\mathcal{B}$.

Step 4 Compute $C^* = M_\lambda \cdot f^*$.

The ciphertext $\delta^* = (i^*, T^*, C^*)$ is then delivered to $\mathcal{A}$ as a target challenge.

Phase 2: $\mathcal{A}$ makes new queries as those stated in Phase 1 except the KE(ID^*), HK(i^*, ID^*), KU(i^*, ID^*) and Dec(δ^*, ID^*) queries. When $\mathcal{A}$ makes a KU query for (i, ID^*) where $i \in \{1, \ldots, i^*-1, i^*+1, \ldots, N\}$, $\mathcal{B}$ directly terminates. When $\mathcal{A}$ makes a Dec query for some pair (ID^*, δ) where $\delta = (i, T, C)$, $\mathcal{B}$ searches F_list for a matched entry (T_j, σ_j, f_j) where $T_j = T$ and then returns $M = C \cdot f_j^{-1}$ to $\mathcal{A}$. Otherwise, an error symbol $\perp$ is returned as a result.

Analysis of the game: We first evaluate the simulation of Dec queries. One can observe that it is possible for a Dec query of some valid pair (ID^*, δ) where $\delta = (i, T, C)$ to return the

error symbol $\perp$ on condition that $\mathcal{A}$ doesn't query the corresponding $F(T, \sigma)$ random oracle. However, such the probability for any Dec query is not greater than 2^{-k}. Since $\mathcal{A}$ is allowed to make at most q_{Dec} Dec queries, the above situation happens during the entire simulation game, denoted by Dec_ERR, would be less than $(q_{Dec})2^{-k}$, i.e., Pr[Dec_ERR] ≤ $(q_{Dec})2^{-k}$. Also note that $\mathcal{B}$ terminates for some KU queries with respect to (i, ID^*) where $i \in \{1, \ldots, i^* - 1, i^* + 1, \ldots, N\}$. We express such an event during the entire simulation game as KU_ERR and Pr[KU_ERR] ≤ $(N - 1)(q_{KU})^{-1}$. Additionally, in the challenge phase, $\mathcal{B}$ has returned a simulated ciphertext $\delta^* = (i^*, T^*, C^*)$ where $H(ID^*) = yP$ and $T^* = zP$, which implies the parameter σ^* is implicitly defined as

$$\begin{aligned}\sigma^* &= e(P_{TA}, zH(ID^*))e(P_{HK}, zH(ID^*, i)) \\ &= e(xP, z(yP))e(dP, z(h^*_{,i^*}P)) \\ &= e(P, P)^{xyz}\, e(dP, (h^*_{,i^*})(zP)).\end{aligned}$$

Let NA be the event that the entire simulation game does not abort. Obviously, if the adversary $\mathcal{A}$ never asks an $F(T^*, \sigma^*)$ oracle query in Phase 2, the entire simulation game could be normally terminated. We denote the event that $\mathcal{A}$ does ask such an oracle query in Phase 2 by QF*. When the entire simulation game does not abort, it can be seen $\mathcal{A}$ gains no advantage in guessing λ due to the randomness of random oracles, i.e.,

$$\Pr[\lambda' = \lambda \mid \mathrm{NA}] = 1/2. \tag{8}$$

Rewriting the expression of $\Pr[\lambda' = \lambda]$, we have

$$\begin{aligned}\Pr[\lambda' = \lambda] &= \Pr[\lambda' = \lambda \mid \mathrm{NA}]\ \Pr[\mathrm{NA}] + \Pr[\lambda' = \lambda \mid \neg\mathrm{NA}]\ \Pr[\neg\mathrm{NA}] \\ &\le (1/2)\Pr[\mathrm{NA}] + \Pr[\neg\mathrm{NA}] \qquad \text{(by Eq. (8))} \\ &= (1/2)(1 - \Pr[\neg\mathrm{NA}]) + \Pr[\neg\mathrm{NA}] \\ &= (1/2) + (1/2)\Pr[\neg\mathrm{NA}]. \qquad (9)\end{aligned}$$

On the other hand, we can also derive that

$$\begin{aligned}\Pr[\lambda' = \lambda] &\ge \Pr[\lambda' = \lambda \mid \mathrm{NA}]\ \Pr[\mathrm{NA}] \\ &= (1/2)(1 - \Pr[\neg\mathrm{NA}]) \\ &= (1/2) - (1/2)\Pr[\neg\mathrm{NA}]. \qquad (10)\end{aligned}$$

With inequalities (9) and (10), we know that

$$|\ \Pr[\lambda' = \lambda] - 1/2\ | \le (1/2)\Pr[\neg\mathrm{NA}]. \tag{11}$$

Recall that in Definition 2, $\mathcal{A}$'s advantage is defined as $Adv(\mathcal{A}) = |\ \Pr[\lambda' = \lambda] - 1/2\ |$. By assumption, $\mathcal{A}$ has non-negligible probability ε to break the proposed scheme. We therefore have

$$\begin{aligned}\varepsilon &= |\ \Pr[\lambda' = \lambda] - 1/2\ | \\ &\le (1/2)\Pr[\neg\mathrm{NA}] \qquad \text{(by Eq. (11))} \\ &= (1/2)(\Pr[\mathrm{QF}^* \vee \mathrm{Dec\_ERR} \vee \mathrm{KU\_ERR}]) \\ &\le (1/2)(\Pr[\mathrm{QF}^*] + \Pr[\mathrm{Dec\_ERR}] + \Pr[\mathrm{KU\_ERR}])\end{aligned}$$

Rewriting the above inequality, we get

$$\begin{aligned}\Pr[\mathrm{QF}^*] &\ge 2\varepsilon - \Pr[\mathrm{Dec\_ERR}] - \Pr[\mathrm{KU\_ERR}] \\ &\ge 2\varepsilon - \frac{N-1}{q_{KU}} - \frac{q_{Dec}}{2^k}.\end{aligned}$$

If the event QF* happens, we claim that $\sigma^* = e(P, P)^{xyz}\, e(dP, (h^*_{,i^*})(zP))$ will be left in some entry of F_list. Consequently, $\mathcal{B}$ has non-negligible probability

$$\varepsilon' \geq (q_F{}^{-1})(2\varepsilon - \frac{N-1}{q_{KU}} - \frac{q_{Dec}}{2^k})$$

to solve the BDHP by computing $e(dP, (h^*_{,i^*})(zP))^{-1}\sigma^*$. The computational time required for $\mathcal{B}$ is $t' \approx t + t_\lambda(2q_{Enc} + q_{Dec})$.

Q.E.D.

5. Conclusions

Key-insulated cryptosystems aim at reducing the damage caused by the key exposure. In this paper, we combine identity-based and key-insulated systems to propose the first novel IB-KIE scheme with message linkages for facilitating the encryption of a large plaintext in peer-to-peer communication networks. In addition to the inherent property of key-insulated systems that each client can periodically update his private key while the public one remains unchanged, the proposed scheme also supports unbounded time periods and random-access key-updates. By integrating with identity-based systems, it is unnecessary to maintain public key certificates. The underlining computational assumption of our scheme is based on the well-known bilinear Diffie-Hellman problem (BDHP) which is believed to be no harder than the computational Diffie-Hellman (CDH) problem and is intractable in polynomial time. Furthermore, the security requirement of confidentiality against indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2) is realized in the random oracle model. Our proposed scheme is also suitable for the encryption and transmission of DNA/RNA biological sequences and the data structure such as linked list. In the future research, we will attempt to develop an enhanced variant with error correction capability. That is, the receiving client can identify the erroneous ciphertext blocks during the transmission and request to resend only these blocks again, rather than all ones, which helps gain more bandwidth saving.

Acknowledgement

We would like to thank anonymous referees for their valuable suggestions. We thank Healthy Aging Research Center (HARC) of Chang Gung University for excellent technical assistance. This work was supported in part by the Chang Gung University Grant UARPD3B0061 and in part by the National Science Council of Republic of China under the contract numbers NSC 100-2628-H-182-001-MY3 and NSC 102-2221-E-019-041.

References

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644-654, 1976.

[2] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. IT-31, no. 4, pp. 469-472, 1985.

[3] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978. http://dx.doi.org/doi:10.1145/359340.359342

[4] C. P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161-174, 1991. http://dx.doi.org/doi:10.1007/BF00196725

[5] H. Delfs and H. Knebl, *Introduction to Cryptography: Principles and Applications*, Springer, 2002.
[6] W. Stallings, *Cryptography and Network Security: Principles and Practices*, 4th. Ed., Pearson, 2005.
[7] B. Meng, S. Wang and Q. Xiong, "A fair non-repudiation protocol," in *Proc. of the 7th International Conference on Computer Supported Cooperative Work in Design (CSCW'02)*, Brazil, pp. 68-73, 2002.
[8] A. Shamir, "Identity-based cryptosystems and signature schemes," *Advances in Cryptology – CRYPTO'84*, Springer-Verlag, pp. 47-53, 1984.
[9] Y. Dodis, J. Katz, S. Xu and M. Yung, "Key-insulated public key cryptosystems," *Advances in Cryptology – EUROCRYPT'02*, Springer-Verlag, pp. 65-82, 2002.
[10] Y. Dodis, J. Katz, S. Xu and M. Yung, "Strong key-insulated signature schemes," in *Proc. of Public Key Cryptography 2003 (PKC'03)*, LNCS 2567, Springer-Verlag, pp. 130-144, 2003.
[11] Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai, "Identity-based hierarchical strongly key-insulated encryption and its application," *Advances in Cryptology – ASIACRYPT'05*, Springer-Verlag, pp. 495-514, 2005.
http://dx.doi.org/doi:10.1007/11593447_27
[12] Y. Zhou, Z. Cao, and Z. Chai, "Identity based key insulated signature," in *Proc. of ISPEC 2006*, LNCS 3903, pp. 226-234, 2006.
http://dx.doi.org/doi:10.1007/11689522_21
[13] G. Hanaoka, Y. Hanaoka and H. Imai, "Parallel key-insulated public key encryption," in *Proc. of Public Key Cryptography 2006 (PKC'06)*, LNCS 3958, pp. 105-122, 2006.
http://dx.doi.org/doi:10.1007/11745853_8
[14] J. Weng, S. Liu, K. Chen, D. Zheng and W. Qiu, "Identity-based threshold key-insulated encryption without random oracles," in *Proc. of CT-RSA 2008*, LNCS 4964, pp. 203-220, 2008.
http://dx.doi.org/doi:10.1007/978-3-540-79263-5_13
[15] Z. Wan, X. Lai, J. Weng, S. Liu and X. Hong, "Identity-based key-insulated proxy signature," *Journal of Electronics*, vol. 26, no. 6, pp. 853-858, 2009.
http://dx.doi.org/doi:10.1007/s11767-008-0128-2
[16] C. W. Yu, Y. M. Tseng and T. Y. Wu, "A new key-insulated signature and its novel application," in *Proc. of Cryptology and Information Security Conference (CISC 2010)*, 2010.
http://dx.doi.org/doi:10.1007/s11767-008-0128-2

Chien-Lung Hsu is a Professor and the Chairman of Information Management Department at Chang Gung University (CGU), in Taiwan from August 2011. He was an Associate Professor and an Assistant Professor in the Department of Information Management of Chang Gung University from 2007 to 2011 and 2004 to 2007, respectively. He received a B.S. degree in business administration, an M.S. degree in information management, and a Ph.D. degree in information management from the National Taiwan University of Science and Technology, Taiwan in 1995, 1997, and 2002, respectively. He is also the director of the Ubiquitous Security and Applications Lab, the director of Chinese Cryptology & Information Security Association, the chair of Program of RFID Applications in Logistics Supply Chain Management of CGU, the chair of Program of Information Security with Medical Applications of CGU, the director of Division of Instructional Support of Computer Center of CGU, the researcher of Healthy Aging Research Center (HARC) of CGU, the researcher of Elder Industry Development and Research Center (EIDRC) of CGU, and the senior researcher of Taiwan Information Security Center (TWISC). His current research includes cryptography, information security, wireless sensor network, mobile commerce, digital forensics, vehicular system security, healthcare system and user acceptance, smart home system, etc.

Han-Yu Lin received his Ph.D. degree in computer science and engineering from the National Chiao Tung University, Taiwan in 2010. He served as a part-time Assistant Professor in both the Department of Information Management, Chang Gung University, Taiwan and the Department of Information Management, Kainan University, Taiwan from 2011. He was an engineer in CyberTrust Technology Institute, Institute for Information Industry, Taiwan from January 2012 to July 2012. Since August 2012, he has been an Assistant Professor in the Department of Computer Science and Engineering, National Taiwan Ocean University, Taiwan. His research interests include Cryptology, Network Security, Digital Forensics, RFID Privacy and Application, Cloud Computing Security and E-commerce Security.