Perspectives in Science (2016) 7, 81—86

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/pisc

Proceedings of the 1st Czech-China Scientific Conference 2015
Perspectives in Science

A brief review of revocable ID-based public key cryptosystem☆

Tsu-Yang Wu[a,b,*], Jerry Chun-Wei Lin[a,b], Chien-Ming Chen[a,b], Yuh-Min Tseng[c], Jaroslav Frnda[d], Lukas Sevcik[d], Miroslav Voznak[d]

[a] Shenzhen Graduate School, Harbin Institute of Technology, China
[b] Shenzhen Key Laboratory of Internet Information Collaboration, Shenzhen, China
[c] Department of Mathematics, National Changhua University of Education, Taiwan, ROC
[d] Department of Telecommunications, Faculty of Electrical Engineering and Computer Science, VSB-Technical University of Ostrava, 17. listopadu 15, Ostrava-Poruba 708 00 Czech Republic

Received 26 October 2015; accepted 11 November 2015
Available online 10 December 2015

KEYWORDS
Identity-based;
Revocable;
Encryption;
Bilinear pairings

Summary The design of ID-based cryptography has received much attention from researchers. However, how to revoke the misbehaviour/compromised user in ID-based public key cryptosystem becomes an important research issue. Recently, Tseng and Tsai proposed a novel public key cryptosystem called revocable ID-based public key cryptosystem (RIBE) to solve the revocation problem. Later on, numerous research papers based on the Tseng-Tsai key RIBE were proposed. In this paper, we brief review Tseng and Tsai's RIBE. We hope this review can help the readers to understand the Tseng and Tsai's revocable ID-based public key cryptosystem.

Introduction

In the traditional public key cryptosystems (Diffie and Hellman, 1976; ElGamal, 1985; Rivest et al., 1978), certificates play important roles to make publicly available the mapping between identities and public keys. Certificate is a signature generated by a trusted certificate authority (CA) which usually include the identity of a user, its associated public key, the issuing date and the expiration date. When user's public key is used, the associated certificate must be checked to ensure its validity (revoked or non-revoked). In general, Certificate Revocation List (CRL) (Housley et al., 2002) is used to revoke the user's public key. Anyone can check these revoked users' public keys by querying the CRL.

In order to solve the management of users' certificates, Shamir (1984) first proposed the concept of ID-based public key cryptosystem (ID-PKS). In his system, each user's

☆ This article is part of a special issue entitled ''Proceedings of the 1st Czech-China Scientific Conference 2015''.

* Corresponding author at: Shenzhen Graduate School, Harbin Institute of Technology, China.
URL: https://www.linkedin.com/in/tsu-yang-wu-4a6b029a/en (T.-Y. Wu).

http://dx.doi.org/10.1016/j.pisc.2015.11.014

identity (e.g. e-mail address or social security number) can be viewed as public key and the user's private key is generated by a trusted private key generation center (PKG). However, Shamir' ID-PKS was not easy in practice because the underlying mathematical methods are not suitable. In 2001, Boneh and Franklin, (2001) followed Shamir's concept to propose a practical ID-based encryption scheme (IBE) from the Weil pairing. Later on, the design of ID-based cryptographic schemes and protocols using bilinear pairings has received much attention from researchers.

For the revocation problem in the ID-PKS system, Boneh and Franklin, (2001) have suggested a solution in which the PKG can periodically renew the private keys for non-revoked users. In other words, when the PKG wants to revoke a specific user, it only stops to issue the new private key. However, this solution has following drawbacks: (1) the workload of generating new private keys of non-revoked users is too heavy for the PKG; (2) secure channels are needed between the PKG and the non-revoked users to transmit the new private keys for each time period.

Boldyreva et al. (2008) proposed a revocable ID-based encryption scheme (RIBE) by using binary tree to reduce the PKG's workload in the Boneh—Franklin IBE. Unfortunately, their scheme is based on the relaxed selective-ID model (Canetti et al., 2003), a weak security model. In the next year, Libert and Vergnaud (2009) based on the Boldyreva et al.'s RIBE to propose a more secure RIBE scheme under an adaptive-ID model, a strong security model. Seo and Emura (2013a) demonstrated Boldyreva et al.'s RIBE (Boldyreva et al., 2008) is vulnerable to the decryption key exposure. They also proposed a provably secure tree-based revocable ID-based encryption scheme. Subsequently, Seo and Emura (2013b) presented a hierarchical revocable ID-based encryption scheme which solved the open problem mentioned in the Libert—Vergnaud RIBE.

Tseng and Tsai (2012) proposed a practical RIBE scheme over a public channel. The key construction their scheme is different from the previous schemes (Boldyreva et al., 2008; Libert and Vergnaud, 2009; Seo and Emura, 2013a,b). In the Tseng-Tsai RIBE, each user's private key consists of a fixed initial private key and an updating time key, where the updating time key is renewed along with the current period. For an honest (non-revoked) user, the PKG periodically issues new time key and sends it to the user via a public channel. Upon receiving the new time key, the user can renew her/his private key by herself/himself. To revoke a malicious/misbehaviour user, the PKG only stops issuing the new time key in current period. In other words, the malicious/misbehaviour user cannot compute the newest private. She/he cannot execute any cryptographic behaviours in later periods. Later on, several revocable ID-based cryptographic schemes and protocols based on the key construction of the Tseng-Tsai RIBE were proposed such as encryption (Tsai et al., 2012, 2014), signature (Hung et al., 2014; Tsai et al., 2013; Wu et al., 2012a), signcryption (Wu et al., 2012b), and authenticated group key exchange (Wu et al., 2012, 2014).

In this paper, we brief review Tseng and Tsai's RIBE scheme which contains the underlying mathematical problems and assumptions, the framework of RIBE, a concrete RIBE scheme, the security notion of RIBE, the security analysis of RIBE (sketched), and a full RIBE scheme. We hope this review can help the readers to understand the Tseng and Tsai's revocable ID-based public key cryptosystem.

Underlying mathematical problems and assumptions

Bilinear pairings

Bilinear pairings defined on elliptic curves over finite fields have been used to establish many ID-based cryptographic mechanisms. Let G_1 be an additive cyclic group of large prime order q and G_2 be a multiplicative cyclic group of the same order q. Specifically, particular, G_1 is a subgroup of the group of points on an elliptic curve over a finite field and G_2 is a subgroup of the multiplicative group over a finite field. A bilinear pairing is a map e: $G_1 \times G_1 \rightarrow G_2$ and satisfies the following three properties:

(1) Bilinear. $e(aP, bQ) = e(P, Q)^{ab}$, for all P, $Q \in G_1$ and $a, b \in Z_q^*$.
(2) Non-degenerate. There exist P, $Q \in G_1$ such that $e(P, Q) \neq 1$.
(3) Computable. For all P, $Q \in G_1$, there is an efficient algorithm to compute $e(P, Q)$.

A bilinear map that satisfies the above three properties is called an admissible bilinear map. Such non-degenerate admissible bilinear maps can be obtained from the Weil, Tate, or Ate pairings over supersingular elliptic curves or abelian varieties (Boneh and Franklin, 2001; Chen et al., 2007). Some research results (Galbraith et al., 2008; Wu and Tseng, 2010) for the relationship between security levels and speed of pairing computations on microprocessors were presented.

Bilinear Diffie—Hellman (BDH) assumption

The BDH assumption is often used in the security proof of ID-based encryption scheme. The BDH problem is described as follows. Given P, aP, bP, $cP \in G_1$ for some a, b, $c \in Z_q^*$, this problem is to compute the value $e(P, P)^{abc} \in G_2$. The BDH assumption is stated as follows.

Definition 1 *(BDH assumption)*. Given an additive cyclic group G_1 and P, aP, bP, $cP \in$ G$_1$ for unknown a, b, $c \in Z_q^*$, no probabilistic polynomial time (PPT) algorithm A with non-negligible probability which can compute $e(P, P)^{abc} \in G_2$. The successful probability (advantage) of A is presented as

$$\begin{aligned} \mathrm{Adv}_A &= Pr[P \in G_1, a, b, c \in Z_q^* | A(P, aP, bP, cP) \\ &= e(P, P)abc \in G_2], \end{aligned}$$

where the probability is over the random choice consumed by A.

Framework of the Tseng-Tsai RIBE

The Tseng-Tsai RIBE consists of two roles: a trusted PKG and users. Without loss of generality, the whole lifetime of the system is divided into distinct time periods 1, 2, ..., z. For simplicity, these time periods may be viewed as 1 day, 1 week, or 1 month. The PKG selects a master secret key and generates public parameters. For a given user's identity ID, the PKG computes his/her associated initial private key and sends it to the user via a secure channel. At the beginning of each time period, the PKG uses the master secret key to generate a time updating key for each non-revoked user's identity ID and then sends them to users via a public channel. For a revoked user, it is unable to receive the associated time updating key in the current time period.

Remark 1. For a RIBE, the point is that any sender can encrypt a message to some identity ID without concerning with the key updating process. In a RIBE, encrypting a message m to a receiver with identity ID during time period i that results in a ciphertext tuple (ID, i, C). Upon receiving (ID, i, C), a non-revoked user with the valid private key can recover the message m.

A RIBE with a public channel is a 5-tuple of polynomial-time algorithms (G, *IKE*, *TKU*, E, D):

(1) System setup algorithm G is a probabilistic algorithm that takes as input a security parameter 1^k and the total number z of time periods. It returns a master private key and the public parameters *Parms*. The public parameters *Parms* are made public and implicitly inputted to all the following algorithms.
(2) Initial key extract algorithm *IKE* is a deterministic algorithm that takes as input the master private key s and a user's identity ID $\in \{0, 1\}^*$, and then returns the user's initial secret key DID.
(3) Time key updating algorithm *TKU* takes as input the master private key s, a user's identity ID $\in \{0, 1\}^*$ and a time period i, and then returns the user's time update key TID_i.
(4) Encryption algorithm E takes as input a time period i, a message m and a user's ID. Then it returns a ciphertext C.
(5) Decryption algorithm D takes as input a ciphertext C and an entire private key DID_i. Then it returns a plaintext m.

Remark 2. The user's entire private key DID_i for the time period i is not explicitly provided for the user. Each legitimate (non-revoked) user may obtain the corresponding entire decryption key DID_i by $\mathrm{DID}_i = \mathrm{DID} + \mathrm{TID}_i$, where the user's initial private key DID is generated by the initial key extract algorithm and the user's time updating key TID_i is periodically generated by the PKG along with time.

Concrete basic RIBE scheme

Basic RIBE scheme consists of five algorithms: the system setup, the initial key extract, the time key updating, the encryption, and the decryption algorithms.

(1) *System setup*. Given a security parameter k and the total number z of time periods, a trusted private key generator (PKG) generates two groups G_1, G_2 of prime order $q > 2^k$, an admissible bilinear map e: $G_1 \times G_1 \to G_2$ and a generator P of G_1. The PKG randomly chooses a master secret key $s \in Z_q^*$ and computes $P_{pub} = s \cdot P \in G_1$ as the system public key. The PKG picks three hash functions H_0: $\{0, 1\}^* \to G_1$, H_1: $\{0, 1\}^* \to G_1$, and H_2: $G_2 \to \{0, 1\}^n$. The public parameters and functions are presented as $\mathrm{Parms} = \{q, G_1, G_2, e, P, P_{pub}, H_0, H_1, H_2\}$.
(2) *Initial key extract*. For a given user's identity ID $\in \{0, 1\}^*$, the PKG computes $\mathrm{QID} = H_1(\mathrm{ID})$ and the associated initial secret key $\mathrm{DID} = s \cdot \mathrm{QID} \in G_1$. Then DID is transmitted to the user via a secure channel.
(3) *Time key updating*. Given a non-revoked user's identity ID and time period i, the PKG computes $\mathrm{RID}_i = H_0(\mathrm{ID}, i)$ and the associated user's time update key $\mathrm{TID}_i = s \cdot \mathrm{RID}_i \in G_1$ for time period i. The PKG sends TID_i to the user using a public channel. Thus, the non-revoked user can update his/her entire private key $\mathrm{DID}_i = DID + \mathrm{TID}_i$ for time period i.
(4) *Encryption*. In time period i, given a message m and a non-revoked receiver with identity ID, a sender chooses a random number $r \in Z_q^*$ and computes $\mathrm{QID}_i = \mathrm{QID} + \mathrm{RID}_i = H_1(\mathrm{ID}) + H_0(\mathrm{ID}, i)$. Then, the sender uses QID_i to compute $U = r \cdot P$ and $V = m \oplus H_2(g^r)$, where $g = e(\mathrm{QID}_i, P_{pub})$. The ciphertext for the message m is $C = (U, V)$.
(5) *Decryption*. Given a ciphertext $C = (U, V)$, the receiver can use his/her entire decryption key to compute $V \oplus H_2(e(\mathrm{DID}_i, U)) = m$.

Here, we present the correctness of the decryption equation as follows:

$$\begin{aligned} V \oplus H_2(e(\mathrm{DID}_i, U)) &= V \oplus H_2(e(s \cdot H_1(\mathrm{ID}) + s \cdot H_0(\mathrm{ID}, i), r \cdot P)) \\ &= V \oplus H_2(e(s \cdot H_1(\mathrm{ID}) + s \cdot H_0(\mathrm{ID}, i), P)^r) \\ &= V \oplus H_2(e(H_1(\mathrm{ID}) + H_0(\mathrm{ID}, i), s \cdot P)^r) \\ &= V \oplus H_2(e(\mathrm{QID}_i, P_{pub})^r). \end{aligned}$$

Security analysis of basic RIBE scheme

Security notions

Tseng and Tsai followed the security requirement of IBE (Boneh and Franklin, 2001) to propose the requirements of RIBE. A RIBE is semantically secure against an adaptive CPA (IND-RID-CPA) if no PPT adversary A has a non-negligible advantage against the challenger B in the following IND-RID-CPA game:

(1) *System setup*. The challenger B runs the *System setup algorithm*. It gives the adversary A the resulting public parameters *Parms* and B keeps the master private key s.
(2) *Phase* 1. The adversary A may make a number of different queries adaptively to the challenger B as follows:
    (i) *Initial key extract query* (ID). Upon receiving this query with ID, the challenger B runs the initial key extract algorithm *IKE* to return the user's initial secret key DID to A.
    (ii) *Time key updating query* (ID, i). The challenger B responds by running the time key update algorithm

TKU to generate the user's time updating key TID_i corresponding to the time period *i* and the identity ID. It returns TID_i to *A*.

(3) *Challenge*. The adversary *A* outputs a target plaintext pair (M_0, M_1) and target identity (ID^*, i^*). A restriction here is that either ID* or (ID^*, i^*) did not appear in the initial key extract query or the time key updating query, respectively. The challenger *B* picks $\beta \in \{0, 1\}$ at random and creates a target ciphertext $C^* = E(\text{ID}^*, i^*, M_\beta)$. Then the challenger *B* returns C^* to *A*.

(4) *Phase* 2. The adversary *A* may issue more queries as follows:
   (i) Initial key extract query (ID) as in Phase 1.
   (ii) Time key updating query (ID, *i*) as in Phase 1.

   The restriction here is that either ID* or (ID^*, i^*) is disallowed to be queried in the initial key extract query or the time key update query, respectively.

(5) *Guess*. The adversary *A* outputs its guess $\beta' \in \{0, 1\}$ and wins this game if $\beta' = \beta$.

We refer to such an adversary *A* as an IND-RID-CPA adversary. We define the adversary *A*'s advantage in attacking the RIBE as the following function of the security parameter *k*: $\text{Adv}_A(k) = |\Pr[\beta' = \beta] - 1/2|$.

Definition 2. We say that a RIBE is semantically secure against an adaptive CPA if, for any polynomial time IND-RID-CPA adversary *A*, the function $\text{Adv}_A(k)$ is negligible.

Then, a more secure security model than CPA model is introduced called CCA model. We say that a RIBE is semantically secure against an adaptive CCA (IND-RID-CCA) if no PPT adversary *A* has a non-negligible advantage against the challenger *B* in the following IND-RID-CCA game:

(1) *System setup*. As in the IND-RID-CPA game.

(2) *Phase* 1. The adversary *A* may make a number of different queries adaptively to the challenger *B* as follows:
   (i) *Initial key extract query* (ID). As in the IND-RID-CPA game.
   (ii) *Time key updating query* (ID, *i*). As in the IND-RID-CPA game.
   (iii) *Decryption query* (ID, *i*, *C*). Upon receiving the query, the challenger *B* obtains an entire decryption key associated with (ID, *i*) which is denoted by DID_i. The entire decryption key DID_i is implicitly obtained by issuing the initial key extract query (ID) and the time key update query (ID, *i*). *B* runs the decryption algorithm *D* to decrypt the ciphertext *C* using this entire decryption key DID_i. Then it returns $D(\text{DID}_i, C)$ to *A*.

(3) *Challenge*. The adversary *A* outputs a target plaintext pair (M_0, M_1) and target identity (ID^*, i^*). A restriction here is that either ID* or (ID^*, i^*) did not appear in the initial key extract query or the time key updating query, respectively. The challenger *B* picks $\beta \in \{0, 1\}$ at random and creates a target ciphertext $C^* = E(\text{ID}^*, i^*, M_\beta)$. Then the challenger *B* returns C^* to *A*.

(4) *Phase* 2. The adversary *A* may issue more queries as follows:
   (i) Initial key extract query (ID) as in Phase 1.
   (ii) Time key update query (ID, *i*) as in Phase 1.
   (iii) *Decryption query* (ID, *i*, *C*). The challenger *B* responds as in *Phase* 1, where $(\text{ID}, i, C) \neq (\text{ID}^*, i^*, C^*)$.

   The restriction here is that either ID* or (ID^*, i^*) is disallowed to be queried in the initial key extract query or the time key update query, respectively.

(5) *Guess*. The adversary *A* outputs its guess $\beta' \in \{0, 1\}$ and wins this game if $\beta' = \beta$.

We refer to such an adversary *A* as an IND-RID-CCA adversary. We define the adversary *A*'s advantage in attacking the RIBE as the following function of the security parameter *k*: $\text{Adv}_A(k) = |\Pr[\beta' = \beta] - 1/2|$.

Definition 3. We say that a RIBE is semantically secure against an adaptive CPA if, for any polynomial time IND-RID-CCA adversary *A*, the function $\text{Adv}_A(k)$ is negligible.

Remark 3. In the IND-RID-CPA and IND-RID-CCA games, an adversary *A* is disallowed to issue both an *initial key extract query* on ID* and a *time key update query* on (ID^*, i^*) because it is obvious that the user's entire decryption key DID_i^* will be revealed. Hence, it is only allowed that the adversary *A* may issue either the *initial key extract query* on ID* or the *time key updating query* on (ID^*, i^*). If the *initial key extract query* on ID* is allowed, it simulates the ability of a revoked user (an inside adversary) without the corresponding time key update key TID_i^* for time period i^*. On the other hand, an outside adversary is only allowed to obtain the time key update key TID_i^* for time period i^*. Certainly, the adversary *A* is allowed to obtain the initial key and the time key for any other ID and any time period.

Security analysis (CPA)

Tseng and Tsai applied the work of Boneh and Franklin, (2001) to provide a tight security proof in the random model (Bellare and Rogaway, 1993; Canetti et al., 2004). The following two theorems are given to show that the Basic RIBE scheme is semantically secure against adaptive CPA (IND-RID-CPA) for the outside adversary and the revoked user (or an inside adversary).

Theorem 1. *Suppose that the hash functions H_0, H_1, and H_2 are random oracles. Then the basic RIBE is a semantically outsider-secure IBE scheme (IND-O-RID-CPA) assuming that the BDH problem is hard in groups generated by G. Concretely, assume that there is an outside adversary A that has advantage $\varepsilon(k)$ against the Basic RIBE scheme. Suppose that A makes at most $q_E > 0$ initial key extraction queries, $q_U > 0$ time key updating queries, and $q_{Hi} > 0$ queries to hash functions H_i ($i = 0, 1, 2$). Then there is an algorithm B that solves the BDH problem in groups generated by G with advantage at least $\text{Adv}_{G,B}(k) = 2\varepsilon(k)/[e(1 + q_E) \cdot q_{H2}]$, where e is the base of the natural logarithm.*

Theorem 2. *Suppose that the hash functions H_0, H_1, and H_2 are random oracles. Then the basic RIBE is a semantically insider-secure IBE scheme (IND-I-RID-CPA) assuming that the BDH problem is hard in groups generated by G. Concretely, assume that there is an outside adversary A that has advantage $\varepsilon(k)$ against the basic RIBE scheme. Suppose that A* *makes at most $q_E > 0$ initial key extraction queries, $q_U > 0$ time key updating queries, and $q_{Hi} > 0$ queries to hash functions H_i ($i = 0, 1, 2$). Then there is an algorithm B that solves the BDH problem in groups generated by G with advantage at least $Adv_{G,B}(k) = 2\varepsilon(k)/[e(1+q_U)\cdot q_{H2}]$, where e is the base of the natural logarithm.*

Full RIBE scheme

Fujisaki and Okamoto (1999) presented a simple conversion from a weak public-key encryption scheme (IND-CPA) to a strong public-key encryption scheme (IND-CCA) in the random oracle model. Kitagawa et al. (2006) proposed an improvement on Fujisaki and Okamoto's (1999) conversion to IBE. They can transform a weak IBE scheme (IND-ID-CPA) to a strong IBE scheme (IND-ID-CCA). In Kitagawa et al.'s conversion, a weak IBE scheme (IND-ID-CPA) must be γ-uniformity, where γ-uniformity means that the used hash functions are random oracles. Meanwhile, the weak IBE scheme must be proved to be semantically secure against an adaptive CPA (IND-RID-CPA). Meanwhile, an extra hash function (also random oracle) must be added to the system to achieve strong IBE scheme.

Based on the basic RIBE scheme (IND-RID-CPA), Tseng and Tsai applied the transformation technique (Kitagawa et al., 2006) to construct the full RIBE scheme (IND-RID-CCA). The full RIBE scheme consists of five algorithms that include the *system setup*, the *initial key extract*, the *time key updating*, the *encryption*, and the *decryption* algorithms.

(1) *System setup*. As in the basic RIBE scheme. In addition, the other hash function $H_3 : \{0,1\}^l \times \{0,1\}^{n-l} \times \{0, l\}^* \to Z_q^*$ is needed.
(2) *Initial key extract*. As in the basic RIBE scheme.
(3) *Time key updating*. As in the basic RIBE scheme.
(4) *Encryption*. In time period *i*, given a message $m \in \{0,\ 1\}^l$ and a non-revoked receiver with identity ID, a sender chooses a random number $\sigma \in \{0,\ 1\}^{n-l}$ and sets $r = H_3(m,\ \sigma,\ \mathrm{ID})$. Then the sender computes $\mathrm{QID}_i = \mathrm{QID} + \mathrm{RID}_i = H_1(\mathrm{ID}) + H_0(\mathrm{ID},\ i)$ and uses QID_i to compute $U = r\cdot P$ and $V = (m||\sigma) \oplus H_2(g^r)$, where $g = e(\mathrm{QID}_i,\ P_{\mathrm{pub}})$. The ciphertext for the message is $C = (U,\ V)$.
(5) *Decryption*. Given a ciphertext $C = (U,\ V)$, the non-revoked receiver with identity ID can use his/her entire private key DID_i to do the following procedures:
   (i) Computing $V \oplus H_2(e(\mathrm{DID}_i,\ U)) = m'$ and let $[m']^l = m$ and $[m']^{n-l} = \sigma$, where $[a]^b$ and $[a]_b$ denote the first and the last *b* bits of a string *a*, respectively.
   (ii) Testing that $(H_3(m,\ \sigma,\ \mathrm{ID})\cdot P,\ m' \oplus H_2(g^r)) = (U,\ V) = C$. If it does not hold, then the receiver rejects it.
   (iii) Outputting *m*as the decryption of *C*.

For the general transformation from a basic IBE scheme with γ-uniformity to a full IBE scheme, Kitagawa et al. have already given a theorem to prove the security of the full IBE scheme (IND-ID-CCA) using the basic IBE scheme (IND-ID-CPA). Here, we introduce their theorem. Without loss of generality, let Π_1 and Π_2 be the basic IBE scheme and the full IBE scheme, respectively. An extra hash function is $H : \{0,1\}^l \times \{0,1\}^{n-l} \times \{0, l\}^* \to Z_q^*$.

Theorem 3. *Suppose that the hash function H is a random oracle and Π_1 is a γ-uniform basic IBE scheme. Let A be an IND-ID-CCA adversary that has an advantage $\varepsilon(k)$ against the full IBE scheme Π_2. Suppose the challenger B makes at most $q_H > 0$ queries to hash function H, $q_E > 0$ initial key extraction queries, and $q_D > 0$ decryption queries. Then, there is an IND-ID-CPA adversary that has advantage at least $(\varepsilon(k) + 1/2 - q_H/2^{n-l})\cdot(1 - \gamma q_D) - 1/2$ against the basic IBE scheme Π_1.*

Since the hash functions used in the basic RIBE scheme are random oracles, it is γ-uniformity (Fujisaki and Okamoto, 1999; Kitagawa et al., 2006). The full RIBE scheme is constructed from basic RIBE scheme by applying the general transformation technique proposed by Kitagawa et al. (2006). Thus, we can enjoy Theorem 3 to obtain two theorems, directly. The following two theorems state that the full RIBE is semantically outsider-secure (IND-O-RID-CCA) and insider-secure (IND-I-RID-CCA) based on the basic RIBE scheme.

Theorem 4. *Suppose that the hash function H_3 is a random oracle. Let A be an outsider adversary (IND-O-RID-CCA) which has advantage $\varepsilon(k)$ against the full RIBE scheme. Suppose the challenger B makes at most $q_{Hi} > 0$ queries to hash functions H_i ($i = 0, 1, 2, 3$), $q_E > 0$ initial key extraction queries, $q_U > 0$ time key updating queries, and $q_D > 0$ decryption queries. Then there is an outsider adversary (IND-O-RID-CPA) that has advantage at least $(\varepsilon(k) + 1/2 - q_{H3}/2^{n-l})\cdot(1 - \gamma q_D) - 1/2$ against the basic RIBE scheme.*

Theorem 5. *Suppose that the hash function H_3 is a random oracle. Let A be an insider adversary (IND-I-RID-CCA) which has advantage $\varepsilon(k)$ against the full RIBE scheme. Suppose the challenger B makes at most $q_{Hi} > 0$ queries to hash functions H_i ($i = 0, 1, 2, 3$), $q_E > 0$ initial key extraction queries, $q_U > 0$ time key updating queries, and $q_D > 0$ decryption queries. Then there is an outsider adversary (IND-I-RID-CPA) that has advantage at least $(\varepsilon(k) + 1/2 - q_{H3}/2^{n-l})\cdot(1 - \gamma q_D) - 1/2$ against the basic RIBE scheme.*

Conclusion

In this paper, we have given a brief review of Tseng and Tsai's RIBE. We have introduced the underlying mathematical problems and assumptions, framework of RIBE, two concrete RIBE schemes (basic RIBE and full RIBE), sketched security analysis of two RIBE schemes. For the details of security analysis, readers can refer to the full paper.

Conflict of interest

The authors declare that there is no conflict of interest.

Acknowledgements

This publication has been created within the project Support of VŠB-TUO activities with China with financial support from the Moravian-Silesian Region and partially was supported by the grant SGS reg. no. SP2015/82 conducted at VSB-Technical University of Ostrava, Czech Republic, and was partially supported by the Natural Scientific Research Innovation Foundation in Harbin Institute of Technology under grant no. HIT.NSRIF.2015089, by the National Natural Science Foundation of China under grant no. 61402135, by the Shenzhen Strategic Emerging Industries Program of China under grant no. ZDSY20120613125016389.

References

Bellare, M., Rogaway, P., 1993. Random oracles are practical: a paradigm for designing efficient protocols. In: Proceedings of the 1st ACM Conference on Computer and Communications Security, pp. 62—73.

Boldyreva, A., Goyal, V., Kumart, V., 2008. Identity-based encryption with efficient revocation. In: Proceedings of the 15th ACM Conference on Computer and Communications Security, pp. 417—426.

Boneh, D., Franklin, M., 2003. Identity-based encryption from the Weil pairing. SIAM J. Comput. 32 (3), 586—615, Preliminary version: Advances in Cryptology — CRYPTO 2001, LNCS 2139, 213—229.

Canetti, R., Goldreich, O., Halevi, S., 2004. The random oracle methodology, revisited. J. ACM 51, 557—594.

Canetti, R., Halevi, S., Katz, J., 2007. A forward-secure public key encryption scheme. J. Cryptol. 20 (3), 265—294, Preliminary version: Advances in Cryptology — EUROCRYPT 2003, LNCS 2656, 255—271.

Chen, L., Cheng, Z., Smart, N.P., 2007. Identity-based key agreement protocols from pairings. Int. J. Inf. Secur. 6, 213—241.

Diffie, W., Hellman, M.E., 1976. New directions in cryptography. IEEE Trans. Inf. Theory 22 (6), 644—654.

ElGamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inf. Theory 31 (4), 469—472.

Fujisaki, E., Okamoto, T., 1999. How to enhance the security of public key encryption at minimum cost. In: Proceedings of 2nd International Workshop on Practice and Theory in Public Key Cryptography, LNCS 1560, pp. 53—68.

Galbraith, S., Paterson, K., Smart, N.P., 2008. Pairings for cryptographers. Discrete Appl. Math. 156, 3113—3121.

Housley, R., Polk, W., Ford, W., Solo, D., 2002. Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile, RFC 3280. IETF, CA.

Hung, Y.H., Tsai, T.T., Tseng, Y.M., Huang, S.S., 2014. Strongly secure revocable ID-based signature without random oracles. Inf. Technol. Control 43 (3), 264—276.

Kitagawa, T., Yang, P., Hanaoka, G., Zhang, R., Matsuura, K., Imai, H., 2006. Generic transforms to acquire CCA-security for identity based encryption: the cases of FOPKC and REACT. In: Proceedings of 11th Australasian Conference on Information Security and Privacy, LNCS 4058, pp. 348—359.

Libert, B., Vergnaud, D., 2009. Adaptive-ID secure revocable identity-based encryption. Top. Cryptol. — CT-RSA, LNCS 5473, 1—15.

Rivest, R., Shamir, A., Adleman, L., 1978. A method for obtaining digital signatures and public key cryptosystems. CACM 21 (2), 120—126.

Seo, J.H., Emura, K., 2013a. Revocable identity-based encryption revisited: security model and construction. In: Proceedings of 16th International Conference on Practice and Theory in Public Key Cryptography, LNCS 7778, pp. 216—234.

Seo, J.H., Emura, K., 2013b. Efficient delegation of key generation and revocation functionalities in identity-based encryption. Top. Cryptol. — CT-RSA, LNCS 7779, 343—358.

Shamir, A., 1984. Identity-based cryptosystems and signature schemes. Adv. Cryptol. — CRYPTO, LNCS 196, 47—53.

Tsai, T.T., Tseng, Y.M., Wu, T.Y., 2012. A fully secure revocable ID-based encryption in the standard model. Informatica 23 (3), 487—505.

Tsai, T.T., Tseng, Y.M., Wu, T.Y., 2013. Provably secure revocable ID-based signature in the standard model. Secur. Commun. Netw. 6 (10), 1250—1260.

Tsai, T.T., Tseng, Y.M., Wu, T.Y., 2014. RHIBE: constructing revocable hierarchical ID-based encryption from HIBE. Informatica 25 (2), 299—326.

Tseng, Y.M., Tsai, T.T., 2012. Efficient revocable ID-based encryption with a public channel. Comput. J. 55 (4), 475—486.

Wu, T.Y., Tsai, T.T., Tseng, Y.M., 2012. Revocable ID-based signature scheme with batch verifications. In: Proceedings of the 8th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 49—54.

Wu, T.Y., Tsai, T.T., Tseng, Y.M., 2012a. A revocable ID-based signcryption scheme. J. Inf. Hiding Multimedia Signal Process. 3 (3), 240—251.

Wu, T.Y., Tseng, Y.M., 2010. An ID-based mutual authentication and key exchange protocol for low-power mobile devices. Comput. J. 53 (7), 1062—1070.

Wu, T.Y., Tseng, Y.M., Tsai, T.T., 2012b. A revocable ID-based authenticated group key exchange protocol with resistant to malicious participants. Comput. Netw. 56 (12), 2994—3006.

Wu, T.Y., Tsai, T.T., Tseng, Y.M., 2014. A provably secure revocable ID-based authenticated group key exchange protocol with identifying malicious participants. Sci. World J. 2014, Article ID 367264, 10 pp.