Journal of Information Hiding and Multimedia Signal Processing ©2012 ISSN 2073-4212
Ubiquitous International Volume **3**, Number **3**, July **2012**

A Revocable ID-based Signcryption Scheme

Tsu-Yang Wu

Innovative Information Industry Research Center
Harbin Institute of Technology Shenzhen Graduate School
Shenzhen 518055, P.R. China
wutsuyang@gmail.com

Tung-Tso Tsai and Yuh-Min Tseng

Department of Mathematics
National Changhua University of Education
Jin-De Campus, Chang-Hua City 500, Taiwan, R.O.C.
d98211001@mail.ncue.edu.tw; ymtseng@cc.ncue.edu.tw

Received February 2012; revised July 2012

Abstract. *Signcryption scheme can efficiently perform encryption and signing procedures in a single step to obtain message confidentiality and non-reputation properties. As compared to the traditional public key system, identity (ID)-based public key system (IDPKS) can simplify the management of required certificates. However, how to revoke these compromised or misbehaving identities in the IDPKS becomes a critical problem. Recently, Tseng and Tsai proposed a novel construction in the IDPKS with revocation mechanism called revocable ID-based public key system (R-IDPKS). In this paper, we follow their R-IDPKS to propose an important cryptographic primitive "signcryption". Security analysis is made to demonstrate that the proposed scheme is provably secure and provides confidentiality and unforgeability.*
Keywords: Signcryption, Identity-based, Revocation, Bilinear pairings, Cryptography

1. **Introduction.** In cryptography, encryption and digital signature are two fundamentals to provide message confidentiality and non-reputation properties. Precisely, an encryption scheme must guarantee that any information about plaintext form ciphertext cannot be learned and a signature scheme must guarantee that a valid signature on a message cannot be forged by any adversary. Nevertheless, many cryptographic applications such as secure channel establishment protocols and secure e-mail system are required to combine the confidentiality and non-reputation properties simultaneously. To achieve it, Zheng [1] proposed the concept of signcryption (or called authenticated encryption) in 1997. In signcryption scheme, it can efficiently perform encrypting and signing procedures in a single step. Later on, there are many signcryption schemes based on the traditional public key system and the ID-based public key system were presented in [2, 3, 4, 5, 6, 7, 8, 9].

In the traditional public key system, certificates are made publicly available the mapping between users public keys and identities. It is a signature generated by a trusted certificate authority (CA) which binds various information including identity, associated public key, issuing and expiration date. In some situations, it requires the users certificate must be revoked before its expiration date. For instance, the employees certificate may request revocation while he/she leaves the company because he/she has not entitled to use the associated public key. Hence, the users certificate must be checked to guarantee that

it has not been revoked and is still valid before public key is used. In general, Certificate revocation list (CRL) [10] is used to revoke the users public keys. Users can become aware of the revoked public keys by querying the CRL. Actually, efficient revocation problem is well-studied in the traditional public key system [11, 12, 13, 14, 15].

In 1984, Shamir [16] introduced the concept of identity (ID)-based public key system (IDPKS) to simplify the management of required certificates. In particular, each user's public key is determined by his/her identity such as e-mail address or social security number in the IDPKS. Later on, Boneh and Franklin [17] followed the Shamir's concept to propose the first practical ID-based encryption scheme using the Weil pairing in 2001. Thus, the design of ID-based cryptographic schemes and protocols from bilinear pairings has received much attention from researchers. A numerous primitives have been published in this topic such as encryption [18, 19], signature [20, 21, 22], signcryption [4, 5], key agreement [23, 24, 25], group key agreement [26, 27, 28], and authentication [29, 30].

As we all know, the advantage of IDPKS is to simplify the management of users certificates but it is a critical problem that how to revoke compromised or misbehaving identities in the IDPKS. To solve this issue, Boneh and Franklin [17] have suggested that the private key generator (PKG) can periodically renew private keys for non-revoked users. However, the suggestion exist the following two disadvantages that (1) the workload of renewing private keys is too heavy for the PKG; (2) it requires secure channels between the PKG and these non-revoked users to transmit renewed private keys. In 2008, Boldyreva *et al.* [31] presented a revocable IBE (RIBE) scheme to reduce the PKG's workload mentioned in [17]. In the next year, Libert and Vergnaud [32] presented an adaptive-ID secure RIBE scheme to enhance the security of Boldyreva *et al.*'s work [31]. Though the three schemes [17, 31, 32] provide revocation mechanism in the IDPKS, they still exist some drawbacks.

Recently, Tseng and Tsai [33] proposed a novel construction in the IDPKS with revocation mechanism called revocable ID-based public key system (R-IDPKS). In their system, each user's private key contains two parts: a fixed initial private key and an update key, where the update key is renewed along with time period. For a non-revoked user, the PKG periodically renews update key and sends it to the user via a public channel. Upon receiving the new update key, these non-revoked users can update own private keys by themselves. It is easy to see that these compromised/misbehaving users can be revoke in the IDPKS while the PKG stops to issue the new update keys. Meanwhile, Tseng and Tsai also defined the framework and related security requirements for the R-IDPKS. Very recently, Wu *et al.* followed the Tseng-Tsai R-IDPKS [33] to propose a signature scheme [34] and a group key exchange protocol [35], respectively.

In this paper, we present an important cryptographic primitive "signcryption" based on the R-IDPKS. The framework and security notions of revocable ID-based signcryption (RID-SC) scheme are defined to formalize possible threats and attacks in this paper. The security of our proposed scheme is demonstrated in the random oracle model [36, 37]. We show that our scheme is a secure signcryption scheme providing confidentiality and unforgeability under the bilinear Diffie-Hellman and the computational Diffie-Hellman assumptions.

The rest of this paper is organized as follows. In Section 2, we briefly review the concepts of bilinear pairings and related mathematical problems. The security model and notions of RID-SC are presented in Section 3. In Section 4, we propose a concrete RID-SC scheme. Security analysis of the proposed scheme is given in Section 5. In Section 6, we make the performance analysis and comparisons. Conclusions are drawn in Section 7.

2. **Preliminaries.** In this section, we briefly review the properties of bilinear pairings and related mathematical problems.

2.1. **Bilinear Pairings.** An admissible bilinear pairing e is a map defined by $e : G_1 \times G_1 \to G_2$, where G_1 is an additive cyclic group with a large prime order q and G_2 is a multiplicative cyclic group with the same order q. Here, e satisfies the following three conditions:

(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. For each $P \in G_1$, there exists some $Q \in G_1$ such that $e(P, Q) \neq 1$.
(3) Computable. There exists an algorithm to compute $e(P, Q)$ for all P, $Q \in G_1$.

For the details of bilinear pairings, readers can refer to [17, 23, 38] for full descriptions.

2.2. **Mathematical Hard Problem and Assumption.** Here, we define the bilinear Diffie-Hellman (BDH) and the computational Diffie-Hellman (CDH) problems and its security assumptions.

- BDH problem. Given P, aP, bP, $cP \in G_1$ for some a, b, $c \in Z_q^*$, the BDH problem is to compute $e(P, P)^{abc} \in G_2$.
- CDH problem. Given P, aP, $bP \in G_1$ for some a, $b \in Z_q^*$, the CDH problem is to compute $abP \in G_1$.

Definition 2.1. BDH assumption. *Given P, aP, bP, $cP \in G_1$ for some a, b, $c \in Z_q^*$, there does not exist a probabilistic polynomial-time adversary A with non-negligible probability that can compute $e(P, P)^{abc} \in G_2$. The advantage of A within running time t is defined by $Adv_{BDH}(t) = Pr[A(P, aP, bP, cP) = e(P, P)^{abc} | P, aP, bP, cP \in G_1]$.*

Definition 2.2. CDH assumption. *Given P, aP, $bP \in G_1$ for some a, b, $c \in Z_q^*$, there does not exist a probabilistic polynomial-time adversary A with non-negligible probability that can compute $abP \in G_1$. The advantage of A within running time t is defined by $Adv_{CDH}(t) = Pr[A(P, aP, bP) = abP | P, aP, bP \in G_1]$.*

3. **Model and Security Notions.** In this section, we define the model and security notions of RID-SC scheme. Note that some of notations and definitions are referred to [3, 4, 5, 33, 34].

3.1. **Model.** A revocable ID-based signcryption (RID-SC) scheme consists of the following five polynomial-time algorithms:

- *Setup algorithm*: This algorithm is a probabilistic algorithm which takes a security parameter l and a total number z of time periods. Note that the whole life time of the system is divide into distinct time periods 1, 2,..., z. The algorithm returns the master key s and the public parameters *param* which is made public and implicit input to the following four algorithms.
- *Initial key extract algorithm*: This algorithm is a deterministic algorithm which takes the master key s and a user's identity ID. It returns the user's initial private key DID.
- *Key update algorithm*: This algorithm is a deterministic algorithm which takes the master key s, a user's identity ID, and a time period index j, where $1 \leq j \leq z$. It returns the user's update key TID_j. Note that a non-revoked user's private key for time period j is $DID_j = DID + TID_j$, where the update key TID_j is periodically published by a trust private key generator (PKG).
- *Signcryption algorithm*: This algorithm is a probabilistic algorithm which takes a time period index j, a message M, a sender's identity ID_S, the sender's private key $DID_{S,j}$, and a receiver's identity ID_R. It returns a ciphertext C.

- *Designcryption algorithm*: This algorithm is a deterministic algorithm which takes a ciphertext C, the receiver's identity ID_R, the receiver's private key $DID_{R,j}$ for time period j, and the sender's identity ID_S. It returns a message M, if C is a valid ciphertext on M. Otherwise, it returns reject.

3.2. **Security Notions.**

Definition 3.1. Confidentiality. *We say that a RID-SC scheme is semantically secure against an adaptive chosen ciphertext attack (IND-RIDSC-CCA) if no probabilistic polynomial-time adversary A has a non-negligible advantage in the following IND-RIDSC-CCA game played between a challenger B and the adversary A.*

- **Setup***: The challenger runs Setup algorithm of the RID-SC scheme to generate a master key s and the public parameters param. Then, B sends param to A and keeps s by itself.*
- **Phase 1***: The adversary A may make a number of different queries to the challenger B in an adaptive manner as follows:*
  - **Initial key extract query**. *Upon receiving this query with identity ID, B runs Initial key extract algorithm to generate an initial private key DID corresponding to ID and returns it to A.*
  - **Key update query**. *Upon receiving this query with (ID, j), B runs Key update algorithm to generate an update key TID_j corresponding to (ID, j) and returns it to A. Here, j denotes a time period index.*
  - **Signcryption query**. *Upon receiving this query for a time period index j, a message M, a sender's identity ID_S, and a receiver's identity ID_R, B runs Signcryption algorithm to generate a ciphertext C and returns it to A. Here, C is encrypted under the receiver's identity ID_R and contains a signature on the message M.*
  - **Designcryption query**. *Upon receiving this query for a ciphertext C, a receiver's identity ID_R, and a sender's identity ID_S, B runs Designcryption algorithm to return a message M, if C is a valid ciphertext on M. Otherwise, it returns "reject".*
- **Challenge***: The adversary A outputs a time period index j^*, a sender's identity, a receiver's identity ID_R^*, and a pair of distinct messages (M_0, M_1) to the challenger B. B first randomly select a value $\beta \in \{0, 1\}$. Then, B runs Signcryption algorithm on $(j^*, M_\beta, ID_S^*, DID_{S,j^*}^*, ID_R^*)$ to return a ciphertext C^* and sends it to A. The restrictions are that (1) either ID_R^* or (ID_R^*, j^*) did not appear in Initial key extract or Key update queries, respectively. (2) (j^*, C^*) was not returned by Signcryption query on input $(j^*, M_\beta, ID_S^*, ID_R^*)$ for $\beta \in \{0, 1\}$.*
- **Phase 2***: The adversary A may make more queries (Initial key extract, Key update, Signcryption, Designcryption) which are the same as ones defined in Phase 1. The restrictions are that (1) either ID_R^* or (ID_R^*, j^*) did not appear in Initial key extract or Key update queries, respectively. (2) $(j^*, M_\beta, ID_S^*, ID_R^*)$ did not appear in Signcryption query. (3) $(j^*, C^*, ID_S^*, ID_R^*)$ did not appear in Designcryption query.*
- **Guess***: The adversary A outputs its guess $\beta' \in \{0, 1\}$. We say that A wins the IND-RIDSC-CCA game if $\beta' = \beta$. Here, the advantage of A is defined as the probability that A wins.*

Definition 3.2. Unforgeability. *We say that a RID-SC scheme is existential unforgeability against adaptive chosen message attack (RIDSC-UF-ACMA) if no probabilistic polynomial-time adversary A has a non-negligible advantage in the following RIDSC-UF-ACMA game played between a challenger B and the adversary A.*

- **Setup**: *The phase is the same as one defined in the IND-RIDSC-CCA game.*
- **Queries**: *The adversary A may make a number of different queries to the challenger B. The queries are the same as ones defined in the IND-RIDSC-CCA game.*
- **Forge**: *The adversary A outputs a tuple* $(j^*, C^*, ID_R^*, ID_S^*)$*, where* j^* *is a time period index,* C^* *is a ciphertext,* ID_R^* *is a receiver's identity, and* ID_S^* *is a sender's identity. We say that A wins this game if the following conditions are satisfied: (1) the response of Designcryption algorithm on* $(j^*, C^*, ID_R^*, ID_S^*)$ *is "accept". (2)* (j^*, C^*) *was not returned by Signcryption query on input* (M^*, ID_R^*, ID_S^*)*. (3) Either* ID_R^* *or* (ID_R^*, j^*) *did not appear in Initial key extract or Key update queries, respectively.*

Here, the advantage of the adversary A is defined as the probability that A wins.

Remark 3.1. *In the above definition, the adversary A is disallowed to make both Initial key extract query on target* ID^* *and Key update query on target* (ID^*, j^*) *in the IND-RIDSC-CCA game and RIDSC-UF-ACMA games because the target user's private key will be revealed. Therefore, we allow that A may issue either Initial key extract query on* ID^* *or Key update query on* (ID^*, j^*)*. In other words, we simulate an inside adversary (revoked user) is only to allow making Initial key extract query on* ID^**. On the other hand, an outside adversary is only to allow making Key update query on* (ID^*, j^*)*. Certainly, the adversary A is allowed to obtain the initial private key and the update key for any non-target identities and time periods.*

4. **A Concrete RID-SC Scheme.** Our proposed RID-SC scheme consists of five algorithms which are *Setup*, *Initial key extract*, *Key update*, *Signcryption*, and *Designcryption* algorithms. We describe them in the following.

- *Setup*: Given a security parameter l and a total number of time periods z, a trust private key generator (PKG) first selects an admissible bilinear map $e : G_1 \times G_1 \to G_2$, where G_1 is an additive cyclic group with a large prime order $q > 2^l$ and G_2 is a multiplicative cyclic group with the same order q. Then, the PKG generates a master key $s \in_R Z_q^*$ and computes the system public key $P_{pub} = s \cdot P$, where P is a generator of G_1. Finally, the PKG chooses four cryptographic hash functions $H_1 : \{0,1\}^* \to G_1$, $H_2 : \{0,1\}^* \to G_1$, $H_3 : \{0,1\}^* \times G_1 \to Z_q$, and $H_4 : G_2 \to \{0,1\}^*$. The public parameters *param* is defined as $\{e, G_1, G_2, q, P, P_{pub}, H_1, H_2, H_3, H_4\}$.
- *Initial key extract*: Upon receiving a user's identity $ID \in \{0,1\}^*$, the PKG generates the user's initial private key $DID = s \cdot H_1(ID)$ and transmits it to the user via a secure channel.
- *Key update*: Given a non-revoked user's identity $ID \in \{0,1\}^*$ for a time period index j, the PKG generates the user's update key $TID_j = s \cdot H_2(ID, j)$ and sends it to the user via a public channel. Thus, the non-revoked user can update her/his private key $DID_j = DID + TID_j$ for the time period j.
- *Signcryption*: In time period j, given a message M, a non-revoked sender with identity ID_S chooses a random value $r \in Z_q^*$ and computes the following values: $U = r \cdot P$, $V = DID_{S,j} + r \cdot h \cdot P_{pub}$, $X = e(r \cdot P_{pub}, H_1(ID_R) + H_2(ID_R, j))$, and $Y = H_4(X) \oplus (ID_S, M, V)$, where $h = H_3(ID_S, M, j, U)$ and ID_R denotes the identity of non-revoked receiver. The ciphertext for the message tuple (ID_S, M, V) is $C = (j, U, Y)$.
- *Designcryption*: Given a ciphertext $C = (j, U, Y)$, the receiver first uses her/his private key $DID_{R,j}$ to compute the value $X = e(U, DID_{R,j})$ and then recovers (ID_S, M, V) by $H_4(X) \oplus Y$. Finally, the receiver verifies V by checking $e(P, V) = e(P_{pub}, H_1(ID_S) + H_2(ID_S, j) + h \cdot U)$, where $h = H_3(ID_S, M, j, U)$. If the verification is true, it returns "accept". Otherwise, it outputs "reject".

5. **Security Analysis.** In this section, we demonstrate the security analysis of the proposed RID-SC scheme. As mentioned in Remark 3.1, the adversary is disallowed to make both *Initial key extract query* on target ID^* and *Key update query* on target (ID^*, j^*) in the IND-RIDSC-CCA and RIDSC-UF-ACMA games, respectively. For simplicity of security proof, we consider two types of adversaries: inside adversary (revoked user) and outside adversary. The inside adversary can make all queries mentioned in Subsection 3.2 except *Key update query* on target (ID^*, j^*). Similarly, the outside adversary can also make all queries except *Initial key extract query* on target ID^*. In the following, we first prove that our RID-SC scheme is semantically secure against an adaptive chosen ciphertext attack. Then, we show that our RID-SC scheme is existential unforgeability against adaptive chosen message attack.

[Confidentiality]

Theorem 5.1. *In the random oracle model, assume that an insider adversary (revoked user) A with a non-negligible probability ϵ_1 can break ciphertext indistinguishability of the proposed RID-SC scheme under an adaptive chosen ciphertext attack. Then, there exists a challenger B with a non-negligible probability $\xi \geq \frac{2\epsilon_1}{e(q_U+1)\cdot q_{H_4}}$ can solve the bilinear Diffie-Hellman (BDH) problem, where q_U and q_{H_4} denote the maximum numbers of making Key update and H_4 queries, respectively.*

Proof: We assume that the challenger B receives a BDH instance (P, aP, bP, cP) for a, b, $c \in_R Z_q^*$. By interacting with A, the challenger B will return the BDH solution $D = e(P,P)^{abc}$ in the IND-RIDSC-CCA game defined in Subsection 3.2 as follows:

- *Setup*: The challenger B runs *Setup algorithm* to generate public parameters $params = \{e, G_1, G_2, q, P, P_{pub}, H_1, H_2, H_3, H_4\}$ and sends it to A, where P_{pub} is defined as aP. Note that four hash functions H_i for i =1, 2, 3, 4 behave as oracles [36, 37] controlled by the challenger.
- H_1 *queries*: At any time, the adversary A can query the oracle H_1 with identity ID. To answer these queries, the challenger B maintains a list of tuples (ID, QID, u) called L_{H_1} as described below. Note that this list is initially empty.
  (a) If ID has appeared in L_{H_1}, B returns $H_1(ID) = QID$.
  (b) Otherwise, B firstly selects a value $u \in_R Z_q^*$ and defines $QID = u \cdot P$. Finally, the challenger B adds the tuple (ID, QID, u) to L_{H_1} and responds to A with $H_1(ID) = QID$.
- H_2 *queries*: At any time, the adversary A can query the oracle H_2 with (ID, j), where j is a time period index. To answer these queries, the challenger B maintains a list of tuples $(ID, j, RID_j, v, coin)$ called L_{H_2} as described below. Note that this list is initially empty.
  (a) If (ID, j) has appeared in L_{H_2}, B returns $H_2(ID, j) = RID_j$.
  (b) Otherwise, B generates a random $coin \in \{0, 1\}$ with the probability $Pr[coin = 0] = \delta$ for some δ that will be determined later.
  (c) B randomly selects a value $v \in Z_q^*$ and computes RID_j as follows. If $coin = 0$, $RID_j = v \cdot P$. Otherwise, $RID_j = b \cdot P$.
  (d) Finally, the challenger B adds the tuple $(ID, j, RID_j, v, coin)$ to L_{H_2} and responds to A with $H_2(ID, j)RID_j$.
- H_3 *queries*: At any time, the adversary A can query the oracle H_3 with (ID, M, j, U, h). To answer these queries, the challenger B maintains a list of tuples (ID, M, j, U, h) called L_{H_3} as described below. Note that this list is initially empty.
  (a) If (ID, M, j, U) has appeared in L_{H_3}, B returns $H_3(ID, M, j, U) = h$.

(b) Otherwise, B randomly selects a value $h \in Z_q^*$ and defines $H_3(ID, M, j, U) = h$. Finally, the challenger B adds the tuple (ID, M, j, U, h) to the L_{H_3} and responds to A with $H_3(ID, M, j, U) = h$.

- *H_4 queries*: At any time, the adversary A can query the oracle H_4 with $X \in G_2$. To answer these queries, the challenger B maintains a list of tuples (X, T) called L_{H_4} as described below. Note that this list is initially empty.
  (a) If X has appeared in L_{H_4}, B returns $H_4(X) = T$.
  (b) Otherwise, C randomly selects a string $T \in \{0,1\}^*$ and defines $T = H_4(X)$. Finally, the challenger B adds the tuple (X, T) to the L_{H_4} and responds to A with $H_4(X) = T$.
- *Phase 1*: In this phase, the adversary A may make a number of different queries to the challenger B in an adaptive manner as follows:
  - **Initial key extract query**. Upon receiving this query with identity ID, B accesses the corresponding tuple (ID, QID, u) from L_{H_1}. Then, B defines $DID = u{\cdot}P_{pub}$ and returns it to A. It is easy to see that $DID = u{\cdot}P_{pub} = u{\cdot}a{\cdot}P = a{\cdot}QID$.
  - **Key update query**. Upon receiving this query with (ID, j), B accesses the corresponding tuple $(ID, j, RID_j, v, coin)$ from L_{H_2}. If $coin = 1$, B returns failure and terminates. Otherwise, B defines $TID_j = v \cdot P_{pub}$ and returns it to A. It is easy to see that $TID_j = v \cdot P_{pub} = v \cdot a \cdot P = a \cdot RID_j$.
  - **Signcryption query**. Upon receiving this query with (j, M, ID_S, ID_R), B accesses the corresponding tuples (ID_R, QID_R, u) and $(ID_R, j, RID_{R,j}, v, coin)$ from L_{H_1} and L_{H_2}. Then, B randomly choose a value $r \in Z_q^*$ and computes $V = (DID_S + TID_{S,j}) + r \cdot h \cdot P_{pub}$, $X = e(r \cdot P_{pub},\ QID_R + RID_{R,j})$, and $Y = T \oplus (ID_S, M, V)$, where h from L_{H_3}. Finally, the challenger B returns a ciphertext $C = (j, U, Y)$ to the adversary A, where U is defined by cP.
  - **Designcryption query**. Upon receiving this query with $(C = (j, U, Y), ID_R, ID_S)$, B accesses the corresponding tuples (ID_R, QID_R, u) and $(ID_R, j, RID_{R,j}, v, coin)$ from L_{H_1} and L_{H_2}. Then, B computes $X = e(U, DID_R + TID_{R,j})$ and recovers a tuple of message $N = T \oplus Y$, where T from L_{H_4}. Finally, the challenger B verifies the signature of ID_S in N. If the verification is true, B returns "accept". Otherwise, B returns "reject".
- *Challenge*: The adversary A outputs $(M_0, M_1, j^*, ID_S^*, ID_R^*)$ to the challenger B. B chooses a value $\beta \in \{0,1\}$ as well as a random string $Y^* \in \{0,1\}^*$ and defines a ciphertext $C^* = (j^*, cP, Y^*)$. Finally, B sends C^* to the adversary A. It is easy to see that the decryption of C^* is to compute $Y^* \oplus H_4(e(cP, DID_{R,j^*})) = Y^* \oplus H_4(e(cP, DID_R) \cdot e(cP, TID_{R,j^*}))$.
- *Phase 2*: The adversary A may make *Initial key extract*, *Key update*, *Signcryption*, *Designcryption queries* which are the same as ones defined in Phase 1. The restrictions are that (1) either ID_R^* or (ID_R^*, j^*) did not appear in *Initial key extract* or *Key update queries*, respectively. (2) $(j^*, M_\beta, ID_S^*, ID_R^*)$ did not appear in *Signcryption query*. (3) $(j^*, C^*, ID_S^*, ID_R^*)$ did not appear in *Designcryption query*.
- *Guess*: The adversary A outputs its guess $\beta' \in \{0,1\}$.

By the assumption, A with a non-negligible probability ϵ_1 can distinguish the ciphertext C^* under an adaptive chosen ciphertext attack. At this point, the challenger B picks a tuple (X^*, T^*) from the L_{H_4} and outputs $X^*/e(cP, u^* \cdot P_{pub})$ as the solution for the given BDH instance (P, aP, bP, cP) for $a,\ b,\ c \in_R Z_q^*$, i.e. $X^*/e(cP, u^* \cdot P_{pub}) = e(P, P)^{abc}$. Finally, the proof of Theorem 5.1 remains to compute the probability that the challenger B does not abort during this simulation. Note that we adopt the similar technique in [22] to calculate this probability. Suppose that the adversary A makes a total q_U times *Key*

update queries. Then, the probability that the challenger B does not abort in Phases 1 or 2 is $(\delta)^{q_U}$. The probability that it is not abort during the challenge step is $1-\delta$. Hence, the probability that B does not abort during the simulation is $(\delta)^{q_U} \cdot (1-\delta)$. This value is maximized at $\delta_{opt} = 1 - \frac{1}{q_U+1}$. Using δ_{opt}, the probability that B does not abort is at least $\frac{1}{e(q_U+1)}$ (the analysis uses a similar technique to Coron's analysis of the Full Domain Hash in [39]). The challenger B outputs the correct D with probability at least $2\epsilon_1/q_{H_4}$ [17], where q_{H_4} denotes the total times of A makes H_4 queries. Therefore, the challenger B with a probability $\xi \geq \frac{2\epsilon_1}{e(q_U+1)\cdot q_{H_4}}$ can run the adversary A as a subroutine to solve the BDH problem. This contradicts to the bilinear Diffie-Hellman assumption.

Theorem 5.2. *In the random oracle model, assume that an outsider adversary A with a non-negligible probability ϵ_2 can break ciphertext indistinguishability of the proposed RID-SC scheme under an adaptive chosen ciphertext attack. Then, there exists a challenger B with a non-negligible probability $\xi \geq \frac{2\epsilon_2}{e(q_E+1)\cdot q_{H_4}}$ can solve the bilinear Diffie-Hellman (BDH) problem, where q_E and q_{H_4} denote the maximum numbers of making Initial key extract and H_4 queries, respectively.*

Proof: We assume that the challenger B receives a BDH instance (P, aP, bP, cP) for a, b, $c \in_R Z_q^*$. By interacting with A, the challenger B will return the BDH solution $D = e(P,P)^{abc}$ in the IND-RIDSC-CCA game defined in Subsection 3.2 as follows:

- *Setup*: This phase is the same as one defined in Theorem 5.1.
- H_1 *queries*: At any time, the adversary A can query the oracle H_1 with identity ID. To answer these queries, the challenger B maintains a list of tuples $(ID, QID, u, coin)$ called L_{H_1} as described below. Note that this list is initially empty.
  (a) If ID has appeared in L_{H_1}, B returns $H_1(ID) = QID$.
  (b) Otherwise, B generates a random $coin \in \{0,1\}$ with the probability $Pr[coin = 0] = \delta$ for some δ that will be determined later.
  (c) B randomly selects a value $u \in Z_q^*$ and computes QID as follows. If $coin = 0$, $QID = u \cdot P$. Otherwise, $QID = bP$.
  (d) Finally, the challenger B adds the tuple $(ID, QID, u, coin)$ to L_{H_1} and responds to A with $H_1(ID) = QID$.
- H_2 *queries*: At any time, the adversary A can query the oracle H_2 with (ID, j), where j is a time period index. To answer these queries, the challenger B maintains a list of tuples called L_{H_2} as described below. Note that this list is initially empty.
  (a) If (ID, j) has appeared in L_{H_2}, B returns $H_2(ID, j) = RID_j$.
  (b) Otherwise, B firstly selects a value $v \in_R Z_q^*$ and defines $RID_j = v \cdot P$. Finally, the challenger B adds the tuple (ID, j, RID_j, v) to L_{H_2} and responds to A with $H_2(ID, j) = RID_j$.
- H_3 *and* H_4 *queries*: The two queries are the same as ones defined in Theorem 5.1.
- *Phase 1*: In this phase, the adversary A may make a number of different queries to the challenger B in an adaptive manner as follows:
  - **Initial key extract query**. Upon receiving this query with identity ID, B accesses the corresponding tuple $(ID, QID, u, coin)$ from L_{H_1}. If $coin = 1$, B returns failure and terminates. Otherwise, B defines $DID = u \cdot P_{pub}$ and returns it to A. It is easy to see that $DID = u \cdot P_{pub} = u \cdot a \cdot P = a \cdot QID$.
  - **Key update query**. Upon receiving this query with (ID, j), B accesses the corresponding tuple (ID, j, RID_j, v) from L_{H2}. Then, B defines $RID_j = v \cdot P_{pub}$ and returns it to A. It is easy to see that $TID_j = v \cdot P_{pub} = v \cdot a \cdot P = a \cdot RID_j$.
  - **Signcryption query**. Upon receiving this query with (j, M, ID_S, ID_R), B accesses the corresponding tuples $(ID_R, QID_R, u, coin)$ and $(ID_R, j, RID_{R,j})$ from

L_{H_1} and L_{H_2}. Then, B randomly choose a value $r \in Z_q^*$ and computes the values V, X, and Y as mentioned in Theorem 5.1. Finally, the challenger B returns a ciphertext $C = (j, U, Y)$ to the adversary A, where U is defined by cP.

- **Designcryption query**. Upon receiving this query with $(C = (j, U, Y), ID_R, ID_S)$, B accesses the corresponding tuples $(ID_R, QID_R, u, coin)$ and $(ID_R, j, RID_{R,j}, v)$ from L_{H_1} and L_{H_2}. Then, B computes $X = e(U, DID_R + TID_{R,j})$ and recovers a tuple of message $N = T \oplus Y$, where T from L_{H_4}. Finally, the challenger B verifies the signature of ID_S in N. If the verification is true, B returns "accept". Otherwise, B returns "reject".

- *Challenge*: The adversary A outputs $(M_0, M_1, j^*, ID_S^*, ID_R^*)$ to the challenger B. B chooses a value $\beta \in \{0, 1\}$ as well as a random string $Y^* \in \{0, 1\}^*$ and defines a ciphertext $C^* = (j^*, cP, Y^*)$. Finally, B sends C^* to the adversary A. It is easy to see that the decryption of C^* is to compute $Y^* \oplus H_4(e(cP, DID_{R,j^*})) = Y^* \oplus H_4(e(cP, DID_R) \cdot e(cP, TID_{R,j^*}))$.
- *Phase 2*: The adversary A may make *Initial key extract*, *Key update*, *Signcryption*, *Designcryption queries* which are the same as ones defined in Phase 1. The restrictions are that (1) either ID_R^* or (ID_R^*, j^*) did not appear in *Initial key extract* or *Key update queries*, respectively. (2) $(j^*, M_\beta, ID_S^*, ID_R^*)$ did not appear in *Signcryptionquery*. (3) $(j^*, C^*, ID_S^*, ID_R^*)$ did not appear in *Designcryption query*.
- *Guess*: The adversary A outputs its guess $\beta' = \{0, 1\}$.

By the assumption, A with a non-negligible probability ϵ_2 can distinguish the ciphertext C^* under an adaptive chosen ciphertext attack. At this point, the challenger B picks a tuple (X^*, T^*) from the L_{H_4} and outputs $X^*/e(cP, v^* \cdot P_{pub})$ as the solution for the given BDH instance (P, aP, bP, cP) for a, b, $c \in_R Z_q^*$. Following the similar technique in Theorem 5.1, the challenger B with a probability $\xi \geq \frac{2\epsilon_2}{e(q_E+1)\cdot q_{H_4}}$ can run the adversary A as a subroutine to solve the BDH problem. This contradicts to the bilinear Diffie-Hellman assumption.

[**Unforgeability**]

Theorem 5.3. *In the random oracle model, assume that an inside adversary (revoked user) A with a non-negligible probability ϵ_3 can forge a valid ciphertext of the proposed RID-SC scheme under an adaptive chosen message attack. Then, there exists a challenger B with a non-negligible advantage can solve the computational Diffie-Hellman (CDH) problem.*

Proof: We assume that the challenger B receives a CDH instance (P, aP, bP) for a, $b \in_R Z_q^*$. By interacting with A, the challenger B will return the CDH solution abP in the RIDSC-UF-ACMA game defined in Subsection 3.2 as follows:

- *Setup*: This phase is the same as one defined in Theorem 5.1.
- *Queries*: The *Hash*, *Initial key extract*, *Signcryption*, *Designcryption queries* are the same as ones defined in Theorem 5.1.

By the assumption, A with a non-negligible probability ϵ_3 can forge a valid ciphertext tuple $(C^* = (j^*, U^*, Y^*), ID_R^*, ID_S^*)$. The challenger B decrypts C^* under the private key of ID_R^* and returns $(j^*, M^*, ID_S^*, U^*, V^*)$ as a valid signature tuple. Then, B accesses the corresponding tuple (ID_S^*, QID_S^*, u^*) and $(ID_S^*, j^*, RID_{S,j^*}, v^*, coin)$ from the lists L_{H_1} and L_{H_2}. The challenger B returns "failure" and halts, if one of the following conditions hold: (1) L_{H_1} does not contain the hash value of (ID_S^*, QID_S^*, u^*); (2) the value $coin = 0$ in L_{H_2} for $(ID_S^*, j^*, RID_{S,j^*}, v^*, coin)$. Finally, if the adversary A succeeds in the RIDSC-UF-ACMA game, it denotes $(j^*, M^*, ID_S^*, U^*, V^*)$ is a valid signature. In such a case, the

challenger B has $e(P, V^*) = e(P_{pub}, H_1(ID_S^*) + H_2(ID_S^*, j^*) + h^* \cdot U^*)$, where $P_{pub} = aP$, $H_1(ID_S^*) = u^*P$, and $H_2(ID_S^*, j^*) = bP$, and $U^* = c^*P$ for some known values u^*, c^*, and $h^* \in Z_q^*$. Then, we can obtain $e(P, V^*) = e(aP, u^*P + bP + h^* \cdot c^*P)$. By the bilinear pairing operation, we have $e(P, abP) = e(P_{pub}, bP) = e(P, V^* - (u^* + h^*c^*) \cdot P_{pub})$. Thus, $V^* = (u^* + h^*c^*) \cdot P_{pub}$ is a CDH solution for a CDH instance (P, aP, bP). This contradicts to the computational Diffie-Hellman assumption.

Theorem 5.4. *In the random oracle model, assume that an outside adversary A with a non-negligible probability ϵ_4 can forge a valid ciphertext of the proposed RID-SC scheme under an adaptive chosen message attack. Then, there exists a challenger B with a non-negligible advantage can solve the computational Diffie-Hellman (CDH) problem.*

Proof: The proof is similar to one of Theorem 5.3.

6. **Performance Analysis and Comparisons.** For convenience to evaluate the computational cost of our proposed RID-SC scheme, we define some time-consuming operations as follows:

- TG_e: The time of executing a bilinear pairing operation, $e : G_1 \times G_1 \to G_2$.
- TG_{mul}: The time of executing a point scalar multiplication operation in G_1.
- TG_H: The time of executing a map-to-point hash function.

Table 1 lists the performance comparisons between the proposed RID-SC scheme and the previously presented ID-based signcryption (IDSC) schemes [5, 8, 9] in terms of performance and revocation functionality. In the two schemes [8, 9], we adopt the Boneh-Franklin encryption scheme [17] combining with the Cha-Cheon signature scheme [20] to evaluate their performance. It is easy to see that our scheme is slightly less efficient than the existing IDSC schemes [5, 8, 9] for *Signcryption* and *Designcryption phases*. Our RID-SC scheme only increases TG_H in the two phases. This is a reasonable price to pay for the revocation functionality in our scheme. The main point is that our RID-SC scheme provides a simple and efficient revocation mechanism to revoke the compromised or misbehaving users in the system.

TABLE 1. Comparisons between our RID-SC scheme and the previous presented IDSC schemes

	Chen and Malone-Lee [5]	Pandey and Barua [8]	Lee *et al.* [9]	Our scheme
Signcryption	$TG_e + 3TG_{mul} + TG_H$	$TG_e + 3TG_{mul} + TG_H$	$TG_e + 3TG_{mul} + TG_H$	$TG_e + 3TG_{mul} + 2TG_H$
Decigncryption	$TG_e + TG_{mul} + TG_H$	$TG_e + TG_{mul} + TG_H$	$TG_e + TG_{mul} + TG_H$	$TG_e + TG_{mul} + 2TG_H$
Revocation functionality	No	No	No	Yes

7. **Conclusions.** In this paper, we have proposed a concrete and secure RID-SC scheme relying on the Tseng-Tsai R-IDPKS. We have defined the model of RID-SC scheme and its security notions which are used to formalize the possible threats and attacks. In the random oracle model, we have proven that the proposed scheme is a secure signcryption scheme providing confidentiality and unforgeability under the BDH and the CDH assumptions.

Acknowledgment. The authors would like to thank the referees for their valuable comments and constructive suggestions. This research was partially supported by National Science Council, Taiwan, R.O.C., under contract no. NSC101-2221-E-018-027.

REFERENCES

[1] Y. Zheng, Digital signcryption or how to achieve cost(signature + encryption) << cost(signature) + cost(encryption), *Proc. of 17th Annual International Cryptology Conference*, pp. 165-179, 1997.
[2] Y. Zheng and H. Imai, Efficient signcryption schemes on elliptic curves, *Information Processing Letters*, vol. 68, no. 5, pp. 227-233, 1998.
[3] J. H. An, Y. Dodis, and T. Rabin, On the security of joint signature and encryption, *Proc. of the International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology*, pp. 83-107, 2002.
[4] X. Boyen, Multipurpose identity-based signcryption: a swiss army knife for identity-based cryptography, *Proc. of 23rd Annual International Cryptology Conference*, pp. 383-399, 2003.
[5] L. Chen and J. Malone-Lee, Improved identity-based signcryption, *Proc. of 8th International Workshop on Theory and Practice in Public Key Cryptography*, pp. 362-379, 2005.
[6] S. S. D. Selvi, S. S. Vivek, R. Srinivasan, and C. P. Rangan, An efficient identity-based signcryption scheme for multiple receivers, *Proc. of the 4th International Workshop on Security: Advances in Information and Computer Security*, pp. 71-88, 2009.
[7] T. Matsuda, K. Matsuura, and J. C. N. Schuldt, Efficient constructions of signcryption schemes and signcryption composability, *Proc. of the 10th International Conference on Cryptology in India: Progress in Cryptology*, pp. 321-342, 2009.
[8] S. K. Pandey and R. Barua, Construction of identity based signcryption schemes, *Proc. of the 11th international conference on Information security applications*, pp. 1-14, 2011.
[9] W. Lee, J. W. Seo, and P. J. Lee, Identity-based signcryption from identity-based cryptography, *Proc. of 12th International Workshop on Information Security Applications*, pp. 70-83, 2012.
[10] R. Housley, W. Polk, W. Ford, and D. Solo, Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile, The Internet Society, 2002.
[11] W. Aiello, S. Lodha, and R. Ostrovsky, Fast digital identity revocation, *Proc. of 18th Annual International Cryptology Conference*, pp. 137-152, 1998.
[12] S. Micali, Novomodo: scalable certificate validation and simplified PKI management, *Proc. of 1st Annual PKI Research Workshop*, pp. 15-25, 2002.
[13] C. Gentry, Certificate-based encryption and the certificate revocation problem, *Proc. of International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 272-293, 2003.
[14] F. F. Elwailly, C. Gentry, and Z. Ramzan, QuasiModo: efficient certificate validation and revocation, *Proc. of 7th International Workshop on Theory and Practice in Public Key Cryptography*, pp. 375-388, 2004.
[15] V. Goyal, Certificate revocation using fine grained certificate space partitioning, *Proc. of 11th International Conference on Financial Cryptography and Data Security*, pp. 247-259, 2007.
[16] A. Shamir, Identity-based cryptosystems and signature schemes, *Proc. of the 4th International Cryptology Conference*, pp. 47-53, 1985.
[17] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, *Proc. of 21st Annual International Cryptology Conference*, pp. 216-229, 2001.
[18] B. Waters, Efficient identity-based encryption without random oracles, *Proc. of 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 114-127, 2005.
[19] D. Boneh and M. Hamburg, Generalized identity based and broadcast encryption schemes, *Proc. of 14th International Conference on the Theory and Application of Cryptology and Information Security*, pp. 455-470, 2008.
[20] J. C. Cha and J. H. Cheon, An identity-based signature from gap Diffie-Hellman groups, *Proc. of International Workshop on Practice and Theory in Public Key Cryptography* , pp.18-30, 2003.
[21] H. J. Yoon, J. H. Cheon, and Y. Kim, Batch verifications with ID-based signatures, *Proc. of 7th International Conference on Information Security and Cryptology*, pp. 233-248, 2005.
[22] Y. M. Tseng, T. Y. Wu, and J. D. Wu, An efficient and provably secure ID-based signature scheme with batch verifications, *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 11, pp. 3911-3922, 2009.

[23] L. Chen, Z. Cheng, and N. P. Smart, Identity-based key agreement protocols from pairings, *International Journal of Information Security*, vol. 6, no. 4, pp. 213-241, 2007.
[24] T. Y. Wu and Y. M. Tseng, An ID-based mutual authentication and key exchange protocol for low-power mobile devices, *The Computer Journal*, vol. 53, no. 7, pp. 1062-1070, 2010.
[25] T. Y. Wu and Y. M. Tseng, An efficient user authentication and key exchange protocol for mobile client-server environment, *Journal of Computer Networks*, vol. 54, no. 9, pp. 1520-1530, 2010.
[26] K. Y. Choi, J. Y. Hwang, and D. H. Lee, Efficient ID-based group key agreement with bilinear maps, *Proc. of International Workshop on Theory and Practice in Public Key Cryptography*, pp. 130-144, 2004.
[27] T. Y. Wu, Y. M. Tseng, and C. W. Yu, A secure ID-based authenticated group key exchange protocol resistant to insider attacks, *Journal of Information Science and Engineering*, vol. 27, pp. 915-932, 2011.
[28] T. Y. Wu and Y. M. Tseng, Towards ID-based authenticated group key exchange protocol with identifying malicious participants, *Journal of Informatica*, vol. 23, no. 2, pp. 315-334, 2012.
[29] M. Bellare, C. Namprempre, and G. Neven, Security proofs for identity-based identification and signature schemes, *Journal of Cryptology*, vol. 22, no. 1, pp. 1-61, 2009.
[30] Y. M. Tseng, T. Y. Wu, and J. D. Wu, A pairing-based user authentication scheme for wireless clients with smart cards, *Journal of Informatica*, vol. 19, no. 2, pp. 285-302, 2008.
[31] A. Boldyreva, V. Goyal, and V. Kumar, Identity-based encryption with efficient revocation, *Proc. of the 15th ACM conference on Computer and communications security*, pp. 417-426, 2008.
[32] B. Libert and D. Vergnaud, Adaptive-ID secure revocable identity-based encryption, *Proc. of the The Cryptographers' Track at the RSA Conference on Topics in Cryptology*, pp. 1-15, 2009.
[33] Y. M. Tseng and T. T. Tsai, Efficient revocable ID-based encryption with a public channel, *The Computer Journal*, vol. 55, no. 4, pp. 475-486, 2012.
[34] T. Y. Wu, T. T. Tsai, and Y. M. Tseng, Revocable ID-based signature scheme with batch verifications, *Proc. of 8th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 49-54, 2012.
[35] T. Y. Wu, Y. M. Tseng, and T. T. Tsai, A revocable ID-based authenticated group key exchange protocol with resistant to malicious participants, *Journal of Computer Networks*, vol. 56, no. 12, pp. 2994-3006, 2012.
[36] M. Bellare and P. Rogaway, Random oracles are practical: a paradigm for designing efficient protocols, *Proc. of the 1st ACM conference on Computer and communications security*, pp. 62-73, 1993.
[37] R. Canetti, O. Goldreich, and S. Halevi, The random oracle methodology, revisited, *Journal of ACM*, vol. 51, no. 4, pp. 557-594, 2004.
[38] S. D. Galbraith, K. G. Paterson, and N. P. Smart, Pairings for cryptographers, *Journal of Discrete Applied Mathematics*, vol. 156, no. 16, pp. 3113-3121, 2008.
[39] J. S. Coron, On the exact security of full domain hash, *Proc. of the 20th Annual International Cryptology Conference on Advances in Cryptology*, pp. 229-235, 2000.