Ciphertext-Auditable Identity-based Encryption

Changlu Lin[1], Yong Li[2], Kewei Lv[3], and Chin-Chen Chang[4,5]

(Corresponding author: Chin-Chen Chang)

Fujian Province Key Laboratory of Network Security and Cryptology & Fujian Normal University[1]
Fuzhou 350007, China
Key Laboratory of Communication & Information Systems (Beijing Jiaotong University)[2]
Beijing Municipal Commission of Education, Beijing 100044, China
State Key Laboratory of Information Security, Institute of Information Engineering, CAS [3]
Beijing 100049, China
Department of Information Engineering and Computer Science& Feng Chia University [4]
Taichung 40724, Taiwan
Department of Computer Science and Information Engineering& Asia University [5]
Taichung, 41354, Taiwan
(Email: alan3c@gmail.com)

(Received Aug. 28, 2013; revised and accepted Nov. 6, 2013)

Abstract

Ciphertext-auditability of public key encryption scheme means that the ciphertext should been verified by anyone whether it was actually created by the public key. It also should satisfy two additional requirements: 1) no adversary can create a valid-looking ciphertext and then it can pass the verification process together with a public key and a plaintext; 2) the plaintext cannot be revealed from ciphertext without the help of the correct private key. This paper, in the first time, proposes an ciphertext-auditable identity-based encryption. Our scheme doesn't need the certificates and the sender can directly encrypt message via using the identity without the progress of public key authentication. Furthermore, the proposed scheme is provably secure under the standard model against the k-resilient ciphertext-auditability.

Keywords: Ciphertext-auditability, identity based encryption, public key cryptography

1 Introduction

In current information age, many companies, e.g., Bank (some critical business data), have the number of very important personal information (**PI**), such as the personal consumption information of some productions, customer and account information of the bank, etc. The company may use them for various purposes, including adverting, marketing, etc. Furthermore, if the **PI** is leaked by the malicious employees, then it would cause great losses for the company. Usually, there are two ways against this leakages from insiders: *network security* and *physical security* [8]. When the company wants to store the **PI** in secure warehouse, the company duplicates the **PI** and saves it to backup tape, and then the company requires a transport service (**TS**) to deliver this tape to a secure warehouse. During the transiting, the backup tape may be lost and potentially give out to outsiders. To avoid this kind of potential leakages, the encryption technique is used and the company encrypts the **PI** before copying it to backup tape.

Hada and Sakurai [8] observed that it could *not* prevent the potential attack by using the traditional encryption technique. They introduced an *auditor* who ensured that the message is encrypted by a correct public key, and showed that the backup operation done by the following three entities:

- *Backup manager* (BM): Backup manager does the management service for enterprise-wide backup. Usually, BM needs to inform every department to backup the **PI** data periodically and then deliveries the message to a secure warehouse under the corporate backup policy. In addition, all encryption keys are managed by BM.
- *Operator* (O): Operator holds the **PI** databases in a department and encrypts them via a public key before duplicating the data to the backup tape.
- *Auditor* (A): Auditor is in some same department as the operator and audits the backup tape and ensures that the encrypted message is encrypted by the correct public key.

Ciphertext-Auditable Public Key Encryption. Hada and Sakurai [8] presented the concept of ciphertext-auditable public key encryption, denoted by CA-PKE, to capture the above scenarios, such as backup the very important personal information in the company. They described the general scenario via the public key encryption, and this case should satisfy two special requirements: *verifiability* and *unforgeability* (see Def. 1). Furthermore, a CA-PKE scheme has four steps as follows: 1) BM makes a backup request in an authenticated way and sends a public key to both O and A; 2) O encrypts the **PI** under the public key and duplicates this encrypted message to a backup tape; 3) A audits this backup tape and verifies whether O encrypted the **PI** by the correct public key or not. Furthermore, the audit should ensure that the message cannot be recovered, even if O is malicious, from the backup tape without the help of the corresponding private key; 4) O requires the **TS** to delivery the backup tape to a secure warehouse after it passes the audit. Hada and Sakurai [8] proposed a general CA-PKE with random oracle assumption. There are some cryptographic tools, such as non-interactive zero-knowledge (NIZK) proof of knowledge together with a trapdoor one-way permutation, are used in the concreted construction. Actually, their proposed scheme is a modification of the encryption scheme which is presented by Bellare and Rogaway [2]. Recently, Lin and Liu [9] proposed a ciphertext-auditable public key encryption scheme based on the Paillier's cryptosystem and is secure under the standard model.

Identity-based Encryption. Identity-based encryption [3, 11], denoted by IBE, is a public key encryption scheme and the encryption key is an arbitrary string, e.g., the receiver's unique email address or telephone number. The Private Key Generator (PKG) generates the user's private key via using its master key after the user authenticates itself. Public key certificates and certificate authorities don't be required any more in the IBE scheme. It simplifies public key and the certificate management, that is, such scheme eliminates certificates and the sender could just encrypt the message by using the receiver identity as the public key. In 2001, Boneh and Franklin [3] proposed the first secure and practical IBE scheme based on the pairing. Their scheme is provable security under the random oracle model. After that, many IBE schemes are proposed based on the pairing [5, 10, 12] or lattice [7].

Our Contributions. This paper, in first time, proposes cipertext-auditable identity-based encryption (CA-IBE). Our proposed CA-IBE scheme also has four steps and satisfies the additional two properties of *verifiability* and *unforgeability* as the CA-PKE scheme proposed by Hada and Sakurai [8]. In the second step, it requires t ($t \geq 2$) operators who encrypt the **PI** together and requires at least one operator is honest. Our main contributions are as follows.

- In the CA-IBE scheme, it only requires that the BM sends a backup request to both O and A by authenticated way and does *not* need the public key authentication in the first step;
- In the CA-IBE scheme, the operator O can encrypt the **PI** before receiving the backup request and duplicates the ciphertext to backup tape right now after getting the backup request;
- Our proposed scheme satisfies the provable security under the standard model against the k-resilient ciphertext-auditability.

2 Preliminaries

This section recalls some notations, the formal definition of the identity based encryption, and also gives the formal definition of the ciphertext-auditable identity-based encryption.

Some Notations. Assume $\mathcal{A}$ is a probabilistic algorithm and $\mathcal{A}(x_1, \ldots, x_n; r)$ is the output result of $\mathcal{A}$ on input $(x_1, \ldots, x_n)$ and coins r. Assume $y \leftarrow \mathcal{A}(x_1, \ldots, x_n)$ is an experiment of picking r randomly, and y is $\mathcal{A}(x_1, \ldots, x_n; r)$. If S is a finite set, $x \overset{R}{\leftarrow} S$ is the operation of choosing an element from S uniformly. Assigning a value α to a variable x will be denoted by $x \leftarrow \alpha$. Let $S, T, \ldots,$ denote probability spaces, and then let $\Pr[x \leftarrow S; y \leftarrow T; \ldots : p(x, y, \ldots)]$ denote the probability where the predicate $p(x, y, \ldots)$ is true if the experiments, $x \leftarrow S; y \leftarrow T; \ldots,$ are executed correctly and in order. Function $f : \mathbb{N} \rightarrow \mathbb{R}^+$ is a function and it is *negligible* in k if for any real number $c > 0$, there exists $k_0 \in \mathbb{N}$ such that for any k and $k > k_0$, then have $f(k) \leq (\frac{1}{k})^c$, where $\mathbb{R}^+ := \{x \in \mathbb{R} | x > 1\}$. PPTM stands for "probabilistic polynomial time machine" and PSCF means "polynomial-size circuit family". If $\{D_n\}$ is probability distribution ensemble and the largest probability of an element, that is, $\max_v \Pr[x \leftarrow D_n : x = v]$, is negligible in n [6], then call that a $\{D_n\}$ is *well-spread.*

Identity-based Encryption. An identity-based encryption (IBE) scheme is consisted by following four algorithms: **Setup**, **Key Generation**, **Encryption**, **Decryption**, they denoted by $\mathcal{IBE} = (\mathcal{S}, \mathcal{K}, \mathcal{E}, \mathcal{D})$:

- *Setup* ($\mathcal{S}$): it is the setup algorithm and takes the security parameter $k \in \mathbb{N}$ as input, and this algorithm outputs the system parameters **params** and the master-key **mk**. Usually, the system parameters are all description of the message and ciphertext space $\mathcal{M}$ and $\mathcal{C}$ respectively. Intuitively, **params** is known publicly, while **mk** is the secret key of the PKG.
- *Key Generation* ($\mathcal{K}$): it is the extraction algorithm and takes **params**, **mk**, and an arbitrary **ID** $\in \{0,1\}^*$ as inputs, and this algorithm outputs $d_{\mathbf{ID}}$ as

the private key for the identity **ID**. Here **ID** is a public key, and $d_{\mathbf{ID}}$ is the corresponding private key.

- *Encryption* ($\mathcal{E}$): it is the encryption algorithm and takes **params**, **ID**, and one plaintext M from message space $\mathcal{M}$ as inputs, and then this algorithm outputs the ciphertext $C \in \mathcal{C}$.
- *Decryption* ($\mathcal{D}$): it is the decryption algorithm and takes **params**, one ciphertext C from message space $\mathcal{C}$ and one $d_{\mathbf{ID}}$ as inputs, and then this algorithm outputs the message $M \in \mathcal{M}$ as the corresponding plaintext.

The above algorithms should satisfy the constraint of consistency. That is, the following equation holds if $d_{\mathbf{ID}}$ is the correct private key created from the extraction algorithm $\mathcal{K}$ which is run **ID** as input, and for any message $M \in \mathcal{M}$:

$$\mathcal{D}(\mathbf{params}, C, d_{\mathbf{ID}}) = M, \text{where } C = \mathcal{E}(\mathbf{params}, \mathbf{ID}, M).$$

Definition of Ciphertext-Auditable Identity-based Encryption. As the ciphertext-auditable public key encryption is defined in [8], the ciphertext-auditable identity-based encryption is defined as follows:

Definition 1 (CA-IBE) *An identity-based encryption scheme $\mathcal{IBE} = (\mathcal{S}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is ciphertext-auditable if it satisfies two properties:*

- ***Verifiability:*** *There is a PPTM verification algorithm, $\mathcal{CV}$, such that, for each message M from the space $\{0,1\}^*$, then have*

$$Pr\begin{bmatrix} (\mathbf{ID}, d_{\mathbf{ID}}) \leftarrow \mathcal{K}(\mathbf{params}, \mathbf{mk}); \\ (C, p) \leftarrow \mathcal{E}(M, \mathbf{ID}) : \\ \mathcal{CV}(C, \mathbf{ID}, p) = \mathbf{Accept} \end{bmatrix} = 1.$$

- ***Unforgeability:*** *Given each pair of non-uniform PSCFs as $< \mathcal{A}^e, \mathcal{A}^d >=< \{\mathcal{A}^e_n\}, \{\mathcal{A}^d_n\} >$, and each well-spread distribution $\mathcal{X}(1^k)$, then have*

$$Pr\begin{bmatrix} (\mathbf{ID}, d_{\mathbf{ID}}) \leftarrow \mathcal{K}(\mathbf{params}, \mathbf{mk}); \\ M \leftarrow \mathcal{X}(1^k); (C, p) \leftarrow \mathcal{A}^e_n(M, \mathbf{ID}) : \\ \mathcal{CV}(C, \mathbf{ID}, p) = \mathbf{Accept},\ \mathcal{A}^d_n(C, \mathbf{ID}) = M \end{bmatrix},$$

is negligible in n.

In the real scenario, adversaries $\mathcal{A}^e$ and $\mathcal{A}^d$ are the malicious operator and transport service respectively, and p is the proof string.

To analyze our proposed scheme, a stronger notion than the ciphertext-auditability as above defininition should be defined, called *k-resilient* ciphertext-auditability. This notion satisfies the *verifiability* and *k-unforgeability.* The property of k-unforgeability means that there are at most l ($l \leq k-1, \text{and } k \geq 2$) malicious encryption adversaries $\mathcal{A}^e$ (malicious operators) in the unforgeability notion. In other words, the k-resilient ciphertext-auditability implies that the scheme can pass the verification even there are l malicious operators in the scenario which includes the k operators.

Mix strategy is the generalization of the semi-honest strategy introduced by Hada and Sakurai [8]. There are two settings, the *real* setting and the *ideal* setting, in the mix strategy. In the *real* one, there exist some (but not all) malicious encryption adversaries which could make some modifications on the message and choose some fixed numbers as the randomized inputs in the encryption progress, while all encryption adversaries are honest in the *ideal* one. The gaps between the probabilities which the decryption adversaries obtain messages in the two settings should be considered. The formal definition of the mix strategy is as follows:

Definition 2 (Mix Strategy) *It says that a standard IBE scheme $\mathcal{IBE} = (\mathcal{S}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ satisfies the secure property of the mix strategy if, for each pair of non-uniform PSCFs as $< \mathcal{F}, \mathcal{DA} >=< \{\mathcal{F}_n\}, \{\mathcal{DA}_n\} >$, and each well-spread distribution $\mathcal{X}(1^k)$, for the set $X \subset \{1, 2, \ldots, k\}$, we set the subset Y is $\{1, 2, \ldots, k\} - X$, then the following function*

$$Pr\begin{bmatrix} (\mathbf{ID}, d_{\mathbf{ID}}) \leftarrow \mathcal{K}(\mathbf{params}, \mathbf{mk}); M \leftarrow \mathcal{X}(1^k); \\ (M', r_1, \ldots, r_{|X|}) \leftarrow \mathcal{F}^X_n(\mathbf{ID}, M); \\ (r_{|X|+1}, \ldots, r_k) \leftarrow_R \mathcal{F}^Y_n(\mathbf{ID}); \\ C = \mathcal{E}(\mathbf{ID}, M'; r') : \mathcal{DA}_n(\mathbf{ID}, C) = M \end{bmatrix}$$

$$-Pr\begin{bmatrix} (\mathbf{ID}, d_{\mathbf{ID}}) \leftarrow \mathcal{K}(\mathbf{params}, \mathbf{mk}); M \leftarrow \mathcal{X}(1^k); \\ (r_1, r_2, \ldots, r_k) \leftarrow_R \mathbf{coins}; C = \mathcal{E}(\mathbf{ID}, M; r) : \\ \mathcal{DA}_n(\mathbf{ID}, C) = M \end{bmatrix},$$

is negligible for n, where $r' = \sum_{i=1}^{|X|} r_i + \sum_{j=|X|+1}^{k} r_j$ and $r = \sum_{i=1}^{k} r_i$. And the set X is the set of all malicious encryptors, while Y is the set of all honest encryptors.

The reader is referred to reference [5] for the standard security notions and models for identity-based encryption, such as IND-ID-CPA and IND-ID-CCA.

3 Cipertext-Auditable Identity-based Encryption (CA-IBE)

This section constructs a CA-IBE scheme, denoted by $\mathcal{CA}\text{-}\mathcal{IBE}$, without random oracles. There are k encryptors in our scheme, and anyone who picks randomized input itself encrypts the ciphertext from the former encryptors. In addition, our scheme assumes all encryptors must join in the encryption progress.

Assume $\mathbb{G}$, $\mathbb{G}_1$ are the group with prime order p and g is a generator for group $\mathbb{G}$; the function $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$ is a bilinear map. All public parameters are similar with in the other IBE scheme in [5].

Initialization. Select t-length vector $X = (x_i) \in \mathbb{Z}^t_p$ and compute $Y = (y_i) = (g^{x_i}) \in \mathbb{G}^t$, where x_i and y_i is the private key and the public key for the i-th encryptor respectively.

Setup. The PKG selects a random secret integer $\alpha \in \mathbb{Z}_p$ and $g \in \mathbb{G}$ as a random generator. PKG computes $g_1 = g^{\alpha}$ and choose a random g_2 from $\mathbb{G}$. Furthermore, PKG picks randomly a value $u' \in \mathbb{G}$ and a n-length vector $U = (u_i) \in \mathbb{G}^n$. Then, the public parameters **params** and the private master-key **mk** are as follows.

$$\mathbf{params} = (g, g_1, g_2, u', U), \ \mathbf{mk} = g_2^{\alpha}.$$

Key Generation. Assume $\mathbf{ID} = (v_1, \ldots, v_n)$ from $\{0,1\}^n$ is a bit string, and $\mathcal{V} = \{i | v_i \neq 1\} \subseteq \{1, \ldots, n\}$. The PKG picks a random number $r_{\mathbf{ID}}$ from $\mathbb{Z}_p$ and generates $d_{\mathbf{ID}}$ for identity $\mathbf{ID}$ via using the master key as below:

$$d_{\mathbf{ID}} = (d_1, d_2) = (g_2^{\alpha} \cdot (u' \prod_{i \in \mathcal{V}} u_i)^{r_{\mathbf{ID}}}, g^{r_{\mathbf{ID}}}). \qquad (1)$$

Encryption. This algorithm encrypts any message M from $\mathbb{G}_1$ for a receiver $\mathbf{ID} \in \{0,1\}^n$, set $h = u' \prod_{i \in \mathcal{V}} u_i$, the k encryptors choose $r_j \in_R \mathbb{Z}_p$ randomly and independently, where $j = 1, \ldots, k$. So the ciphertext is

$$C = (C_0, C_1, C_2; T) = (M \cdot e(g_1, g_2)^r, g^r, h^r; (h^i)). \qquad (2)$$

Here, the k encryptors compute as follows:

$$\begin{aligned}
&(C_0^0, C_1^0, C_2^0; T_0) \\
&= (M \cdot e(g_1, g_2)^{r_0 x_0}, g^{r_0 x_0}, h^{r_0 x_0}; h^{r_0}) \\
&= (M \cdot 1, 1, 1; 1, 1), \\
&(C_0^1, C_1^1, C_2^1; T_1) \\
&= (C_0^0 \cdot e(g_1, g_2)^{r_1 x_1}, C_1^0 \cdot g^{r_1 x_1}, C_2^0 \cdot h^{r_1 x_1}; (h^{r_0}, h^{r_1})) \\
&= (M \cdot e(g_1, g_2)^{r_0 x_0 + r_1 x_1}, g^{r_0 x_0 + r_1 x_1}, h^{r_0 x_0 + r_1 x_1}; (h^{r_0}, h^{r_1})),
\end{aligned}$$

$$\vdots$$

$$\begin{aligned}
(C_0^i, C_1^i, C_2^i; T_i) =& (C_0^{i-1} \cdot e(g_1, g_2)^{r_i x_i}, C_1^{i-1} \cdot g^{r_i x_i}, \\
& C_2^{i-1} \cdot h^{r_i x_i}; (h^{r_0}, \ldots, h^{r_i})) \\
=& (M \cdot e(g_1, g_2)^{\sum_{j=1}^{i} r_j x_j}, g^{\sum_{j=1}^{i} r_j x_j}, \\
& h^{\sum_{j=1}^{i} r_j x_j}; (h^{r_0}, \ldots, h^{r_i})),
\end{aligned}$$

$$\vdots$$

$$\begin{aligned}
(C_0^k, C_1^k, C_2^k; T_k) =& (C_0^{k-1} \cdot e(g_1, g_2)^{r_k x_k}, C_1^{k-1} \cdot g^{r_k x_k}, \\
& C_2^{k-1} \cdot h^{r_k x_k}; (h^{r_0}, \ldots, h^{r_k})) \\
=& (M \cdot e(g_1, g_2)^{\sum_{j=1}^{k} r_j x_j}, g^{\sum_{j=1}^{k} r_j x_j}, \\
& h^{\sum_{j=1}^{k} r_j x_j}; (h^{r_0}, \ldots, h^{r_k})) \\
=& (M \cdot e(g_1, g_2)^r, g^r, h^r; (h^{r_0}, \ldots, h^{r_k})) \\
\triangleq& (C_0, C_1, C_2; T) = C,
\end{aligned}$$

where $r = \sum_{j=1}^{k} r_j \in_R \mathbb{Z}_p$, and $x_0 = 0$, $r_0 = 0$. Note that the k encrypters are the k operators in the scenario respectively, and the last encrypter is responsible to send the encrypted message to backup. Usually, there is an honest encrypter at least among the k encrypters.

Audit. When the auditor A reads the ciphertext C from backup tape, he/she computes $h = u' \prod_{j \in \mathcal{V}} u_j$ and checks

$$e(C_1, h) =^? e(y_1, t_1) e(y_2, t_2) \cdot \cdots \cdot e(y_t, t_k),$$

where $C_1 = g^{\sum_{j=1}^{k} r_j x_j}$, and $T = (t_1, t_2, \ldots, t_k) = (h^{r_1}, h^{r_2}, \ldots, h^{r_k})$. That is,

$$e(g^{\sum_{j=1}^{k} r_j x_j}, h) =^? \prod_{j=1}^{k} e(g, h)^{r_j x_j}. \qquad (3)$$

If the above equation is correct and pass the verifiability (whether the ciphertext is actually encrypted by the identity ID or not), then the auditor passes the audit progress.

Decryption. Given the ciphertext $C' = (C_0, C_1, C_2)$, the reciever can get the message as follows via using the private key $d_{\mathbf{ID}} = (d_1, d_2)$:

$$\begin{aligned}
& C_0 \cdot \frac{e(d_2, C_2)}{e(d_1, C_1)} \\
&= M \cdot e(g_1, g_2)^r \cdot \frac{e(g^{r_{\mathbf{ID}}}, (u' \prod_{i \in \mathcal{V}} u_i)^r)}{e(g_2^{\alpha} (u' \prod_{i \in \mathcal{V}} u_i)^{r_{\mathbf{ID}}}, g^r)} \\
&= M \cdot e(g_1, g_2)^r \cdot \frac{e(g, (u' \prod_{i \in \mathcal{V}} u_i)^{r_{\mathbf{ID}}})}{e(g_1, g_2)^r e((u' \prod_{i \in \mathcal{V}} u_i)^{r_{\mathbf{ID}} r}, g)} \\
&= M.
\end{aligned}$$

Theorem 1 *If the decisional BDH assumption holds, the proposed $\mathcal{CA}$-$\mathcal{IBE}$ scheme is a secure CA-IBE scheme which satisfies the k-resilient ciphertext-auditability and the security of the standard IND-ID-CPA in the standard model.*

The proof of the above theorem are with three aspects: the standard IND-ID-CPA security, verifiability and unforgeability respectively.

Proof. Firstly, the $\mathcal{CA}$-$\mathcal{IBE}$ scheme is proved with the standard IND-ID-CPA secure; and then, the proposed scheme is verifiable; lastly, it claims the scheme is secure against the mix strategy in the standard model, that is, the scheme is k-resilient unforgeable.

IND-ID-CPA. In our construction, notice that there always exists one honest encrypter at least in the k encrypters, that is, there exists a real random number at least in the set $\{r_1, \ldots, r_k\}$. This show that the cipertertext encrypted by the k encrypters is same as one encrypted by the honest encrypter. So, the standard security of the proposed $\mathcal{CA}$-$\mathcal{IBE}$ scheme can reduce to the security of the Waters's scheme. Since the Waters's scheme [13] is secure against IND-ID-CPA under decisional BDH assumption in the standard model, the proposed $\mathcal{CA}$-$\mathcal{IBE}$ scheme is also secure against standard IND-ID-CPA under the same hard problem assumption in the standard model.

Verifiability. Note that the *anonymous* identity-based encryption [1, 4] scheme requires that the ciphertext can not reveal the identity of the receiver, so the property of the verifiability is opposite to it. As the observation in [4], some IBE schemes are anonymous, for example, the Boneh et al's IBE scheme [3]; while some IBE schemes are *not* anonymous, for example, Waters's IBE scheme [13]. Since the private key is created randomly, *some extra information* should be embedded into the ciphertext to counteract the randomness of the private key upon decryption. Notice that the "some extra information" is useful for the verifiability in our CA-IBE scheme. The detailed descriptions are as follows:

Given the public **params**=(g, g_1, g_2, u', U), a message M from $\{0,1\}^l$ and a public key $\mathbf{ID} = (v_1, \ldots, v_n)$, and set $h = u' \prod_{i\in\mathcal{V}} u_i$ where $\mathcal{V} = \{i|v_i \neq 0\}$ is a subset of $\{1, \ldots, n\}$, and get the ciphertext as follows.

$$C = (C_0, C_1, C_2) = (M \cdot e(g_1, g_2)^r, g^r, h^r).$$

Notice that the g, u' and U are public parameters, and there are enough "extra information" to ensure whether the ciphertext was created for a given receiver with the identity **ID**. Then, there are the tuple information

$$[g, h, C_1, C_2] = [g, h, g^r, h^r],$$

so it is not hard to test whether the tuple is Diffie-Hellman tuple as below:

$$e(C_1, h) =^? e(C_2, g),$$

that is,

$$e(g^r, h) =^? e(h^r, g).$$

The progress which test whether the above tuple is Diffie-Hellman tuple or not is sufficient to get the goal of the *verifiability* of the CA-IBE, that is, the test can say whether the ciphertext was actually created by using the identity **ID** as public key.

Unforgeability. If the $\mathcal{CA}$-$\mathcal{IBE}$ scheme satisfies the property of the mix strategy, then the proposed scheme satisfies k-resilient unforgeability. So, it only needs to consider the extreme setting, that is, there are $k-1$ malicious encryption adversaries and one honest encryption adversary in our proof. Without loss of generality, a random number j is selected from the set $\{1, \ldots, k\}$, and assume that the j-th encrypter is honest in our above construction. Note that our construction is unforgeable if there only exists one encrypter and it is honest (it is *regular* scheme if $j = k = 1$). This is because the encrypted message always looks like random for anyone (including the decryption adversary) and it can not give any helpful information to get correct message from this ciphertext for decryption adversary.

Now, assume that the scheme is not k-resilient unforgeable, and let adversary $\mathcal{A}$ control the $k-1$ encrypters. It is easy to show that there is a forger $\mathcal{F}$ who can forge successfully a message in the regular scheme using the adversary $\mathcal{A}$. This is contrary to the case the regular scheme is unforgeable and the theorem is proofed. The detailed descriptions are as follows:

First, in our scheme, $\mathcal{F}$ chooses a modified message M' and the $k-1$ fixed randomized input of $\mathcal{A}$, $\{r_1, \ldots, r_{j-1}, r_{j+1}, \ldots, , r_k\}$, and chooses one random randomized input r_j, then the forger can get the following ciphertext by using the adversa ry $\mathcal{A}$:

$$C' = (M' \cdot e(g_1, g_2)^{r_0+\cdots+r_j+\cdots+r_k}, \\ g^{r_0+\cdots+r_j+\cdots+r_k}, (u' \prod_{i\in\mathcal{V}} u_i)^{r_0+\cdots+r_j+\cdots+r_k}).$$

Since the scheme is not k-resilient unforgeable, the adversary $\mathcal{A}$ can get the correct message M with the non-negligible probability from the above ciphertext C'.

Secondly, the forger do as the above progress aside from setting $M' = 1$ and no choosing a random randomized input r_j, then he get the following ciphetext:

$$C'' = (1 \cdot e(g_1, g_2)^{r'}, g^{r'}, (u' \prod_{i\in\mathcal{V}} u_i)^{r'}),$$

where $r' = r_0 + \cdots + r_{j-1} + r_{j+1} + \cdots + r_k$. From the ciphertext C' and C'', the forger can get easily the following ciphertext which is a ciphertext in the regular scheme:

$$C = (M' \cdot e(g_1, g_2)^{r_j}, g^{r_j}, (u' \prod_{i\in\mathcal{V}} u_i)^{r_j}).$$

So, the forger also can output a correct message from the ciphertext C with the non-negligible probability, which implies the regular scheme is forgeable. It makes contradiction. □

Remark 1 *Notice that the above $\mathcal{CA}-\mathcal{IBE}$ scheme can not prevent the decryption adversary to recover a single bit of the plaintext when the t-encryptor is malicious. This is because the malicious encryptor can choose fixed randomized input and hide the single bit in the ciphertext. For example, if the last bit of plaintext is 1 (or 0), then the malicious encryptor can choose the randomized input and compute the ciphertext until make the last bit of ciphertext is 1 (or 0). Hada and Sakurai's scheme also has this limitation as above mentioned (Remark 8 in [8]).*

4 Conclusions

This paper constructs the ciphertext-auditable identity-based encryption without the random oracles. There are four steps in our scheme, and it only requires that the backup manager BM sends a backup request to both O and A by authenticated way and does *not* need the public key authentication in the first step. In our proposed scheme, the operator O can encrypt the **PI** before receiving the backup request and duplicates the ciphertext to backup tape right now after getting the backup request. Our scheme is secure against the k-resilient ciphertext-auditability in the standard model. How to design a secure ciphertext-auditable identity based encryption scheme which can prevent the decryption adversary to reveal a single bit of the plaintext if there are t-malicious encryptor, is still an open problem.

Acknowledgements

This research is supported in part by the National Natural Science Foundation of China under Grant No. 61103247. The work of Yong Li is partially supported by the Fundamental Research Funds for the Central Universities under Grant No. 2012JBM004. The first author also thanks S. Hada and K. Sakurai for their valuable discussions at the early stage of this work.

References

[1] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. M. Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption waterssrevisited: Consistency properties relation to anonymous ibe, and extensions," *Journal of Cryptology*, vol. 21, no. 3, pp. 350–391, 2007.

[2] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proceedings the First Annual Conference Computer and Communications Security*, pp. 62–73, 1993.

[3] D. Boneh and M. Franklin, "Identity based encryption from the weil pairing," in *Advances in Cryptology - Crypto '01*, vol. LNCS 2139, pp. 213–229, Springer-Verlag, 2001.

[4] X. Boyen and B. Waters, "Anonymous hierarchical identity based encryption," in *Advances in Cryptology - Crypto '06*, vol. LNCS 4117, pp. 290–307, Springer-Verlag, 2006.

[5] S. C. and P. Sarkar, *Identity-based encryption*. London: Springer-Heidelberg Publisher, 2010.

[6] R. Canetti, "Towards realizing random oracles: Hash funtions that hide all partial information," in *Advances in Cryptology - Crypto '97*, vol. LNCS 1294, pp. 455–469, Springer-Verlag, 1997.

[7] M. Clear, A. Hughes, and H. Tewari, "Homomorphic encryption with access policies: Characterization and new constructions," in *Proceedings Africacrypt '13*, vol. LNCS 7918, pp. 61–87, Springer-Verlag, 2013.

[8] S. Hada and K. Sakurai, "Ciphertext-auditable public key encryption," in *Proceedings IWSEC '06*, vol. LNCS 4266, pp. 308–321, Springer-Verlag, 2006.

[9] C. Lin and C. Liu, "Ciphertext-auditable public key encryptions without random oracles," *Information*, vol. 15, no. 6, pp. 2599–2602, 2012.

[10] A. Sahai and H. Seyalioglu, "Fully secure accountable-authority identity-based encryption," in *Proccedings PKC '11*, vol. LNCS 6571, pp. 296–316, Springer-Verlag, 2011.

[11] A. Shamir, "Identity based cryptosystems and signature schemes," in *Advances in Cryptology - Crypto '84*, vol. LNCS 196, pp. 47–53, Springer-Verlag, 1984.

[12] M. Tian, W. Yang, and L. Huang, "Security of a biometric identity-based encryption scheme," *International Journal of Network Security*, vol. 14, no. 6, pp. 362–365, 2012.

[13] B. Waters, "Efficient identity based encryption without random oracles," in *Advances in Cryptology - EuroCrypt '05*, vol. LNCS 3494, pp. 114–127, Springer-Verlag, 2005.

Changlu Lin received the BS degree and MS degree in mathematics from the Fujian Normal University, P.R. China, in 2002 and in 2005, respectively, and received the Ph.D degree in information security from the state key laboratory of information security, Graduate University of Chinese Academy of Sciences, P.R. China, in 2010. He works currently for the School of Mathematics and Computer Science, and the Key Laboratory of Network Security and Cryptology, Fujian Normal University. He is interested in cryptography and network security, and has conducted research in diverse areas, including secret sharing, public key cryptography and their applications.

Yong Li received his M.S. degree in Computer Science from Wuhan University in 2003, and the Ph.D. degree from State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences in 2007. He works currently for the Key Laboratory of Communication & Information Systems (Beijing Jiaotong University), Beijing Municipal Commission of Education. He is interested in applied cryptography and secure cloud computing.

Kewei Lv works at the State Key Laboratory of Information Security, Institute of Information Engineering, CAS. He is interested in provable security, design and analysis of algorithm, computational complexity, and secure multiparty protocol.

Chin-Chen Chang received his PhD in Computer Engineering from National Chiao Tung University. He received BS in Applied Mathematics and MS in Computer and Decision Sciences. Both were awarded in National TsingHua University. He served in National Chung Cheng University from 1989 to 2005. He works currently for Chair Professor in Department of Information Engineering and Computer Science, Feng Chia University, from February 2005. He has won many research awards and honorary positions by and in prestigious organizations both nationally and internationally. He is currently a Fellow of IEEE and a Fellow of IEE, UK. His current research interests, including database design, computer cryptography, image compression and data structures.