IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. IX (Sep-Oct. 2014), PP 55-59
www.iosrjournals.org

Research on Strongly Unforgeable Ring Signature Scheme Based on ID

Gang Zeng
(Police Information Department, Liaoning Police Academy, China)

Abstract : *A ring signature system is strongly unforgeable if the ring signature is existential unforgeable and, given ring signatures on some message m, the adversary can not produce a new ring signature on m. Strongly unforgeable ring signatures are useful for constructing chosen-ciphertext secure cryptographic system. For example, it can be used to design the ring signcryptionscheme.In this paper, we analyse the safety of Au et al.'s ID-based ring signature scheme, then we construct a strongly unforgeable ID-based ring signature scheme in the standard model based on the standard discrete logarithm problem (DLP).*
Keywords: *Strong unforgeability, ring signature, bilinear pairings, standard model*

I. Introduction

Ring signature is a group-oriented signature with privacy protection [1]. A user can sign anonymously on behalf of a group on hisown choice,while group members can be totally unaware of being conscripted in the group. Any verifier can be convinced that a message has been signed by one of the members in this group,but the actual identity of the signer is hidden. ID-based ring signature combines the property of ring signature and ID-based signature. For the first time,zhang et al. constructed ID-based ring signature scheme from bilinear pairings [2]. Since then,several construction have been proposed [3, 4, 5, 6, 7]. Within the proposed ring signature schemes, some ring signature schemes are proven secure in the standard model. But these proposed ring signature schemes are all proven existential unforgeable,none of them is strongly unforgeable.

Existential unforgeability prohibits an adversary from forging a valid signature on a message which a signer has not signed. However, it does not prohibit an adversary from forging a new valid signature on a message which a signer has already signed. That is, the adversary, by giving a message/signature pair(M, σ) , may be able forge a new valid signature σ'≠σ on M. Strong unforgeability is a security notion which ensures not only existential unforgeability but also that no adversary can execute the type of forgery mentioned above[8]. For a variety of applications, strong unforgeability is needed. Strong unforgeability ensures the adversary cannot even produce a new signature for a previously signed message. The conversion from existential unforgeability signature to strong unforgeability signature was first studied by Boneh et al [9]. After that, strongly unforgeable signature was studied by many experts [10, 11]. These experts only studied the conversion of the ordinary signature schemes. We studied the conversion of a class signature with special properties, i.e., ring signature. Strongly unforgeable ring signature has a lot of applications. They are useful for building chosen-ciphertext secure signcryption systems. Strong unforgeability is needed to ensure that the adversary cannot somehow modify the signature in the challenge ciphertext and come up with an alternate valid signature on the same ciphertext. This alternate signature would give the adversary a valid ciphertext that is different from the challenge ciphertext. The adversary could then issue a decryption query for this new ciphertext and break the system. Consequently, a ring signature system that is existentially unforgeable but not strongly unforgeable would result into an insecure ring signcryption system. Without random oracle, all the existing ring signature schemes are not strongly unforgeable. They are only existential unforgeable.

Our contribution. In this paper,we construct a strongly unforgeable ring signature scheme (without random oracles) based on the standard discrete logarithm problem (DLP) and Au, et al.'s ring signature scheme which is only existential unforgeable in the standard model. Au, et al.'s ring signature scheme is not strongly unforgeable-given a ring signature on some message m it is easy to derive many other signatures on the same message m. Nevertheless,we use the Au, et al. 's ring signature scheme as our starting point. Through cryptanalysis, our proposed ID-based ring signature scheme is secure in the standard model.

Organization. We organize the rest of the paper as follows. In Section II, we give preliminaries and security definition. In Section III,we describe Au, et al.'s ring signature scheme and security analysis. In Section IV,we present the construction of our ID-based strongly unforgeable ring signature scheme in the standard model and the corresponding security proofs. Finally, we conclude in Section V.

II. Preliminaries And Security Requirement

Our scheme is based on the bilinear pairings and some difficult assumptions. They are given as the preliminaries. Then, we presented the security requirements of our strongly unforgeable ID-based ring signature scheme in the standard model.

2.1 Preliminaries

Let $G_1$and G_2 be two (multiplicative) cyclic groups of prime order $e: G_1 \times G_1 \rightarrow G_2$ is a bilinear map with the following properties:

1. Bilinearity:For all $u, v \epsilon G_1$ and a, b$\in Z_p^*$, $e(u^a, v^b) = e(u, v)^{ab}$;

2. Non-degeneracy: e(g,g)$\neq 1$

3. Computability: It is efficient to compute e(u, v) for all u, v$\in G_1$.

Definition 1(Discrete Logarithm Problem (DLP)). Given a group G of prime order p with generator g and element $g^a \in G$ where a is selected uniformly at random from Z_p^*, the DLP problem in G is to compute a.

Definition 2(Computational Diffie-Hellman (CDH) Problem). Given a group G of prime order p with generator g and elements$g^a, g^b \in G$ where a, b are selected uniformly at random from Z_p^*, the CDH problem in G is to compute g^{ab}.

We select the group G_1 that satisfies that DLP and *CDH* are difficult.

Let H be a hash function $H: \{0,1\}^* \rightarrow \{0,1\}^n$. We say that algorithm A has advantage ε in breaking the collision-resistance of H if

$$Pr[A = (m_0, m_1): m_0 \neq m_1, H(m_0) = H(m_1)] \geq \epsilon \quad (1)$$

where the probability is over the random bits of *A*.

Definition 3(Collision-Resistant Hashing). A hash family H is (t,ϵ)-collision-resistant if no t-time adversary has advantage at leastϵ in breaking the collision-resistance of *H*.

In practice, of course, one would use a standard hash function such as SHA-256 and assume that it is collision-resistant.

2.2 Aggregate Signature

Our proposed ID-based ring signature scheme in the standard model should be strongly unforgeable and anonymous.

Strong unforgeability. We specify a security model which mainly captures the following two attacks:

1. Adaptive chosen message attack
2. Adaptive chosen identity attack

Adaptive chosen message attack allows an adversary to obtain message-signature pairs on demand during the forging attack. Adaptive chosen identity attack allows the adversary to forge a signature with respect to a group chosen by the adversary. To support adaptive chosen message attack, we provide the adversary the following oracle queries.

Let $U = \{ID_1 \cdots ID_n\}$ be a set of identities. An adversary A with Extract Oracle (EO) and Sign Oracle (SO) succeeds if it outputs $(L, m, \sigma) \leftarrow A^{SO,EO}(U)$, such that it satisfies Verify(param, *L, m, σ*) =valid, where $L \subseteq U$ and $|L| = n$ with restriction that (*L, m, σ*) should not be in the set of oracle queries and replies between *A* and SO, and A is not allowed to make an Extraction query on any identity *ID*∈*L*.

The advantage of an adversary A is defined to be

$$Adv_A = Pr[A \text{ succeeds}] \quad (2)$$

Definition 4(strong unforgeability). An adversary A is said to be an $(\varepsilon, t, q_e, q_s)$-forger of an ID-based ring signature scheme if A has advantage at least ε, runs in time at most t, and makes at most q_e and q_s extraction and signing oracles queries respectively. A scheme is said to be $(\varepsilon, t, q_e, q_s)$-strongly unforgeable if no $(\varepsilon, t, q_e, q_s)$-forger exists.

Anonymity. It should not be possible for an adversary to tell the identity of the actual signer with a probability larger than $1/n$, where n is the cardinality of the ring, even assuming that the adversary has unlimited computing resources.

Definition 5(Anonymity). An ID-based ring signature scheme is unconditional anonymous if for any group of n users with identity $\{ID_1 \cdots ID_n\}$, any message m and signature σ, any adversary A, even with unbounded computational power, cannot identify the actual signer with probability better than random guessing. That is, A can only output the identity of the actual signer with probability no better than $1/n$.

III. Au Et Al.'S Id-Based Ring Signature Scheme And Security Analysis

Au et al.'s ID-based ring signature scheme [4] is the startingpoint of our proposed scheme. We convert their scheme into a stronglyunforgeable ring signature scheme in the standard model. First, wereview this scheme. Second, we analyze this scheme in stronglyunforgeable security model.

3.1Review of Au et al.'s ID-based ring signature scheme

Au et al.'s ID-based ring signature scheme in the standard modelconsists of four phases:Setup, Extract, Sign, Verify.

Setup:Let $H_u: \{0,1\}^* \to \{0,1\}^{n_u}$,, $H_m: \{0,1\}^* \to \{0,1\}^{n_m}$ be two collision-resistant hash functionsfor some $n_u, n_m \epsilon Z$. Select a pairing $e: G_1 \times G_1 \to G_2$ where the order of G_1, G_2 is *p*. Let g begenerators of G_1. Randomly select $\alpha \epsilon R\, Z_{p,g2}$, $h \in R\, G_1$ and compute $g_1 = g^{\alpha}$. Also select randomly the elements asfollows: *u',* *v'*,$U_i, v_j \epsilon G_1$, wherei=1, $\cdots n_u$, j=1, $\cdots n_m$. Let *U={ui}, V={vj}*. The publicparameters are *param*=(*e, G_1, G_2, g, g_1, g_2, h, u', v', U, V*) and themaster secret key is g_2^{α}.

Extract. Let $I_j = H_u(ID_j)$) for user *j* with identity ID_j, where$j \epsilon Z$. Let $I_j[i]$ be the i-th bit ofI_j. Define $X_j \subseteq \{1, \cdots n_u\}$ to be the set of indices such that $I_j[i] = 1, i \in X_j$. Randomly selects $R_{uj} \in Z_p^*$ and computes$d_j = \left(g_2^{\alpha}\left(u'\prod_{i\in X_j} u_i\right)^{r_u}, g^{r_{uj}}\right) = (d_j^{(1)}, d_j^{(2)})$.

Sign. Let $L = \{ID_1, \cdots, ID_n\}$ be the list of n identities tobe included in the ring signature, including the one of the actualsigner. The secret key of the user $ID_\pi$is $d_\pi = (d_\pi^{(1)}, d_\pi^{(2)})$. To sign a message $M \epsilon \{0,1\}^*$, the signer I_π does the procedures as follows.

(1)Compute $m = H_m(M, L)$. Let *m[i]* be the i-th bit of m and $Y \subset \{1,2, \cdots, n_m\}$be the set of indices i such thatm[*i*]=1.

(2)Randomly select $r_1, \cdots, r_n, r \epsilon R\, Z_p^*$, compute $U_j = u'\prod_{i\in X_j} u_i$ for $j = 1,2, \cdots, n$ and $\sigma_1 = g^{r_1}$, $\cdots, \sigma_{\pi-1} = g^{r_{\pi-1}}, \sigma_\pi = d_\pi^{(2)} g^{r_\pi}, \sigma_{\pi+1} = g^{r_{\pi+1}} \cdots, \sigma_n = g^{r_n}, \sigma_{n+1} = g^r, \sigma_{n+2} = d_\pi^{(1)}\left(\prod_{j=1}^n U_j^{r_j}\right)\left(v'^{\prod_{i\epsilon Y} v_i}\right)^r$ At last, the signer ID_π outputs the ring signature$\sigma = (\sigma_1, \cdots, \sigma_{n+2})$.

Verify. Given a signature $\sigma = (\sigma_1, \cdots, \sigma_{n+2})$fora list of identities *L* on a message *M,* a verifier verifies asfollows:

(1)Compute $m = H_m(M, L), U_j = u'\prod_{i\epsilon X_j} u_i for\ j = 1,2, \cdots, n;$

(2)Check that whether the following equation holds:

$$e(\sigma_{n+2}, g) = e(g_1, g_2)\left(\prod_{j=1}^n e(U_j, \sigma_j)\right)e(v'\prod_{i\epsilon Y} v_i, \sigma_{n+1}) \quad (3)$$

Output valid if the equality holds. Otherwiseoutputinvalid.

3.2 Analysis of Au et al.'s ID-based ring signature scheme

From the review of the Au et al.'s ID-based ring signature scheme, weknow that it is existential unforgeable, but it is not stronglyunforgeable. This point is also noted in Au et al.'s paper. They didnot give the attack method in detail. We described it as follows.

Suppose $\sigma = (\sigma_1 + \cdots + \sigma_{n+2})$is a valid Au etal. 's ring signature for a list of identitiesL on a messageM. Then, $\sigma' = \left(\sigma_1 g, \cdots, \sigma'_n = \sigma_{n+1} g, \sigma'_{n+2} = \sigma_{n+2}\prod_{j=1}^n U_j\, v'^{\prod_{i\epsilon X} v_i}\right)$is also a valid Au, et al.'s ring signature for a list ofidentities L on the message *M*.

$$e(\sigma'_{n+2}, g) = e\left(\sigma_{n+2}\prod_{j=1}^{n} U_j\left(v'\prod_{i\epsilon X} v_i\right), g\right) = e(\sigma_{n+2}, g)e\left(\prod_{j=1}^{n} U_j, g\right)e\left(v'\prod_{i\epsilon X} v_i, g\right)$$

$$= e(g_1, g_2)\left(\prod_{j=1}^n e(U_j, \sigma_j)\right)e(v'\prod_{i\epsilon Y} v_i, \sigma_{n+1}) \times e\left(\prod_{j=1}^n U_j, g\right)e(v'\prod_{i\epsilon X} v_i, g) =$$

$$e(g_1, g_2)\left(\prod_{j=1}^n e(U_j, \sigma_j g)\right)e(v'\prod_{i\epsilon Y} v_i, \sigma_{n+1} g) = e(g_1, g_2)\left(\prod_{j=1}^n e(U_j, \sigma'_j)\right)e(v'\prod_{i\epsilon Y} v_i, \sigma'_{n+1}) (4)$$

Thus, Au et al.'s scheme is not strongly unforgeable.

IV. The Proposed Strongly Unforgeable Ring Signature Scheme In The Standard Model

Strongly unforgeable ring signature in the standard model has a lotof applications. For example, it can be used in ring signcryption. Auet al.'s ID-based ring signature schemecan not be used in ringsigncryption design because it is not strongly unforgeable. To thebest of our knowledge, there does not exist strongly unforgeable ringsignature scheme in the standard model until now. Based on Au etal. 's ID-based ring signature scheme in standard model, we proposed astrongly unforgeable ring signature scheme in the standard model.

4.1 Our strongly unforgeable ID-based ring signature scheme in the standard model

Our scheme also consists of four phases:Setup, Extract, Sign, Verify.

Setup:It is similar to Au et al.'s Setup phase except that an extraelement$h \in R\, G_1$ and a hash function $H: \{0,1\}^* \to Z_p^*$ are also selected randomly. The public parameters areparam $= (e, G_1, G_2, g, g_1, g_2, h, u', v', U, V)$ and the master secret keyisg_2^{α}.

Extract. It is the same as Au et al.'s Extract phase.

Sign. Let $L = \{ID_1, \cdots, ID_n\}$be the list of n identities tobe included in the ring signature, including the one of the actualsigner. The secret key of the user $ID_\pi$is$d_\pi = (d_\pi^{(1)}, d_\pi^{(2)})$. To sign a message $M \in \{0,1\}^*$, the signer ID_πdoes the procedures as follows.

(1)Select $r_1, \cdots, r_n, r, s \in R\, Z_p^*$,, compute$U_j = u' \prod_{i \in X_j} u_i$ for $j = 1, \cdots, n$;

(2)Compute $R_1 = g^{r_1}, \cdots R_{\pi-1} = g^{r_{\pi-1}}, R_\pi = d_\pi^{(2)} g^{r_\pi}, R_{\pi+1} = g^{r_{\pi+1}}, \cdots, R_n = g^{r_n}, R = g^r$, $t = H(M, L, R_1, \cdots, R_n, R)$;

(3)Compute $m = H_m(g^t h^s, L)$. Let *m[i]* be the i-th bit of mand $Y \subset \{1,2, \cdots, n_m\}$ be the set of indices $i$suchthat$m[i] = 1, i \in Y$.

(4)Compute $U_j = u' \prod_{i \in X_j} u_i$ forj=1, 2, ⋯, nand

$$\sigma_1 = R_1, \cdots, \sigma_{\pi-1} = R_{\pi-1}, \sigma_\pi = d_\pi^{(2)} R_\pi, \sigma_{\pi+1} = R_{\pi+1}, \cdots, \sigma_n = R_n, \sigma_{n+1} = R, \sigma_{n+2} = d_\pi^{(1)} \left(\prod_{j=1}^{n} U_j^{r_j} \right) \left(v' \prod_{i \in Y} v_i \right)^r$$

At last, the signerID_π outputs the ring signature$\sigma = (\sigma_1, \cdots, \sigma_{n+2}, s)$.

Verify. Given a ring signature$\sigma = (\sigma_1, \cdots, \sigma_{n+2}, s)$for a list of identities$L$ on a message *M*, a verifier verifies it as follows:

(1)Compute $t = H(M) \| \sigma_1 \| \| \cdots \| \sigma_{n+1}$;

(2)Compute$m = H_m(g^t h^s, L)$;

(3)Check that whether the following equation holds:

$$e(\sigma_{n+2}, g) = e(g_1, g_2) \left(\prod_{j=1}^{n} e(U_j, R_j) \right) e(v' \prod_{i \in Y} v_i, R) \quad (5)$$

Output valid if the equality holds. Otherwise outputinvalid.

4.2 Security analysis

We will prove that ourproposed scheme is unconditional anonymous and strongly unforgeableunder a chosen message and identity attack in the standard model.

Theorem 1(Anonymity):Our proposed ID-based ring signature scheme isunconditional anonymous.

Proof:In the ID-based ring signature $\sigma = (\sigma_1, \cdots, \sigma_{n+1}, \sigma_{n+2}, s), \{\sigma_i\}, i \in \{1, \cdots, n\}/\pi$ and σ_{n+1} are randomly generatedwhich provide no information on the actualsigner. $\sigma_\pi = d_\pi^{(2)} g^{r_\pi}$. $r_\pi$is randomlygenerated by the actual signer. Thus, σ_π is also randomlydistributed. In addition to $\{\sigma_i\}, i \in \{1, \cdots, n+1\}/\pi$,

$$\sigma_{n+2} = d_\pi^{(1)} \left(\prod_{j=1}^{n} U_j^{r_j} \right) (v' \prod_{i \in Y} v_i)^r = g_2^\alpha (\prod_{j=1, j \neq \pi}^{n} U_j^{r_j}) U_\pi^{r_\pi + r_{u\pi}} (v' \prod_{i \in Y} v_i)^r \quad (6)$$

According to the Sign procedure, we know that$r_1, \cdots, r_{\pi-1}, r_{u_\pi} + r_\pi, r_{\pi+1}, \cdots, r_n, r, s$ arerandom numbers while $g_2^\alpha$is the master's secret key. All ofthem provide no information on the actual signer. Our proposed schemeis unconditional anonymous.

Theorem 2(Strong unforgeability): The proposed ID-based ringsignature scheme is strongly unforgeable in the standardmodel, assuming that Au et al.'s ID-based ring signature isexistential unforgeable in the standard model and DLP assumption inthe group G1 holds.

Proof:According to the Ref. [4], Au et al.'s ID-based ring signaturescheme is known to be existential unforgeable based on CDHassumption. Suppose A is a forger that(t, q_e, q_s, e)-breaks strong unforgeability of the proposednew scheme which is denoted as$\sum n$, where q_e, q_s denote thetotal number of the Extract queries and Sign queries. Forger A asksfor signatures on message/ring pairs$(M_1, L_1), \cdots, (M_q, L_q)$and is given signatures$\bar{\sigma} = (\sigma_{1,j}, \cdots, \sigma_{n+2,j}, s_j)$, wherej=1,⋯, q on the message/ring pairs. Let$t_j = H(M_j, L, \sigma_{1,j}, \cdots \sigma_{n+1}), \bar{m}_j = g^{t_j} h^{s_j}, m_j = H_m(\bar{m}_j, L_j)$, where j=1, 2,⋯, q. Let$\hat{\sigma} = (\hat{\sigma}, \cdots, \hat{\sigma}_{n+2}, \hat{s})$bethe forgery on the message/ring pair$(\widehat{M}, \widehat{L})$. Let$\hat{t} = H(\widehat{M}, \widehat{L}, \hat{\sigma}_1, \cdots \hat{\sigma}_{n+1}), \widehat{m} = g^{\hat{t}} h^{\hat{s}}, \widehat{m}' = H_m(\widehat{m}, \widehat{L})$. We distinguish two types forgery:

Type 1:$\widehat{m}' \neq m_j$ for all $j \in \{1,2, \cdots q\}$.

Type 2:$\widehat{m}' = m_j$ for some $j \in \{1,2, \cdots q\}$.

Type 1 forger: Suppose *A* is a type 1 forger. We construct achallenger *B* that can break Au et al.'s ID-based ring signaturescheme. *B* runs *A* as follows.

Setup is similar to the Setup phase in Au et al.'s securityproof of existential unforgeability. The only except is that *B*chooses randomly$\alpha \in R\, Z_p^*$ and computes$h=g^a$, i.e., thediscrete logarithm of *h* is known to *B*.

Extractis the same with the Extract phase in Au et al.'ssecurity proof of existential unforgeability.

Signature Oracles. When *A* queries a ring signature on themessage/ring pair (*M, L*), *B* responds as follows.

1. Select a random exponent $\omega \in Z_p^*$and set $m' = g^\omega$.

2. *B* asks Au et al.'s Sign Oracle on the message *m'* and signergroup *L*. *B* obtains a ring signature$(\sigma_1, \cdots, \sigma_{n+2})$.

3. Compute $t = H(M, L, \sigma_1, \cdots, \sigma_{n+1})$, $s = (\omega - t)/\alpha$

4. Return $\sigma = (\sigma_1, \sigma_2, \cdots, \sigma_{n+2}, s)$to A.

Verify:A can verify the simulated ring signatureσas follows:

(1)Compute$t = H(M||\sigma_1|| \cdots ||\sigma_{n+1})$;

(2)Compute$m = H_m(g^t h^s, L) = H_m(g^{t+as}, L) = H_m(g^{\omega}, L) = H_m(m', L)$

(3)Check that whether the following equation holds:

$$e(\sigma_{n+2}, g) = e(g_1, g_2)(\prod_{j=1}^{n} e(U_j, R_j))e(v' \prod_{i \in Y} v_i, R) \quad (7)$$

Because $(\sigma_1, \sigma_2, \cdots, \sigma_{n+2})$ comesfrom Au et al.'s Sign Oracle, the above equation holds.

Output. Finally, algorithm A outputs a forgery$\hat{\sigma} = (\hat{\sigma}_1, \cdots, \hat{\sigma}_{n+2}, \hat{s})$ bethe forgery on the message/ring pair $(\widehat{M}, \widehat{L})$. Takingusing of A's forgery, B can produce a existential forgery on Auet al.'s scheme as follows:

(1)Compute$\hat{t} = H(\widehat{M}, \widehat{L}, \hat{\sigma}_1, \cdots, \hat{\sigma}_{n+1})$, $\widehat{m} = g^{\hat{t}} h^{\hat{s}}$;

(2)The message signature pairing$(\widehat{m}, (\hat{\sigma}_1, \hat{\sigma}_2, \cdots, \hat{\sigma}_{n+2}))$onthe signer group $\widehat{L}$ is a successful forgery on Au et al.'sring signature.

Type 2 forger:Suppose$A$ is a type 2 forger. We construct achallenger B that can break DLP on the group G1. B runs A asfollows. B is given a random pair (g', h') and its goal is to

Setup$B$sets $g \leftarrow g', h \leftarrow h'$, and generatesthe remaining elements of the public key the private key accordingto Setup procedure of our proposed ring signature scheme. B gives$A$ the public key param=(e, G1, G2, g, g1, g2, h, u', v', U, V) andkeeps the master secret key g_2^{α} private.

Extract is the same as the Extract procedure of our proposedring signature scheme.

Signature Oracles. When A queries a ring signature on themessage/ring pair (*M, L*), *B* responds by runningSign(g_2^{α}, *M, L*) and returning the signature to *A*.

Verify:Because the Sign oracle is the same as the actualsignature phase, the received signature can pass the verification.

Output. Finally, algorithm A outputs a forgery$\hat{\sigma} = (\hat{\sigma}_1, \cdots, \hat{\sigma}_{n+2}, \hat{s})$ bethe forgery on the message/ring pair $(\widehat{M}, \widehat{L})$. Takingusing of A's forgery, B can break the DLP of h' as follows:

Compute$\hat{t} = H(\widehat{M}, \widehat{L}, \hat{\sigma}_1, \cdots, \hat{\sigma}_{n+1})$,$\widehat{m} = g^{\hat{t}} h^{\hat{s}}$.AS $\widehat{m}' \in \{m_1, m_2, \cdots, m_{q_s}\}$, w. l. o. g, we denote$\widehat{m}' = m_i, i \in \{1,2, \cdots, q_s\}$, i.e.,$g^{\hat{t}} h^{\hat{s}} = g^{t_i} h^{s_i}, \widehat{L} = L_i$.

Case 1:When$t_i = \hat{t}$, i.e., $H(\widehat{M}, \hat{\sigma}_1, \cdots, \hat{\sigma}_{n+1}) = H(M_i, \sigma_{1,i}, \cdots, \sigma_{n+1,i})$. Wecan get $s_i = \hat{s}, \widehat{L} = L_i$. The hash function$H: \{0,1\}^* \rightarrow Z_p^*$ is collision resistant. We can get

$$(\widehat{M}, \hat{\sigma}_1, \cdots, \hat{\sigma}_{n+1}) = (M_i, \sigma_{1,i}, \cdots, \sigma_{n+1,i})$$

$$\sigma_{n+2,i} = d_{\pi}^{(1)} \left(\prod_{j=1}^{n} U_j^{r_{j,i}}\right) \left(v' \prod_{j \in Y} v_{j,i}\right)^{r} = \sigma_{n+2} (8)$$

$$s_i = \hat{s}$$

At last, $(\widehat{M}, \hat{\sigma}, \widehat{L}) = (M_i, \sigma_i, L_i)$, which is contrary to A'svalid forgery.

Case 2:$t_i \neq t'$, we can get $s_i \neq s'$from $g^{\hat{t}} h^{\hat{s}} = g^{t_i} h^{s_i}$. The discrete logarithm of$h$ based on g isunknown to the forger B. B can suppose the discrete logarithm is$b$. Then, $b = \frac{t' - t_i}{s_i - s'}$. This is contrary to the DLPassumption.

Thus, our proposed ID-based ring signature scheme in the standardmodel is strongly unforgeable.

V. Conclusion

In this paper, we have proposed a ID-based ring signature scheme which are strongly unforgeable in the standard model. To the best of our knowledge, it is the first one. Our scheme's strongly unforgeability is based on Au, et al.'s ring signature scheme security and DLP assumption.

Acknowledgements

This work was partly supported by general scientific research project of education department of Liaoning Province of China (No. L2013490).

References

[1] Rivest, R. L. , Shamir, A. , Tauman, Y. How to leak a secret. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 2001, 552-565.
[2] F. Zhang and K. Kim. ID-Based Blind Signature and Ring Signature from Pairings. In ASIACRYPT 2002, volume 2501 of LNCS, 2002, 533-547.
[3] Jung Yeon Hwang, A note on an identity-based ring signature scheme with signer verifiability, Theoretical Computer Science, Vol. 412, 2012,796-804.
[4] Man Ho Au, Joseph K. Liu, Tsz Hon Yuen, and Duncan S. Wong, "ID-Based Ring Signature Scheme Secure in the Standard Model", IWSEC 2006, LNCS 4266, 2006,1-16 .
[5] Man Ho Au, Joseph K. Liu, Willy Susilo, Tsz Hon Yuen, Secure ID-based linkable and revocable-iff-linked ring signature with constant-size construction, Theoretical Computer Science, Vol. 469, 2013, 1-14.
[6] HovavShacham, Brent Waters, Efficient Ring Signatures Without Random Oracles, PKC 2007, LNCS 4450, 2007,166-180 .
[7] Nan Li, Yi Mu, Willy Susilo, FuchunGuo, Self-Certified Ring Signatures, ASIACCS'11, 2011,396-400,.
[8] Isamu Teranishi, TakuroOyama, Wakaha Ogata, General Conversion for Obtaining Strongly Existentially Unforgeable Signatures, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E91-A , 1(2008), 94-106.
[9] Dan Boneh, Emily Shen, Brent Waters, Strongly Unforgeable Signatures Based on Computational Diffie-Hellman, PKC 2006, LNCS 3958, 2006,229-240.
[10] Yi Qian, Yiming Zhao, "Strongly unforgeable attribute-based group signature in the standard model," 2010 IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS), 2010,843-852.
[11] Huang Q, Wong DS, Li J et al. Generic transformation from weakly to strongly unforgeable signatures. Journal of Computer Science and Technology, 23(2), 2008,240-252.