ID-Based Deniable Ring Signature With Constant-Size Signature And Its Extention

Chengyu HU 1†, Pengtao LIU 2

1School of Computer Science and Technology, Shandong University, Jinan, 250101, China
2Institute of Information Science and Technology, Shandong University of Political Science and Law, Jinan, 250014, China

Abstract

The ring signature can guarantee the signer’s anonymity. Most proposed ring signature schemes have two problems: One is that the size of ring signature depends linearly on the ring size, and the other is that the signer can shift the blame to victims because of the anonymity. Some authors have studied the constant-size ring signature and deniable ring signature to solve these two problems. This paper shows that an identity-based ring signature scheme with constant size has some security problems by using an insecure accumulator and its verification process does not include the message m. Then we combine “constant-size” and “deniable” to form an id-based deniable ring signature with constant-size signature. The new scheme with constant-size signature length is proposed based on an improved accumulator from bilinear pairings and it solves the problem of anonymity abuse. At last, based on the new identity-based deniable ring signature scheme, an anonymous signcryption scheme is proposed which succeeds in simultaneously encrypting the message while digitally signing and is useful in cases where the identity of a sender must remain secret, yet the message verifiable.

Keywords: ID-Based; Deniable Ring Signature; Constant-size; Accumulator; Anonymous Signcryption

1. Introduction

Ring signature was first introduced by Rivest, Shamir and Tauman in 2001[1] to provide anonymity for the message signer. In a ring signature scheme, the message signers form a ring of any set of possible signers and himself. The actual signer can then generate a ring signature entirely using only his secret key and the others’ public keys without the assistance or even awareness of the other ring members. However, the generated ring signature can convince an arbitrary verifier that the message was indeed signed by one of the ring members while the real signer’s identity is totally anonymous to the verifier. Ring signatures have been shown as a powerful tool for applications in the field of management, military affairs, politics, economics and the like. It plays a very important role in keeping the confidential information, voting for the crucial leaders, carrying out the ebusiness and so on. Bersson et al.[2] proved the security in the random oracle model of the scheme proposed in [1] and presented the notion of a threshold ring signature scheme, and applied it to Ad-hoc networks. In 2002, ID-Based ring signature[3] was first introduced by Zhang et al. Tang et al. found some weakness of the scheme in [3] and proposed an enhanced scheme[4].

† Corresponding author.

Email addresses: hcy@mail.sdu.edu.cn (Chengyu HU)
ID-based cryptosystem was first introduced by Shamir\cite{5} in 1984 as an alternative to traditional public key cryptography. In an ID-based cryptosystem, each user’s identity information can be used as his public key and can be used to generate his private key by a trust key generation center. This secret key is sent to the user throughout a secure channel. The advantage is that the key distribution is easier than the conventional ones. In Shamir’s paper\cite{5}, an ID-based signature scheme from RSA was proposed. The following breakthrough result in the area of id-based cryptography came in 2001, when Boneh et al. designed a practical id-based scheme from bilinear pairings\cite{6}. In the design, they used as a tool bilinear pairings, a kind of maps which can be constructed on some elliptic curves. Since the appearance of this work, a lot of identity-based schemes have been proposed for encryption, signature, key agreement, etc., and they all employ such bilinear pairings.

As the verifier needs to know the information of ring members, the signature length of many proposed ring signature schemes is linear with the number of ring members which is inefficient especially when the ring size is large. Some authors have studied the constant size of ring signature scheme and some schemes with constant size signature length have been suggested\cite{7,8,9}.

In some situations, the ring signature allows the signer to shift the blame to victims because of its anonymity called “anonymity abuse”. In [10], Y. Komano et al. proposes a new concept of deniable ring signature which can allow the non-signer to deny the signature and solve the anonymity abuse problem.

Signcryption, a kind of public key cryptosystem, succeeds in simultaneously encrypting the message while digitally signing which makes signcryption system secure and more efficient. In 1997, Zheng\cite{11} introduced the conception of the signcryption. From then on, many researchers had addressed and discussed many variations of signcryption schemes\cite{12,13,14}. Nevertheless, the above-mentioned schemes were unable to satisfy the requirement of anonymity for signers. Anonymous signcryption is useful in cases where the identity of a sender must remain secret, yet the message verifiable.

This paper suggests that there are some problems in an constant size id-based ring signature scheme\cite{9} whose verification process does not include the message information and the weakness of the used accumulator leads to some security problems. Then we combine the concepts of ”constant-size” and ”deniable” and form an id-based deniable ring signature with constant-size signature. The new scheme with constant-size signature length is based on an improved accumulator from bilinear pairings and it solves the problem of anonymity abuse. Based on the proposed deniable ring signature scheme, an anonymous signcryption scheme is developed.

The rest of this paper is organized as follows. In Section 2, we review bilinear pairings and some related complexity assumptions briefly and a accumulator. In Section 3, we analyze a constant-size id-based ring signature scheme and present a new deniable one. The security analysis is given in Section 4. In Section 5, an anonymous signcryption scheme is discussed. Finally, we draw our conclusions in Section 6.

### 2. Preliminaries

For convenience, throughout the paper we use the following notations. $Z_p$ denotes all positive integer which is less than $p$. $Z_p^*$ denotes multiplicative group modulo $p$. The notation $x \in_R X$ denotes that $x$ is selected randomly from the set $X$. We let $\{0,1\}^l$ be the bit string of length $l$. 
2.1. Bilinear Pairings

Let \( G_1 \) be a cyclic additive group generated by \( P \), with a prime order \( p \), and \( G_2 \) be a cyclic multiplicative group with the same prime order \( p \). Let \( e : G_1 \times G_1 \rightarrow G_2 \) be a map with the following properties\(^{[15]}\):

1. Bilinearity: \( e(aP, bQ) = e(P, Q)^{ab} \) for all \( P, Q \in G_1, a, b \in \mathbb{Z}_p^* \);
2. Non-degeneracy: There exists \( P, Q \in G_1 \) such that \( e(P, Q) \neq 1 \);
3. Computability: There is an efficient algorithm to compute \( e(P, Q) \) for all \( P, Q \in G_1 \);

**Definition 1.** \( q \)-Strong Diffie-Hellman (q-SDH) problem

Let \( e : G_1 \times G_1 \rightarrow G_2 \) be a bilinear map, given \( (P, sP, \ldots, tP) \) where \( s \in \mathbb{Z}_p^* \), compute \( (c, 1/(s+c)P) \), \( c \in \mathbb{Z}_p \). The q-SDH problem is **hard** if for all PPT adversaries \( A \), the following function \( \text{Adv}_{A}^{q\text{-SDH}}(l) \) is negligible.

\[
\text{Adv}_{A}^{q\text{-SDH}}(l) = \Pr[A(P, sP, \ldots, tP) = (c, P/(s+c)) : c \in \mathbb{Z}_p; s \in \mathbb{Z}_l]
\]

2.2. Accumulator

An accumulator\(^{[16]}\) is a tuple \((\{X_1, F_1\})\) where \( l \in \mathbb{N} \), \( \{ X_i \} \) is called the value domain of the accumulator; and \( \{F_i\} \) is a sequence of families of pairs of functions such that each \((f, g) \in F_1 \) is defined as: \( f : U_f \times X_f \rightarrow U_f \) and \( g : U_g \rightarrow U_g \) is a bijective function. In addition, the following properties are satisfied:

- **Efficient generation:** There exists an efficient algorithm that takes as input a security parameter \( l \) and outputs a random element \((f, g) \in F_1\) possibly together with some auxiliary information \( \alpha_l \).
- **Quasi commutativity:** For every \( i \in \mathbb{N} \), \((f, g) \in F_i \), \( u \in U_f \), \( x_1, x_2 \in X_i \): \( f(f(u, x_1), x_2) = f(f(u, x_2), x_1) \).
- **Efficient evaluation:** For every \((f, g) \in F_i \), \( u \in U_f \) and \( X = \{x_1, \ldots, x_q\} \subseteq X_i \), we call \( g(f(f(u, x_1), \ldots, x_q)) \) the accumulated value of the set \( X \) over \( u \). Due to quasi commutativity, the value \( f(f(u, x_1), \ldots, x_q) \) is independent of the order of the \( x_i \) and is denoted by \( f(u, X) \).

**Definition 2.** Collision Resistant Accumulator\(^{[16]}\)

An accumulator is defined as collision resistant if for every PPT algorithm \( A \), the following function \( \text{Adv}_{A}^{\text{col}.\text{acc}}(l) \) is negligible.

\[
\text{Adv}_{A}^{\text{col}.\text{acc}}(l) = \Pr[(f, g) \in F_i; u \in U_f; (x, w, X) \in A(g, f, U_f, U_g, u) : (X \subseteq X_i)^{\nu}(w \in U_g) : (x \in X_i^{\nu}; X_i^{\nu}; x)^{(g^{-1}(w), x)} = f(u, X)]
\]

where \( w \) is a witness for the fact that \( x \in X_i \) has been accumulated in \( v \in U_g \) whenever \( g(v^{-1}(w), x) = v \).

In this paper, an improved accumulator\(^{[17]}\) from the one in \([16]\) with some security measures is used to construct our constant-size length scheme. The basic accumulator is: Let \( e : G_1 \times G_1 \rightarrow G_2 \) be a bilinear map, the parameter \( t = (P, P_{pa}=sP, \ldots, tP) \), \( s \in \mathbb{Z}_p^* \), \( q \) is the max number of members to be accumulated. The corresponding functions \((f, g)\) are defined as:

\[
\begin{align*}
Z_p \times Z_p & \rightarrow Z_p \\
(u, x) & \rightarrow (x+s)u \\
g : Z_p & \rightarrow G_1 \\
u & \rightarrow uP
\end{align*}
\]

\( f \) is quasi-commutative. In addition, for \( u \in Z_p \) and a set \( X = \{x_1, \ldots, x_k\} \subseteq Z_p \{s\} \) where \( k \leq q \), the accumulated value \( g(f(u, X)) = (\prod_{i=1}^{k} (x_i+s)u)P \) is computable in time polynomial in \( l \) from the tuple \( t \) and without the knowledge of the auxiliary information \( s\)^\(^{[16]}\).
3. Our Deniable Constant-size Id-based Ring Signature Scheme

3.1. Analysis of the Scheme in [9]

We don’t describe the scheme in [9] in detail. In [17], a PPT algorithm was constructed to break the Collision Resistance property of the accumulator from [16] used by the scheme in [9] with non-negligible probability. The algorithm construction is as follows:

Algorithm A:
Input: The pair of function \((f, g)\) and the value \(u\).
1. Compute \(s=f(1,0)\)
2. Let \(k\) be any polynomial function of \(l\). Choose uniformly at random \(k+1\) elements of \(\mathbb{Z}_p\setminus\{s\}\) denoted \(x_1, \ldots, x_k, x\) and set \(X=[x_1, \ldots, x_k]\).
3. Compute \(\lambda:=\prod_{j=1}^{k+1}(x+j)s\mod p\) and \(\mu:=(x+s)^{-1}\lambda\mod p\). Denote \(\xi:=\lambda\mu\mod p\) and set \(w:=g(\xi)\).
Output: The triple \((x, w, X)\).

Due to Step 2, \(X\subseteq X_f\) and \(x\in X_{\text{fin}}\). From Step 3, \(w\in U_p\). Note that \(f(\mu, X)=\prod_{j=1}^{k+1}(x+j)s\mod p\), so the following equalities can be obtained: \(f(\xi, X)=(x+s)\xi\mod p=(x+s)\mu\mod p=(x+s)(x+s)^{-1}\lambda\mod p=\lambda\mod p\). Therefore, \(f(\xi^l(w), x)=f(\mu, X)\) and the construction of triple \((x, w, X)\) is deterministic. So \(Adv_{\text{acc}}^\text{coll}(l)=1\).

Therefore, \(A\) is a PPT algorithm breaking the collision resistance of the accumulator with non-negligible probability. Thus, the accumulator from [16] is not collision resistant.

Also, Zhang et al. [18] pointed that there are flaws with the accumulator from [16] which make the accumulator forgeable and lead to some security problems of the scheme in [9].

And the verification process of the scheme in [9] does not include the message information, so that the verification can not check whether the signature is corresponding to the message \(m\).

3.2. Our New Scheme

In this section, we present our new ID-based deniable ring signature scheme from bilinear pairings. The construction method of our scheme is similar to the scheme in [9], but our scheme is based on the improved accumulator from bilinear pairings[17]. The scheme includes system setup, user key generation, ring signature and verification.

1) **Setup**() On a security parameter \(l\), choose a bilinear map: \(e : G_1 \times G_1 \rightarrow G_2\), where \(P\) is a generator of \(G_1\). Generate tuples \(t'=(P, P_p=P^sP, \ldots, \delta^sP)\), where \(s \in \mathbb{Z}_p^*\), \(q\) is the max number of members to be aggregated. Chooses randomly \(P_0, Q, H \in \mathbb{G}_1, u, s_u \in \mathbb{Z}_p^*\), computes \(Q_{pub}=s_uQ\).

Generate an instance of the accumulator, including functions \((f, g)\) that \(f:(u, a)\rightarrow(a+s_u)u, g:\{0,1\}^*\rightarrow\mathbb{G}_1\). Select \(H_1: \{0,1\}^*\rightarrow\mathbb{G}_2, H_2: \{0,1\}^*\rightarrow\mathbb{G}_1\) and publish the system parameters \((l, e, P, P_0, t', f, g, H, Q, Q_{pub}, u, H_1, H_2)\), \(s, s_u\) is the system master key and \(H_2\) is just used in confirmation and disavowal.

2) **KeyGen**(id) User \(U_{id}\) selects his secret key \(x_{id}\) and sends a committed value \(x_{id}P\) to KGC. KGC extracts a private key \(S_{id}\) for \(U_{id}\) as \(S_{id}=(x_{id}P+P_0)/(H_1(id)+s)\) satisfying \(e(H_1(id)P+P_{pub}, S_{id})=e(x_{id}P+P_0, P)\).

3) **RSign**(n, Sid) Let \(\{i_1, \ldots, i_n\}, n\leq q\) be the ring of users, and \(m\) be the message to be signed. The real signer is \(i_{id}\). The signer computes \(X'=H_1(i_{id}), X=HX_1(i_{id}), V=g(f(u, X)), W=g(f(u, X'))\), \(h_{id}=H_1(id)\), and firstly checks whether the following two equations hold:
\[
e(h_{\text{id}}P + P_{\text{pub}}, S_{\text{id}}) = e(x_{\text{id}}P + P_{0}, P) \text{ and } e(h_{\text{id}}Q + Q_{\text{pub}}, W) = e(Q, V)
\]

If the check fails, then the signer declares that KGC generates wrong user private key and stops. Otherwise, the signer picks \(r_1, r_2, k_1, k_2, k_3, k_4, k_5 \in \mathbb{Z}_p\) randomly and computes

\[
U_1 = S_{\text{id}}r_1H, U_2 = W + r_2H, R_1 = r_1K, R_2 = r_2K, T_1 = k_1R_1 + k_3K, T_2 = k_2R_2 + k_5K, T_3 = k_4K, T_4 = k_6K,
\]

\[
\prod = e(P, U_1)^s e(P, H)^e e(P_{\text{pub}}, H)^{4e} e(P, P)^{2e} [e(P_0, P)e(P_{\text{pub}}, U_1)]^f,
\]

\[
\prod = e(Q, U_2)^s e(Q, H)^e e(Q_{\text{pub}}, H)^{4e} e(Q, V)^{e} [e(Q_0, V)e(Q_{\text{pub}}, U_2)]^f
\]

If all the checks pass, then the signature is valid.

3. Security

Firstly, our scheme is correct. For a valid signature \(\sigma\), we have:

\[
s_1r_2 - s_2K = (k_1 - \text{id}_{\text{id}})r_2 - (k_2 - \text{cr}_{\text{id}})K = T_1;
\]

\[
s_1r_2 - s_2K = (k_1 - \text{id}_{\text{id}})r_2 - (k_2 - \text{cr}_{\text{id}})K = T_2;
\]

\[
s_1r_2 + s_2K = (k_2 + s_2K) + (k_1 - \text{id}_{\text{id}})r_2 - (k_2 - \text{cr}_{\text{id}})K = T_3;
\]

\[
s_1r_2 + s_2K = (k_2 + s_2K) + (k_1 - \text{id}_{\text{id}})r_2 - (k_2 - \text{cr}_{\text{id}})K = T_4;
\]

\[
e(P, U_1)^s e(P, H)^e e(P_{\text{pub}}, H)^{4e} e(P, P)^{2e} [e(P_0, P)e(P_{\text{pub}}, U_1)]^f
\]

\[
e(Q, U_2)^s e(Q, H)^e e(Q_{\text{pub}}, H)^{4e} e(Q, V)^{e} [e(Q_0, V)e(Q_{\text{pub}}, U_2)]^f
\]

So our scheme satisfies correctness.

Secondly, our scheme satisfies anonymity. As Lemma 1 of [17], we can get that under the Discrete Logarithm assumption on \(G_1\), the signature \((m, U_1, U_2, R_1, R_2, R_3, R_4, T_1, T_2, T_3, T_4, T_5, T_6, T_7, T_8, T_9, T_{10})\) is a zero knowledge proof of knowledge of \((h_{\text{id}}; S_{\text{id}}; x_{\text{id}}; W)\)

\[
e(h_{\text{id}}P + P_{\text{pub}}, S_{\text{id}}) = e(x_{\text{id}}P + P_{0}, P) \text{ and } e(h_{\text{id}}Q + Q_{\text{pub}}, W) = e(Q, V).
\]

The proof is as follow:[17]:

\[
\text{Soundness: The goal is to show that if the verify process accepts with non-negligible probability the proof of knowledge, then a PPT prover must have the knowledge of } (h_{\text{id}}; S_{\text{id}}; x_{\text{id}}; W) \text{ satisfying the stated relations, under the Discrete Logarithm assumption on } G_1.
\]

Suppose the protocol accepts for the same commitment \((U_1, U_2, R_1, R_2, T_1, T_2, T_3, T_4, T_5, T_6, T_7, T_8, T_9, T_{10})\) with two different pairs of challenges and responses \((c, s_1, s_2, s_3, s_4, s_5, s_6)\) and \((c', s_1', s_2', s_3', s_4', s_5', s_6')\). Let \(f_i = (s_i - s_i')/(c-c')\), then the following equations are obtained according to the verification algorithms of the scheme:

\[
f_1r_2 = f_1P
\]

\[
f_1r_2 = f_1P
\]

\[
f_1r_2 = f_1P
\]

\[
f_1r_2 = f_1P
\]

\[
e(P, U_1)^s e(P, H)^e e(P_{\text{pub}}, H)^{4e} e(P, P)^{2e} [e(P_0, P)e(P_{\text{pub}}, U_1)]^f = 1
\]

\[
e(Q, U_2)^s e(Q, H)^e e(Q_{\text{pub}}, H)^{4e} e(Q, V)^{e} [e(Q_0, V)e(Q_{\text{pub}}, U_2)]^f = 1
\]
Since $P$ is generator of $G_1$, from Equations (1), (2), (3) and (4), we obtain: \(-f_if_iP=f_iP, -f_if_iP=f_iP\).

Then:

\begin{align}
-f_if_iP &= f_6 \tag{7} \\
-f_if_iP &= f_4 \tag{8}
\end{align}

From Equation(5), we get: \(e(P, f_iU_1+f_jH)e(P_{pub}, f_iH+U_1)=e(-f_jP+P_{pub}, P)\)

Applying Equation(7), we obtain: \(e(-f_iP+P_{pub}, f_iH+U_1)=e(-f_jP+P_{pub}, P)\) \hspace{1cm} (9)

Similarly, from Equation(6) and (8), we get: \(e(-f_iQ+Q_{pub}, f_iH+U_2)=e(Q, V)\) \hspace{1cm} (10)

From Equation(9) and (10), we can get that if we set \(x_{id}=f_2, u_{id}=-f_1, S_{id}=f_iH+U_1, W=f_iH+U_2\), they satisfy the relations.

Zero-knowledge: The simulator chooses \(c,s_1,s_2,s_3,s_4,s_5\in\mathbb{Z}_p\) and computes

\[
T_1=s_1R_1s_5K; \quad T_2=s_1R_1s_5K; \quad T_3=s_3K+cR_4; \quad T_4=s_3K+cR_4; \quad T_5=s_5K+cR_4;
\]

\[
\prod_1=e(P, U_1)^c e(P, H)^{s_1} e(P_{pub}, H)^{s_2} e(P, P)^{s_3} e(P_{pub}, U_1)^{s_4} e(Q, U_1)^{s_5} e(Q_{pub}, H)^{s_6} e(Q, V)^{s_6};
\]

It is easy to see that the distribution of the simulation is the same as the distribution of the real transcript.

So our scheme satisfies anonymity.

Thirdly, our scheme is unforgeable. Suppose an APT adversary can forge a ring signature \((m, U_1, U_2, R_1, R_2, R_3, R_4, T_1, T_2, T_3, T_4, T_5, U_1, U_2, U_3, U_4, U_5)\). Then given a q-SDH instance \((P, zP, \cdots, z^dP)\), we can construct a PPT algorithm to solve the q-SDH problem using A. That is to say, B can compute \((x, 1/(z+x))P, x\in\mathbb{Z}_p\).

Given the public system parameter \((l, e, P, P_0, t^i, f, g, H, Q, Q_{pub}, u, H_i, H_2, t^i = (P, zP, \cdots, z^dP)\), B chooses users \(\{id_1, \cdots, id_k\}, k\leq q\) and computes \(V\). For the user whose identity is id, B can forge new \(h^i\), \(W\). Based on the properties of accumulator, we have \((h^i+z)W=\prod(h^i+z)uP\).

Let \(f(z)=\sum_{\mathbb{Z}_p} z^r \) for \(z\neq 0\).

As \((h^i+z)W=\prod(h^i+z)uP\), this can be represented as \((h^i+z)W=uf(z)P\) that is \(W/uf(z)P=(h^i+z)\).

Then \(f(z)\) can be written as \(f(z)=a(z)(z+h^i)+r\), where \(a(z)=\sum_{\mathbb{Z}_p} z^r, r\in\mathbb{Z}_p\), so that \(f(z)/(h^i+z)=a(z)+r/(h^i+z)\).

So \(W/uf(z)P=rP(h^i+z)\), and \(P/(h^i+z)=W/uf(z)P/r\).

Given a q-SDH instance \((P, zP, \cdots, z^dP)\), then \(h, W/uf(z)P/r\) is a solution.

Finally, the non-signer in our scheme can, if desired, deny the signing action of a ring signature. When the a signer \(i\) tries to shift the blame to user \(j\), then the user \(j\) can interact with the verifier to claim the false charge. The protocol is executed as follows:

- The verifier selects randomly \(m\in\{0,1\}\) and sends \(H_2(m)\) to user \(j\).
- User \(j\) chooses \(r\in\mathbb{Z}_p\) and computes \(rH_2(m)\), \(rS_j, rP, rH\). Then user \(j\) sends them with \(x_jP\) to verifier;
- The verifier checks \(e(hP+P_{pub}, rS_j)=e(hP+P_P, rP), e(rH_2(m), P)=e(H_2(m), rP), e(rH, P)=e(H, rP)\).
- If not all checks succeed, then user \(j\) give the wrong information and the verifier stops the protocol;
- Otherwise, the verifier checks whether \(e(U_i(m), rP)=e(rS_j, P)e(rH, R_j)\). If the checks fails, then the verifier can confirm that user \(j\) is not the real signer. Otherwise, user \(j\) is the real signer.

The user must calculate \(rH_2(m)\), \(rS_j, rP, rH\) with right form, otherwise the checks in step 3) will certainly fail. Consider that the real signer get the victims’ \(S_j\) but as he can’t get \(r\), so he can’t get right \(rH_2(m)\) for \(m\) randomly selected by verifier. Moreover, in the protocol, there is not a trusted third party who revokes the anonymity and the user need not leak his secret key.
4. Extention to Anonymous Signcryption

Based on proposed deniable ring signature scheme, an anonymous signcryption scheme is developed. The process comprises four steps, namely system construction, generation of signcryption text, verification of signcryption text, and conversion of signcryption text to standard signature.

1) **System construction.** On a security parameter \( l \), choose a bilinear map \( e : G_1 \times G_1 \rightarrow G_2 \), where \( P \) is a generator of \( G_1 \). Generate tuples \( t' = (P, P_{pub}^w, \cdots, s^P) \), where \( s \in \mathbb{Z}_q ^* \) \( q \) is the max number of members to be aggregated. Chooses randomly \( P_0, Q, H \in G_1 \), \( u, su \in G \), computes \( Q_{pub} = suQ \).

Generate an instance of the accumulator, including functions \( f, g \) that \( f : (u, a) \rightarrow (a+u)a \), \( g : u \rightarrow uP \). Select \( H_i : \{0,1\} ^* \rightarrow \mathbb{Z}_q \), \( H_i : G_2 \rightarrow \{0,1\} ^* \) and publish the system parameters \( l, e, P_0, t', f, g, H, Q, Q_{pub}, u, H_1, H_2, H_3 \). \( s, su \) is the system master key.

User \( U_{id} \) selects his secret key \( x_{id} \) and sends a committed value \( x_{id}P \) to KGC. KGC extracts a private key \( S_{id} \) for \( U_{id} as \ S_{id} = (x_{id}P+P_0)/(H_1(id)+s) \) satisfying \( e(H_1(id)P+P_{pub}, S_{id}) = e(x_{id}P+P_0, P) \). Then KGC publishes \( x_{id}P \). The private key of verifier \( U_1 \) is \( S_{id} = (x_{id}P+P_0)/(H_1(v)+s) \) and \( x_{id}P \) is public.

2) **Generation of signcryption text.** Let a member \( id_i \) in \( \{id_1, \ldots, id_d\} \) send the signcryption text of message \( m \) to verifier \( id_i \). \( id_i \) executes the process of generating signcryption text as follows.

Step 1. Computes \( X = \{H_1(id_1), \ldots, H_1(id_d)\} \), \( X = H_1(id_i), V = g(f(uX)), W = g(f(uX^a)), h_{id} = H_1(id_i) \).

Step 2. Select randomly \( r \in \mathbb{Z}_q \) and calculate \( R = h_{id}P+rP_{pub}, k = H_3(e(s, P^P_0rP)) \).

Step 3. Chooses randomly \( r_1, r_2, k_1, k_2, k_3, k_4, k_5, k_6 \in \mathbb{Z}_q \) and computes

\[
U_1 = S_{id} + r_1U, U_2 = W + r_2H, R_1 = r_1K, R_2 = r_2K, T_1 = k_1R_2k_2K, T_2 = k_1R_1k_2K, T_3 = k_3K, T_4 = k_4K,
\]

\[
\prod_1 = e(P, U_1)^{r_1}e(P, H)^{r_2}e(P_{pub}, H)^{r_3}e(P, P)^{r_4}, \prod_2 = e(Q, U_2)^{r_1}e(Q, H)^{r_2}e(Q_{pub}, H)^{r_3},
\]

\[
c = H_1(m)[T_1][T_2][T_3][T_4][\prod_1][\prod_2], s_1 = k_1c_{hid}, s_2 = k_2c_{sid}, s_3 = k_3cr_2,
\]

\[
s_4 = k_4cr_1h_{id}, s_5 = k_5cr_1, s_6 = k_6cr_1h_{id}.
\]

Step 4. Encrypt the message \( m \) as \( m^{'} = E_2(m) \) using the symmetric secret key \( k \).

3) **Verification of signcryption text.** On receiving the encrypted text \( \sigma \), the verifier \( U_1 \) performs the following steps to verify.

Step 1. Calculate \( k = H_3(e(R, S_{id})), m^{'} = E_2(m^{'}), \) and \( c = H_1(m)[T_1][T_2][T_3][T_4][\prod_1][\prod_2] \).

Step 2. Let \( X = \{H_1(id_1), \ldots, H_1(id_d)\} \). Calculate \( V = g(f(uX)) \).

Step 3. With the following equalities checked

\[
T_1 = s_1R_2s_2K, T_2 = s_1R_1s_2K, T_3 = s_3K+cP, T_4 = s_3K+cP_1,
\]

\[
\prod_1 = e(P, U_1)^{r_1}e(P, H)^{r_2}e(P_{pub}, H)^{r_3}e(P, P)^{r_4}, \prod_2 = e(Q, U_2)^{r_1}e(Q, H)^{r_2}e(Q_{pub}, H)^{r_3},
\]

\[
\prod = e(Q, V)^{r_1}e(Q, H)^{r_2}e(Q_{pub}, H)^{r_3}e(Q, V)^{r_4}e(Q_{pub}, U_2)^{r_5}.
\]

Confirm that \( \sigma \) is a valid anonymous signcryption text from the group \( \{H_1(id_1), \ldots, H_1(id_d)\} \); otherwise, reject the encrypted text.

4) **Conversion of signcryption text to standard Signature.** On receiving signcryption text \( \sigma = (m^{'}, U_1, U_2, R_1, R_2, R_3, R_4, T_1, T_2, T_3, T_4]\prod_1, T_2, T_3, T_4]\prod_2, s_1, s_2, s_3, s_4, s_5, s_6 \), the verifier \( U_1 \) applies the verification process in the above to confirm the validity of signcryption text \( \sigma \). Thus, \( m^{'} \) denotes the signed message from a group, and \( \sigma = (m^{''}, U_1, U_2, R_1, R_2, R_3, R_4, T_1, T_2, T_3, T_4]\prod_1, T_2, T_3, T_4]\prod_2, s_1, s_2, s_3, s_4, s_5, s_6 \) indicates the standard ring signature converted from \( \sigma \). Only verifier \( U_1 \) can perform the signature conversion process. Any third party can verify the validity of the converted signature.
5. Conclusion

In this paper, we analyze the constant-size id-based ring signature scheme in [9] and suggest that there are some drawbacks in the scheme. Then, based on bilinear pairings and improved accumulator, a new constant-size id-based deniable ring signature scheme is proposed and we prove that our scheme provides anonymity, unforgeability and deniability. The suggested scheme solves the problem of anonymity abuse. Finally, we extend our identity-based deniable ring signature scheme to an anonymous signcryption scheme which succeeds in simultaneously encrypting the message while digitally signing and is useful in cases where the identity of a sender must remain secret, yet the message verifiable.

Acknowledgement

This project was supported by Shandong Postdoctoral Special Fund for Innovative Research(200803051)

References