Traceable Certificateless Ring Signature Scheme For No Full Anonymous Applications

Ke Gu[1,2], LinYu Wang[1], Na Wu[1] and NianDong Liao[1]

(Corresponding author: Ke Gu)

School of Computer and Communication Engineering, Changsha University of Science and Technology[1]
Wangjiali Rd, Tianxin district, Changsha, Hunan Province 410114, China
Hunan Provincial Key Laboratory of Intelligent Processing of Big Data on Transportation,
Changsha University of Science and Technology[2]
(Email: gk4572@163.com)

(Received Jan. 26, 2017; revised and accepted June 25, 2017)

Abstract

With the rapid development of identity-based cryptography, several traceable (or linkable) identity-based ring signature (TIBRS) schemes have been proposed. Compared with ring signature based on public key cryptography, TIBRS can simplify public key management and be used for more applications. However, identity-based cryptography still has the problem of private key management and few traceable ring signature schemes are constructed in the standard model. In this paper, we present a fully traceable certificateless ring signature (TCRS) scheme in the standard model, which has a security reduction to the computational Diffie-Hellman (CDH) assumption.

Keywords: Certificateless Cryptography; Ring Signature; Standard Model; Traceability

1 Introduction

Ring signature [1,12,22,24,42,49,51] allows ring member to hide his identifying information to a ring when ring member signs any message, thus ring signature only reveals the fact that a message was signed by possible one of ring members (a list of possible signers). Ring signature is also called as a special group signature [20]. However, compared with group signature, ring signature has more advantages: the group (ring) must not be constructed by a group manager, who can revoke the anonymity of any signer or identify the real group signer; additionally, because a list of possible signers must be constructed to form a group, some intricate problems need to be solved in a group signature scheme, such as joining the new members and the revocation of group members. Although ring signature can provide more flexibility and full anonymity, it is vulnerable to keep the signers from abusing their signing rights. Namely, it is infeasible for the verifier to determine whether the signatures are generated by the same signer on the same event. Thus, in a practical ring signature scheme, the third trusted authority or the verifier must be able to know who signs the messages on the same event many times and the verifier can not accept the signatures generated by the same signer on the same event [2,10,15,33,35,39].

Traceable ring signature[1] [27] is a ring signature that restricts abusing anonymity. Unlike group signature has too strong a traceability characteristic and ring signature has too strong an anonymity characteristic, traceable ring signature has the balance characteristic of anonymity and traceability. Namely, traceable ring signature provides restricted anonymity and traceability. In a traceable ring signature scheme, traceable ring signature can provide full anonymity for the responsible or honest signer when the singer signs any message and provide traceability for the verifier (or the third trusted authority) to determine whether the signatures are generated by the same signer on the same event when the irresponsible signer abuses anonymity in some applications. In order to achieve this requirement of traceable ring signature, we need to consider the two notions ”one-more unforgeability” and ”double-spending traceability” [18,19,27] in the context of ring signature, which originate from blind signature. First, any user can not generate a ”one-more” new signature after he obtained a signature from the original signer. Second, if an irresponsible user signs any message twice on the same event, the signatures generated by the user can be traced to reveal the identity of the signer [14,40]. In the second notion, a responsible user can be anonymously protected. Obviously, traceable ring signature can provide more practicality because of its restricted anonymity in many no full anonymous applications.

Currently ring signatures are used in many different applications, such as whistle blowing [42], anonymous au-

[1] This notion is closely related to linkable ring signature in [5,35–37].

thentication for ad-hoc network [35], e-voting [21] and e-cash [45], non-interactive deniable authentication [44] and multi designated verifiers signature [34], *etc.* Because ring signature is not linkable, no one can determine whether two ring signatures are generated by the same signer. Thus, it exists high risk that ring signatures are used in e-voting and e-cash. For example, if a user signs a message twice for double votes in anonymous e-voting, no one can find the two signatures are linkable so as to detect the irregularity. Obviously, traceable ring signature is suitable for the kind of applications, because it can find the two signatures are linkable. There also are other applications for traceable ring signature. In the "off-line" anonymous e-cash systems, a user is permitted to anonymously signs a message once during one cash transaction, thus traceable ring signature is a natural choice for this application [27]. Damgard *et al.* [23] proposed an unclonable group identification without the group manager, traceable ring signature is also suitable for this application because of not employing the group manager and its balance of anonymity and traceability.

In public key cryptography, the management of public keys is a critical problem. For example, certificate authority (CA) generates a digital certificate, which assures that public key belongs to corresponding user [38]. Thus, in a ring signature scheme based on public key cryptography, because a list (ring) of public keys is corresponding to ring member's private keys (signing keys), the management cost of public keys is proportional to the number of ring members. Additionally, in the ring signature schemes based on public key cryptography, the proposed schemes also suffers from other drawbacks such as verification and revocation of certificates. Obviously, removing public key certificates can simplify the procedure of joining and revocation of ring member. Identity-based cryptography is another cryptographic primitive. In identity-based cryptography, a user's public key is obtained from his/her public identity, such as name, IP address or email address, *etc.* Thus, the user's private key is distributed from a private key generator (PKG). The main target of application of identity-based cryptography is to simplify public key management and remove public key certificates. However, identity-based cryptography still has the problem of private key management. For example, the private key generator may be not fully trusted or be corrupted, so identity-based cryptography has a certain risk in practice. Al-Riyami and Paterson [3] proposed the certificateless public key cryptography, which not only solves the problem of private key management, but also removes public key certificates. Therefore, compared with ring signatures based on public key cryptography and identity-based cryptography, certificateless ring signature [17, 29] can lessen the risk of private key management and the suffering of joining and revocation of ring member.

In this paper, we present a traceable certificateless ring signature scheme in the standard model, which has the properties of anonymity and traceability with enough security.

2 Related Works

Liu *et al.* [35] first proposed the notion of linkable ring signature. In their scheme, if an irresponsible user anonymously signs any message twice on the same event, the two signatures generated by the user can be linked. Base on this notion, some similar schemes were proposed in [4, 35–37, 45, 46]. In [35, 36], the proposed schemes cannot resist the attack that an irresponsible signer forges the signature of a honest signer so as to make the honest signer accused of "double-signing". In [4, 46], the proposed schemes overcome this weakness, but the security conditions are more complicated. In [45], Tsang *et al.* proposed a short linkable ring signature scheme, which is based on the group identification scheme from [25]. Their scheme provides weak traceability, namely it can only detect the linkable ring signatures. In [46], Tsang *et al.* proposed a separable linkable threshold ring signature scheme, where the threshold setting is to restrict abusing signing. However, their scheme is complicated. In [53], Liu *et al.* proposed a revocable ring signature scheme, which supports that any ring member may revoke the anonymity of the real signer when the ring signature is proved to be argumentative. Their scheme provides that all the ring members can reveal the identity of the real signer of any ring signature generated on behalf of their ring. In 2007 and 2011, Fujisaki *et al.* [27, 28] proposed two traceable ring signature schemes and a security model of traceable ring signature was formally proposed. In their scheme, if two signatures are linked, the identity of this signer will be revealed. In other words, the anonymity of the signer will be revoked if and only if the signer generates two ring signatures on the same event. Compared with revocable ring signature [53], traceable ring signature needs the condition of revoking anonymity that the same signer generates two ring signatures on the same event. However, the two secure schemes [27, 28] are based on public key cryptography. With the rapid development of identity-based cryptography [11, 13, 41, 47], many researchers proposed many identity-based signature (IBS) schemes in the random oracle model or standard model [9, 16, 30, 41]. Also, with these identity-based signature schemes, a lot of variants, such as the identity-based proxy signature schemes [43, 48, 50], the identity-based ring signature schemes [5–8, 43], the identity-based group signature schemes [26, 31], *etc.* have also been proposed. In 2006, Au *et al.* [6] proposed a constant size identity-based linkable and revocable-iff-linked ring signature. However, their scheme was later proved to be insecure [32]. In 2012, Au *et al.* [5] proposed a new identity-based event-oriented linkable ring signature scheme with an option as revocable-iff-linked. With this option, if a user generates two linkable ring signatures in the same event, everyone can compute his identity from these two signatures. In the Au *et al.*'s frame, they consider the PKG system is partially trusted, which is similar to certificateless public key cryptography. However, their scheme is constructed in the random oracle model.

3 Preliminaries

3.1 Bilinear Maps

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be groups of prime order q and g be a generator of $\mathbb{G}_1$. We say $\mathbb{G}_2$ has an admissible bilinear map, $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ if the following two conditions hold. The map is bilinear; for all a, b, we have $e\left(g^a, g^b\right) = e(g,g)^{a \cdot b}$. The map is non-degenerate; we must have that $e\left(g, g\right) \neq 1$.

3.2 Computational Diffie-Hellman Assumption

Definition 1. *Computational Diffie-Hellman (CDH) Problem: Let $\mathbb{G}_1$ be a group of prime order q and g be a generator of $\mathbb{G}_1$; for all $(g, g^a, g^b) \in \mathbb{G}_1$, with $a, b \in \mathbb{Z}_q$, the CDH problem is to compute $g^{a \cdot b}$.*

Definition 2. *The $(\hbar, \varepsilon)$-CDH assumption holds if no $\hbar$-time algorithm can solve the CDH problem with probability at least ε.*

4 A Framework for TCRS

In the section, we present a formal definition of TCRS. Let $\mathbb{A}$ be universe of possible identities, we set $ID \subseteq \mathbb{A}$ as the identity of user.

Definition 3. *Traceable Certificateless Ring Signature Scheme:* Let *TCRS*=(System-Setup, Generate-Key, Sign, Verify, Trace-User) be a traceable certificateless ring signature scheme on $\mathbb{A}$, where the algorithm Generate-Key includes four sub-procedures[2]. In *TCRS*, all algorithms are described as follows:

1) *System-Setup: The randomized algorithm run by key generate center (KGC) inputs a security parameter 1^k and then outputs all system parameters $TCRK$ and a system private key spk on the security parameter 1^k.*

2) *Generate-Key: The randomized algorithm run by key generate center (or user) inputs ($TCRK$, spk, $ID_i \subseteq \mathbb{A}$) and then the following steps are finished:*

   - *Generate-Partial Key: The algorithm run by key generate center outputs a user's partial private key psk_{ID_i} to a ring member, where ID_i is the identity of the ring member with $i \in \{1, 2......n\}$ (n is the number of the ring members in a ring).*
   - *Set-Secret: The algorithm run by the ring member outputs the corresponding secret sx_{ID_i} according to ID_i.*
   - *Generate-Signing Key: The algorithm run by the ring member outputs the corresponding signing (private) key sk_{ID_i} according to psk_{ID_i} and sx_{ID_i}.*
   - *Generate-Public Key: The algorithm run by the ring member outputs and publishes the corresponding public key pk_{ID_i}.*

3) *Sign: The randomized algorithm is a standard traceable certificateless ring signature algorithm. A ring member needs to sign a message $\mathfrak{M} \in \{0,1\}^*$ on an event identifier $\mathfrak{E} \in \{0,1\}^*$. The algorithm run by the ring member with the identity ID_i inputs ($TCRK$, sk_{ID_i}, RL_ID, RL_PK, $\mathfrak{M}$, $\mathfrak{E}$) and then outputs a signature σ, where RL_ID is an identity list including all identities of the ring members belong to this ring, RL_PK is a public key list including all public keys of the ring members belong to this ring, $\sigma \in \{0,1\}^* \cup \{\perp\}$, sk_{ID_i} is the signing key of the ring member with $i \in \{1, 2......n\}$.*

4) *Verify: The signature verifiers verify a standard traceable certificateless ring signature σ. The deterministic algorithm run by a signature verifier inputs ($TCRK$, RL_ID, RL_PK, $\mathfrak{M}$, $\mathfrak{E}$, σ) and then outputs the boolean value, accept or reject.*

5) *Trace-User: The trusted authority traces a real ring member (signer) by two traceable certificateless ring signatures σ_1 on $\mathfrak{M}_1$ and σ_2 on $\mathfrak{M}_2$. The deterministic algorithm run by the trusted authority inputs ($TCRK$, RL_ID, RL_PK, $\{\mathfrak{M}_1, \sigma_1\}$, $\{\mathfrak{M}_2, \sigma_2\}$, $\mathfrak{E}$) and then outputs one of the following results: "the identity ID of the real signer", or "Independent" or "Linked", where $ID \in RL\_ID$.*

5 Traceable Certificateless Ring Signature Scheme

In the section, we show a traceable certificateless ring signature scheme in the standard model under our framework for TCRS. Let TCRS=(*System-Setup*, *Generate-Key*, *Sign*, *Verify*, *Trace-User*) be a traceable certificateless ring signature scheme. In TCRS, all algorithms are described as follows:

1) TCRS.*System-Setup*: The algorithm run by the KGC system inputs a security parameter 1^k. Additionally, let $\mathbb{G}_1$ and $\mathbb{G}_2$ be groups of prime order q and g be a generator of $\mathbb{G}_1$ and let $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ denote the bilinear map. The size of the group is determined by the security parameter and we set $\mathbb{A} \subseteq \mathbb{Z}_q$ as the universe of identities. And one hash function, $H : \{0,1\}^* \rightarrow \mathbb{Z}_{1^k \cdot q}$ can be defined and used to generate any integer value in $\mathbb{Z}_{1^k \cdot q}$ (where 1^k represents the corresponding decimal number).

   Then the system parameters are generated as follows for a ring system setup. The algorithm chooses a

[2] In certificateless public key cryptography, the algorithm *Generate-Key* is divided to four algorithms.

random $a \in \mathbb{Z}_q$ and then sets $g_1 = g^a$. Eight group elements g_2, ϑ, ψ, ϖ, μ, τ, χ and $\kappa \in \mathbb{G}_1$ are randomly chosen. Finally, the algorithm outputs the public parameters $TCRK$=($\mathbb{G}_1$, $\mathbb{G}_2$, e, g, g_1, g_2, ϑ, ψ, ϖ, μ, τ, χ, κ), where $spk = g_2^a$ is seen as a master private key.

2) TCRS.Generate-Key: The algorithm run by the KGC system generates user's signing key with respect to the identity of ring member when user joins ring. The algorithm inputs ($TCRK$, spk, $ID \subseteq \mathbb{A}$), where ID is the identity of a ring member and then the following steps are finished:

- Generate-Partial Key: The algorithm run by the KGC system randomly chooses $r_1, r_L \in \mathbb{Z}_q$, computes $x_0 = g_2^a \cdot \vartheta^{r_1 \cdot H(ID)} \cdot \psi^{r_1} \cdot \varpi^{r_L}$, $x_1 = g^{r_1}$, $sx_L = g^{r_L}$. The algorithm outputs a partial private key $psk_{\{ID\}} = \{x_0, x_1, sx_L\}$ to the ring member and publishes a new identity ring RL_ID, where sx_L is the traced ring secret for the ring member, RL_ID is an identity list including all identities of the ring members belong to this ring and $ID \in RL\_ID$.

  Remark 1. *Every ring member may verify his partial private key by the following equation:*

$$\begin{aligned} e(x_0, g) &= e(g_1, g_2) \cdot e(\vartheta, x_1^{H(ID)}) \cdot e(\psi, x_1) \\ &\quad \cdot e(\varpi, sx_L). \end{aligned}$$

- Set-Secret: The algorithm run by the corresponding ring member randomly chooses $r_2 \in \mathbb{Z}_q$, computes the member secret $sx_{\{ID\}} = \vartheta^{r_2 \cdot H(ID)} \cdot \psi^{r_2}$.
- Generate-Signing Key: The algorithm run by the corresponding ring member computes $x_2 = x_0 \cdot sx_{\{ID\}} = g_2^a \cdot \vartheta^{r_1 \cdot H(ID)} \cdot \psi^{r_1} \cdot \varpi^{r_L} \cdot \vartheta^{r_2 \cdot H(ID)} \cdot \psi^{r_2} = g_2^a \cdot \vartheta^{(r_1+r_2) \cdot H(ID)} \cdot \psi^{r_1+r_2} \cdot \varpi^{r_L}$ and then outputs the signing key $sk_{\{ID\}} = \{x_1, x_2, sx_L\}$.
- Generate-Public Key: The algorithm run by the corresponding ring member outputs and publishes the public key $pk_{\{ID\}} = g^{r_2}$, which is added to the public key ring RL_PK, where RL_PK is a public key list including all public keys of the ring members belong to this ring and $pk_{\{ID\}} \in RL\_PK$.

3) TCRS Sign: A ring member with the identity ID needs to sign a message $\mathfrak{M} \in \{0,1\}^*$ on an event identifier $\mathfrak{E} \in \{0,1\}^*$. The algorithm run by the ring member inputs ($TCRK$, $sk_{\{ID\}}$, RL_ID, RL_PK, $\mathfrak{M}$, $\mathfrak{E}$) and then randomly chooses $r_3, r_4, r_5 \in \mathbb{Z}_q$, computes

$$\begin{aligned} \sigma_0 &= x_2 \cdot \vartheta^{r_3 \cdot H(ID)} \cdot \psi^{r_3} \cdot \varpi^{r_3} \cdot \mu^{r_4 \cdot H(RL\_ID \| RL\_PK)} \cdot \\ &\quad \tau^{r_4} \cdot \chi^{r_5 \cdot H(\mathfrak{M} \| \mathfrak{E})} \cdot \kappa^{r_5} \\ &= g_2^a \cdot \vartheta^{(r_1+r_2+r_3) \cdot H(ID)} \cdot \psi^{r_1+r_2+r_3} \cdot \varpi^{r_L+r_3} \cdot \\ &\quad \mu^{r_4 \cdot H(RL\_ID \| RL\_PK)} \cdot \tau^{r_4} \cdot \chi^{r_5 \cdot H(\mathfrak{M} \| \mathfrak{E})} \cdot \kappa^{r_5}, \\ \sigma_1 &= e(\vartheta^{H(ID)} \cdot \psi, x_1 \cdot pk_{\{ID\}}) \cdot e(\vartheta^{r_3 \cdot H(ID)} \cdot \psi^{r_3}, g) \\ &= e(\vartheta^{H(ID)} \cdot \psi, g^{r_1+r_2}) \cdot e(\vartheta^{r_3 \cdot H(ID)} \cdot \psi^{r_3}, g) \\ &= e(\vartheta^{(r_1+r_2+r_3) \cdot H(ID)} \cdot \psi^{r_1+r_2+r_3}, g), \\ \sigma_2 &= sx_L \cdot g^{r_3} = g^{r_L+r_3}, \\ \sigma_3 &= g^{r_4}, \\ \sigma_4 &= g^{r_5}. \end{aligned}$$

Finally, the algorithm outputs a signature $\Phi = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4\}$.

4) TCRS.Verify: The signature verifiers verify a standard traceable certificateless ring signature Φ. The algorithm run by a signature verifier inputs ($TCRK$, RL_ID, RL_PK, $\mathfrak{M}$, $\mathfrak{E}$, Φ) and then the following computation is finished:

$$\begin{aligned} e(\sigma_0, g) &= e(g_1, g_2) \cdot \sigma_1 \\ &\quad \cdot e(\varpi, \sigma_2) \cdot e(\mu^{H(RL\_ID \| RL\_PK)} \cdot \tau, \sigma_3) \\ &\quad \cdot e(\chi^{H(\mathfrak{M} \| \mathfrak{E})} \cdot \kappa, \sigma_4). \end{aligned}$$

If the above equation is correct, then the algorithm outputs the boolean value *accept*, otherwise the algorithm outputs the boolean value *reject*.

5) TCRS.Trace-User: The trusted authority traces a ring member (signer) by two traceable certificateless ring signatures Φ_1 on $\mathfrak{M}_1$ and Φ_2 on $\mathfrak{M}_2$ when the signatures need to be arbitrated. The algorithm run by the trusted authority inputs ($TCRK$, RL_ID, RL_PK, $\{\mathfrak{M}_1, \Phi_1\}$, $\{\mathfrak{M}_2, \Phi_2\}$, $\mathfrak{E}$), where the trusted authority may get x_1 and sx_L from the KGC or the ring members[3] and then the following steps are finished:

   a. For any potential identity $ID_1 \in RL\_ID$ and the tuple $\{\mathfrak{M}_1, \Phi_1\}$, the algorithm computes the equation:

$$e(\vartheta^{H(ID_1)} \cdot \psi, x_1 \cdot pk_{\{ID\}} \cdot \tfrac{\sigma_2}{sx_L}) = \frac{e(\sigma_0, g)}{e(g_1, g_2) \cdot e(\varpi, \sigma_2) \cdot e(\mu^{H(RL\_ID \| RL\_PK)} \cdot \tau, \sigma_3) \cdot e(\chi^{H(\mathfrak{M}_1 \| \mathfrak{E})} \cdot \kappa, \sigma_4)}.$$

   If the above equation is correct, then the algorithm securely records the identity ID_1 of the real signer, otherwise if the algorithm does not find the corresponding identity, the algorithm aborts; similarly, the same computation is finished for any potential identity $ID_2 \in RL\_ID$ and the tuple $\{\mathfrak{M}_2, \Phi_2\}$ and then the algorithm securely records the identity ID_2 of the real signer, otherwise the algorithm aborts.

   b. The algorithm outputs the following results according to the comparisons:

   - *Result*="*Independent*", if $ID_1 \neq ID_2$;
   - *Result*="*Linked*", else if $\mathfrak{M}_1 = \mathfrak{M}_2$;
   - *Result*="ID_1", otherwise.

[3] This setting does not break the security of the whole scheme according to the Paterson *et al.*'s signature scheme [41].

6 Analysis of the Proposed Scheme

6.1 Correctness

In the proposed scheme, the traceable certificateless ring signature is $\Phi = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4\}$, where

$$\begin{aligned}
\sigma_0 &= x_2 \cdot \vartheta^{r_3 \cdot H(ID)} \cdot \psi^{r_3} \cdot \varpi^{r_3} \cdot \mu^{r_4 \cdot H(RL\_ID \| RL\_PK)} \\
&\quad \cdot \tau^{r_4} \cdot \chi^{r_5 \cdot H(\mathfrak{M} \| \mathfrak{E})} \cdot \kappa^{r_5} \\
&= g_2^a \cdot \vartheta^{(r_1+r_2+r_3) \cdot H(ID)} \cdot \psi^{r_1+r_2+r_3} \cdot \varpi^{r_L+r_3} \\
&\quad \cdot \mu^{r_4 \cdot H(RL\_ID \| RL\_PK)} \cdot \tau^{r_4} \cdot \chi^{r_5 \cdot H(\mathfrak{M} \| \mathfrak{E})} \cdot \kappa^{r_5}, \\
\sigma_1 &= e(\vartheta^{H(ID)} \cdot \psi, x_1 \cdot pk_{\{ID\}}) \cdot e(\vartheta^{r_3 \cdot H(ID)} \cdot \psi^{r_3}, g) \\
&= e(\vartheta^{H(ID)} \cdot \psi, g^{r_1+r_2}) \cdot e(\vartheta^{r_3 \cdot H(ID)} \cdot \psi^{r_3}, g) \\
&= e(\vartheta^{(r_1+r_2+r_3) \cdot H(ID)} \cdot \psi^{r_1+r_2+r_3}, g), \\
\sigma_2 &= sx_L \cdot g^{r_3} = g^{r_L+r_3}, \\
\sigma_3 &= g^{r_4}, \\
\sigma_4 &= g^{r_5}.
\end{aligned}$$

So, we have that

$$\begin{aligned}
e(\sigma_0, g) &= e(g_2^a \cdot \vartheta^{(r_1+r_2+r_3) \cdot H(ID)} \cdot \psi^{r_1+r_2+r_3} \\
&\quad \cdot \varpi^{r_L+r_3} \cdot \mu^{r_4 \cdot H(RL\_ID \| RL\_PK)} \cdot \tau^{r_4} \\
&\quad \cdot \chi^{r_5 \cdot H(\mathfrak{M} \| \mathfrak{E})} \cdot \kappa^{r_5}, g) \\
&= e(g_2^a, g) \cdot e(\vartheta^{(r_1+r_2+r_3) \cdot H(ID)} \cdot \psi^{r_1+r_2+r_3}, g) \\
&\quad \cdot e(\varpi^{r_L+r_3}, g) \cdot e(\mu^{r_4 \cdot H(RL\_ID \| RL\_PK)} \cdot \tau^{r_4}, g) \\
&\quad \cdot e(\chi^{r_5 \cdot H(\mathfrak{M} \| \mathfrak{E})} \cdot \kappa^{r_5}, g) \\
&= e(g_1, g_2) \cdot \sigma_1 \cdot e(\varpi, \sigma_2) \cdot e(\mu^{H(RL\_ID \| RL\_PK)} \\
&\quad \cdot \tau, \sigma_3) \cdot e(\chi^{H(\mathfrak{M} \| \mathfrak{E})} \cdot \kappa, \sigma_4).
\end{aligned}$$

6.2 Efficiency

In the proposed scheme, $\Phi = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4\}$, where

$$\begin{aligned}
\sigma_0 &= x_2 \cdot \vartheta^{r_3 \cdot H(ID)} \cdot \psi^{r_3} \cdot \varpi^{r_3} \cdot \mu^{r_4 \cdot H(RL\_ID \| RL\_PK)} \\
&\quad \cdot \tau^{r_4} \cdot \chi^{r_5 \cdot H(\mathfrak{M} \| \mathfrak{E})} \cdot \kappa^{r_5}, \\
\sigma_1 &= e(\vartheta^{H(ID)} \cdot \psi, x_1 \cdot pk_{\{ID\}}) \cdot e(\vartheta^{r_3 \cdot H(ID)} \cdot \psi^{r_3}, g), \\
\sigma_2 &= sx_L \cdot g^{r_3}, \quad \sigma_3 = g^{r_4}, \quad \sigma_4 = g^{r_5}.
\end{aligned}$$

Thus, the length of signature is $4 \cdot |\mathbb{G}_1| + |\mathbb{G}_2|$, where $|\mathbb{G}_1|$ is the size of element in $\mathbb{G}_1$ and $|\mathbb{G}_2|$ is the size of element in $\mathbb{G}_2$. Additionally, because $x_2 \cdot \vartheta^{r_3 \cdot H(ID)} \cdot \psi^{r_3} \cdot \varpi^{r_3} \cdot \mu^{r_4 \cdot H(RL\_ID \| RL\_PK)} \cdot \tau^{r_4} \cdot \kappa^{r_5}$, χ^{r_5} in $\chi^{r_5 \cdot H(\mathfrak{M} \| \mathfrak{E})}$, σ_1, σ_2, σ_3 and σ_4 may be precomputed and we assume that the time for integer multiplication and hash computation can be ignored, signing a message for a traceable certificateless ring signature only needs to compute at most 1 exponentiation in $\mathbb{G}_1$ and 1 multiplication in $\mathbb{G}_1$. Also, in the following equation

$$\begin{aligned}
e(\sigma_0, g) = e(g_1, g_2) \cdot \sigma_1 \cdot e(\varpi, \sigma_2) \cdot e(\mu^{H(RL\_ID \| RL\_PK)} \cdot \\
\tau, \sigma_3) \cdot e(\chi^{H(\mathfrak{M} \| \mathfrak{E})} \cdot \kappa, \sigma_4),
\end{aligned}$$

because the value $e(g_1, g_2)$ can be precomputed and cached, verification requires 4 pairing computations, 2 exponentiations in $\mathbb{G}_1$, 2 multiplications in $\mathbb{G}_1$ and 4 multiplications in $\mathbb{G}_2$.

In this paper, we compare the proposed scheme (the scheme of Section 5) with other traceable (or linkable) ring signature schemes proposed by [5, 27, 28, 36, 52]. Table 1 shows the comparisons of the traceable or linkable ring signature schemes. Compared with other schemes, our scheme is certificateless and constructed in the standard model and has constant signature size in the comparison of the performance.

6.3 Security

In the section, we show the proposed scheme (the scheme of Section 5) has a security reduction to the CDH assumption and the TCRS unforgeability (against *linkability attacks* and *exculpability attacks*) under the adaptive chosen message and identity attacks and has the TCRS anonymity. Our proofs of the following theorems are based on the security models of [5, 27][4].

Theorem 1. *The scheme of Section 5 is ($\hbar$, ε, q_g, q_s)-unforgeable, assuming that the ($\hbar'$, ε')-CDH assumption holds in $\mathbb{G}_1$, where*

$$\varepsilon' = [(1 - \tfrac{q_g}{q}) \cdot (1 - \tfrac{q_s}{q})^2 \cdot \tfrac{\varepsilon}{q^2}] \parallel [(1 - \tfrac{q_g}{q}) \cdot (1 - \tfrac{q_s}{q})^2 \cdot \varepsilon],$$

$\hbar' = \max\{\hbar + O(q_g \cdot (10 \cdot C_{exp} + 3 \cdot C_{mul}) + q_s \cdot (15 \cdot C_{exp} + 11 \cdot C_{mul})), \hbar + O(q_g \cdot (3 \cdot C_{exp} + C_{mul}) + q_s \cdot (12 \cdot C_{exp} + 7 \cdot C_{mul}))\}$,
and q_g is the maximal number of "Generate-Key" oracle queries, q_s is the maximal number of "Sign" oracle queries, C_{mul} and C_{exp} are respectively the time for a multiplication and an exponentiation in $\mathbb{G}_1$.

Proof. The procedure of the whole proof is divided to two following parts for two types of attack. □

Type I:

Let **TCRS** be a traceable certificateless ring signature scheme of Section 5. Additionally, let $\mathcal{A}$ be an ($\hbar$, ε, q_g, q_s)-adversary attacking **TCRS**. From the adversary $\mathcal{A}$, we construct an algorithm $\mathcal{B}$, for (g, g^a, g^b)$\in \mathbb{G}_1$, the algorithm $\mathcal{B}$ is able to use $\mathcal{A}$ to compute $g^{a \cdot b}$. Thus, we assume the algorithm $\mathcal{B}$ can solve the CDH with probability at least ε' and in time at most $\hbar'$, contradicting the ($\hbar'$, ε')-CDH assumption. Such a simulation may be created in the following way.

Setup: The KGC system inputs a security parameter 1^k. Additionally, let $\mathbb{G}_1$ and $\mathbb{G}_2$ be groups of prime order q and g be a generator of $\mathbb{G}_1$ and let $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ denote the bilinear map. The size of the group is determined by the security parameter and we set $\mathbb{A} \subseteq \mathbb{Z}_q$ as the universe of identities. One hash function, $H : \{0,1\}^* \to \mathbb{Z}_{1^k \cdot q}$ can be defined and used to generate any integer value in $\mathbb{Z}_{1^k \cdot q}$ (where 1^k represents the corresponding decimal number).

Then the system parameters are generated as follows. The algorithm sets $g_1 = g^a$ and $g_2 = g^b$ with $a, b \in$

[4] As the proofs of Theorem 2, Theorem 3 and Theorem 4 are similar to the proof of Theorem 1, we omit the similar proofs in this paper.

Table 1: Comparisons of the six schemes

	Signature Size	Cryptography	Traceability	Linking Cost	Model
Scheme [36]	$O(n)$	Public Key	No	$O(1)$	random oracle model
Scheme [52]	$O(n)$	Public Key	No	$O(1)$	random oracle model
Scheme [28]	$O(\sqrt{n})$	Public Key	Yes	$O(n \cdot \log n)$	standard model
Scheme [27]	$O(n)$	Public Key	Yes	$O(n)$	random oracle model
Scheme [5]	$O(1)$	Identity-Based	Yes	$O(1)$	random oracle model
Our Scheme	$O(1)$	Certificateless	Yes	$O(n)$	standard model

$\mathbb{Z}_q$ ($\mathcal{B}$ doesn't know a and b). Also, the algorithm chooses ℓ, ∂, ν, λ, η, α and $\pi \in \mathbb{Z}_q$ and then sets $\vartheta = g_2^{\ell} \cdot g$, $\psi = g^{\partial}$, $\mu = g^{\nu}$, $\tau = g^{\lambda}$, $\chi = g_2^{\alpha} \cdot g$, $\kappa = g^{\pi}$ and $\varpi = g^{\eta}$. Finally, the system outputs the public parameters $TCRK$=($\mathbb{G}_1$, $\mathbb{G}_2$, e, g, g_1, g_2, ϑ, ψ, μ, τ, χ, κ, ϖ).

Queries: When running the adversary $\mathcal{A}$, the relevant queries can occur. The algorithm $\mathcal{B}$ answers these in the following way:

- Generate-Key Queries:
  Given the public parameters $TCRK$ and the identity ID of the ring member ($ID \in RL\_ID$ where RL_ID is an identity list), the algorithm $\mathcal{B}$ can construct a private key of the ring member u by the following computation (ID is the identity of u):

  - Generate-Partial Key:
    The algorithm chooses random $r_1, r_L \in \mathbb{Z}_q$ and computes $x_0 = g_1^{-\frac{1}{\ell}} \cdot \vartheta^{r_1} \cdot g_1^{-\frac{\partial}{\ell} \cdot \frac{1}{H(ID)}} \cdot \psi^{\frac{r_1}{H(ID)}} \cdot \varpi^{r_L}$, $x_1 = (g_1^{-\frac{1}{\ell}} \cdot g^{r_1})^{\frac{1}{H(ID)}}$, $sx_L = g^{r_L}$ and then generates a partial private key $psk_{\{ID\}} = \{x_0, x_1, sx_L\}$.

    Remark 2. *To the correctness of* $psk_{\{ID\}}$, $psk_{\{ID\}}$ *may be changed as follows:*

    $$\begin{aligned} x_0 &= g_1^{-\frac{1}{\ell}} \cdot \vartheta^{r_1} \cdot g_1^{-\frac{\partial}{\ell} \cdot \frac{1}{H(ID)}} \cdot \psi^{\frac{r_1}{H(ID)}} \\ &\quad \cdot \varpi^{r_L} \\ &= g_2^a \cdot g_2^{-a} \cdot g_1^{-\frac{1}{\ell}} \cdot \vartheta^{r_1} \cdot g_1^{-\frac{\partial}{\ell} \cdot \frac{1}{H(ID)}} \\ &\quad \cdot \psi^{\frac{r_1}{H(ID)}} \cdot \varpi^{r_L} \\ &= g_2^a \cdot (g_2^{\ell} \cdot g)^{-\frac{a}{\ell}} \cdot \vartheta^{r_1} \cdot g^{a \cdot (-\frac{\partial}{\ell}) \cdot \frac{1}{H(ID)}} \\ &\quad \cdot \psi^{\frac{r_1}{H(ID)}} \cdot \varpi^{r_L} \\ &= g_2^a \cdot \vartheta^{-\frac{a}{\ell}} \cdot \vartheta^{r_1} \cdot \psi^{-\frac{a}{\ell} \cdot \frac{1}{H(ID)}} \cdot \psi^{\frac{r_1}{H(ID)}} \\ &\quad \cdot \varpi^{r_L} \\ &= g_2^a \cdot \vartheta^{r_1 - \frac{a}{\ell}} \cdot \psi^{\frac{r_1}{H(ID)} - \frac{a}{\ell} \cdot \frac{1}{H(ID)}} \cdot \varpi^{r_L} \\ &= g_2^a \cdot \vartheta^{r_1 - \frac{a}{\ell}} \cdot \psi^{(r_1 - \frac{a}{\ell}) \cdot \frac{1}{H(ID)}} \cdot \varpi^{r_L}, \\ x_1 &= (g_1^{-\frac{1}{\ell}} \cdot g^{r_1})^{\frac{1}{H(ID)}} \\ &= (g^{-\frac{a}{\ell}} \cdot g^{r_1})^{\frac{1}{H(ID)}} \\ &= g^{(r_1 - \frac{a}{\ell}) \cdot \frac{1}{H(ID)}}. \end{aligned}$$

    Setting $r'_1 = (r_1 - \frac{a}{\ell}) \cdot \frac{1}{H(ID)}$, $psk_{\{ID\}} = \{x_0, x_1, sx_L\} = \{g_2^a \cdot \vartheta^{r'_1 \cdot H(ID)} \cdot \psi^{r'_1} \cdot \varpi^{r_L}, g^{r'_1}, g^{r_L}\}$ is a valid partial private key, where we assure that $\ell \cdot H(ID) \neq 0$ **mod** q.

  - Set-Secret:
    The algorithm randomly chooses $r_0 \in \mathbb{Z}_q$, computes the member secret $sx_{\{ID\}} = \vartheta^{r_0 \cdot H(ID)} \cdot \psi^{r_0}$.

  - Generate-Signing Key:
    The algorithm computes $x_2 = x_0 \cdot sx_{\{ID\}}$ and then outputs the signing key $sk_{\{ID\}} = \{x_1, x_2, sx_L\}$ to $\mathcal{A}$.

  - Generate-Public Key:
    The algorithm outputs the public key $pk_{\{ID\}} = g^{r_0}$, which is added to the public key ring RL_PK, where RL_PK is a public key list including all public keys of the ring members belong to this ring.

- Sign Queries:
  Given the public parameters $TCRK$, the identity list RL_ID ($ID \in RL\_ID$ where ID is the identity of the ring member that belongs to this ring), the public key list RL_PK, the message $\mathfrak{M}$ and the event identifier $\mathfrak{E}$, the algorithm $\mathcal{B}$ chooses random $r_2, r_3, r_4, r_5 \in \mathbb{Z}_q$ and computes

  $$\begin{aligned} \sigma_0 &= g_1^{-\frac{1}{2 \cdot \ell}} \cdot \vartheta^{r_2} \cdot g_1^{-\frac{\partial}{2 \cdot \ell} \cdot \frac{1}{H(ID)}} \cdot \psi^{\frac{r_2}{H(ID)}} \cdot \varpi^{r_3} \cdot \\ &\quad \mu^{r_4 \cdot H(RL\_ID \| RL\_PK)} \cdot \tau^{r_4} \cdot g_1^{-\frac{1}{2 \cdot \alpha}} \cdot \chi^{r_5} \cdot \\ &\quad g_1^{-\frac{\pi}{2 \cdot \alpha} \cdot \frac{1}{H(\mathfrak{M} \| \mathfrak{E})}} \cdot \kappa^{\frac{r_5}{H(\mathfrak{M} \| \mathfrak{E})}}, \\ \sigma'_1 &= (g_1^{-\frac{1}{2 \cdot \ell}} \cdot g^{r_2})^{\frac{1}{H(ID)}}, \\ \sigma_2 &= g^{r_3}, \\ \sigma_3 &= g^{r_4}, \\ \sigma_4 &= (g_1^{-\frac{1}{2 \cdot \alpha}} \cdot g^{r_5})^{\frac{1}{H(\mathfrak{M} \| \mathfrak{E})}}. \end{aligned}$$

  Finally, the algorithm outputs a forgery $\Phi = \{\sigma_0, \sigma'_1, \sigma_2, \sigma_3, \sigma_4\}$ to the adversary $\mathcal{A}$. Where we maximize the adversary's advantage, σ'_1 is passed to $\mathcal{A}$.

Remark 3. *To the correctness of* Φ, Φ *may be* *changed as follows:*

$$\begin{aligned}
\sigma_0 &= g_1^{-\frac{1}{2\cdot\ell}} \cdot \vartheta^{r_2} \cdot g_1^{-\frac{\partial}{2\cdot\ell}\cdot\frac{1}{H(ID)}} \cdot \\
&\quad \psi^{\frac{r_2}{H(ID)}} \cdot \varpi^{r_3} \cdot \mu^{r_4\cdot H(RL\_ID\|RL\_PK)} \cdot \\
&\quad \tau^{r_4} \cdot g_1^{-\frac{1}{2\cdot\alpha}} \cdot \chi^{r_5} \cdot \\
&\quad g_1^{-\frac{\pi}{2\cdot\alpha}\cdot\frac{1}{H(\mathfrak{M}\|\mathfrak{E})}} \cdot \kappa^{\frac{r_5}{H(\mathfrak{M}\|\mathfrak{E})}} \\
&= g_2^a \cdot g_2^{-\frac{a}{2}} \cdot g_2^{-\frac{a}{2}} \cdot g_1^{-\frac{1}{2\cdot\ell}} \cdot \vartheta^{r_2} \cdot g_1^{-\frac{\partial}{2\cdot\ell}\cdot\frac{1}{H(ID)}} \cdot \\
&\quad \psi^{\frac{r_2}{H(ID)}} \cdot \varpi^{r_3} \cdot \mu^{r_4\cdot H(RL\_ID\|RL\_PK)} \\
&\quad \cdot\tau^{r_4} \cdot g_1^{-\frac{1}{2\cdot\alpha}} \cdot \chi^{r_5} \cdot g_1^{-\frac{\pi}{2\cdot\alpha}\cdot\frac{1}{H(\mathfrak{M}\|\mathfrak{E})}} \cdot \kappa^{\frac{r_5}{H(\mathfrak{M}\|\mathfrak{E})}} \\
&\quad g_2^a \cdot g_2^{-\frac{a}{2}} \cdot g_1^{-\frac{1}{2\cdot\ell}} \cdot \vartheta^{r_2} \cdot g_1^{-\frac{\partial}{2\cdot\ell}\cdot\frac{1}{H(ID)}} \cdot \\
&\quad \psi^{\frac{r_2}{H(ID)}} \cdot \varpi^{r_3} \cdot \mu^{r_4\cdot H(RL\_ID\|RL\_PK)} \cdot \tau^{r_4} \cdot \\
&\quad g_2^{-\frac{a}{2}} \cdot g_1^{-\frac{1}{2\cdot\alpha}} \cdot \chi^{r_5} \cdot g_1^{-\frac{\pi}{2\cdot\alpha}\cdot\frac{1}{H(\mathfrak{M}\|\mathfrak{E})}} \cdot \\
&\quad \kappa^{\frac{r_5}{H(\mathfrak{M}\|\mathfrak{E})}} g_2^a \cdot (g_2^\ell \cdot g)^{-\frac{a}{2\cdot\ell}} \cdot \vartheta^{r_2} \cdot g^{-\frac{a\cdot\partial}{2\cdot\ell}\cdot\frac{1}{H(ID)}} \cdot \\
&\quad \psi^{\frac{r_2}{H(ID)}} \cdot \varpi^{r_3} \cdot \mu^{r_4\cdot H(RL\_ID\|RL\_PK)} \cdot \tau^{r_4} \cdot \\
&\quad (g_2^\alpha \cdot g)^{-\frac{a}{2\cdot\alpha}} \cdot \chi^{r_5} \cdot g^{-\frac{a\cdot\pi}{2\cdot\alpha}\cdot\frac{1}{H(\mathfrak{M}\|\mathfrak{E})}} \cdot \kappa^{\frac{r_5}{H(\mathfrak{M}\|\mathfrak{E})}} \\
&\quad g_2^a \cdot \vartheta^{-\frac{a}{2\cdot\ell}} \cdot \vartheta^{r_2} \cdot \psi^{-\frac{a}{2\cdot\ell}\cdot\frac{1}{H(ID)}} \cdot \\
&\quad \psi^{\frac{r_2}{H(ID)}} \cdot \varpi^{r_3} \cdot \mu^{r_4\cdot H(RL\_ID\|RL\_PK)} \cdot \tau^{r_4} \cdot \\
&\quad \chi^{-\frac{a}{2\cdot\alpha}} \cdot \chi^{r_5} \cdot \kappa^{-\frac{a}{2\cdot\alpha}\cdot\frac{1}{H(\mathfrak{M}\|\mathfrak{E})}} \cdot \kappa^{\frac{r_5}{H(\mathfrak{M}\|\mathfrak{E})}} \\
&\quad g_2^a \cdot \vartheta^{r_2-\frac{a}{2\cdot\ell}} \cdot \psi^{(r_2-\frac{a}{2\cdot\ell})\cdot\frac{1}{H(ID)}} \cdot \varpi^{r_3} \cdot \\
&\quad \mu^{r_4\cdot H(RL\_ID\|RL\_PK)} \cdot \tau^{r_4} \cdot \chi^{r_5-\frac{a}{2\cdot\alpha}} \cdot \\
&\quad \kappa^{(r_5-\frac{a}{2\cdot\alpha})\cdot\frac{1}{H(\mathfrak{M}\|\mathfrak{E})}}, \\
\sigma_1' &= (g_1^{-\frac{1}{2\cdot\ell}} \cdot g^{r_2})^{\frac{1}{H(ID)}} = g^{(r_2-\frac{a}{2\cdot\ell})\cdot\frac{1}{H(ID)}}, \\
\sigma_4 &= (g_1^{-\frac{1}{2\cdot\alpha}} \cdot g^{r_5})^{\frac{1}{H(\mathfrak{M}\|\mathfrak{E})}} = g^{(r_5-\frac{a}{2\cdot\alpha})\cdot\frac{1}{H(\mathfrak{M}\|\mathfrak{E})}}.
\end{aligned}$$

Setting $r_2' = (r_2 - \frac{a}{2\cdot\ell}) \cdot \frac{1}{H(ID)}$ and $r_5' = (r_5 - \frac{a}{2\cdot\alpha}) \cdot \frac{1}{H(\mathfrak{M}\|\mathfrak{E})}$, $\mathcal{A}$ may get that

$$\begin{aligned}
\sigma_0 &= g_2^a \cdot \vartheta^{r_2'\cdot H(ID)} \cdot \psi^{r_2'} \cdot \varpi^{r_3} \\
&\quad \cdot\mu^{r_4\cdot H(RL\_ID\|RL\_PK)} \cdot \tau^{r_4} \\
&\quad \cdot\chi^{r_5'\cdot H(\mathfrak{M}\|\mathfrak{E})} \cdot \kappa^{r_5'}, \\
\sigma_1 &= e(\vartheta^{H(ID)} \cdot \psi, \sigma_1') = e(\vartheta^{H(ID)} \cdot \psi, g^{r_2'}), \\
\sigma_2 &= g^{r_3}, \\
\sigma_3 &= g^{r_4}, \\
\sigma_4 &= g^{r_5'}.
\end{aligned}$$

Thus, $\Phi' = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ is a valid signature, where we assure that $\ell \cdot H(ID) \neq 0$ **mod** q and $\alpha \cdot H(\mathfrak{M} \parallel \mathfrak{E}) \neq 0$ **mod** q.

Forgery: If the algorithm $\mathcal{B}$ does not abort as a consequence of one of the queries above, the adversary $\mathcal{A}$ will, with probability at least ε, return a message $\mathfrak{M}^*$, an event identifier $\mathfrak{E}^*$ and a valid forgery, $\Phi^* = \{\sigma_0^*, \sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*\}$ for RL_ID^* and RL_PK^*, where RL_ID^* is an identity list including all identities of the ring members belong to this ring and RL_PK^* is a public key list including all public keys of the ring members belong to this ring, where

$$\begin{aligned}
\sigma_0^* &= g_2^a \cdot \vartheta^{r_2^*\cdot H(ID^*)} \cdot \psi^{r_2^*} \cdot \varpi^{r_3^*} \\
&\quad \cdot\mu^{r_4^*\cdot H(RL\_ID^*\|RL\_PK^*)} \cdot \tau^{r_4^*} \\
&\quad \cdot\chi^{r_5^*\cdot H(\mathfrak{M}^*\|\mathfrak{E}^*)} \cdot \kappa^{r_5^*}, \\
\sigma_1^* &= g^{r_2^*}, \\
\sigma_2^* &= g^{r_3^*}, \\
\sigma_3^* &= g^{r_4^*}, \\
\sigma_4^* &= g^{r_5^*}.
\end{aligned}$$

And $\mathcal{A}$ did not query ***Generate-Key*** on input $ID^* \in RL\_ID^*$ and did not query ***Sign*** on inputs RL_ID^*, RL_PK^*, $\mathfrak{M}^*$ and $\mathfrak{E}^*$.

If $\ell \cdot H(ID^*) \neq 0$ **mod** q or $\alpha \cdot H(\mathfrak{M}^* \parallel \mathfrak{E}^*) \neq 0$ **mod** q, then the algorithm $\mathcal{B}$ will abort.

If $\ell \cdot H(ID^*) = 0$ **mod** q and $\alpha \cdot H(\mathfrak{M}^* \parallel \mathfrak{E}^*) = 0$ **mod** q, then the algorithm $\mathcal{B}$ computes and outputs $\frac{\sigma_0^*}{Q} = g^{a\cdot b}$, which is the solution to the given CDH problem, where $Q = g^{r_2^*\cdot H(ID^*)} \cdot g^{r_2^*\cdot\partial} \cdot g^{r_3^*\cdot\eta} \cdot g^{r_4^*\cdot\nu\cdot H(RL\_ID^*\|RL\_PK^*)} \cdot g^{r_4^*\cdot\lambda} \cdot g^{r_5^*\cdot H(\mathfrak{M}^*\|\mathfrak{E}^*)} \cdot g^{r_5^*\cdot\pi}$.

Now, we analyze the probability of the algorithm $\mathcal{B}$ not aborting. For the simulation to complete without aborting, we require that all ***Generate-Key*** queries will have $\ell \cdot H(ID) \neq 0$ **mod** q, all ***Sign*** queries will have $\ell \cdot H(ID) \neq 0$ **mod** q and $\alpha \cdot H(\mathfrak{M} \parallel \mathfrak{E}) \neq 0$ **mod** q and that $\ell \cdot H(ID^*) = 0$ **mod** q and $\alpha \cdot H(\mathfrak{M}^* \parallel \mathfrak{E}^*) = 0$ **mod** q in forgery. If the algorithm $\mathcal{B}$ does not abort, then the following conditions must hold:

1) $\ell \cdot H(ID_i) \neq 0$ **mod** q in ***Generate-Key*** queries, with i=$1, 2......q_g$;

2) $\ell \cdot H(ID_i) \neq 0$ **mod** q and $\alpha \cdot H(\mathfrak{M}_i \parallel \mathfrak{E}_i) \neq 0$ **mod** q in ***Sign*** queries, with i=$1, 2......q_s$;

3) The algorithm $\mathcal{B}$ does not abort in forgery, namely $\ell \cdot H(ID^*) = 0$ **mod** q and $\alpha \cdot H(\mathfrak{M}^* \parallel \mathfrak{E}^*) = 0$ **mod** q.

To make the analysis simpler, we will define the events E_i, F_i, T_i, R^*, F^* as

E_i :$\ell \cdot H(ID_i) \neq 0$ **mod** q, with i=$1, 2......q_g$;
F_i :$\ell \cdot H(ID_i) \neq 0$ **mod** q, with i=$1, 2......q_s$;
T_i :$\alpha \cdot H(\mathfrak{M}_i \parallel \mathfrak{E}_i) \neq 0$ **mod** q, with i=$1, 2......q_s$;
R^* :$\ell \cdot H(ID^*) = 0$ **mod** q;
F^* :$\alpha \cdot H(\mathfrak{M}^* \parallel \mathfrak{E}^*) = 0$ **mod** q.

Then the probability of $\mathcal{B}$ not aborting is

$$\Pr(not\_abort) = \Pr\left(\bigcap_{i=1}^{q_g} E_i \wedge \bigcap_{i=1}^{q_s} (F_i \wedge T_i) \wedge R^* \wedge F^*\right).$$

It is easy to see that the events $\bigcap_{i=1}^{q_g} E_i$, $\bigcap_{i=1}^{q_s} F_i$, $\bigcap_{i=1}^{q_s} T_i$, R^* and F^* are independent. Then we may compute

$$\begin{aligned}
\Pr(\bigcap_{i=1}^{q_g} E_i) &= 1 - \Pr(\bigcup_{i=1}^{q_g} \neg E_i) = 1 - q_g \cdot \frac{1^k}{1^k \cdot q} \\
&= 1 - \frac{q_g}{q}; \\
\Pr(\bigcap_{i=1}^{q_s} F_i) &= 1 - \Pr(\bigcup_{i=1}^{q_s} \neg F_i) = 1 - q_s \cdot \frac{1^k}{1^k \cdot q} \\
&= 1 - \frac{q_s}{q}; \\
\Pr(\bigcap_{i=1}^{q_s} T_i) &= 1 - \Pr(\bigcup_{i=1}^{q_s} \neg T_i) = 1 - q_s \cdot \frac{1^k}{1^k \cdot q} \\
&= 1 - \frac{q_s}{q}; \\
\Pr(R^*) &= \frac{1^k}{1^k \cdot q} = \frac{1}{q}; \quad \Pr(F^*) = \frac{1^k}{1^k \cdot q} = \frac{1}{q}.
\end{aligned}$$

Thus,

$$\Pr(not\_abort) = \Pr\left(\bigcap_{i=1}^{q_g} E_i \wedge \bigcap_{i=1}^{q_s} (F_i \wedge T_i) \wedge R^* \wedge F^*\right)$$

$$= \Pr(\bigcap_{i=1}^{q_g} E_i) \cdot \Pr(\bigcap_{i=1}^{q_s} F_i) \cdot \Pr(\bigcap_{i=1}^{q_s} T_i) \cdot \Pr(R^*) \cdot \Pr(F^*)$$

$$= \left(1 - \frac{q_g}{q}\right) \cdot \left(1 - \frac{q_s}{q}\right)^2 \cdot \frac{1}{q^2}.$$

We can get that $\varepsilon' = (1 - \frac{q_g}{q}) \cdot (1 - \frac{q_s}{q})^2 \cdot \frac{\varepsilon}{q^2}$.

If the simulation does not abort, the adversary $\mathcal{A}$ will create a valid forgery with probability at least ε. The algorithm $\mathcal{B}$ can then compute $g^{a \cdot b}$ from the forgery as shown above. The time complexity of the algorithm $\mathcal{B}$ is dominated by the time for the exponentiations and multiplications in the queries. We assume that the time for integer addition and integer multiplication and the time for hash computation can both be ignored, then the time complexity of the algorithm $\mathcal{B}$ is

$$\hbar' = \hbar + O(q_g \cdot (10 \cdot C_{exp} + 3 \cdot C_{mul}) + q_s \cdot (15 \cdot C_{exp} + 11 \cdot C_{mul})).$$

Type II:

Let **TCRS** be a traceable certificateless ring signature scheme of Section 5. Additionally, let $\mathcal{A}$ be an ($\hbar$, ε, q_g, q_s)-adversary attacking **TCRS**. From the adversary $\mathcal{A}$, we construct an algorithm $\mathcal{B}$, for (g, g^a, g^b)$\in \mathbb{G}_1$, the algorithm $\mathcal{B}$ is able to use $\mathcal{A}$ to compute $g^{a \cdot b}$. Thus, we assume the algorithm $\mathcal{B}$ can solve the CDH with probability at least ε' and in time at most $\hbar'$, contradicting the ($\hbar'$, ε')-CDH assumption. Such a simulation may be created in the following way:

Setup: The KGC system inputs a security parameter 1^k. Additionally, let $\mathbb{G}_1$ and $\mathbb{G}_2$ be groups of prime order q and g be a generator of $\mathbb{G}_1$ and let e : $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ denote the bilinear map. The size of the group is determined by the security parameter and we set $\mathbb{A} \subseteq \mathbb{Z}_q$ as the universe of identities. One hash function, $H : \{0,1\}^* \rightarrow \mathbb{Z}_{1^k \cdot q}$ can be defined and used to generate any integer value in $\mathbb{Z}_{1^k \cdot q}$ (where 1^k represents the corresponding decimal number).

Then the system parameters are generated as follows. The algorithm chooses $y \in \mathbb{Z}_q$ and then sets $g_1 = g^y$ and $g_2 = g^b$ with $b \in \mathbb{Z}_q$ ($\mathcal{B}$ doesn't know b). Also, the algorithm chooses ℓ, ∂, ν, λ, η, α and $\pi \in \mathbb{Z}_q$ and then sets $\vartheta = g_2^{\ell} \cdot g$, $\psi = g^{\partial}$, $\mu = g^{\nu}$, $\tau = g^{\lambda}$, $\chi = g_2^{\alpha} \cdot g$, $\kappa = g^{\pi}$ and $\varpi = g^{\eta}$. Finally, the system outputs the public parameters $TCRK$=($\mathbb{G}_1$, $\mathbb{G}_2$, e, g, g_1, g_2, ϑ, ψ, μ, τ, χ, κ, ϖ) and the master private key $spk = g_2^y$ to $\mathcal{A}$.

Additionally, the user u^* is a challenger, whose identity and public key respectively are ID^* and $pk_{\{ID^*\}}$, we set that the member secret of the user u^*, $sx_{\{ID^*\}} = \vartheta^{a \cdot H(ID^*)} \cdot \psi^a$ and that the public key of u^*, $pk_{\{ID^*\}} = g^a$ ($\mathcal{B}$ doesn't know a).

Queries: When running the adversary $\mathcal{A}$, the relevant queries can occur. The algorithm $\mathcal{B}$ answers these in the following way:

- Generate-Key Queries: Given the public parameters $TCRK$ and the identity ID of the ring member ($ID \in RL\_ID$ where RL_ID is an identity list), the algorithm $\mathcal{B}$ can construct a private key of the ring member u by the following computation (ID is the identity of u):
  - Set-Secret: The algorithm randomly chooses $r_0 \in \mathbb{Z}_q$, computes the member secret $sx_{\{ID\}} = \vartheta^{r_0 \cdot H(ID)} \cdot \psi^{r_0}$, where we assure that $H(ID) \neq 0$ **mod** q.
  - Generate-Public Key: The algorithm outputs the public key $pk_{\{ID\}} = g^{r_0}$, which is added to the public key ring RL_PK, where RL_PK is a public key list including all public keys of the ring members belong to this ring.

- Sign Queries: Given the public parameters $TCRK$, the identity list RL_ID ($ID \in RL\_ID$ where ID is the identity of the ring member that belongs to this ring), the public key list RL_PK, the message $\mathfrak{M}$ and the event identifier $\mathfrak{E}$, the algorithm $\mathcal{B}$ chooses random $r_2, r_3, r_4, r_5 \in \mathbb{Z}_q$ and computes

$$\begin{aligned}
\sigma_0 &= g_2^y \cdot \vartheta^{r_2 \cdot H(ID)} \cdot \psi^{r_2} \cdot \varpi^{r_3} \\
&\quad \cdot \mu^{r_4 \cdot H(RL\_ID \| RL\_PK)} \cdot \tau^{r_4} \\
&\quad \cdot \chi^{r_5 \cdot H(\mathfrak{M} \| \mathfrak{E})} \cdot \kappa^{r_5}, \\
\sigma_1' &= g^{r_2}, \\
\sigma_2 &= g^{r_3}, \\
\sigma_3 &= g^{r_4}, \\
\sigma_4 &= g^{r_5}.
\end{aligned}$$

Finally, the algorithm outputs a forgery $\Phi = \{\sigma_0, \sigma_1', \sigma_2, \sigma_3, \sigma_4\}$ to the adversary $\mathcal{A}$, where we maximize the adversary's advantage, σ_1' is passed to $\mathcal{A}$. Thus, $\Phi' = \{\sigma_0, \sigma_1 = e(\vartheta^{H(ID)} \cdot \psi, \sigma_1'), \sigma_2, \sigma_3, \sigma_4\}$ is a valid signature, where we assure that $H(ID) \neq 0 \textbf{ mod } q$ and $H(\mathfrak{M} \parallel \mathfrak{E}) \neq 0 \textbf{ mod } q$.

Forgery: If the algorithm $\mathcal{B}$ does not abort as a consequence of one of the queries above, the adversary $\mathcal{A}$ will, with probability at least ε, return its forgeries, ($\mathfrak{M}_1^*$, $\mathfrak{E}^*$, Φ_1^*, RL_ID^*, RL_PK^*) and ($\mathfrak{M}_2^*$, $\mathfrak{E}^*$, Φ_2^*, RL_ID^*, RL_PK^*) for the challenger u^*, with $ID^* \in RL\_ID^*$, $pk_{\{ID^*\}} \in RL\_PK^*$, $\Phi_1^* = \{\sigma_{10}^*, \sigma_{11}^*, \sigma_{12}^*, \sigma_{13}^*, \sigma_{14}^*, \sigma_{15}^*, \sigma_{16}^*\}$ and $\Phi_2^* = \{\sigma_{20}^*, \sigma_{21}^*, \sigma_{22}^*, \sigma_{23}^*, \sigma_{24}^*, , \sigma_{25}^*, \sigma_{26}^*\}$, where

$$\begin{aligned}
\sigma_{10}^* &= g_2^y \cdot \vartheta^{(r_{12}^*+a)\cdot H(ID^*)} \cdot \psi^{r_{12}^*+a} \cdot \varpi^{r_{13}^*} \\
&\quad \cdot \mu^{r_{14}^* \cdot H(RL\_ID^* \| RL\_PK^*)} \cdot \tau^{r_{14}^*} \\
&\quad \cdot \chi^{r_{15}^* \cdot H(\mathfrak{M}_1^* \| \mathfrak{E}^*)} \cdot \kappa^{r_{15}^*}, \\
\sigma_{11}^* &= g^{r_{12}^*}, \\
\sigma_{12}^* &= g^{r_{13}^*}, \\
\sigma_{13}^* &= g^{r_{14}^*}, \\
\sigma_{14}^* &= g^{r_{15}^*}, \\
\sigma_{15}^* &= g_2^{r_{12}^*}, \\
\sigma_{16}^* &= g_2^{r_{15}^*}.
\end{aligned}$$

$$\begin{aligned}
\sigma_{20}^* &= g_2^y \cdot \vartheta^{(r_{22}^*+a)\cdot H(ID^*)} \cdot \psi^{r_{22}^*+a} \cdot \varpi^{r_{23}^*} \\
&\quad \cdot \mu^{r_{24}^* \cdot H(RL\_ID^* \| RL\_PK^*)} \cdot \tau^{r_{24}^*} \\
&\quad \cdot \chi^{r_{25}^* \cdot H(\mathfrak{M}_2^* \| \mathfrak{E}^*)} \cdot \kappa^{r_{25}^*}, \\
\sigma_{21}^* &= g^{r_{22}^*}, \\
\sigma_{22}^* &= g^{r_{23}^*}, \\
\sigma_{23}^* &= g^{r_{24}^*}, \\
\sigma_{24}^* &= g^{r_{25}^*}, \\
\sigma_{25}^* &= g_2^{r_{22}^*}, \\
\sigma_{26}^* &= g_2^{r_{25}^*}.
\end{aligned}$$

Remark 4. *In fact, σ_{11}^* should be equal to $g^{r_{12}^*} \cdot pk_{\{ID^*\}}$, σ_{21}^* should be equal to $g^{r_{22}^*} \cdot pk_{\{ID^*\}}$. Additionally, because the adversary $\mathcal{A}$ can compute $\sigma_{11}^* = g^{r_{12}^*}$ and $\sigma_{14}^* = g^{r_{15}^*}$, $\mathcal{A}$ can easily convert these computations to $\sigma_{15}^* = g_2^{r_{12}^*}$ and $\sigma_{16}^* = g_2^{r_{15}^*}$, where σ_{15}^* and σ_{16}^* return to the algorithm $\mathcal{B}$ so as to make $\mathcal{B}$ solve the CDH problem. Similarly, σ_{25}^* and σ_{26}^* also return to the algorithm $\mathcal{B}$.*

And the forgeries satisfy the following conditions:

1) $1 \leftarrow$ ***Verify***($TCRK$, RL_ID^*, RL_PK^*, $\mathfrak{M}_1^*$, $\mathfrak{E}^*$, Φ_1^*);

2) $1 \leftarrow$ ***Verify***($TCRK$, RL_ID^*, RL_PK^*, $\mathfrak{M}_2^*$, $\mathfrak{E}^*$, Φ_2^*);

3) $ID^* \leftarrow$ ***Trace-User***($TCRK$, RL_ID^*, RL_PK^*, $\{\mathfrak{M}_1^*, \Phi_1^*\}$, $\{\mathfrak{M}_2^*, \Phi_2^*\}$, $\mathfrak{E}^*$);

4) $\mathcal{A}$ did not query ***Generate-Key*** on input $ID^* \in RL\_ID^*$ and did not query ***Sign*** on inputs RL_ID^*, RL_PK^*, $\mathfrak{M}_1^*$ ($\mathfrak{M}_2^*$) and $\mathfrak{E}^*$.

So, the algorithm $\mathcal{B}$ computes and outputs

$$\frac{\sigma_{10}^*}{Q} = g_2^{\ell \cdot a \cdot H(ID^*)},$$

where $Q = g_2^y \cdot g_2^{r_{12}^* \cdot \ell \cdot H(ID^*)} \cdot g^{r_{12}^* \cdot H(ID^*)} \cdot pk_{\{ID^*\}}{}^{H(ID^*)} \cdot g^{r_{12}^* \cdot \partial} \cdot pk_{\{ID^*\}}{}^{\partial} \cdot g^{r_{13}^* \cdot \eta} \cdot g^{r_{14}^* \cdot \nu \cdot H(RL\_ID^* \| RL\_PK^*)} \cdot g^{r_{14}^* \cdot \lambda} \cdot g_2^{r_{15}^* \cdot \alpha \cdot H(\mathfrak{M}_1^* \| \mathfrak{E}^*)} \cdot g^{r_{15}^* \cdot H(\mathfrak{M}_1^* \| \mathfrak{E}^*)} \cdot g^{r_{15}^* \cdot \pi}$. Further, we can compute $\sqrt[\ell \cdot H(ID^*)]{g_2^{\ell \cdot a \cdot H(ID^*)}} = g_2^a = g^{a \cdot b}$, which is the solution to the given CDH problem.

Now, we analyze the probability of the algorithm $\mathcal{B}$ not aborting. For the simulation to complete without aborting, we require that all ***Generate-Key*** queries will have $H(ID) \neq 0 \textbf{ mod } q$, all ***Sign*** queries will have $H(ID) \neq 0 \textbf{ mod } q$ and $H(\mathfrak{M} \parallel \mathfrak{E}) \neq 0 \textbf{ mod } q$. If the algorithm $\mathcal{B}$ does not abort, then the following conditions must hold:

1) $H(ID_i) \neq 0 \textbf{ mod } q$ in ***Generate-Key*** queries, with i=$1, 2 ...... q_g$;

2) $H(ID_i) \neq 0 \textbf{ mod } q$ and $H(\mathfrak{M}_i \parallel \mathfrak{E}_i) \neq 0 \textbf{ mod } q$ in ***Sign*** queries, with i=$1, 2 ...... q_s$;

To make the analysis simpler, we will define the events E_i, F_i, T_i as

$E_i : H(ID_i) \neq 0 \textbf{ mod } q$, with i=$1, 2 ...... q_g$;
$F_i : H(ID_i) \neq 0 \textbf{ mod } q$, with i=$1, 2 ...... q_s$;
$T_i : H(\mathfrak{M}_i \parallel \mathfrak{E}_i) \neq 0 \textbf{ mod } q$, with i=$1, 2 ...... q_s$;

Then the probability of $\mathcal{B}$ not aborting is

$$\Pr(not\_abort) = \Pr\left(\bigcap_{i=1}^{q_g} E_i \wedge \bigcap_{i=1}^{q_s} (F_i \wedge T_i)\right).$$

It is easy to see that the events $\bigcap_{i=1}^{q_g} E_i$, $\bigcap_{i=1}^{q_s} F_i$, $\bigcap_{i=1}^{q_s} T_i$ are independent. Then we may compute

$$\Pr(\bigcap_{i=1}^{q_g} E_i) = 1 - \Pr(\bigcup_{i=1}^{q_g} \neg E_i) = 1 - q_g \cdot \frac{1^k}{1^k \cdot q} = 1 - \frac{q_g}{q};$$

$$\Pr(\bigcap_{i=1}^{q_s} F_i) = 1 - \Pr(\bigcup_{i=1}^{q_s} \neg F_i) = 1 - q_s \cdot \frac{1^k}{1^k \cdot q} = 1 - \frac{q_s}{q};$$

$$\Pr(\bigcap_{i=1}^{q_s} T_i) = 1 - \Pr(\bigcup_{i=1}^{q_s} \neg T_i) = 1 - q_s \cdot \frac{1^k}{1^k \cdot q} = 1 - \frac{q_s}{q};$$

Thus,

$$\begin{aligned}
\Pr(not\_abort) &= \Pr\left(\bigcap_{i=1}^{q_g} E_i \wedge \bigcap_{i=1}^{q_s} (F_i \wedge T_i)\right) \\
&= \Pr(\bigcap_{i=1}^{q_g} E_i) \cdot \Pr(\bigcap_{i=1}^{q_s} F_i) \cdot \Pr(\bigcap_{i=1}^{q_s} T_i)
\end{aligned}$$

$$= \left(1 - \frac{q_g}{q}\right) \cdot \left(1 - \frac{q_s}{q}\right)^2$$

We can get that $\varepsilon' = (1 - \frac{q_g}{q}) \cdot (1 - \frac{q_s}{q})^2 \cdot \varepsilon$.

If the simulation does not abort, the adversary $\mathcal{A}$ will create a valid forgery with probability at least ε. The algorithm $\mathcal{B}$ can then compute $g^{a \cdot b}$ from the forgery as shown above. The time complexity of the algorithm $\mathcal{B}$ is dominated by the time for the exponentiations and multiplications in the queries. We assume that the time for integer addition and integer multiplication and the time for hash computation can both be ignored, then the time complexity of the algorithm $\mathcal{B}$ is

$$\hbar' = \hbar + O(q_g \cdot (3 \cdot C_{exp} + C_{mul}) + q_s \cdot (12 \cdot C_{exp} + 7 \cdot C_{mul})).$$

Then, from the above proofs, we may get that

$$\varepsilon' = [(1 - \frac{q_g}{q}) \cdot (1 - \frac{q_s}{q})^2 \cdot \frac{\varepsilon}{q^2}] \parallel [(1 - \frac{q_g}{q}) \cdot (1 - \frac{q_s}{q})^2 \cdot \varepsilon],$$

$\hbar' = \max\{\hbar + O(q_g \cdot (10 \cdot C_{exp} + 3 \cdot C_{mul}) + q_s \cdot (15 \cdot C_{exp} + 11 \cdot C_{mul})), \hbar + O(q_g \cdot (3 \cdot C_{exp} + C_{mul}) + q_s \cdot (12 \cdot C_{exp} + 7 \cdot C_{mul}))\}$. Thus, Theorem 1 follows.

Theorem 2. *The scheme of Section 5 is a linkable (traceable) TCRS scheme when it satisfies the following condition—the scheme of Section 5 is ($\hbar$, ε, q_g, q_s)-secure, assuming that the ($\hbar'$, ε')-CDH assumption holds in $\mathbb{G}_1$, where*

$$\varepsilon' = [\left(1 - \frac{q_g}{q}\right) \cdot \left(1 - \frac{q_s}{q}\right)^2 \cdot \left(\prod_{i=0}^{i=t} \frac{1^k - i}{1^k \cdot q - i}\right)^2 \cdot \varepsilon] \parallel [(1 - \frac{q_g}{q}) \cdot (1 - \frac{q_s}{q})^2 \cdot \varepsilon],$$

$\hbar' = \max\{\hbar + O(q_g \cdot (10 \cdot C_{exp} + 3 \cdot C_{mul}) + q_s \cdot (15 \cdot C_{exp} + 11 \cdot C_{mul})), \hbar + O(q_g \cdot (3 \cdot C_{exp} + C_{mul}) + q_s \cdot (12 \cdot C_{exp} + 7 \cdot C_{mul}))\}$,
and q_g is the maximal number of ”Generate-Key” oracle queries, q_s is the maximal number of ”Sign” oracle queries, t is the number of user (ring member) private keys possessed by adversary, C_{mul} and C_{exp} are respectively the time for a multiplication and an exponentiation in $\mathbb{G}_1$.

Theorem 3. *The scheme of Section 5 is exculpable when it satisfies the following condition—the scheme of Section 5 is ($\hbar$, ε, q_g, q_s)-secure, assuming that the ($\hbar'$, ε')-CDH assumption holds in $\mathbb{G}_1$, where*

$$\varepsilon' = [(1 - \frac{q_g}{q}) \cdot (1 - \frac{q_s}{q})^2 \cdot \frac{\varepsilon}{q^2}] \parallel [(1 - \frac{q_g}{q}) \cdot (1 - \frac{q_s}{q})^2 \cdot \varepsilon],$$

$\hbar' = \max\{\hbar + O(q_g \cdot (10 \cdot C_{exp} + 3 \cdot C_{mul}) + q_s \cdot (15 \cdot C_{exp} + 11 \cdot C_{mul})), \hbar + O(q_g \cdot (3 \cdot C_{exp} + C_{mul}) + q_s \cdot (12 \cdot C_{exp} + 7 \cdot C_{mul}))\}$,
and q_g is the maximal number of ”Generate-Key” oracle queries, q_s is the maximal number of ”Sign” oracle queries, C_{mul} and C_{exp} are respectively the time for a multiplication and an exponentiation in $\mathbb{G}_1$.

Theorem 4. *The scheme of Section 5 is ($\hbar$, ε, q_g, q_s)-anonymous, assuming that the ($\hbar'$, ε')-CDH assumption holds in $\mathbb{G}_1$, where*

$$\varepsilon' = [(1 - \frac{q_{g_1}}{q}) \cdot (1 - \frac{q_{s_1}}{q})^2 \cdot (1 - \frac{q_{g_2}}{q}) \cdot (1 - \frac{q_{s_2}}{q})^2 \cdot \frac{\varepsilon}{q^2}] \parallel$$
$$[(1 - \frac{q_{g_1}}{q}) \cdot (1 - \frac{q_{s_1}}{q})^2 \cdot (1 - \frac{q_{g_2}}{q}) \cdot (1 - \frac{q_{s_2}}{q})^2 \cdot \varepsilon],$$
$$\hbar' = \max\{\hbar +$$
$$O\left((q_{g_1} + q_{g_2}) \cdot (7 \cdot C_{exp} + C_{mul}) + (q_{s_1} + q_{s_2}) \cdot (15 \cdot C_{exp} + 11 \cdot C_{mul})\right),$$
$$\hbar +$$
$$O\left((q_{g_1} + q_{g_2}) \cdot (3 \cdot C_{exp} + C_{mul}) + (q_{s_1} + q_{s_2}) \cdot (12 \cdot C_{exp} + 7 \cdot C_{mul})\right)\},$$

q_{g_1} and q_{g_2} are respectively the maximal numbers of ”Generate-Key” oracle queries in the Queries Phases 1 and 2, q_{s_1} and q_{s_2} are respectively the maximal numbers of ”Sign” oracle queries in the Queries Phases 1 and 2, C_{mul} and C_{exp} are respectively the time for a multiplication and an exponentiation in $\mathbb{G}_1$.

7 Conclusions

In this paper, we present a fully traceable certificateless ring signature scheme, which has a security reduction to the computational Diffie-Hellman assumption. Also, we give a formal security model for traceable certificateless ring signature. Under our security model, the proposed scheme is proved to have the properties of anonymity and traceability with enough security. Compared with other traceable ring signature schemes, the proposed scheme is efficient. However, because the proposed scheme is not enough efficient in computing linking of signatures, the work about TCRS still needs to be further progressed.

Acknowledgments

This study is funded by the National Natural Science Foundations of China (No.61402055, No.61504013), the Hunan Natural Science Foundation (2018JJ2445) and the Hunan Provincial Scientific Research Project (No.15C0041,No.12C0010). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] M. Abe, M. Ohkubo and K. Suzuki, “1-out-of-n signatures from a variety of keys,” in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 415–432, 2002.

[2] M. Abe, M. Ohkubo and K. Suzuki, “Efficient threshold signer-ambiguous signatures from variety of keys,” *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, vol. E87-A, no. 2:471–479, 2004.

[3] S. S. Al-Riyami, K. G. Paterson, “Certificateless public key cryptography,” in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 452–473, 2003.

[4] M. H. Au, S. S. M. Chow, W. Susilo and P. P. Tsang, “Short linkable ring signatures revisited,” in *European Public Key Infrastructure Workshop*, pp. 101–115, 2006.

[5] M. H. Au, J. K. Liu, W. Susilo, T. H. Yuen, “Secure ID-based linkable and revocable-iff-linked ring signature with constant-size construction,” *Preprint Submitted to Theoretical Computer Science*, pp. 1-14, vol. 469, Apr. 23, 2013.

[6] M. H. Au, J. K. Liu, W. Susilo and T. H. Yuen, "Constantsize ID-based linkable and revocable-iff-linked ring signature," in *International Conference on Cryptology in India*, pp. 364–378, 2006.

[7] M. H. Au, J. K. Liu, T. H. Yuen, D. S. Wong, "ID-based ring signature scheme secure in the standard model", in *Proceeding of IWSEC 2006*, pp.1–16, 2006.

[8] A. K. Awasthi, S. Lal, "ID-based ring signature and proxy ring signature schemes from bilinear pairings," *International Journal of Network Security*, vol.4, no.2, pp. 187-192, Mar. 2007.

[9] P. S. L. M. Barreto, B. Libert, N. McCullagh, J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 515–532, 2005.

[10] A. Bender, J. Katz and R. Morselli, "Ring signatures:stronger definitions and constructions without random oracles," in *Theory of Cryptography Conference*, pp. 60–79, 2006.

[11] D. Boneh, M. Franklin, "Identity-based encryption from the Weil pairing," in *Annual International Cryptology Conference*, pp. 213–229, 2001.

[12] D. Boneh, C. Gentry, B. Lynn and H. Shacham, "Aggregate and verifieably encrypted signatures from bilinear maps," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 416–432, 2003.

[13] D. Boneh, M. Hanburg, "Generalized identity based and broadcast encryption schemes," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 455–470, 2008.

[14] S. Brands, "Untraceable off-line cash in wallet with observers," in *Annual International Cryptology Conference*, pp. 302–318, 1993.

[15] E. Bresson, J. Stern and M. Szydlo, "Threshold ring signatures and applications to Ad-hoc groups," in *Annual International Cryptology Conference*, pp. 465–480, 2002.

[16] J. C. Cha, J. H. Cheon, "An identity-based signature from gap diffie-hellman groups," in *International Workshop on Public Key Cryptography*, pp. 18–30, 2002.

[17] C. C. Chang, C. Y. Sun, S. C. Chang, "A strong RSA-based and certificateless-based signature scheme," *International Journal of Network Security*, vol.18, no.2, pp.201-208, Mar. 2016.

[18] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*, pp. 199–204.

[19] D. Chaum, A. Fiat and M. Naor, "Untraceable electronic cash," in *Conference on the Theory and Application of Cryptography*, pp. 319–327, 1990.

[20] D. Chaum and E. Van Heyst, "Group signatures," in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 257–265, 1991.

[21] S. S. M. Chow, J. K. Liu and D. S. Wong, "Robust receipt-free election system with ballot secrecy and verifieability," in *Network and Distributed System Security Symposiumndss*, 2008.

[22] S. S. M. Chow, S. M. Yiu and L. C. K. Hui, "Efficient Identity Based Ring Signature," in *Applied Cryptography and Network Security*, pp. 499–512, 2005.

[23] I. Damgard, K. Dupont and M. Pedersen, "Unclonable group identification," in *Advances in Cryptology*, pp. 555–572, 2006.

[24] Y. Dodis, A. Kiayias, A. Nicolosi and V. Shoup, "Anonymous identification in Ad hoc groups," in *Advances in Cryptology*, pp. 609–626, 2004.

[25] Y. Dodis, A. Kiayias, A. Nicolosi and V. Shoup, "Anonymous identification in Ad hoc groups," in *Advances in Cryptology*, pp. 609–626, 2004.

[26] K. Emura, A. Miyaji, K. Omote, "An r-Hiding revocable group signature scheme: Group signatures with the property of hiding the number of revoked users," *Journal of Applied Mathematics*, vol. 2014, pp. 14, 2014.

[27] E. Fujisaki, K. Suzuki, "Traceable ring signature," in *International Workshop on Public Key Cryptography*, pp. 181–200, 2007.

[28] E. Fujisaki, "Sub-linear size traceable ring signatures without random oracles," in *Cryptographers Track at the RSA Conference*, pp. 393–415, 2011.

[29] D. He, M. K. Khan, S. Wu, "On the Security of a RSA-based Certificateless Signature Scheme," *International Journal of Network Security*, vol. 16, no. 1, pp. 78-80, Jan. 2014.

[30] F. Hess, "Efficient identity based signature schemes based on pairings," in *International Workshop on Selected Areas in Cryptography*, pp. 310–324, 2003

[31] L. Ibraimi, S. Nikova, P. Hartel, W. Jonker, "An Identity-Based Group Signature with Membership Revocation in the Standard Model," *Faculty of Electrical Engineering, Mathematics & Computer Science*, pp. 16, 2010.

[32] I. R. Jeong, J. O. Kwon, D.g H. Lee, "Analysis of revocable-iff-linked ring signature scheme," *IEICE Transactions on Fundamentals of Electronics Communications & Computer Sciences*, pp.322–325, 2009.

[33] Y. Komano, K. Ohta, A. Shimbo and S. Kawamura, "Toward the fair anonymous signatures: Deniable ring signatures," in *Cryptographers Track at the RSA Conference*, pp. 174–191, 2006.

[34] F. Laguillaumie and D. Vergnaud, "Multi-designated Verifiers Signatures," in *Information and Communications Security*, pp. 495–507, 2004.

[35] J. K. Liu, V. K. Wei and D. S. Wong, "Linkable spontaneous anonymous group signature for ad hoc groups (extended abstract)," in *Information Security and Privacy*, pp. 325–335, 2004.

[36] J. K. Liu and D. S. Wong, "Linkable ring signatures: Security models and new schemes," in *International Conference on Computational Science and Its Applications*, pp. 614–623, 2005.

[37] J. K. Liu and D. S. Wong, "Enhanced security models and a generic construction approach for linkable ring signature," *International Journal of Foundations of Computer Science*, vol. 17, no. 6, pp. 1403–1422, 2006.

[38] E. J. L. Lu, M. S. Hwang, and C. J. Huang, "A new proxy signature scheme with revocation", *Applied Mathematics and Computation*, vol. 161, no. 3, PP. 799-806, Feb. 2005.

[39] M. Naor, "Deniable ring authentication," in *Annual International Cryptology Conference*, pp. 481–498, 2002.

[40] T. Okamoto and K. Ohta, "Universal electronic cash," in *Annual International Cryptology Conference*, pp. 324-337, 1992.

[41] K. G. Paterson, J. C. N. Schuldt, "Efficient identity-based signatures secure in the standard model," in *Information Security and Privacy*, pp.207–222, 2006.

[42] R. Rivest, A. Shamir and Y. Tauman, "How to leak a secret," in *Advances in Cryptology*, pp. 552–565, 2001.

[43] H. Singh, G. K. Verma, "ID-based proxy signature scheme with message recovery," *Journal of Systems and Software*,pp. 209–214, 2012.

[44] W. Susilo and Y. Mu, "Non-interactive deniable ring authentication," in *Information Security and Cryptology*, pp. 386–401, 2004.

[45] P. P. Tsang and V. K. Wei, "Short linkable ring signatures for e-voting, e-cash and attestation," in *Information Security Practice and Experience*, pp. 48–60, 2005.

[46] P. P. Tsang, V. K. Wei, T. K. Chan, M. H. Au, J. K. Liu and D. S. Wong, "Separable linkable threshold ring signatures," in *Progress in Cryptology*, pp. 389–398, 2004.

[47] B. Waters, "Efficient identity-based encryption without random oracles," in *Advances in Cryptology*, pp.114–127, 2005.

[48] F. T. Wen, S.J. Cui, J. N. Cui, "An ID-based proxy signature scheme secure against proxy key exposure," *International Journal of Advancements in Computing Technology*, pp. 108–116, 2011.

[49] D. S. Wong, K. Fung, J. K. Liu and Victor K. Wei, "On the RS-code construction of ring signature schemes and a threshold setting of RST," in *Information and Communications Security*, pp. 34–46, 2003.

[50] W. Wu, Y. Mu, W. Susilo, J. Seberry, X.Y. Huang, "Identity-based proxy signature from pairings," in *International Conference on Autonomic and Trusted Computing*, pp. 22–31, 2007.

[51] F. Zhang and K. Kim, "ID-Based blind signature and ring signature from pairings," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 533–547, 2002.

[52] D. Zheng, X. Li, K. Chen and J. Li, "Linkable ring signatures from linear feedback shift register," in *International Conference on Embedded and Ubiquitous Computing*, pp. 716–727, 2007.

[53] D. Y. W. Liu, J. K. Liu, Y. Mu, W. Susilo and D. S. Wong, "Revocable ring signature," *Journal of Computer Science and Technology*, vol. 22, no. 6, pp. 785–794, 2007.

Biography

Ke Gu received his Ph.D. degree in School of Information Science and Engineering from Central South University in 2012. He is currently a Lecturer at Changsha University of Science and Technology. His research interests include cryptography, network and information security.

LinYu Wang is pursuing her master degree. Her research interests include social network, network and information security.

Na Wu is pursuing her master degree. Her research interests include fog computing, network and information security.

NianDong Liao is currently a Lecturer at Changsha University of Science and Technology. His research interests include cloud computing, network and information security.