2015

Identity-based quotable ring signature

Kefeng Wang
University of Wollongong, kw909@uowmail.edu.au

Yi Mu
University of Wollongong, ymu@uow.edu.au

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Publication Details
Wang, K., Mu, Y. & Susilo, W. (2015). Identity-based quotable ring signature. Information Sciences, 321 (November), 71-89.

Identity-based quotable ring signature

Abstract
We present a new notion of identity-based quotable ring signature. This new cryptographic primitive can be used to derive new ring signatures on substrings of an original message from an original ring signature on the original message, which is generated by the actual signer included in the ring. No matter whether a ring signature is originally generated or is quoted from another valid ring signature, it will convince the verifier that it is generated by one of the ring members, without revealing any information about which ring member is the actual signer. The set of ring members could be arbitrarily selected by the actual signer without need of other ring members' approval. The actual signer is anonymous among this set of ring members. At the same time, the verifier could not distinguish whether a ring signature is originally generated or is quoted from another ring signature. In this paper, we propose a concrete identity-based quotable ring signature scheme based on bilinear pairing. We make use of bilinear groups of composite order. The construction is identity-based to alleviate the problem of certificate verification, especially for applications involving a large number of public keys in each execution such as ring signature schemes. The proposed scheme is proven to be anonymous under the assumption that the Subgroup Decision Problem is hard, selectively unforgeable against adaptively chosen message attacks in the random oracle model under the assumption that the Computational Diffie-Hellman problem is hard, and strongly context hiding

Keywords
quotable, identity, ring, signature

Disciplines
Engineering | Science and Technology Studies

Publication Details
Wang, K., Mu, Y. & Susilo, W. (2015). Identity-based quotable ring signature. Information Sciences, 321 (November), 71-89.

Identity-Based Quotable Ring Signature

Kefeng Wang[a], Yi Mu[a], Willy Susilo[a]

[a] *Centre for Computer and Information Security Research*
School of Computer Science and Software Engineering
University of Wollongong, Wollongong NSW 2522, Australia

Abstract

We present a new notion of *identity-based quotable ring signature*. It could be applied for anyone deriving new ring signatures on substrings of an original message from an original ring signature on the original message, which is generated by an actual signer included in the ring. No matter whether a signature is originally generated or is quoted from another valid ring signature, it will convince the verifier that it is generated by one of the ring members, without revealing any information about which ring member is the actual signer. The set of signers could be arbitrarily selected by the actual signer without need of other signers' approval. The actual signer is anonymous among this set of signers. At the same time, the verifier could not distinguish whether a signature is originally generated or is quoted from another ring signature. In this paper, we propose a concrete identity-based quotable ring signature scheme based on bilinear pairing. We make use of bilinear groups of composite order. The construction is identity-based to alleviate the problem of certificate verification, especially for applications involving a large number of public keys in each execution such as ring signature schemes. The proposed scheme is proven to be anonymous under the assumption that the Subgroup Decision Problem is hard, selectively unforgeable against adaptively chosen message attacks in the random oracle model under the assumption that the Computational Diffie-Hellman problem is hard, and strongly context hiding.

Keywords: Identity-based cryptography, quotable signature, ring signature

1. Introduction

In ring signature schemes, the actual signer can choose arbitrary other signers to form a ring that includes himself. The actual signer anonymously signs messages by using his private key and other users' public keys on behalf of the whole ring. There is no requirement to get other users' approval. On one hand, similar with group signature schemes, the verifier must be convinced that a signature has been generated by a member of this ring, but could not have better way to identify the actual signer than at random to guess which member is the actual signer. The actual signer remains completely anonymous. On the other hand, unlike group signature schemes, there is no group manager, no setup procedure, no revocation procedure, and no coordination in traditional ring signature. There is no way to revoke the anonymity of the actual signer. Ring signature schemes can be considered as simplified group signature schemes which consist of only users without managers. Recently, in order to realize an efficient ring signature scheme provably secure in the standard model, Shacham and Waters [26] introduced an efficient ring signature scheme by allowing for a trusted global setup step by an authority.

In ring signature schemes, all ring members' information serves as a part of the ring signature. In traditional Public Key Infrastructure, prior to the generation of a ring signature, the actual signer has to check the validity of public keys of other users which are included in the ring. Similarly, prior to the verification of a ring signature, the verifier has to check the validity of public keys of all the users in the ring. This increases both the generation and the verification cost of ring signatures. In identity-based

Email addresses: kw909@uowmail.edu.au (Kefeng Wang), ymu@uow.edu.au (Yi Mu), wsusilo@uow.edu.au (Willy Susilo)

setting, introduced by Shamir, it avoids these checks about public keys. In this way, the public keys of users can be easily and publicly computed from their identities by anyone. This is especially desirable for applications which involve a large number of public key checks such as ring signature schemes.

Quoting are usually applied to derive a signature on a substring when text messages are signed. It can also be applied to derive a signature on a subregion of an image when images are signed, such as a face. In quotable signature schemes, for every substring m' of a message m, it is possible for a third party to derive a signature on m' from a signature on m on behalf of the same signer. Moreover, the derived signature on m' reveals no extra information about m, which means the derived signature cannot be distinguished from a fresh one even when the original signature on m is given. The inability to link derived signatures to their original sources prevents some practical privacy and linking attacks. It is desirable to allow repeated computation on the signatures, which means it is possible to quote from a quoted signature. It is also desirable that the size of the signatures depend only on the size of the object being signed, no matter whether the signature is fresh or derived, even if being quoted several times. This means the signature size will not grow with every derivation.

Our Contributions. For the first time, this paper presents a provably secure (correct, anonymous, selectively unforgeable, and strongly context hiding) identity-based quotable ring signature scheme based on bilinear pairing, under the Subgroup Decision Problem assumption and Computational Diffie-Hellman assumption in the composite order groups. We also present a security model and concrete security analysis by the reduction to prove the security of the proposed scheme. More precisely, we can show that if there exists an attacker who can identify the actual signer among a ring of signers, then the Subgroup Decision Problem is solved, and if there exists an attacker who can selectively forge a valid quotable ring signature, then the Computational Diffie-Hellman problem is solved. We also prove the scheme is strongly context hiding in a statistical definition.

Paper Organization. The rest of this paper is organized as follows: Section 2 introduces some related work that has been studied in the literature. Section 3 introduces some mathematical background used throughout this paper. In Section 4, we recall some known results about homomorphic encryption and NIZK, which are used as building blocks in the proposed scheme. In Section 5, we propose a notion of identity-based quotable ring signature scheme and present a concrete scheme based on bilinear pairing in the composite order groups. We also present a security model and security proofs about correctness, anonymity, selectively unforgeability against adaptively chosen message attacks and strongly context hiding property in this section. Section 6 concludes the paper.

2. Related Work

In 1984, Shamir [27] introduced the concept of identity-based cryptography to simplify key management procedures in traditional public key setting. In identity-based setting, user's public key could be easily and publicly computed from his identity. Digital certificates are not needed.

The concept of ring signature schemes were formalized by Rivest, Shamir, and Tauman [24, 25]. They proposed a scheme based on certificate-based public key setting, which is proved existentially unforgeable under adaptive chosen-message attacks assuming the hardness of the RSA problem. Before the concept of ring signature scheme is formalized, it is used as a tool to construct group signature schemes in [16, 14]. There are two main differences between the concepts of ring signature schemes and group signature schemes. First, the ring is determined by the actual signer and is dynamic, while the group members are controlled by the manager and are fixed at any given time. Second, no one can identify the actual signer in ring signature schemes, while the group manager can identify the actual signer in group signature schemes. Bresson, Stern, and Szydlo [10] gave a simpler proof of the security of the scheme in [24], under the strictly weaker assumption of the random oracle model. Abe, Ohkubo, and Suzuki [1] proposed some general constructions of ring signature schemes, where the public keys of the users can be totally independent. Their scheme is also based on the certificate-based public key setting. Herranz and Sáez [20] gave some security results for generic ring signature schemes, and they designed a new specific scheme based on Schnorr's signature scheme.

Shacham and Waters [26] described the first efficient ring signature scheme secure without random oracles, based on standard assumptions. Their scheme is related to a group signature scheme secure without

random oracles due to Boyen and Waters [9]. The main difference is that in [9] the master public key is public and the first level message is encrypted, while in [26] the signer's public key is encrypted and the message is public.

The first identity-based ring signature scheme was proposed by Zhang and Kim [29] based on pairings. But they did not provide a formal proof of the existential unforgeability of their scheme. Herranz [19] proposed such a proof of [29]. Later, Lin and Wu [23] proposed a more efficient identity-based ring signature scheme. Tang, Liu, and Wang [28] pointed out some mistakes in [23] and proposed an improved scheme. Herranz and Sáez [21] extended their work [20] on ring forking lemmas to the identity-based scenario.

Ahn et al. [2] proposed an efficient quotable signature scheme, which equipped with strongly context hiding and selectively unforgeability property. Early work regarding anyone deriving quoted signatures such as redactable signature schemes [22, 15, 11, 6, 7] supports quoting from a single document, but does not achieve the privacy or unforgeability properties required in [2]. The work whose definition is closest to [2] is that on redacted signatures of Chang, Lim, and Xu [15], and Brzuska et al. [11], and Boneh, and Freeman [6, 7]. However, in [2], a quoted signature should be indistinguishable from a fresh signature, even when the distinguisher is given the original signature. In contrast, the definitions of [15, 11, 6, 7] do not provide the distinguisher with the original signature. Thus, it may be possible to link a quoted document to its original source, which can have negative privacy implications.

Another type of studies computing on authenticated data requires secret information of the original signer, such as sanitizable signatures [3, 12, 13], and incremental signatures [4], where the signer can efficiently make small edits to his signed data. In contrast, our work followed [2] concentrate more about anyone can compute on the authenticated data.

3. Preliminaries

3.1. Bilinear Groups of Composite Order

Let n be a composite number with factorization $n = pq$, where p and q are sufficient large prime numbers. We have: $\mathbb{G}$ is a multiplicative cyclic group of composite order n. $\mathbb{G}_p$ is its cyclic order-p subgroup, and $\mathbb{G}_q$ is its cyclic order-q subgroup. g is a generator of $\mathbb{G}$. h is a generator of $\mathbb{G}_q$. $\mathbb{G}_T$ is a multiplicative cyclic group of composite order n. $\mathbb{G}_{T,p}$ and $\mathbb{G}_{T,q}$ are its order-p and order-q subgroups, respectively.

Let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be a bilinear mapping with the following properties:

- Bilinearity: $e(u^a, v^b) = e(u,v)^{ab}$ for all $\{u,v\} \in \mathbb{G}, \{a,b\} \in \mathbb{Z}_n$.
- Non-degeneracy: $< e(g,g) >= \mathbb{G}_T$ whenever $< g >= \mathbb{G}$.
- Computability: There exists an efficient algorithm to compute $e(u,v)$ for all $\{u,v\} \in \mathbb{G}$.

3.2. Subgroup Hiding Assumption

The Subgroup Decision Problem is as follows. Given a composite order $n = pq$ cyclic group $\mathbb{G}$ and its subgroup $\mathbb{G}_q$ of order q, w is selected at random either from $\mathbb{G}$ (with probability 1/2) or from $\mathbb{G}_q$ (with probability 1/2). Decide whether w is in $\mathbb{G}_q$.

The advantage of an algorithm $\mathcal{A}$ solving the Subgroup Decision Problem is defined as $\mathcal{A}$'s excess probability beyond 1/2 of outputting the correct solution. The Subgroup Decision Problem is said to be intractable, if for every probabilistic polynomial time algorithm $\mathcal{A}$, the success probability of guessing advantage for the problem is negligible. The assumption that the Subgroup Decision Problem is hard is called the Subgroup Hiding (SGH) assumption, and was introduced by Boneh, Goh, and Nissim [8].

3.3. CDH Problem

Let $\mathbb{G}$ be a cyclic group of composite order n. Let g be a generator of $\mathbb{G}$. Let $\mathcal{A}$ be an attacker. $\mathcal{A}$ tries to solve the following problem: Given (g, g^a, g^b) for some unknown $a, b \in \mathbb{Z}_n$, compute g^{ab}.

The CDH problem is said to be intractable, if for every probabilistic polynomial time algorithm $\mathcal{A}$, the success probability is negligible.

4. NIZK Proof That C Encrypts 0 or 1

We use some cryptographic primitives as building blocks in this scheme. The first one is a homomorphic public key encryption scheme, which is proposed by Boneh, Goh and Nissim [8]. The homomorphic encryption scheme consists of three algorithms, which are as follows.

- **KeyGen:** Given a security parameter λ, run $\mathcal{G}(1^\lambda)$ to obtain a tuple $(p,q,\mathbb{G},\mathbb{G}_T,e)$. Let $n=pq$, where p,q are sufficient large prime numbers. Both $\mathbb{G},\mathbb{G}_T$ are cyclic groups of composite order n. Select g as a random generator of $\mathbb{G}$ and h as a random generator of $\mathbb{G}_q$, which is a cyclic order q subgroup of $\mathbb{G}$. The public key is $(n,\mathbb{G},\mathbb{G}_T,e,g,h)$. The private key is q.
- **Encrypt:** To encrypt a message m, pick a random $s \leftarrow \{0,1,\cdots,n-1\}$ and compute $C = g^m h^s \in \mathbb{G}$. Output C as the ciphertext.
- **Decrypt:** To decrypt a ciphertext C, compute $C^q = g^{mq}h^{sq} = (g^q)^m$. Let $\hat{g} = g^q$ and exhaustively searth for m.

Note that decryption in this system takes polynomial time in the size of the message space. Therefore, the system can only be used to encrypt short messages.

The second building block is a non-interactive zero-knowledge proof which is proposed by Groth, Ostrovsky and Sahai [18], which proofs that a BGN-ciphertext has either 0 or 1 as plaintext. The non-interactive zero-knowledge proof is described as follows.

- **Common reference string:** Given a security parameter λ, run $\mathcal{G}(1^\lambda)$ to obtain a tuple $(p,q,\mathbb{G},\mathbb{G}_T,e)$. Let $n=pq$, where p,q are sufficient large prime numbers. Both $\mathbb{G},\mathbb{G}_T$ are cyclic groups of composite order n. Select g as a random generator of $\mathbb{G}$ and h as a random generator of $\mathbb{G}_q$, which is a cyclic order q subgroup of $\mathbb{G}$. The common reference string is $\sigma = (n,\mathbb{G},\mathbb{G}_T,e,g,h)$.
- **Statement:** The statement is an element $C \in \mathbb{G}$. The claim is that there exists a pair $(m,s) \in \mathbb{Z}^2$ such that $m \in \{0,1\}$ and $C = g^m h^s$.
- **Proof:** Input $(\sigma, C, (m,s))$.
  - Check $m \in \{0,1\}$ and $C = g^m h^s$. Return failure if check fails.
  - $r \leftarrow \mathbb{Z}_n^*$;
  - $\pi_1 = h^r, \pi_2 = (g^{2m-1}h^s)^{sr^{-1}}, \pi_3 = g^r$;
  - Return $\pi = (\pi_1,\pi_2,\pi_3)$.
- **Verification:** Input $(\sigma, C, \pi = (\pi_1,\pi_2,\pi_3))$.
  - Check $C \in \mathbb{G}$ and $\pi \in \mathbb{G}^3$;
  - Check $e(C, Cg^{-1}) \stackrel{?}{=} e(\pi_1,\pi_2)$ and $e(\pi_1, g) \stackrel{?}{=} e(h,\pi_3)$;
  - Return 1 if both checks pass, else return 0.

In order to make these building blocks suitable for the quotable signature scheme, we should slightly change the random number s used in the Encrypt algorithm of Boneh, Goh and Nissim encyrption scheme to $s \leftarrow \mathbb{Z}_n^*$.

The Proof algorithm of Groth, Ostrovsky and Sahai NIZK proof scheme should also be slightly changed as follows.

- **Proof:** Input $(\sigma, C, (m,s))$.
  - Check $m \in \{0,1\}$ and $C = g^m h^s$. Return failure if check fails.
  - $\hat{r} \leftarrow \mathbb{Z}_n^*, r = \hat{r}s$;
  - $\pi_1 = h^r, \pi_2 = (g^{2m-1}h^s)^{sr^{-1}}, \pi_3 = g^r$;
  - Return $\pi = (\pi_1,\pi_2,\pi_3)$.

In fact, as $\hat{r}$ is a random number, after multiplied to s, r is still a random number. The modified proof algorithm is essentially the same as the original one. But the elements π_1,π_2, and π_3 have been changed to $\pi_1 = h^{sr}, \pi_2 = (g^{2m-1}h^s)^{r^{-1}}$, and $\pi_3 = g^{sr}$, respectively.

5. Identity-Based Quotable Ring Signature

5.1. Definitions

There will be two types of different signatures named Type I signature and Type II signature, where Type I signature can be quoted down to another Type I or Type II signature, Type II signature cannot be quoted again but with a shorter signature size. The trusted party Private Key Generator (PKG) generates all users' private keys. An identity-based quotable ring signature scheme for message space $\mathcal{M}$ consists of the following five algorithms:

Setup: On input of a security parameter λ, PKG selects the master secret key of this scheme and publishes public parameters *params*.

Extract: When a party requires its private key corresponding to its identity, this algorithm generates the private key using the master secret key and the identity, then returns the private key to the party.

Sign: This algorithm takes as input the actual signer's private key S_{ID} and a set of public keys R that constitutes the ring, along with a message M in the message space to be signed. It is required that $Q_{ID} \in R$ hold. This algorithm returns a ring signature σ on M on behalf of the ring R.

Quote: This algorithm takes as input a Type I ring signature σ with the corresponding ring R and message M, and a substring M' of M. It first checks the validity of σ with respect to R and M. If σ is valid, it produces a new ring signature σ', which is either Type I or Type II, of M' on behalf of the ring R. Otherwise, it output a special symbol $\perp$ to represent failure.

Verify: The verification algorithm takes as input a set of public keys R that constitutes the ring, and a purported ring signature σ of a message M on behalf of the ring R. It returns either valid or invalid.

5.2. Security Model

Informally, a ring signature scheme should satisfy two security properties. First, it should be anonymous, which means an adversary should not be able to determine which member of a ring generated a signature. Second, it should be unforgeable, which means an adversary should be able to construct a valid signature on behalf of a ring only if he knows the secret key corresponding to one of them. Rivest, Shamir, and Tauman [24] gave a formalization which has been used in much subsequent work. Bender, Katz, and Morselli [5] described several possible stronger formulations of each notion. In addition to this, as a quotable signature, it also should be context hiding, which means a derived signature on M', from an honestly generated original signature on M, is statistically indistinguishable from a fresh signature on M', even if the original signature on M is known. Ahn et al. [2] proposed a strong definition of context hiding for quotable signature.

For identity-based quotable ring signature scheme, the security model should be slightly modified. For example, in terms of the unforgeability property, new ring signatures quoted from an valid original ring signature should not be considered as a forgery even if the adversary did not know the secret key corresponding to one of the members of the ring.

- *Correctness.* We require that for all private key S_{ID} generated by Extract algorithm and for all $M \in \mathcal{M}$, all substring $M' \subseteq M$, and all ring of public keys R where $Q_{ID} \in R$ we have:
  - For both Type I and Type II signatures, $\text{Sign}(S_{ID}, R, M) \neq \perp$ and $\text{Verify}(R, M, Sign(S_{ID}, R, M)) = 1$,
  - For all Type I signature σ_I generated by $\sigma_I \leftarrow Sign(S_{ID}, R, M')$ or $\sigma_I \leftarrow \text{Quote}(\sigma_I', R, M, M')$, $\text{Quote}(\sigma_I, R, M', M'') \neq \perp$, and $\text{Verify}\ (R, M'', Quote(\sigma_I, R, M', M'')) = 1$.

  In particular, correctness implies that a signature generated by Quote algorithm can be used as an input to Quote algorithm so that signatures can be further quoted from quoted signatures.

- *Anonymity.* We require that any verifier should not have probability greater than $1/d$ to guess the identity of the actual signer who has computed a ring signature on behalf of a ring of d members. If the verifier is a member of the ring distinct from the actual signer, then his probability to guess the identity of the actual signer should not be greater than $1/(d-1)$.

  Anonymity against full key exposure for an identity-based quotable ring signature scheme is defined using the following game between a challenger and an adversary $\mathcal{A}$:

– **Setup.** The challenger selects $\mathcal{ID} = \{ID_1, \cdots, ID_\xi\}$ where ξ is a game parameter. The adversary $\mathcal{A}$ is given the public key set $\mathcal{ID}$.

– **Queries.** Algorithm $\mathcal{A}$ is allowed to make ring signing queries and extract queries. A ring signing query is of the form (i', R, M). Here M is the message to be signed. R is a set of public keys, and i' is an index such that $Q_{ID_{i'}} \in R$ holds. (The other keys in R need not be keys in the set $\mathcal{ID}$). The challenger responds with $\sigma = Sign(S_{ID_{i'}}, R, M)$. An extract query is of the form ID_i. The challenger provides S_{ID_i} to $\mathcal{A}$.

– **Chanllenge.** Algorithm $\mathcal{A}$ requests a challenge by sending to the challenger the values (i_0, i_1, R, M). Here M is to be signed with respect to the ring R, and i_0 and i_1 are indices such that $\{Q_{ID_{i_0}}, Q_{ID_{i_0}}\} \in R$. (The other keys in R need not be keys in the set $\mathcal{ID}$.) The challenger chooses a bit $b \leftarrow \{0,1\}$, computes the challenge signature $\sigma \leftarrow \text{Sign}(S_{ID_{i_b}}, R, M)$, and provides $\mathcal{A}$ with σ.

– **Output.** Algorithm $\mathcal{A}$ finally outputs its guess b' for b, and wins if $b = b'$.

We define $Adv^{anon-ke}_{\mathcal{IDQRS},\mathcal{A}}$ to be the advantage over $1/2$ of $\mathcal{A}$ in the above game.

- *Unforgeability.* We prove our construction selectively secure. Selective security for signatures requires the attacker to give the forgery message before seeing the verification key.

  To define unforgeability, we extend the basic notion of existential unforgeability with respect to adaptive chosen-message attacks [17]. The definition captures the idea that if the attacker is given a set of signed messages (either primary or quoted), then the only messages he can sign are derivations of the signed messages he was given.

  Unforgeability for an identity-based quotable ring signature scheme $\mathcal{IDQRS}$ is defined using the following game between a challenger and an adversary $\mathcal{A}$.

  – **Setup.** The challenger selects $\mathcal{ID} = \{ID_1, \cdots, ID_\xi\}$ where ξ is a game parameter. The adversary $\mathcal{A}$ is given the public key set $\mathcal{ID}$.

  – **Queries.** Algorithm $\mathcal{A}$ is allowed to make ring signing queries and extract queries. A ring signing query is of the form (i', R, M). Here M is the message to be signed. R is a set of public keys, and i' is an index such that $ID_{i'} \in R$ holds. (The other keys in R need not be keys in the set $\mathcal{ID}$). The challenger responds with $\sigma = Sign(S_{ID_{i'}}, R, M)$. An extract query is of the form ID_i. The challenger provides S_{ID_i} to $\mathcal{A}$.

  – **Output.** Eventually, $\mathcal{A}$ outputs a tuple (R^*, M^*, σ^*) and wins the game if (1) it never made a ring signing query (i, R, M) such that $ID_i \in R^*$ and M equals to or is a superstring of M^*; (2) it never made an extract query ID_i for any $ID_i \in \mathcal{ID}$, and $R^* \subseteq \mathcal{ID}$; and (3) Verify $(R^*, M^*, \sigma^*) =$ valid.

  An identity-based quotable ring signature schemes is selectively unforgeable with respect to adaptive chosen-message attacks if for all PPT adversaries $\mathcal{A}$, the probability that he wins the game is negligible in λ.

  We define $Adv^{sel-uf}_{\mathcal{IDQRS},\mathcal{A}}$ to be the probability that $\mathcal{A}$ wins in the above game.

- *Context Hiding.* The notion of anonymity has considered the problem of hiding the identity of a signer among a set of users. Context hiding ensures privacy for the data rather than the signer. Our goal is to hide how a ring signature was created. Context hiding captures an important privacy property, which means a ring signature should reveal nothing more than the message being signed. In particular, if a ring signature on M' was quoted from a ring signature on M, an attacker should not learn anything about M other than what can be inferred from M'. This should be true even if the original ring signature on M is revealed. For example, a signed quote should not reveal anything about the message from which it was quoted, including its length, the position of the quote, whether its parent document is the same as another quote, whether it was derived from a given signed message or generated freshly, etc.

  We can view a message M as a pair $(t, m) \in \{0,1\}, \{0,1\}^*$. The bit t will identify the message as being Type I or Type II (assume $t = 1$ signifies Type I signatures) and m will be the message to be

signed. We note that this description allows an attacker to distinguish between any Type I signature from any Type II signature since the "type bit" of the messages will be different and thus they will technically be two different messages even if the message components are equal. For this reason we will only need to prove context hiding between messages of Type I or Type II, but not across types. In general, flipping the bit t will not result in a valid signature of a different type on the same core message, because the format will be wrong. However, moving from a Type I to a Type II on the same core message is not considered a forgery since Type II signatures can be legally derived from Type I.

We put forth the following powerful statistical definition of context hiding.

Let $M \in \mathcal{M}$ and $M' \subseteq M$ be a substring of M. Let $S_{ID_i} \leftarrow Extract(ID_i)$, R be a ring such that $Q_{ID_i} \in R$. An identity-based quotable ring signature scheme is strongly context hiding if for all such triples (S_{ID_i}, M, M'), the following two distribution are statistically close:

$$\{\big(S_{ID_i}, \sigma_M \leftarrow Sign(S_{ID_i}, R, M), Sign(S_{ID_i}, R, M')\big)\}_{S_{ID_i}, M, M'}$$

$$\{\big(S_{ID_i}, \sigma_M \leftarrow Sign(S_{ID_i}, R, M), Quote(\sigma_M, R, M, M')\big)\}_{S_{ID_i}, M, M'}$$

The definition states that a derived signature on M', from an honestly generated original ring signature, is statistically indistinguishable from a fresh ring signature on M'. This implies that a derived ring signature on M' is indistinguishable from a ring signature generated independently of M. Therefore, the derived ring signature cannot (provably) reveal any information about M beyond what is revealed by M'.

Using statistical indistinguishability meaning that even an unbounded adversary cannot distinguish derived ring signatures from newly created ones. The same holds even if the signing key is leaked.

5.3. Proposed Scheme

The design of this scheme follows the idea of the Ahn et al. quotable signature scheme [2], which is not identity-based and not ring signature.

Setup (1^λ)**:** On input of the security parameter 1^λ, construct a group $\mathbb{G}$ of composite order $n = pq$ as described in Sect.3.1. Let L be the maximum message length supported and denote $n' = \lfloor lg(L) \rfloor$. Let $H_a : \{0,1\}^* \to \mathbb{G}^*, H_b : \{0,1\}^* \to \mathbb{G}^*$ and $H : \{0,1\}^* \to \mathbb{G}^*$ be three hash functions. Choose random $w, z_0, \cdots, z_{n'-1}, \alpha \leftarrow \mathbb{Z}_n^*$. Set $W = g^w, U = h^\alpha, P_{pub} = g^\alpha$. The master secret key is MK = (α). The public parameter is *params* = $\big(H_a, H_b, H, g, h, n, g^{z_0}, \cdots, g^{z_{n'-1}}, W, U, P_{pub}\big)$.

Extract (MK, ID)**:** On input of the master secret key MK and a user's identity ID, compute $Q_{ID} = H(ID)$, the user's secret key is $S_{ID} = Q_{ID}^\alpha$.

Sign $(S_{ID}, R, M = (t,m) \in \{0,1\} \times \sum^{l \le L})$**:** We sketch how this algorithm works for a message of length l. Firstly, visualize a matrix with $(l+1)$ columns and $(\lfloor \lg l \rfloor + 2)$ rows. The columns correspond to the characters of the message, with a character in between each column. The rows correspond to the numbers lg$l$ down to 0, plus an extra row at the bottom. Each location (i_c, i_r) in the matrix (except along the bottom-most row) contains one or more out-going arrows. A "start" arrow goes down one row and over 2^{i_r} columns ending in $(i_c + 2^{i_r}, i_r - 1)$, if this end point is in the matrix. This type of arrow indicates that a quote starts here. A "one" arrow operates similarly to start arrows and is used to include characters after a start arrow includes the quote prefix. A "zero" arrow goes straight down one row ending in $(i_c, i_r - 1)$. This does not add any characters to the quoted substring. We refer the reader to [2] for more details about this.

This algorithm takes as input a signer's private key S_{ID}, a ring R of public keys, and a message M. No public key may appear twice in R, and R must include Q_{ID}. If $t = 1$, ring signatures produced by this algorithm are Type I as described below. If $t = 0$, the Type II signature can be obtained by running this algorithm and then running the Quote-Type II algorithm below to obtain a quote on the entire message. The message space is treated as $l \le L$ symbols from alphabet $\sum$. We use notation $m_{i,j}$ to denote the substring of m of length j starting at position i.

Let $d = |R|$, parse the elements of R as $Q_{ID_k} \in \mathbb{G}, 1 \le k \le d$. Let k^* be the index such that $Q_{ID_{k^*}} = Q_{ID}$. Define $\{f_k\}_{k=1}^d$ as $f_k = \begin{cases} 1 & \text{if } k = k^*, \\ 0 & \text{otherwise.} \end{cases}$

For $i = 3$ to $l+1$ and $j = 0$ to $\lfloor \lg(i-1) - 1 \rfloor$, choose random values $x_{i,j} \in \mathbb{Z}_n$. Set $x_{i,-1} := 0$ for all $i = 1$ to $l+1$.

- Choose random number u from $\mathbb{Z}_n^*$ and set $\bar{U} = h^u, \widehat{U} = h^{1/u}, \widetilde{U} = g^u$.
- For each $k, 1 \leq k \leq d$, choose random exponents s_k from $\mathbb{Z}_n^*$ and set

$$V_k = (Q_{ID_k}/W)^{f_k} h^{s_k}$$

$$\pi_{k1} = h^{s_k u}, \pi_{k2} = \left((Q_{ID_k}/W)^{2f_k - 1} h^{s_k}\right)^{1/u}, \pi_{k3} = g^{s_k u}, \pi_{k4} = g^{s_k}$$

- Let $s = \sum_{k=1}^{d} s_k$ and set $G = P_{pub}^s = g^{\alpha s}$.
- For $i = 1$ to l and $j = 0$ to $\lfloor \lg(l - i + 1) \rfloor$, for randomly chosen values $r_{i,j} \in \mathbb{Z}_n$:

$$B_{i,j} = H_b(m_{i,2^j})^{r_{i,j}} g^{-x_{i+2^j,j-1}} S_{ID} \cdot U^s, \qquad \widetilde{B_{i,j}} = g^{r_{i,j}}$$

- For $i = 3$ to l and $j = 0$ to $\min(\lfloor \lg(i-1) - 1 \rfloor, \lfloor \lg(l - i + 1) \rfloor)$, for randomly chosen values $r'_{i,j} \in \mathbb{Z}_n$:

$$A_{i,j} = H_a(m_{i,2^j})^{r'_{i,j}} g^{x_{i,j}} g^{-x_{i+2^j,j-1}}, \qquad \widetilde{A_{i,j}} = g^{r'_{i,j}}$$

- For $i = 3$ to $l+1$ and $j = 0$ to $\lfloor \lg(i-1) - 1 \rfloor$, for randomly chosen values $r''_{i,j} \in \mathbb{Z}_n$:

$$D_{i,j} = g^{x_{i,j}} g^{-x_{i,j-1}} g^{z_j \cdot r''_{i,j}}, \qquad \widetilde{D_{i,j}} = g^{r''_{i,j}}$$

The ring signature is $\sigma = \left(\bar{U}, \widehat{U}, \widetilde{U}, \{V_k, \pi_{k1}, \pi_{k2}, \pi_{k3}, \pi_{k4}\}_{k=1}^d, G, B_{i,j}, \widetilde{B_{i,j}}, A_{i,j}, \widetilde{A_{i,j}}, D_{i,j}, \widetilde{D_{i,j}}\right)$.

The values $\pi_{k1}, \pi_{k2}, \pi_{k3}$ and π_{k4} act as a proof that V_k is well-formed, which means that $f_k \in \{0, 1\}$.

Observe that, when there is exactly one non-zero value amongst $\{f_k\}$, say f_{k^*}, we have $W \cdot \prod_{k=1}^{d} V_k = Q_{ID^*} h^s$, so $\prod_{k=1}^{d} V_k$ serves as an encryption of the user's public key.

Quote $(\sigma, R, M = (t, m), M' = (t', m'))$: To derive a new ring signature on a substring M' of M, one roughly removes the group elements not associated with the new substring and then re-randomizes the remaining part of the ring signature. In addition, there is a second option in our quote algorithm that allows for the derivation of a short ring signature. However the quote procedure cannot be applied again to this short ring signature. Thus, we support quoting from quotes, and also provide a compression option which produces a very short quote, but the price for this is that it cannot be quoted from further.

First, check the validity of σ with respect to R and M. If it is not valid, output $\perp$. If M' is not a substring of M, output $\perp$. Otherwise, if $t' = 1$, output Quote-Type I (σ, R, m, m'); if $t' = 0$, output Quote-Type II (σ, R, m, m').

Quote-Type I (σ, R, m, m'): This quote algorithm takes a Type I signature and produces another Type I signature that maintains the ability to be quoted again.

If m' is not a substring of m, then output $\perp$. Otherwise, let $l' = |m'|$. Determine the first index δ at which substring m' occurs in m. Parse σ as a collection of $\bar{U}, \widehat{U}, \widetilde{U}, \{V_k, \pi_{k1}, \pi_{k2}, \pi_{k3}, \pi_{k4}\}_{k=1}^d, G, B_{i,j}, \widetilde{B_{i,j}}, A_{i,j}, \widetilde{A_{i,j}}, D_{i,j}, \widetilde{D_{i,j}}$ values.

Choose re-randomization values to re-randomize the $x_{i,j}$ terms of σ. For $i = 2$ to $l'+1$ and $j = 0$ to $\lfloor \lg(i-1) - 1 \rfloor$, choose random values $y_{i,j} \in \mathbb{Z}_n$. Set $y_{i,-1} := 0$ for all $i = 1$ to $l'+1$.

- Choose random number u' from $\mathbb{Z}_n^*$ and set $\bar{U}' = \bar{U}^{u'} = h^{uu'}, \widehat{U'} = \widehat{U}^{(1/u')} = h^{(1/uu')}, \widetilde{U'} = \widetilde{U}^{u'} = g^{uu'}$.
- For each $k, 1 \leq k \leq d$, choose random exponents s'_k from $\mathbb{Z}_n^*$ and set

$$V'_k = V_k \cdot h^{s'_k} = (Q_{ID_k}/W)^{f_k} h^{(s_k + s'_k)}$$

$$\pi'_{k1} = (\pi_{k1} \cdot \bar{U}^{s'_k})^{u'} = (h^{(s_k + s'_k)})^{uu'}, \qquad \pi'_{k2} = (\pi_{k2} \cdot \widehat{U}^{s'_k})^{(1/u')} = \left((Q_{ID_k}/W)^{2f_k - 1} h^{(s_k + s'_k)}\right)^{(1/uu')},$$

$$\pi'_{k3} = (\pi_{k3} \cdot \widetilde{U}^{s'_k})^{u'} = (g^{(s_k + s'_k)})^{uu'}, \qquad \pi'_{k4} = \pi_{k4} \cdot g^{s'_k} = g^{(s_k + s'_k)}$$

- Let $s' = \sum_{k=1}^{d} s'_k$ and set $G' = G \cdot P_{pub}^{s'} = g^{\alpha(s+s')}$.
- For $i = 1$ to l' and $j = 0$ to $\lfloor \lg(l'-i+1) \rfloor$, for randomly chosen $t_{i,j} \in \mathbb{Z}_n$:

$$B'_{i,j} = B_{i+\delta-1,j} \cdot H_b(m_{i+\delta-1,2^j})^{t_{i,j}} \cdot g^{-y_{i+2^j,j-1}} \cdot U^{\sum_{k=1}^{d} s'_k}, \qquad \widetilde{B'_{i,j}} = \widetilde{B_{i+\delta-1,j}} \cdot g^{t_{i,j}}$$

- For $i = 3$ to l' and $j = 0$ to $\min(\lfloor \lg(i-1)-1 \rfloor, \lfloor \lg(l'-i+1) \rfloor)$, for randomly chosen values $t'_{i,j} \in \mathbb{Z}_n$:

$$A'_{i,j} = A_{i+\delta-1,j} \cdot H_a(m_{i+\delta-1,2^j})^{t'_{i,j}} \cdot g^{y_{i,j}} \cdot g^{-y_{i+2^j,j-1}}, \qquad \widetilde{A'_{i,j}} = \widetilde{A_{i+\delta-1,j}} \cdot g^{t'_{i,j}}$$

- For $i = 3$ to $l'+1$ and $j = 0$ to $\lfloor \lg(i-1)-1 \rfloor$, for randomly chosen values $t''_{i,j} \in \mathbb{Z}_n$:

$$D'_{i,j} = D_{i+\delta-1,j} \cdot g^{y_{i,j}} \cdot g^{-y_{i,j-1}} \cdot g^{z_j \cdot t''_{i,j}}, \qquad \widetilde{D'_{i,j}} = \widetilde{D_{i+\delta-1,j}} \cdot g^{t''_{i,j}}$$

The ring signature is $\sigma' = \left(\bar{U}', \widehat{U'}, \widetilde{U'}, \{V'_k, \pi'_{k1}, \pi'_{k2}, \pi'_{k3}, \pi'_{k4}\}_{k=1}^{d}, G', B'_{i,j}, \widetilde{B'_{i,j}}, A'_{i,j}, \widetilde{A'_{i,j}}, D'_{i,j}, \widetilde{D'_{i,j}}\right)$.

Quote-Type II (σ, R, m, m'): This quote algorithm takes a Type I signature and produces a Type II signature. A Type II quote will trace a $(\lg l'+1)$-length path on those arrows through the matrix of the original Type I signature, where l' is the length of the quote. It always starts with a start arrow and then contains one and zero arrows according to the binary representation of the length of the quote. Intuitively, taking an arrow over a character includes it in the quote.

Consider the length l' written as a binary string. Let β be the largest index of $l' = |m'|$ that is set to 1, where we start counting with zero as the least significant bit. That is, set $\beta = \lfloor lg(l') \rfloor$. Select random values $v, v_{\beta-1}, \cdots, v_0 \in \mathbb{Z}_n$.

Choose random number u' from $\mathbb{Z}_n^*$ and set $\widetilde{U'} = \widetilde{U}^{u'} = g^{uu'}$.

For each $k, 1 \le k \le d$, choose random exponents s'_k from $\mathbb{Z}_n^*$ and set

$$V'_k = V_k \cdot h^{s'_k} = (Q_{ID_k}/W)^{f_k} h^{(s_k+s'_k)}$$

$$\begin{aligned}
\pi'_{k1} &= (\pi_{k1} \cdot \bar{U}^{s'_k})^{u'} & \pi'_{k2} &= (\pi_{k2} \cdot \widehat{U}^{s'_k})^{(1/u')} & \pi'_{k3} &= (\pi_{k3} \cdot \widetilde{U}^{s'_k})^{u'} & \pi'_{k4} &= \pi_{k4} \cdot g^{s'_k} \\
&= (h^{(s_k+s'_k)})^{uu'}, & &= \left((Q_{ID_k}/W)^{2f_k-1} h^{(s_k+s'_k)}\right)^{(1/uu')}, & &= (g^{(s_k+s'_k)})^{uu'}, & &= g^{(s_k+s'_k)}
\end{aligned}$$

Let $s' = \sum_{k=1}^{d} s'_k$ and set $G' = G \cdot P_{pub}^{s'} = g^{\alpha(s+s')}$.

Set the start position as $K' = B_{\delta,\beta} \cdot U^{\sum_{k=1}^{d} s'_k}$ and $\delta' = \delta + 2^\beta$. Then, from $j = \beta - 1$ down to 0, proceed as follows:

- If the jth bit of l' is 1, set $K' = K' \cdot A_{\delta',j} \cdot H_a(m_{\delta',2^j})^{v_j}$, and $Z'_j = \widetilde{A_{\delta',j}} \cdot g^{v_j}$, set $\delta' = \delta' + 2^j$;
- If the jth bit of l' is 0, set $K' = K' \cdot D_{\delta',j} \cdot g^{z_j \cdot v_j}$ and $Z'_j = \widetilde{D_{\delta',j}} \cdot g^{v_j}$.

To end, re-randomize as $K' = K' \cdot H_b(m_{\delta,2^\beta})^v$ and $\widetilde{B'} = \widetilde{B_{\delta,\beta}} \cdot g^v$.

Output the quote as $\sigma' = \left(\widetilde{U'}, \{V'_k, \pi'_{k1}, \pi'_{k2}, \pi'_{k3}, \pi'_{k4}\}_{k=1}^{d}, G', K', \widetilde{B'}, Z'_{\beta-1}, \cdots, Z'_0\right)$.

Verify $(R, M = (t,m), \sigma)$: Let $d = |R|$, parse the elements of R as $Q_{ID_k} \in \mathbb{G}, 1 \le k \le d$. Verify that no element is repeated in R and reject otherwise.

Parse Type I signature as $\sigma = \left(\bar{U}, \widehat{U}, \widetilde{U}, \{V_k, \pi_{k1}, \pi_{k2}, \pi_{k3}, \pi_{k4}\}_{k=1}^{d}, G, B_{i,j}, \widetilde{B_{i,j}}, A_{i,j}, \widetilde{A_{i,j}}, D_{i,j}, \widetilde{D_{i,j}}, \right)$. Parse Type II signature as $\sigma = \left(\widetilde{U}, \{V_k, \pi_{k1}, \pi_{k2}, \pi_{k3}, \pi_{k4}\}_{k=1}^{d}, G, K, \widetilde{B}, Z_{\beta-1}, \cdots, Z_0, \right)$.

Check first that the proofs $\{V_k, \pi_{k1}, \pi_{k2}, \pi_{k3}, \pi_{k4}\}_{k=1}^{d}$ are valid.

First check $\{V_k, \pi_{k1}, \pi_{k2}, \pi_{k3}, \pi_{k4}\}_{k=1}^{d} \in \mathbb{G}^{5d}$. Then, for each $k, 1 \le k \le d$, check whether

$e(V_k, V_k/(Q_{ID_k}/W)) \stackrel{?}{=} e(\pi_{k1}, \pi_{k2}), e(\pi_{k1}, g) \stackrel{?}{=} e(h, \pi_{k3})$ and $e(\pi_{k4}, \widetilde{U}) \stackrel{?}{=} e(g, \pi_{k3})$ hold.

If any of the proofs is invalid, reject.

Otherwise, set $V = \prod_{k=1}^{d} V_k$. Then, check whether $e(\prod_{k=1}^{d} \pi_{k4}, P_{pub}) \stackrel{?}{=} e(G,g)$ holds. If it is invalid, reject.

If $t = 1$, output **Verify-Type I**(R,m,σ). Otherwise, output **Verify-Type II**(R,m,σ).

Verify-Type I (R,m,σ)**:** Let $l = |m|$. Let $X_{i,j}$ denote $e(g,g)^{x_{i,j}}$.

The value $X_{i,-1} = 1$, since for all $i = 1$ to $l+1$, $x_{i,-1} = 0$.

For $i = 3$ to $l+1$ and $j = 0$ to $\lfloor \lg(i-1) - 1 \rfloor$, let $I = i - 2^{j+1}$ and $J = j+1$. Compute

$$X_{i,j} = \left(e\left(H_b(m_{I,2^J}), \widetilde{B_{I,J}} \right) \cdot e\left(WV, P_{pub} \right) \right) / e\left(B_{I,J}, g \right)$$

The verification accepts if and only if all of the following hold:

- For $i = 3$ to l and $j = 0$ to $\min(\lfloor \lg(i-1) - 1 \rfloor, \lfloor \lg(l-i+1) \rfloor)$,

$$e\left(A_{i,j}, g \right) = X_{i,j} / X_{i+2^j, j-1} \cdot e\left(H_a(m_{i,2^j}), \widetilde{A_{i,j}} \right) \tag{1}$$

- For $i = 3$ to $l+1$ and $j = 0$ to $\lfloor \lg(i-1) - 1 \rfloor$,

$$e(D_{i,j}, g) = X_{i,j} / X_{i,j-1} \cdot e\left(g^{z_j}, \widetilde{D_{i,j}} \right) \tag{2}$$

Verify-Type II (R,m,σ)**:** Let $l = |m|$ and β be the index of the highest bit of l that is set to 1.

Set $N = 1$ and $\delta = 1 + 2^{\beta}$. From $j = \beta - 1$ down to 0, proceed as follows:

- If the jth bit of l is 1, set $N = N \cdot e\left(H_a\left(m_{\delta,2^j} \right), Z_j \right)$ and $\delta = \delta + 2^j$;
- If the jth bit of l is 0, set $N = N \cdot e(g^{z_j}, Z_j)$.

Accept if and only if

$$e(K,g) = e\left(H_b\left(m_{1,2^{\beta}} \right), \widetilde{B} \right) \cdot e\left(WV, P_{pub} \right) \cdot N \tag{3}$$

5.4. Security Analysis

Theorem 1. *This identity-based quotable ring signature scheme is correct.*

PROOF. For the **Type I signature.**

Parse σ as the set of $\bar{U}, \widehat{U}, \widetilde{U}, \{V_k, \pi_{k1}, \pi_{k2}, \pi_{k3}, \pi_{k4}\}_{k=1}^{d}, G, B_{i,j}, \widetilde{B_{i,j}}, A_{i,j}, \widetilde{A_{i,j}}, D_{i,j}, \widetilde{D_{i,j}}$. Let $l = |m|$.

For $f_k = 1$,

$$\begin{aligned} e\left(V_k, V_k / (Q_{ID_k}/W) \right) &\stackrel{?}{=} e(\pi_{k1}, \pi_{k2}) \\ e\left((Q_{ID_k}/W) h^{s_k}, h^{s_k} \right) &\stackrel{?}{=} e\left(h^{s_k u}, \left((Q_{ID_k}/W) h^{s_k} \right)^{1/u} \right) \\ e\left((Q_{ID_k}/W) h^{s_k}, h^{s_k} \right) &= e\left(h^{s_k}, (Q_{ID_k}/W) h^{s_k} \right) \end{aligned}$$

For $f_k = 0$,

$$\begin{aligned} e\left(V_k, V_k / (Q_{ID_k}/W) \right) &\stackrel{?}{=} e(\pi_{k1}, \pi_{k2}) \\ e\left(h^{s_k}, h^{s_k} / (Q_{ID_k}/W) \right) &\stackrel{?}{=} e\left(h^{s_k u}, \left((Q_{ID_k}/W)^{-1} h^{s_k} \right)^{1/u} \right) \\ e\left(h^{s_k}, h^{s_k} (Q_{ID_k}/W)^{-1} \right) &= e\left(h^{s_k}, (Q_{ID_k}/W)^{-1} h^{s_k} \right) \end{aligned}$$

$e(\pi_{k1}, g) \stackrel{?}{=} e(h, \pi_{k3})$
$e(h^{s_k u}, g) = e(h, g^{s_k u})$

$e(\pi_{k4}, \widetilde{U}) \stackrel{?}{=} e(g, \pi_{k3})$
$e(g^{s_k}, g^{u}) = e(g, g^{s_k u})$

$e(\prod_{k=1}^{d} \pi_{k4}, P_{pub}) \stackrel{?}{=} e(G,g)$
$e(g^{s}, g^{\alpha}) = e(g^{\alpha s}, g)$

For $i = 3$ to $l+1$ and $j = 0$ to $\lfloor \lg(i-1) - 1 \rfloor$,

$$\begin{aligned}
X_{i,j} &= \left(e\left(H_b(m_{I,2^J}), \widetilde{B_{I,J}}\right) \cdot e\left(WV, P_{pub}\right)\right) / e\left(B_{I,J}, g\right) \\
&= \left(e\left(H_b(m_{i-2^{j+1},2^{j+1}}), \widetilde{B_{i-2^{j+1},j+1}}\right) \cdot e\left(Q_{ID} \cdot h^s, g^\alpha\right)\right) / e\left(B_{i-2^{j+1},j+1}, g\right) \\
&= \left(e\left(H_b(m_{i-2^{j+1},2^{j+1}}), g^{r_{i-2^{j+1},j+1}}\right) \cdot e\left(Q_{ID} \cdot h^s, g^\alpha\right)\right) / e\left(H_b\left(m_{i-2^{j+1},2^{j+1}}\right)^{r_{i-2^{j+1},j+1}} g^{-x_{i-2^{j+1}+2^{j+1},j+1-1}} S_{ID} \cdot U^s, g\right) \\
&= \left(e\left(H_b(m_{i-2^{j+1},2^{j+1}}), g^{r_{i-2^{j+1},j+1}}\right) \cdot e\left(Q_{ID} \cdot h^s, g^\alpha\right)\right) / e\left(H_b\left(m_{i-2^{j+1},2^{j+1}}\right)^{r_{i-2^{j+1},j+1}} g^{-x_{i,j}} Q_{ID}^\alpha \cdot h^{\alpha s}, g\right) \\
&= 1 / e\left(g^{-x_{i,j}}, g\right) \\
&= e(g,g)^{x_{i,j}}
\end{aligned}$$

For $i = 3$ to l and $j = 0$ to $\min(\lfloor \lg(i-1) - 1 \rfloor, \lfloor \lg(l-i+1) \rfloor)$,

$$\begin{aligned}
e(A_{i,j}, g) &= X_{i,j} / X_{i+2^j,j-1} \cdot e\left(H_a(m_{i,2^j}), \widetilde{A_{i,j}}\right) \\
e\left(H_a(m_{i,2^j})^{r'_{i,j}} g^{x_{i,j}} g^{-x_{i+2^j,j-1}}, g\right) &= e(g,g)^{x_{i,j}} / e(g,g)^{x_{i+2^j,j-1}} \cdot e\left(H_a(m_{i,2^j}), g^{r'_{i,j}}\right)
\end{aligned}$$

Both sides of equation (1) are equal.

For $i = 3$ to $l+1$ and $j = 0$ to $\lfloor \lg(i-1) - 1 \rfloor$,

$$\begin{aligned}
e(D_{i,j}, g) &= X_{i,j} / X_{i,j-1} \cdot e\left(g^{z_j}, \widetilde{D_{i,j}}\right) \\
e\left(g^{x_{i,j}} g^{-x_{i,j-1}} g^{z_j \cdot r''_{i,j}}, g\right) &= e(g,g)^{x_{i,j}} / e(g,g)^{x_{i,j-1}} \cdot e\left(g^{z_j}, g^{r''_{i,j}}\right)
\end{aligned}$$

Both sides of equation (2) are equal.

For the **Type II signature.**

Parse σ' as the set of $\widetilde{U'}, \{V'_k, \pi'_{k1}, \pi'_{k2}, \pi'_{k3}, \pi'_{k4}\}_{k=1}^d, G', K', \widetilde{B'}, Z'_{\beta-1}, \cdots, Z'_0$.

$K' = H_b\left(m_{\delta,2^\beta}\right)^{\left(r_{\delta,\beta}+v\right)} S_{ID} \cdot U^{(s+s')} \cdot \prod_{j<\beta, l'_j=1} H_a(m'_j)^{\left(r'_{\delta+\hat{s}_{j-1},j}+v_j\right)} \cdot \prod_{j'<\beta, l'_{j'}=0} g^{z_{j'}\left(r''_{\delta+\hat{s}_{j'-1},j'}+v_{j'}\right)}$

$\widetilde{B'} = g^{(r_{\delta,\beta}+v)}, (Z'_j)_{j<\beta,l'_j=1} = g^{\left(r'_{\delta+\hat{s}_{j-1},j}+v_j\right)}, (Z'_{j'})_{j'<\beta,l'_{j'}=0} = g^{\left(r''_{\delta+\hat{s}_{j'-1},j'}+v_{j'}\right)}$

$N' = \prod_{j<\beta,l'_j=1} e\left(H_a(m'_j), Z'_j\right) \cdot \prod_{j'<\beta,l'_{j'}=0} e\left(g^{z_j}, Z'_{j'}\right)$

For $f_k = 1$,

$$\begin{aligned}
e\left(V'_k, V'_k / (Q_{ID_k}/W)\right) &\stackrel{?}{=} e(\pi'_{k1}, \pi'_{k2}) \\
e\left((Q_{ID_k}/W) h^{(s_k+s'_k)}, h^{(s_k+s'_k)}\right) &\stackrel{?}{=} e\left((h^{(s_k+s'_k)})^{uu'}, \left((Q_{ID_k}/W) h^{(s_k+s'_k)}\right)^{(1/uu')}\right) \\
e\left((Q_{ID_k}/W) h^{(s_k+s'_k)}, h^{(s_k+s'_k)}\right) &= e\left(h^{(s_k+s'_k)}, (Q_{ID_k}/W) h^{(s_k+s'_k)}\right)
\end{aligned}$$

For $f_k = 0$,

$$\begin{aligned}
e\left(V'_k, V'_k / (Q_{ID_k}/W)\right) &\stackrel{?}{=} e(\pi'_{k1}, \pi'_{k2}) \\
e\left(h^{(s_k+s'_k)}, h^{(s_k+s'_k)} / (Q_{ID_k}/W)\right) &\stackrel{?}{=} e\left((h^{(s_k+s'_k)})^{uu'}, \left((Q_{ID_k}/W)^{-1} h^{(s_k+s'_k)}\right)^{(1/uu')}\right) \\
e\left(h^{(s_k+s'_k)}, h^{(s_k+s'_k)} (Q_{ID_k}/W)^{-1}\right) &= e\left(h^{(s_k+s'_k)}, (Q_{ID_k}/W)^{-1} h^{(s_k+s'_k)}\right)
\end{aligned}$$

$$\begin{aligned}
e(\pi'_{k1}, g) &\stackrel{?}{=} e(h, \pi'_{k3}) \\
e\left((h^{(s_k+s'_k)})^{uu'}, g\right) &= e\left(h, (g^{(s_k+s'_k)})^{uu'}\right)
\end{aligned}$$

$$
\begin{aligned}
e(\pi'_{k4}, \widetilde{U'}) &\stackrel{?}{=} e(g, \pi'_{k3}) \\
e\left(g^{(s_k+s'_k)}, g^{uu'}\right) &= e\left(g, (g^{(s_k+s'_k)})^{uu'}\right)
\end{aligned}
$$

$$
\begin{aligned}
e(\prod_{k=1}^{d} \pi'_{k4}, P_{pub}) &\stackrel{?}{=} e(G', g) \\
e(g^{(s+s')}, g^{\alpha}) &= e(g^{\alpha(s+s')}, g)
\end{aligned}
$$

The left side of equation (3)

$$
\begin{aligned}
& e(K', g) \\
&= e\left(H_b\left(m_{\delta,2^\beta}\right)^{\left(r_{\delta,\beta}+v\right)} S_{ID} \cdot U^{(s+s')} \cdot \prod_{j<\beta, l'_j=1} H_a(m'_j)^{\left(r'_{\delta+\hat{s}_{j-1},j}+v_j\right)} \cdot \prod_{j'<\beta, l'_{j'}=0} g^{z_{j'}\left(r''_{\delta+\hat{s}_{j'-1},j'}+v_{j'}\right)}, g\right)
\end{aligned}
$$

The right side of equation (3)

$$
\begin{aligned}
& e\left(H_b\left(m'_{1,2^\beta}\right), \widetilde{B}\right) \cdot e\left(WV', P_{pub}\right) \cdot N' \\
&= e\left(H_b\left(m_{\delta,2^\beta}\right), g^{\left(r_{\delta,\beta}+v\right)}\right) \cdot e\left(Q_{ID} \cdot h^{(s+s')}, g^{\alpha}\right) \cdot \prod_{j<\beta, l'_j=1} e\left(H_a(m'_j), Z'_j\right) \cdot \prod_{j'<\beta, l'_{j'}=0} e\left(g^{z_j}, Z'_{j'}\right)
\end{aligned}
$$

Both sides of equation (3) are equal.

Theorem 2. *This identity-based quotable ring signature scheme is anonymous against full key exposure under the assumption that the subgroup decision problem is hard.*

PROOF. The anonymity proof closely follows that given by Shacham and Waters for their ring signature scheme [26].

The proof proceeds in games. We define Game 0 as follows. Algorithm $\mathcal{B}$ is given the group order n (but not its factorization), the description of the group $\mathbb{G}$, together with generators g of $\mathbb{G}$ and h which is uniformly chosen from $\mathbb{G}_q$. $\mathcal{B}$ follows the Setup algorithm to obtain system parameters $(w, z_0, \cdots, z_{n'-1}, \alpha)$ and (W, U, P_{pub}). $\mathcal{B}$ also chooses three hash functions H_a, H_b, H and selects $\mathcal{ID} = \{ID_1, \cdots, ID_\xi\}$.

$\mathcal{B}$ runs $\mathcal{A}$, providing to it the description of the group $\mathbb{G}$, including its order n and the generators g and h. $\mathcal{B}$ also provides to $\mathcal{A}$ system parameters $(w, z_0, \cdots, z_{n'-1}, \alpha)$ and (W, U, P_{pub}), along with the description of the hash functions H_a, H_b, H, and the challenge public keys $\{Q_{ID_i}\}_{i=1}^{\xi}$. When $\mathcal{A}$ makes a ring signing query of the form (j, R, M), $\mathcal{B}$ responds with $\sigma = Sign(S_{ID_j}, R, M)$. Finally, $\mathcal{A}$ requests a challenge with the values (j_0, j_1, R, M). Algorithm $\mathcal{B}$ chooses a bit $b \leftarrow \{0, 1\}$, computes the challenge ring signature $\sigma = Sign(S_{ID_{j_b}}, R, M)$, and provides $\mathcal{A}$ with σ. In addition, the challenger provides $\mathcal{A}$ with the Extract oracle, which can be queried for any identity. Actually, as the secret key is also given to the adversary $\mathcal{A}$, ring signing queries and Extract queries could be answered by himself. Algorithm $\mathcal{A}$ finally outputs its guess b' for b. $\mathcal{B}$ outputs 1 if $b = b'$, 0 otherwise.

Game 1 is identical to Game 0, except for the h is uniformly chosen from $\mathbb{G}$.

Denote by $Adv_{\mathcal{B}}^{game-0}$ the advantage $\mathcal{B}$ has over $1/2$ in Game 0, and by $Adv_{\mathcal{B}}^{game-1}$ the advantage over $1/2$ it has in Game 1. We have $Adv_{\mathcal{B}}^{game-0} = Adv_{IDQRS,\mathcal{A}}^{anon-ke}$, since in Game 0 $\mathcal{A}$'s environment is exactly as specified in the anonymity game. Moreover, suppose that $\mathcal{B}$'s output were different in the two games. Then we could use $\mathcal{B}$, with $\mathcal{A}$ as a subroutine, to solve the subgroup decision problem: given generators (g, h) to test, we provide them to $\mathcal{B}$ and output 1 if $\mathcal{B}$ does. This gives a new algorithm $\mathcal{C}$ for which we have

$$
\begin{aligned}
Adv_{\mathcal{C}}^{sdp} &= \left| Pr[\mathcal{B} = 1 | h \stackrel{R}{\leftarrow} \mathbb{G}_q] - Pr[\mathcal{B} = 1 | h \stackrel{R}{\leftarrow} \mathbb{G}] \right| \\
& \frac{1}{2} \left| (2Pr[\mathcal{B} = 1, h \stackrel{R}{\leftarrow} \mathbb{G}_q] - 1) - (2Pr[\mathcal{B} = 1 | h \stackrel{R}{\leftarrow} \mathbb{G}] - 1) \right| \\
& \frac{1}{2} \left| (Adv_{\mathcal{B}}^{game-0} - Adv_{\mathcal{B}}^{game-1} \right|
\end{aligned}
$$

We argue that $Adv_{\mathcal{B}}^{game-1} = 0$, even if $\mathcal{A}$ is computationally unbounded. Consider the distinguishing challenge $\left(\bar{U}, \widehat{U}, \widetilde{U}, \{(V_k, \pi_{k1}, \pi_{k2}, \pi_{k3}, \pi_{k4})\}_{k=1}^{d}, G, B_{i,j}, \widetilde{B_{i,j}}, A_{i,j}, \widetilde{A_{i,j}}, D_{i,j}, \widetilde{D_{i,j}}, \right)$. For each k, we have $V_k = (Q_{ID_k}/W)^{f_k} h^{s_k}$ with $f_k \in \{0,1\}$ and $s_k \in \mathbb{Z}_n^*$. But when h is a generator of $\mathbb{G}$ there exist $\tau_{k0}, \tau_{k1} \in \mathbb{Z}_n$ and $\gamma \in \mathbb{Z}_n^*$ such that $V_k = (Q_{ID_k}/W)h^{\tau_{k1}} = h^{\tau_{k0}}$ and $g = h^{\gamma}$. Moreover, denoting by $(\pi_k | f_k = b)$ the values which $\pi_{k1}, \pi_{k2}, \pi_{k3}, \pi_{k4}$ are assigned if f_k is set to $b \in \{0,1\}$, we have

$$
\begin{aligned}
& (\pi_k | f_k = 1) \\
= \; & \left(\pi_{k1} = (h^{\tau_{k1}})^u, \pi_{k2} = ((Q_{ID_k}/W)h^{\tau_{k1}})^{1/u}, \pi_{k3} = (g^{\tau_{k1}})^u = (h^{\tau_{k1}})^{u\gamma}, \pi_{k4} = g^{\tau_{k1}} = (h^{\tau_{k1}})^{\gamma}\right) \\
= \; & \left(\pi_{k1} = (h^{\tau_{k0}}/(Q_{ID_k}/W))^u, \pi_{k2} = (h^{\tau_{k0}})^{1/u}, \pi_{k3} = (h^{\tau_{k0}}/(Q_{ID_k}/W))^{u\gamma}, \pi_{k4} = (h^{\tau_{k0}}/(Q_{ID_k}/W))^{\gamma}\right) \\
= \; & (\pi_k | f_k = 0)
\end{aligned}
$$

so for each k the tuple $(V_k, \pi_{k1}, \pi_{k2}, \pi_{k3}, \pi_{k4})$ is consistent with either $f_k = 0$ or $f_k = 1$, and $\mathcal{A}$ can gain no information from this part of the signature. The values $\bar{U}, \widehat{U}, \widetilde{U}, G, \widetilde{B_{i,j}}, A_{i,j}, \widetilde{A_{i,j}}, D_{i,j}, \widetilde{D_{i,j}}$ are unrelated to the choice of signer. Thus if $\mathcal{A}$ can gain information, it is only from $B_{i,j}$. But, having fixed $(\bar{U}, \widehat{U}, \widetilde{U}, \{(V_k, \pi_{k1}, \pi_{k2}, \pi_{k3}, \pi_{k4})\}_{k=1}^{d}, G, \widetilde{B_{i,j}}, A_{i,j}, \widetilde{A_{i,j}}, D_{i,j}, \widetilde{D_{i,j}})$, $B_{i,j}$ are fixed values to satisfy the verification equations. Specifically, letting $P_{pub} = g^{\alpha}, \widetilde{B_{i,j}} = g^{r_{i,j}}$, and $WV = g^c$ which serves as an encryption of the user's public key, we have $B_{i,j} = H_b(m_{i,2^j})^{r_{i,j}} g^{-x_{i+2^j,j-1}} \cdot g^{\alpha c}$. Thus these values give no information about whether $S_{ID_{j0}}$ or $S_{ID_{j1}}$ was used to generate the challenge signature, and $\mathcal{A}$ can do no better than guess b. This establishes $Adv_{\mathcal{B}}^{game-1} = 0$. We see that $Adv_{IDQRS,\mathcal{A}}^{anon-ke} \leq 2Adv_{\mathcal{C}}^{sdp}$. If $Adv_{IDQRS,\mathcal{A}}^{anon-ke}$ is non-negligible, then so is $Adv_{\mathcal{C}}^{sdp}$.

Theorem 3. *If the CDH assumption holds in $\mathbb{G}$, then this identity-based quotable ring signature scheme is selectively unforgeable in the random oracle model.*

PROOF. The algorithm that makes the reduction is given the factorization of n. This allows it to undo BGN blinding with h^s terms, and to recover from a signature the values f_k used in generating it.

Suppose an adversary $\mathcal{A}$ can produce a forgery, then we can construct an adversary $\mathcal{B}$ that breaks the CDH assumption.

On input the CDH challenge (g, g^a, g^b), $\mathcal{B}$ begins to run $\mathcal{A}$ and proceeds as follows:

$\mathcal{A}$ first announces the message M^* on which he will forge.

Let L be the maximum size of any message and let $n' = \lfloor lg(L) \rfloor$. Let $M^* = (t^*, m^*)$ and $l^* = |m^*|$ and let β be the highest bit of l^* set to 1 (numbering the least significant bit as zero). Let g be the generator of $\mathbb{G}$. Algorithm $\mathcal{B}$ is given $g_1, g_2 \in \mathbb{G}$. Here, $g_1 = g^a, g_2 = g^b$, and (g, g_1, g_2) is a random instance of the *CDH* problem. Its goal is to compute g^{ab}.

Algorithm $\mathcal{B}$ starts by setting $P_{pub} = g_1 = g^a, h = g^p, U = (g^a)^p = h^a$. $\mathcal{B}$ randomly selects $w \in \mathbb{Z}_n^*$ and set $W = g^w$. For $i = 0$ to $n' - 1$, choose a random $v_i \in \mathbb{Z}_n^*$ and set $g^{z_i} = \begin{cases} g^{bv_i} & \text{if the } i\text{th bit of } l^* \text{ is 1;} \\ g^{v_i} & \text{otherwise.} \end{cases}$

Algorithm $\mathcal{B}$ selects $\mathcal{ID} = \{ID_1, \cdots, ID_\xi\}$. Algorithm $\mathcal{B}$ sends $(g, h, n, g^{z_0}, \cdots, g^{z_{n'-1}}, W, U, P_{pub}, \mathcal{ID})$ to the algorithm $\mathcal{A}$. Algorithm $\mathcal{B}$ will simulate the oracles and interact with the forger $\mathcal{A}$ as described below.

- *H* **queries:** In the simulation, $\mathcal{B}$ maintains a list H-List of tuples $(ID_i, H(ID_i), \mu_i)$ as explained below. This list is initially empty.

  If the query ID_i already appears on the H-List in a tuple $(ID_i, H(ID_i), \mu_i)$, then algorithm $\mathcal{B}$ responds with $H(ID_i)$. Otherwise, for the ith new query ID_i, the following conditions are satisfied:

  - if $ID_i \notin \mathcal{ID}, \mathcal{B}$ chooses $\mu_i \in_R \mathbb{Z}_n^*$ and sets $H(ID_i) = g^{\mu_i}$. Then $\mathcal{B}$ adds $(ID_i, H(ID_i), \mu_i)$ to the H-List;
  - otherwise $ID_i \in \mathcal{ID}, \mathcal{B}$ chooses $\mu_i \in_R \mathbb{Z}_n^*$ and sets $H(ID_i) = g_2^{\mu_i} = g^{b\mu_i}$ where g_2 is in the instance of the *CDH* problem. Then $\mathcal{B}$ adds $(ID_i, H(ID_i), \mu_i)$ to the H-List.

  In either case, $H(ID_i)$ is returned to $\mathcal{A}$ as the answer.

- H_b **queries:** If the query has been made before, return the same response as before.

  Imagine dividing up m^* into a sequence of segments whose lengths are decreasing powers of two; that is, the first segment would be of length 2^β where β is the largest power of two less than l^*, the second segment would contain the next largest power of two, etc. Let $m^*_{(j)}$ denote the segment of m^* corresponding to power j. If no such segment exists, let $m^*_{(j)} = \perp$.

  Select a random $\eta \in \mathbb{Z}^*_n$ and return the response as:

  $$H_b(x) = \begin{cases} g^\eta & \text{if } |x| = 2^\beta \text{ and } m^*_{(\beta)} = x; \\ g^{b\eta} & \text{otherwise.} \end{cases}$$

  Note that $H_b(m^*_{(j)})$ is set according to the first method only for the first segment of m^*.

- H_a **queries:** If the query has been made before, return the same response as before. Otherwise, select a random $\theta \in \mathbb{Z}^*_n$ and return the response as:

  $$H_a(x) = \begin{cases} g^\theta & \text{if } |x| = 2^j \text{ and } j < \beta \text{ and } m^*_{(j)} = x \quad (x \text{ is on the selective path}); \\ g^{b\theta} & \text{otherwise} \quad (x \text{ is not on the selective path}). \end{cases}$$

  Note that $H_a(m^*_{(j)})$ is set according to the first method for all segments of m^* except the first segment $m^*_{(\beta)}$.

- **Extract queries:** If the query has been made before, return the same response as before. Otherwise, algorithm $\mathcal{B}$ checks H-List. If there is no tuple on the H-List containing ID_i, $\mathcal{B}$ will issue this query by itself to ensure that there is a tuple $(ID_i, H(ID_i), \mu_i)$ on the H-List. $\mathcal{B}$ creates and keeps one list Ex-List to simulate Extract oracle. At the beginning of the simulaiton, this list is empty.

  For each Extract query with respect to a user ID_i except for those in the set $\mathcal{ID}$, using the μ_i value in the record on H-List corresponding to ID_i, $\mathcal{B}$ computes and returns $S_{ID_i} = P^{\mu_i}_{pub} = g^{a\mu_i} = (g^{\mu_i})^a = Q^a_{ID_i}$ as the user ID_i's private key. Then, $\mathcal{B}$ records the tuple (ID_i, S_{ID_i}) in the Ex-List.

- **Sign queries:** For every query (i', R, M), check whether $ID_{i'} \in R$. If $ID_{i'}$ is not in the ring R, output $\perp$ to indicate the query is invalid. Otherwise, choose random number u from $\mathbb{Z}^*_n$ and set $\bar{U} = h^u, \hat{U} = h^{1/u}, \tilde{U} = g^u$.

  Let $d = |R|$, parse the elements of R as $Q_{ID_k} \in \mathbb{G}, 1 \le k \le d$. Define $\{f_k\}^d_{k=1}$ as $f_k = \begin{cases} 1 & \text{if } k = i', \\ 0 & \text{otherwise.} \end{cases}$

  For each $k, 1 \le k \le d$, choose random exponents s_k from $\mathbb{Z}^*_n$ and set

  $$V_k = (Q_{ID_k}/W)^{f_k} h^{s_k}$$

  $$\pi_{k1} = h^{s_k u}, \pi_{k2} = \left((Q_{ID_k}/W)^{2f_k - 1} h^{s_k}\right)^{1/u}, \pi_{k3} = g^{s_k u}, \pi_{k4} = g^{s_k}$$

  Let $s = \sum^d_{k=1} s_k$. Set $G = P^s_{pub} = g^{\alpha s}$.

  Let $M = (t, m)$ and $l = |m|$. Recall that β^* is the highest bit of l^* set to 1 and that we are counting up from zero as the least significant bit.

  We describe how to create signatures. If $ID_{i'} \notin \mathcal{ID}$, $S_{ID_{i'}}$ could be derived by querying the Extract oracle. Then the challenger could use $S_{ID_{i'}}$ to generate signatures via the normal Sign algorithm. Otherwise, the challenger could simulate signatures as follows.

  1. When $t = 1$ and m^* is not a substring of m (Type I Signature Generation):
     Here $m_{i,j}$ denotes the substring m of length j starting at position i. It will help us to first establish the variables $X_{i,j}$, which will be set to 1 if on the selective forgery path and 0 otherwise. We give a set of "rules" defining terms and make a few observations. Then we describe how the reduction algorithm creates the signatures.
     Rules.
     For $i = 1$ up to $l + 1$,
     For $j = \lfloor lg(l - i + 1) \rfloor$ down to -1,

(a) If $j+1=\beta^*$ and $m_{i-2^{j+1},2^{j+1}}=m^*_{(j+1)}$, then set $X_{i,j}=1$.
(b) Else, if $j+1<\beta^*$ and $(j+1)$th bit of l^* is 1 and $m_{i-2^{j+1},2^{j+1}}=m^*_{(j+1)}$ and $X_{i-2^{j+1},j+1}=1$, then set $X_{i,j}=1$.
(c) Else if $j+1<\beta^*$ and $(j+1)$th bit of l^* is 0 and $X_{i,j+1}=1$, then set $X_{i,j}=1$.
(d) Else set $X_{i,j}=0$.

Observations. Before we show how $\mathcal{B}$ will simulate the signatures, we make a set of useful observations.

(a) For all i and $j\geq\beta^*$, $X_{i,j}=0$.
(b) For all $i, X_{i,-1}=0$. Otherwise, $m_{i-l^*,l^*}=m^*$.
(c) For all i,j, if $X_{i,j}=1$ and $X_{i,j-1}=0$, then the jth bit of $l*$ is 1. If the jth bit were 0, then $X_{i,j-1}$ would have been set to 1 by Rule 1c.
(d) For all i,j, if $X_{i,j}=0$ and $X_{i,j-1}=1$, then the jth bit of $l*$ is 1. If the jth bit were 0, then the only way to set $X_{i,j-1}$ to 1 would be by Rule 1c, however, $X_{i,j}=0$ so Rule 1c does not apply.
(e) For all i,j, if $X_{i,j}=1$ and $X_{i+2^j,j-1}=0$, then $H_a(m_{i,2^j})=g^{b\theta}$ for some known $\theta\in\mathbb{Z}^*_n$. Otherwise, $X_{i+2^j,j-1}$ would have been set by Rule 1b to be 1.
(f) For all i,j, if $X_{i,j}=0$ and $X_{i+2^j,j-1}=1$, then $H_a(m_{i,2^j})=g^{b\theta}$ for some known $\theta\in\mathbb{Z}^*_n$. If $X_{i+2^j,j-1}=1$ and $X_{i,j}=0$, then $X_{i-2^j,j-1}$ was set to be 1 either by Rule 1a or Rule 1c. If it were Rule 1a, then $j=\beta^*$ and it follows from the programming of the random oracle that $H_a(m_{i,2^j})=g^{b\theta}$. If it were Rule 1c, then the jth bit of l^* is 0, meaning $m_{(j)}$ cannot be on the selective path and therefore again $H_a(m_{i,2^j})=g^{b\theta}$.
(g) For all i,j, if $X_{i+2^j,j-1}=0$, then $H_b(m_{i,2^j})=g^{b\eta}$ for some known $\eta\in\mathbb{Z}^*_n$. If $j\neq\beta^*$, this follows immediately from the programming of the random oracle. Otherwise, if $j=\beta^*$, then the only way for $X_{i+2^j,j-1}=0$ would be if $m_{(\beta)}\neq m^*_{(\beta)}$ by Rule 1a. Thus, it also follows that $H_b(m_{i,2^j})=g^{b\eta}$.

Signature Components. Next, for $i=1$ to $l+1$ and $j=0$ to $\lfloor lg(l-i+1)\rfloor$, choose a random $x'_{i,j}\in\mathbb{Z}_n$ and logically set $x_{i,j}=x'_{i,j}+X_{i,j}\cdot(ab\mu_{i'})$, where $\mu_{i'}$ has been used in the H-list corresponding to $ID_{i'}$. For $i=1$ to $l+1$, set $x_{i,-1}=0$ (as consistent with Observation 1b).
A signature is comprised of the following values:

– *Start.* For $i=1$ to l and $j=0$ to $\lfloor lg(l-i+1)\rfloor$:
(a) If $X_{i+2^j,j-1}=0$, then it follows by Observation 1g that $H_b(m_{i,2^j})=g^{b\eta}$ for some known $\eta\in\mathbb{Z}^*_n$, so choose random $\widehat{s_{i,j}}\in\mathbb{Z}_n$, implicitly set $r_{i,j}=-a\mu_{i'}/\eta+\widehat{s_{i,j}}$ and set

$$\begin{aligned}
B_{i,j} &= g^{-x'_{i+2^j,j-1}}g^{b\eta\widehat{s_{i,j}}}U^s\\
&= g^{-x_{i+2^j,j-1}}g^{b\eta(r_{i,j}+a\mu_{i'}/\eta)}h^{as}\\
&= (g^{b\eta})^{r_{i,j}}g^{-x_{i+2^j,j-1}}(g^{b\mu_{i'}})^a h^{as}\\
&= H_b(m_{i,2^j})^{r_{i,j}}g^{-x_{i+2^j,j-1}}S_{ID_{i'}}h^{as}\\
\widetilde{B_{i,j}} &= g^{-a\mu_{i'}/\eta+\widehat{s_{i,j}}}=g^{r_{i,j}}
\end{aligned}$$

(b) Else $X_{i+2^j,j-1}=1$, so choose random $r_{i,j}\in\mathbb{Z}_n$ and with $x_{i+2^j,j-1}=x'_{i+2^j,j-1}+ab\mu_{i'}$ set

$$\begin{aligned}
B_{i,j} &= H_b(m_{i,2^j})^{r_{i,j}}g^{-x'_{i+2^j,j-1}}U^s\\
&= H_b(m_{i,2^j})^{r_{i,j}}g^{-x_{i+2^j,j-1}}(g^{b\mu_{i'}})^a h^{as}\\
&= H_b(m_{i,2^j})^{r_{i,j}}g^{-x_{i+2^j,j-1}}S_{ID_{i'}}h^{as}\\
\widetilde{B_{i,j}} &= g^{r_{i,j}}
\end{aligned}$$

– *Across.* Together with the following values for $i=3$ to l and $j=0$ to $\min(\lfloor lg(i-1)-1\rfloor,\lfloor lg(l-i+1)\rfloor)$:

(a) If $X_{i,j}=1$ and $X_{i+2^j,j-1}=1$, choose random $r'_{i,j}\in\mathbb{Z}_n$ with implicitly set $x_{i,j}=x'_{i,j}+ab\mu_{i'}$ and $x_{i+2^j,j-1}=x'_{i+2^j,j-1}+ab\mu_{i'}$ and set

$$\begin{aligned} A_{i,j} &= H_a(m_{i,2^j})^{r'_{i,j}} g^{x'_{i,j}} g^{-x'_{i+2^j,j-1}} \\ &= H_a(m_{i,2^j})^{r'_{i,j}} g^{x_{i,j}} g^{-x_{i+2^j,j-1}} \\ \widetilde{A_{i,j}} &= g^{r'_{i,j}} \end{aligned}$$

(b) Else, if $X_{i,j}=1$ and $X_{i+2^j,j-1}=0$, then $H_a(m_{i,2^j})=g^{b\theta}$ for some known $\theta\in\mathbb{Z}_n^*$ by Observation 1e. Choose random $\widehat{s'_{i,j}}\in\mathbb{Z}_n$ with implicitly set $x_{i,j}=x'_{i,j}+ab\mu_{i'}, x_{i+2^j,j-1}=x'_{i+2^j,j-1}$ and $r'_{i,j}=-a\mu_{i'}/\theta+\widehat{s'_{i,j}}$ and set

$$\begin{aligned} A_{i,j} &= g^{x'_{i,j}} g^{-x'_{i+2^j,j-1}} g^{b\theta\widehat{s'_{i,j}}} \\ &= g^{(x_{i,j}-ab\mu_{i'})} g^{-x_{i+2^j,j-1}} g^{b\theta(r'_{i,j}+a\mu_{i'}/\theta)} \\ &= (g^{b\theta})^{r'_{i,j}} g^{x_{i,j}} g^{-x_{i+2^j,j-1}} \\ &= H_a(m_{i,2^j})^{r'_{i,j}} g^{x_{i,j}} g^{-x_{i+2^j,j-1}} \\ \widetilde{A'_{i,j}} &= g^{-a\mu_{i'}/\theta+\widehat{s'_{i,j}}} = g^{r'_{i,j}} \end{aligned}$$

(c) Else, if $X_{i,j}=0$ and $X_{i+2^j,j-1}=1$, then $H_a(m_{i,2^j})=g^{b\theta}$ for some known $\theta\in\mathbb{Z}_n^*$ by Observation 1f. Choose random $\widehat{s'_{i,j}}\in\mathbb{Z}_n$ with implicitly set $x_{i,j}=x'_{i,j}, x_{i+2^j,j-1}=x'_{i+2^j,j-1}+ab\mu_{i'}$ and $r'_{i,j}=a\mu_{i'}/\theta+\widehat{s'_{i,j}}$ and set

$$\begin{aligned} A_{i,j} &= g^{x'_{i,j}} g^{-x'_{i+2^j,j-1}} g^{b\theta\widehat{s'_{i,j}}} \\ &= g^{x_{i,j}} g^{(-x_{i+2^j,j-1}+ab\mu_{i'})} g^{b\theta(r'_{i,j}-a\mu_{i'}/\theta)} \\ &= (g^{b\theta})^{r'_{i,j}} g^{x_{i,j}} g^{-x_{i+2^j,j-1}} \\ &= H_a(m_{i,2^j})^{r'_{i,j}} g^{x_{i,j}} g^{-x_{i+2^j,j-1}} \\ \widetilde{A'_{i,j}} &= g^{a\mu_{i'}/\theta+\widehat{s'_{i,j}}} = g^{r'_{i,j}} \end{aligned}$$

(d) Else, $X_{i,j}=0$ and $X_{i+2^j,j-1}=0$, so choose random $r'_{i,j}\in\mathbb{Z}_n$ with implicitly set $x_{i,j}=x'_{i,j}$ and $x_{i+2^j,j-1}=x'_{i+2^j,j-1}$ and set

$$\begin{aligned} A_{i,j} &= H_a(m_{i,2^j})^{r'_{i,j}} g^{x'_{i,j}} g^{-x'_{i+2^j,j-1}} \\ &= H_a(m_{i,2^j})^{r'_{i,j}} g^{x_{i,j}} g^{-x_{i+2^j,j-1}} \\ \widetilde{A_{i,j}} &= g^{r'_{i,j}} \end{aligned}$$

– *Down.* Together with the following values for $i=3$ to $l+1$ and $j=0$ to $\lfloor lg(i-1)-1\rfloor$:

(a) If $X_{i,j}=1$ and $X_{i,j-1}=1$, choose random $r''_{i,j}\in\mathbb{Z}_n$ with implicitly set $x_{i,j}=x'_{i,j}+ab\mu_{i'}$ and $x_{i,j-1}=x'_{i,j-1}+ab\mu_{i'}$ and set

$$\begin{aligned} D_{i,j} &= g^{x'_{i,j}} g^{-x'_{i,j-1}} g^{z_j r''_{i,j}} = g^{x_{i,j}} g^{-x_{i,j-1}} g^{z_j r''_{i,j}} \\ \widetilde{D_{i,j}} &= g^{r''_{i,j}} \end{aligned}$$

(b) Else, if $X_{i,j}=1$ and $X_{i,j-1}=0$, then the jth bit of l^* is 1 by Observation 1c. Thus $z_j=bv_j$, so choose random $\widehat{s''_{i,j}}\in\mathbb{Z}_n$ with implicitly set $x_{i,j}=x'_{i,j}+ab\mu_{i'}, x_{i,j-1}=x'_{i,j-1}$, and $r''_{i,j}=-a\mu_{i'}/v_j+\widehat{s''_{i,j}}$ and set

$$\begin{aligned} D_{i,j} &= g^{x'_{i,j}} g^{-x'_{i,j-1}} g^{bv_j\widehat{s''_{i,j}}} = g^{x_{i,j}} g^{-x_{i,j-1}} g^{z_j r''_{i,j}} \\ \widetilde{D_{i,j}} &= g^{-a\mu_{i'}/v_j+\widehat{s''_{i,j}}} = g^{r''_{i,j}} \end{aligned}$$

(c) Else, if $X_{i,j}=0$ and $X_{i,j-1}=1$, then the jth bit of l^* is 1 by Observation 1d. Thus $z_j = bv_j$, so choose random $\widehat{s''_{i,j}} \in \mathbb{Z}_n$ with implicitly set $x_{i,j}=x'_{i,j}, x_{i,j-1}=x'_{i,j-1}+ab\mu_{i'}$, and $r''_{i,j}=a\mu_{i'}/v_j+\widehat{s''_{i,j}}$ and set

$$\begin{aligned} D_{i,j} &= g^{x'_{i,j}} g^{-x'_{i,j-1}} g^{bv_j\widehat{s''_{i,j}}} = g^{x_{i,j}} g^{-x_{i,j-1}} g^{z_j r''_{i,j}} \\ \widetilde{D_{i,j}} &= g^{a\mu_{i'}/v_j+\widehat{s''_{i,j}}} = g^{r''_{i,j}} \end{aligned}$$

(d) Else, $X_{i,j}=0$ and $X_{i,j-1}=0$, so choose random $r''_{i,j} \in \mathbb{Z}_n$ with implicitly set $x_{i,j}=x'_{i,j}$ and $x_{i,j-1}=x'_{i,j-1}$ and set

$$\begin{aligned} D_{i,j} &= g^{x'_{i,j}} g^{-x'_{i,j-1}} g^{z_j r''_{i,j}} = g^{x_{i,j}} g^{-x_{i,j-1}} g^{z_j r''_{i,j}} \\ \widetilde{D_{i,j}} &= g^{r''_{i,j}} \end{aligned}$$

$\mathcal{B}$ returns $\left(\bar{U},\widehat{U},\widetilde{U},\{V_k,\pi_{k1},\pi_{k2},\pi_{k3},\pi_{k4}\}_{k=1}^d, G, B_{i,j}, \widetilde{B_{i,j}}, A_{i,j}, \widetilde{A_{i,j}}, D_{i,j}, \widetilde{D_{i,j}}\right)$.

2. When $t=0$ and $m \neq m^*$ (Type II Signature Generation):
Let $l=|m|$, and $\beta = \lfloor lg(l) \rfloor$. l_i^* denotes i-th bit of l^* when we start counting with zero as the least significant bit, and l_i denotes i-th bit of l.
Parse m^* as $m^*_{\beta^*} m^*_{\beta^*-1} \cdots m^*_0$ where m_i^* is a string of length 2^i or a null string. m_i is of length 2^i if $l_i=1$, and is null otherwise. Similarly, Parse m as $m_\beta m_{\beta-1} \cdots m_0$.
$\mathcal{B}$ constructs $(K, \widetilde{B}, Z_{\beta-1}, \cdots, Z_0)$ in the following way:
   - If $m_\beta \neq m^*_{\beta^*}$, then $H_b(m_\beta) = g^{b\eta}$ for a η which is known to $\mathcal{B}$.
     (a) $\mathcal{B}$ sets $\widetilde{B} = g^{-a\mu_{i'}/\eta+r}$ for a randomly chosen r and $K = g^{b\eta r} U^s$.
     (b) For $j=\beta-1$ down to 0, $Z_j = g^{r_j}$ for a ranodmly chosen r_j, and
        * If $l_j=1$, then $K = K \cdot H_a(m_j)^{r_j}$.
        * If $l_j=0$, then $K = K \cdot g^{z_j r_j}$.
   - Otherwise, if $\beta=\beta^*$ and $m_\beta = m^*_{\beta^*}$, there exists $j_{\hat{s}} < \beta$ such that
        * $l_{j_{\hat{s}}} \neq l^*_{j_{\hat{s}}}$, or
        * $l_{j_{\hat{s}}} = l^*_{j_{\hat{s}}} = 1$ and $H_a(m_{j_{\hat{s}}}) \neq H_a(m^*_{j_{\hat{s}}})$.

     so $\mathcal{B}$ can construct a signature $(K, \widetilde{B}, Z_{\beta-1}, \cdots, Z_0)$ in the following way.
     (a) $\mathcal{B}$ sets $\widetilde{B} = g^{r_c}$ for a randomly chosen r_c and $K = g^{\eta r_c} U^s$.
     (b) For $j=\beta-1$ down to $j_{\hat{s}}+1$ and $j=j_{\hat{s}}-1$ to 0, $Z_j = g^{r_j}$ for randomly chosen r_j, and
        * If $l_j=1$, then $K = K \cdot H_a(m_j)^{r_j}$.
        * If $l_j=0$, then $K = K \cdot g^{z_j r_j}$.
     (c) For $j=j_{\hat{s}}$,
        * If $l_j=1$, whether $l_j^*=0$ or not, $\mathcal{B}$ knows θ such that $H_a(m_j)=g^{b\theta}$. $\mathcal{B}$ sets $Z_j = g^{-a\mu_{i'}/\theta+r_j}$ for a randomly chosen r_j, and $K = K \cdot g^{b\theta r_j}$.
        * If $l_j=0$ and $l_j^*=1$, then $\mathcal{B}$ knows v such that $g^{z_j}=g^{bv}$. $\mathcal{B}$ sets $Z_j = g^{-a\mu_{i'}/v+r_j}$ for a randomly chosen r_j, and $K = K \cdot g^{bvr_j}$.

   $\mathcal{B}$ returns $\left(\widetilde{U}, \{V_k,\pi_{k1},\pi_{k2},\pi_{k3},\pi_{k4}\}_{k=1}^d, G, K, \widetilde{B}, Z_{\beta-1}, \cdots, Z_0\right)$.

- **Response** Eventually, $\mathcal{A}$ outputs a valid signature σ^* on $M^*=(t^*,m^*)$ on behalf of R^*. Recall that $l^*=|m^*|$ and $\beta = \lfloor lg(l^*) \rfloor$. Here l_i^* denotes i-th bit of l^* when we start counting with zero as the least significant bit. Parse m^* as $m^*_\beta m^*_{\beta-1} \cdots m^*_0$ where m_i^* is a string of length 2^i (when $l_i^*=1$) or a null string (when $l_i^*=0$).

  Because of the selective disclosure and setup, $\mathcal{B}$ knows the following exponents:

  1. η such that $H_b(m^*_\beta) = g^\eta$.
  2. θ_j such that $H_a(m^*_{\hat{s}_j,2^j}) = g^{\theta_j}$ when $l_j^*=1$ and $j \neq \beta$.

3. z_j when $l_j^* = 0$.

t^* is either 1 or 0. As the challenger is given the factorization of n, this allows the challenger to recover from a signature the values f_k used in generating it. Therefore, the challenger knows the actual signer of σ^* and the corresponding $\mu_{i'}$ in the H-List.

– If $t^* = 1$,

$\hat{s}_i$ denotes the position where m_i^* starts. $\mathcal{B}$ can compute the information of some $x_{i,j}$ with the following components of σ^*.

∗ $B_{1,\beta} = H_b(m_\beta^*)^{r_{1,\beta}} g^{-x_{1+2^\beta,\beta-1}} g^{ab\mu_{i'}U^s}, \widetilde{B_{1,\beta}} = g^{r_{1,\beta}}$

$\mathcal{B}$ knows η such that $H_b(m_\beta^*) = g^\eta$, so $\mathcal{B}$ can compute $g^{-x_{1+2^\beta,\beta-1}} g^{ab\mu_{i'}U^s} = B_{1,\beta}/\widetilde{B_{1,\beta}}^\eta$.

∗ For $j = \beta - 1$ down to 0,

· when $l_j = 1, A_{\hat{s}_j,j} = H_a(m_j^*)^{r'_{\hat{s}_j,j}} g^{x_{\hat{s}_j,j}} g^{-x_{\hat{s}_{j-1},j-1}}, \widetilde{A_{\hat{s}_j,j}} = g^{r'_{\hat{s}_j,j}}$

$\mathcal{B}$ knows θ such that $H_a(m_j^*) = g^\theta$, so $\mathcal{B}$ can compute $g^{x_{\hat{s}_j,j}} g^{-x_{\hat{s}_{j-1},j-1}} = A_{\hat{s}_j,j}/\widetilde{A_{\hat{s}_j,j}}^\theta$.

· when $l_j = 0, D_{\hat{s}_j,j} = g^{x_{\hat{s}_j,j}} g^{-x_{\hat{s}_{j-1},j-1}} g^{z_j r''_{\hat{s}_j,j}}, \widetilde{D_{\hat{s}_j,j}} = g^{r''_{\hat{s}_j,j}}$

$\mathcal{B}$ knows z_j, so $\mathcal{B}$ can compute $g^{x_{\hat{s}_j,j}} g^{-x_{\hat{s}_{j-1},j-1}} = D_{\hat{s}_j,j}/\widetilde{D_{\hat{s}_j,j}}^{z_j}$.

so $\mathcal{B}$ can compute $g^{x_{\hat{s}_j,j}} g^{-x_{\hat{s}_{j-1},j-1}}$.

$\mathcal{B}$ has the values of $g^{x_{\hat{s}_j,j}} g^{-x_{\hat{s}_{j-1},j-1}}$ for $j = \beta - 1$ down to 0 and $g^{-x_{1+2^\beta,\beta-1}} g^{ab\mu_{i'}U^s}$, so can compute $g^{-x_{1+2^\beta,\beta-1}} g^{ab\mu_{i'}U^s} \prod_{j=0}^{\beta-1} g^{x_{\hat{s}_j,j}} g^{-x_{\hat{s}_{j-1},j-1}} = g^{ab\mu_{i'}U^s} g^{-x_{s_{-1},-1}} = g^{ab\mu_{i'}U^s}$.

Then, $\mathcal{B}$ can compute $g^{ab} = \left((g^{ab\mu_{i'}U^s})/G^p\right)^{1/\mu_{i'}}$.

– If $t^* = 0$,

$\mathcal{B}$ parses σ^* as $(K, \widetilde{B}, Z_{\beta-1}, \cdots, Z_0)$, with

$$\widetilde{B} = g^c, Z_{\beta-1} = g^{c_{\beta-1}}, \cdots, Z_0 = g^{c_0}$$

for some $c, c_{\beta-1}, \cdots, c_0 \in \mathbb{Z}_n$.

$$K = g^{ab\mu_{i'}U^s} \cdot H_b(m_\beta^*)^c \prod_{j<\beta, l_j^*=1} H_a(m_j^*)^{c_j} \prod_{j'<\beta, l_{j'}^*=0} (g^{z_{j'}})^{c_{j'}}$$

because the signature is valid.

∗ $\mathcal{B}$ knows η such that $H_b(m_\beta^*) = g^\eta$. $\mathcal{B}$ sets $N = \widetilde{B}^\eta$.

∗ From $j = \beta - 1$ down to 0, $\mathcal{B}$ proceeds as:

· If $l_j = 1$, $\mathcal{B}$ knows θ_j such that $H_a(m_j^*) = g^{\theta_j}$. $\mathcal{B}$ sets $N = N \cdot Z_j^{\theta_j}$;

· If $l_j = 0$, $\mathcal{B}$ knows z_j. $\mathcal{B}$ sets $N = N \cdot Z_j^{z_j}$.

Then

$$N = H_b(m_\beta^*)^c \prod_{j<\beta, l_j^*=1} H_a(m_j^*)^{c_j} \prod_{j'<\beta, l_{j'}^*=0} (g^{z_{j'}})^{c_{j'}}$$

so $\mathcal{B}$ can compute $K/N = g^{ab\mu_{i'}U^s}$.

Then, $\mathcal{B}$ can compute $g^{ab} = \left((g^{ab\mu_{i'}U^s})/G^p\right)^{1/\mu_{i'}}$.

Thus, whether t^* is 1 or 0, $\mathcal{B}$ can solve for g^{ab} and correctly answer to the CDH challenge.

Theorem 4. *This identity-based quotable ring signature scheme is strongly context hiding.*

PROOF. Given any two challenge messages $M=(t,m), M'=(t',m')$ such that m' is a substring of m, we claim that whether $t'=1$ or 0, $\sigma' \leftarrow \text{Quote}(\sigma,R,M,M')$ has an identical distribution to that of $\sigma \leftarrow \text{Sign}(S_{ID_i},R,M')$, which implies that the two distributions are statistically close.

$$\{(S_{ID_i}, \sigma \leftarrow Sign(S_{ID_i},R,M), Sign(S_{ID_i},R,M'))\}_{S_{ID_i},M,M'}$$

$$\{(S_{ID_i}, \sigma \leftarrow Sign(S_{ID_i},R,M), Quote(\sigma,R,M,M'))\}_{S_{ID_i},M,M'}$$

Let l, l' denote $|m|$ and $|m'|$ respectively. Let $\Gamma = min(\lfloor lg(i-1)-1 \rfloor, \lfloor lg(l-i+1) \rfloor)$. $\text{Sign}(S_{ID_i},R,M)$ is composed of the following values:

- $\bar{U}=h^u, \widehat{U}=h^{1/u}, \widetilde{U}=g^u$
- $V_k=(Q_{ID_k}/W)^{f_k}h^{s_k}, \pi_{k1}=h^{s_k u}, \pi_{k2}=\left((Q_{ID_k}/W)^{2f_k-1}h^{s_k}\right)^{1/u}, \pi_{k3}=g^{s_k u}, \pi_{k4}=g^{s_k}$, for each $1 \le k \le d$
- $G=P_{pub}^{s}=g^{\alpha s}$, where $s=\sum_{k=1}^{d} s_k$
- $B_{i,j}=H_b(m_{i,2^j})^{r_{i,j}}g^{-x_{i+2^j,j-1}}S_{ID}\cdot U^s, \quad \widetilde{B_{i,j}}=g^{r_{i,j}}$, for $i=1$ to l and $j=0$ to $\lfloor lg(l-i+1) \rfloor$
- $A_{i,j}=H_a(m_{i,2^j})^{r'_{i,j}}g^{x_{i,j}}g^{-x_{i+2^j,j-1}}, \quad \widetilde{A_{i,j}}=g^{r'_{i,j}}$, for $i=3$ to l and $j=0$ to $\min(\lfloor lg(i-1)-1 \rfloor, \lfloor lg(l-i+1) \rfloor)$
- $D_{i,j}=g^{x_{i,j}}g^{-x_{i,j-1}}g^{z_j\cdot r''_{i,j}}, \quad \widetilde{D_{i,j}}=g^{r''_{i,j}}$, for $i=3$ to $l+1$ and $j=0$ to $\lfloor lg(i-1)-1 \rfloor$

for randomly chosen $u \in \mathbb{Z}_n^*$ and $r_{i,j}, r'_{i,j}, r''_{i,j}, x_{i,j}, s_k \in \mathbb{Z}_n$.

- **Type I Signatures.** Let $\Gamma' = min(\lfloor lg(i-1)-1 \rfloor, \lfloor lg(l'-i+1) \rfloor)$. When $t'=1$, $\text{Sign}(S_{ID_i},R,M')$ is composed of the following values:
  - $\bar{U}''=h^{\tilde{u}}, \widehat{U}''=h^{1/\tilde{u}}, \widetilde{U}''=g^{\tilde{u}}$
  - $V''_k=(Q_{ID_k}/W)^{f_k}h^{\tilde{s}_k}, \pi''_{k1}=h^{\tilde{s}_k\tilde{u}}, \pi''_{k2}=\left((Q_{ID_k}/W)^{2f_k-1}h^{\tilde{s}_k}\right)^{1/\tilde{u}}, \pi''_{k3}=g^{\tilde{s}_k\tilde{u}}, \pi''_{k4}=g^{\tilde{s}_k}$, for each $1 \le k \le d$
  - $G''=P_{pub}^{\tilde{s}}=g^{\alpha\tilde{s}}$, where $\tilde{s}=\sum_{k=1}^{d}\tilde{s}_k$
  - $B''_{i,j}=H_b(m'_{i,2^j})^{\tilde{r}_{i,j}}g^{-\tilde{x}_{i+2^j,j-1}}S_{ID}\cdot U^{\tilde{s}}, \quad \widetilde{B''_{i,j}}=g^{\tilde{r}_{i,j}}$, for $i=1$ to l' and $j=0$ to $\lfloor lg(l'-i+1) \rfloor$
  - $A''_{i,j}=H_a(m'_{i,2^j})^{\widetilde{r'}_{i,j}}g^{x_{i,j}}g^{-\tilde{x}_{i+2^j,j-1}}, \quad \widetilde{A''_{i,j}}=g^{\widetilde{r'}_{i,j}}$, for $i=3$ to l' and $j=0$ to $\min(\lfloor lg(i-1)-1 \rfloor, \lfloor lg(l'-i+1) \rfloor)$
  - $D''_{i,j}=g^{\tilde{x}_{i,j}}g^{-\tilde{x}_{i,j-1}}g^{z_j\cdot\widetilde{r''}_{i,j}}, \quad \widetilde{D''_{i,j}}=g^{\widetilde{r''}_{i,j}}$, for $i=3$ to $l'+1$ and $j=0$ to $\lfloor lg(i-1)-1 \rfloor$

  for randomly chosen $\tilde{u} \in \mathbb{Z}_n^*$ and $\tilde{r}_{i,j}, \widetilde{r'}_{i,j}, \widetilde{r''}_{i,j}, \tilde{x}_{i,j}, \tilde{s}_k \in \mathbb{Z}_n$.

  And $\text{Quote}(\sigma,R,M,M')$ is Quote-Type I(σ,R,m,m'), which is comprised of the following:
  - $\bar{U}=h^{uu'}, \widehat{U}=h^{1/uu'}, \widetilde{U}=g^{uu'}$
  - $V_k=(Q_{ID_k}/W)^{f_k}h^{(s_k+s'_k)}, \pi_{k1}=h^{(s_k+s'_k)uu'}, \pi_{k2}=\left((Q_{ID_k}/W)^{2f_k-1}h^{(s_k+s'_k)}\right)^{1/uu'}, \pi_{k3}=g^{(s_k+s'_k)uu'}, \pi_{k4}=g^{(s_k+s'_k)}$, for each $1 \le k \le d$
  - $G=P_{pub}^{(s+s')}=g^{\alpha(s+s')}$, where $s=\sum_{k=1}^{d}s_k, s'=\sum_{k=1}^{d}s'_k$
  - $B_{i,j}=H_b(m'_{i,2^j})^{(r_{I,j}+t_{i,j})}g^{(-x_{I+2^j,j-1}-y_{i+2^j,j-1})}S_{ID}\cdot U^{(s+s')}, \quad \widetilde{B_{i,j}}=g^{(r_{I,j}+t_{i,j})}$, for $i=1$ to l and $j=0$ to $\lfloor lg(l-i+1) \rfloor$
  - $A_{i,j}=H_a(m'_{i,2^j})^{(r'_{I,j}+t'_{i,j})}g^{(x_{I,j}+y_{i,j})}g^{(-x_{I+2^j,j-1}-y_{i+2^j,j-1})}, \quad \widetilde{A_{i,j}}=g^{(r'_{I,j}+t'_{i,j})}$, for $i=3$ to l and $j=0$ to $\min(\lfloor lg(i-1)-1 \rfloor, \lfloor lg(l-i+1) \rfloor)$

– $D_{i,j} = g^{(x_{I,j}+y_{i,j})} g^{(-x_{I,j-1}-y_{i,j-1})} g^{z_j \cdot (r''_{I,j}+t''_{i,j})}$, $\widetilde{D_{i,j}} = g^{(r''_{I,j}+t''_{i,j})}$, for $i = 3$ to $l+1$ and $j = 0$ to $\lfloor lg(i-1)-1 \rfloor$

for randomly chosen $u' \in \mathbb{Z}_n^*$ and $t_{i,j}, t'_{i,j}, t''_{i,j}, y_{i,j}, s'_k \in \mathbb{Z}_n$, where m' occurs at position δ as a substring of m, $I = i + \delta - 1$.

Since all exponents have been independently re-randomized, one can see by inspection that Quote (σ, R, M, M') has identical distribution as that of Sign(S_{ID_i}, R, M').

- **Type II Signatures.** Parse $m' = m'_\beta m'_{\beta-1} \cdots m'_0$ where m'_j is of length 2^j or a null string where $\beta = \lfloor lg(l') \rfloor$. l'_i denotes i-th bit of l' when we start counting with zero as the least significant bit. m' occurs at position δ of m. Sign$(S_{ID_i}, R, M') = (K, \widetilde{B}, Z_{\beta-1}, \cdots, Z_0)$ is the following, for random $u \in \mathbb{Z}_n^*, s_k, \hat{u}, \hat{u}_i \in \mathbb{Z}_n$:
  - $\widetilde{U} = g^u$
  - $V_k = (Q_{ID_k}/W)^{f_k} h^{s_k}, \pi_{k1} = h^{s_k u}, \pi_{k2} = \left((Q_{ID_k}/W)^{2f_k - 1} h^{s_k}\right)^{1/u}, \pi_{k3} = g^{s_k u}, \pi_{k4} = g^{s_k}$, for each $1 \le k \le d$
  - $G = P_{pub}^s = g^{\alpha s}$, where $s = \sum_{k=1}^d s_k$
  - $K = g^{ab\mu_i} \cdot H_b(m'_\beta)^{\hat{u}} \cdot U^s \cdot \prod_{j<\beta, l'_j=1} H_a(m'_j)^{\hat{u}_j} \cdot \prod_{j'<\beta, l'_{j'}=0} g^{z_{j'} \hat{u}_{j'}}$
  - $\widetilde{B} = g^{\hat{u}}, Z_j = g^{\hat{u}_j}$

  Let each m'_j start at position $\hat{s}_j$ in m'. Quote(σ, R, M, M') = Quote-Type II(σ, R, m, m') is $(K, \widetilde{B}', Z'_{\beta-1}, \cdots, Z'_0)$ such that
  - $\widetilde{U}' = g^{uu'}$
  - $V'_k = (Q_{ID_k}/W)^{f_k} h^{(s_k+s'_k)}, \pi'_{k1} = h^{(s_k+s'_k)uu'}, \pi'_{k2} = \left((Q_{ID_k}/W)^{2f_k-1} h^{(s_k+s'_k)}\right)^{1/uu'}, \pi'_{k3} = g^{(s_k+s'_k)uu'}, \pi'_{k4} = g^{(s_k+s'_k)}$, for each $1 \le k \le d$
  - $G' = P_{pub}^{(s+s')} = g^{\alpha(s+s')}$, where $s = \sum_{k=1}^d s_k, s' = \sum_{k=1}^d s'_k$
  - $K' = g^{ab\mu_i} \cdot H_b(m'_\beta)^{(r_{\delta,\beta}+v)} \cdot U^{(s+s')} \cdot \prod_{j<\beta, l'_j=1} H_a(m'_j)^{(r'_{\delta+\hat{s}_j-1,j}+v_j)} \cdot \prod_{j'<\beta, l'_{j'}=0} g^{z_{j'}(r''_{\delta+\hat{s}_{j'}-1,j'}+v_{j'})}$
  - $\widetilde{B}' = g^{(r_{\delta,\beta}+v)}, (Z'_j)_{j<\beta, l'_j=1} = g^{(r'_{\delta+\hat{s}_j-1,j}+v_j)}, (Z'_{j'})_{j'<\beta, l'_{j'}=0} = g^{(r''_{\delta+\hat{s}_{j'}-1,j'}+v_{j'})}$

  for randomly chosen $u' \in \mathbb{Z}_n^*, s'_k, v, v_j \in \mathbb{Z}_n$. Since all exponents have been independently re-randomized, one can see by inspection that Quote(σ, R, M, M') has identical distribution as that of Sign(S_{ID_i}, R, M').

Thus, this identity-based quotable ring signature scheme is strongly context hiding.

6. Conclusion

We introduced a new notion of identity-based quotable ring signature based on bilinear paring in composite order groups. We extended the quotable signature to an identity-based ring signature scenario. Using this cryptographic primitive, anyone could derive new ring signatures on a substring of an original message from a ring signature on the original message. There are two different types of ring signatures. The first one could be quoted further down to these two types of signature. The other one could not be quoted any further, but will be a shorter signature. We also proved that our scheme is anonymous under the assumption that the Subgroup Decision Problem is hard, selectively unforgeable against adaptively chosen message attacks in the random oracle model under the assumption that the Computational Diffie-Hellman problem is hard, and strongly context hiding.

References

[1] M. Abe, M. Ohkubo, and K. Suzuki. 1-out-of-n signatures from a variety of keys. In Y. Zheng, editor, *Advances in Cryptology ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 415–432. Springer Berlin Heidelberg, 2002.

[2] J. H. Ahn, D. Boneh, J. Camenisch, S. Hohenberger, B. Waters, et al. Computing on authenticated data. In *Theory of Cryptography*, pages 1–20. Springer, 2012.

[3] G. Ateniese, D. Chou, B. de Medeiros, and G. Tsudik. Sanitizable signatures. In S. di Vimercati, P. Syverson, and D. Gollmann, editors, *Computer Security ESORICS 2005*, volume 3679 of *Lecture Notes in Computer Science*, pages 159–177. Springer Berlin Heidelberg, 2005.

[4] M. Bellare, O. Goldreich, and S. Goldwasser. Incremental cryptography: The case of hashing and signing. In Y. Desmedt, editor, *Advances in Cryptology CRYPTO 94*, volume 839 of *Lecture Notes in Computer Science*, pages 216–233. Springer Berlin Heidelberg, 1994.

[5] A. Bender, J. Katz, and R. Morselli. Ring signatures: Stronger definitions, and constructions without random oracles. In *Theory of Cryptography*, pages 60–79. Springer, 2006.

[6] D. Boneh and D. Freeman. Homomorphic signatures for polynomial functions. In K. Paterson, editor, *Advances in Cryptology EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 149–168. Springer Berlin Heidelberg, 2011.

[7] D. Boneh and D. Freeman. Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures. In D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, editors, *Public Key Cryptography PKC 2011*, volume 6571 of *Lecture Notes in Computer Science*, pages 1–16. Springer Berlin Heidelberg, 2011.

[8] D. Boneh, E.-J. Goh, and K. Nissim. Evaluating 2-dnf formulas on ciphertexts. In *Theory of cryptography*, pages 325–341. Springer, 2005.

[9] X. Boyen and B. Waters. Compact group signatures without random oracles. In S. Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 427–444. Springer Berlin Heidelberg, 2006.

[10] E. Bresson, J. Stern, and M. Szydlo. Threshold ring signatures and applications to ad-hoc groups. In M. Yung, editor, *Advances in Cryptology CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 465–480. Springer Berlin Heidelberg, 2002.

[11] C. Brzuska, H. Busch, O. Dagdelen, M. Fischlin, M. Franz, S. Katzenbeisser, M. Manulis, C. Onete, A. Peter, B. Poettering, and D. Schrder. Redactable signatures for tree-structured data: Definitions and constructions. In J. Zhou and M. Yung, editors, *Applied Cryptography and Network Security*, volume 6123 of *Lecture Notes in Computer Science*, pages 87–104. Springer Berlin Heidelberg, 2010.

[12] C. Brzuska, M. Fischlin, T. Freudenreich, A. Lehmann, M. Page, J. Schelbert, D. Schrder, and F. Volk. Security of sanitizable signatures revisited. In S. Jarecki and G. Tsudik, editors, *Public Key Cryptography PKC 2009*, volume 5443 of *Lecture Notes in Computer Science*, pages 317–336. Springer Berlin Heidelberg, 2009.

[13] C. Brzuska, M. Fischlin, A. Lehmann, and D. Schrder. Unlinkability of sanitizable signatures. In P. Nguyen and D. Pointcheval, editors, *Public Key Cryptography PKC 2010*, volume 6056 of *Lecture Notes in Computer Science*, pages 444–461. Springer Berlin Heidelberg, 2010.

[14] J. Camenisch. Efficient and generalized group signatures. In W. Fumy, editor, *Advances in Cryptology EUROCRYPT 97*, volume 1233 of *Lecture Notes in Computer Science*, pages 465–479. Springer Berlin Heidelberg, 1997.

[15] E.-C. Chang, C. Lim, and J. Xu. Short redactable signatures using random trees. In M. Fischlin, editor, *Topics in Cryptology CT-RSA 2009*, volume 5473 of *Lecture Notes in Computer Science*, pages 133–147. Springer Berlin Heidelberg, 2009.

[16] D. Chaum and E. van Heyst. Group signatures. In D. Davies, editor, *Advances in Cryptology EUROCRYPT 91*, volume 547 of *Lecture Notes in Computer Science*, pages 257–265. Springer Berlin Heidelberg, 1991.

[17] S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17(2):281–308, 1988.

[18] J. Groth, R. Ostrovsky, and A. Sahai. Perfect non-interactive zero knowledge for np. In *Advances in Cryptology-EUROCRYPT 2006*, pages 339–358. Springer, 2006.

[19] J. Herranz. A formal proof of security of zhang and kim's id-based ring signature scheme. *WOSIS*, 4:63–72, 2004.

[20] J. Herranz and G. Sáez. Forking lemmas for ring signature schemes. In T. Johansson and S. Maitra, editors, *Progress in Cryptology - INDOCRYPT 2003*, volume 2904 of *Lecture Notes in Computer Science*, pages 266–279. Springer Berlin Heidelberg, 2003.

[21] J. Herranz and G. Sáez. A provably secure id-based ring signature scheme. In *eprint*. Citeseer, 2003.

[22] R. Johnson, D. Molnar, D. Song, and D. Wagner. Homomorphic signature schemes. In B. Preneel, editor, *Topics in Cryptology CT-RSA 2002*, volume 2271 of *Lecture Notes in Computer Science*, pages 244–262. Springer Berlin Heidelberg, 2002.

[23] C.-Y. Lin and T.-C. Wu. An identity-based ring signature scheme from bilinear pairings. In *2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA)*, volume 2, pages 182–182. IEEE Computer Society, 2004.

[24] R. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In C. Boyd, editor, *Advances in Cryptology ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 552–565. Springer Berlin Heidelberg, 2001.

[25] R. Rivest, A. Shamir, and Y. Tauman. How to leak a secret: Theory and applications of ring signatures. In O. Goldreich, A. Rosenberg, and A. Selman, editors, *Theoretical Computer Science*, volume 3895 of *Lecture Notes in Computer Science*, pages 164–186. Springer Berlin Heidelberg, 2006.

[26] H. Shacham and B. Waters. Efficient ring signatures without random oracles. In T. Okamoto and X. Wang, editors, *Public Key Cryptography PKC 2007*, volume 4450 of *Lecture Notes in Computer Science*, pages 166–180. Springer Berlin Heidelberg, 2007.

[27] A. Shamir. Identity-based cryptosystems and signature schemes. In G. Blakley and D. Chaum, editors, *Advances in Cryptology*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer Berlin Heidelberg, 1985.

[28] C. Tang, Z. Liu, and M. Wang. An improved identity-based ring signature scheme from bilinear pairings. *NM Research Preprints*, pages 231–234, 2003.

[29] F. Zhang and K. Kim. Id-based blind signature and ring signature from pairings. In Y. Zheng, editor, *Advances in Cryptology ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 533–547. Springer Berlin Heidelberg, 2002.