Relations Among Security Notions for Undeniable Signature Schemes

Kaoru Kurosawa[1] and Swee-Huay Heng[2]

[1] Department of Computer and Information Sciences,
Ibaraki University,
4-12-1 Nakanarusawa, Hitachi, Ibaraki 316-8511, Japan
kurosawa@mx.ibaraki.ac.jp
[2] Centre for Cryptography and Information Security,
Faculty of Information Science and Technology,
Multimedia University,
Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia
shheng@mmu.edu.my

Abstract. In this paper, we conduct a thorough study among various notions of security of undeniable signature schemes and establish some relationships among them. We focus on two adversarial goals which are unforgeability and invisibility and two attacks which are chosen message attack and full attack. In particular,we show that unforgeability against chosen message attack is equivalent to unforgeability against full attack, and invisibility against chosen message attack is equivalent to invisibility against full attack. We also present an undeniable signature scheme whose unforgeability is based on the factoring assumption and whose invisibility is based on the composite decision Diffie-Hellman assumption.

Keywords: Undeniable signature, security notions, factoring assumption, composite decision Diffie-Hellman assumption.

1 Introduction

The concept of undeniable signatures was introduced by Chaum and van Antwerpen in 1989 [10]. As opposed to the ordinary digital signatures which are universally verifiable, the validity and invalidity of undeniable signatures can be verified only by executing with the signer or the designated confirmer through a confirmation protocol and a disavowal protocol respectively. Various variants of undeniable signature schemes which possess variable degrees of security and additional features have emerged in the literature over the past 16 years. While it is impossible to list them all, we note some important papers such as [7,5,11,9,8,20,12,16,6,15,14,23,24,25,26,21]. Most of these schemes are discrete logarithm based, with the exception of a few RSA-based schemes [16,15,14], a pairing-based (identity-based) scheme [23] and some other schemes [24,25].

Meanwhile, Bellare et al. showed relations among security notions for public-key encryption schemes [2]. Due to the importance of the above studies, recently we can see an increasing effort in the studying of relations among various security

R. De Prisco and M. Yung (Eds.): SCN 2006, LNCS 4116, pp. 34–48, 2006.

notions of cryptographic schemes [3,1,13]. Indeed, by knowing the relationships between the various security notions, one can save much effort to prove the individual security notion since it is sufficient to prove the simpler security notion if it also implies that the scheme fulfills other more complicated notions of security.

In this paper, we conduct a thorough study among various notions of undeniable signature schemes and show some relationships among them. We focus on the notions of *unforgeability* and *invisibility*. The first security notion is similar to the one for ordinary digital signatures, which is the notion of existential unforgeability against adaptive chosen message attack [19]. However, for undeniable signatures, the approach to adapt the previous security by allowing the confirmation/disavowal oracle access has been first considered in [12]. The second security notion is essentially the inability to determine whether a given message-signature pair is valid or not. This notion was first introduced by Chaum, van Heijst and Pfitzmann [11] and further enhanced in [6] and [14].

For each of unforgeability (UF) and invisibility (IV), we consider two different attacks, chosen message attack (CMA) and full attack (FULL). By chosen message attack, we mean that the adversary is only allowed to access to the signing oracle, which is similar to the basic chosen message attack considered in [19]. By full attack, we mean that besides the signing oracle access, the adversary is also allowed to access to the confirmation/disavowal oracle. No effort has been put in previously to study the above notions of security and we note that the results we obtain are somewhat surprising.

By combining the above two adversarial goals and two attacks, we can classify them under four notions of security, namely UF-CMA, UF-FULL, IV-CMA and IV-FULL. The rigorous definitions of the respective notions will be provided in Section 3. In particular, we establish an equivalent result between UF-CMA and UF-FULL, and an equivalence between IV-CMA and IV-FULL if the underlying signature scheme is UF-CMA. We also show that IV-CMA implies UF-CMA if the signing algorithm is deterministic. (We assume that the confirmation protocol and the disavowal protocol are perfect auxiliary-input zero-knowledge.)

More precisely, the relationships among various notions of security that we obtain can be shown as follows:

$$\begin{array}{ccc} \text{UF-CMA} & \Longleftrightarrow & \text{UF-FULL} \\ \Uparrow & & \\ \text{IV-CMA} & \Longleftrightarrow & \text{IV-FULL} \end{array}$$

We remark that the related study on the relationships between two notions of unforgeability of message authentication has been recently conducted by Bellare, Goldreich and Mityagin [3], i.e. they explored the unforgeability of message authentication by considering a single verification attempt and multiple verification attempts respectively by the adversary. They also commented that the multiple verification version of the definition of ordinary digital signatures is clearly equivalent to the standard definition in [19] since verification takes place under a key that is public and which is available to the adversary. However, obviously

this is not the case for undeniable signatures since without the consent of the signer or designated confirmer, it is impossible that the adversary can verify the validity or invalidity of a message-signature pair.

The first RSA-based undeniable signature scheme was proposed by Gennaro, Krawczyk and Rabin [16] where they employed the RSA moduli which is a product of safe primes. An extension of the above scheme to allow the use of general RSA moduli was made possible by Galbraith, Mao and Paterson [15]. However, both the above schemes do not have invisibility. Galbraith and Mao [14] showed an improved version which possesses the property of unforgeability and invisibility in the case of RSA moduli which is a product of safe primes.

In this paper, we also present an undeniable signature scheme such that its unforgeability is based on the factoring assumption and its invisibility is based on the composite decision Diffie-Hellman (CDDH) assumption. In the proposed scheme, the size of the signatures is much shorter than the scheme by Galbraith and Mao [14]. Its security can be easily proven by using the relationships we described earlier.

1.1 Organization

The remainder of this paper is organized as follows. In Section 2, we recall the definition of undeniable signatures. In Section 3, we provide the rigorous definitions for the four notions of security: UF-CMA, UF-FULL, IV-CMA and IV-FULL. In Section 4, we conduct a thorough study on the various notions of security of undeniable signatures and establish some important relationships among them. All the related security analyses are given accordingly. In Section 5, we present a new undeniable signature scheme whose unforgeability is based on the factoring assumption and whose invisibility is based on the composite decision Diffie-Hellman assumption. Finally, we conclude this paper in Section 6.

2 Undeniable Signatures

Throughout this paper, k denotes the security parameter and a PPT algorithm denotes a probabilistic polynomial-time algorithm.

An undeniable signature scheme consists of a key generation algorithm G_{sign}, a signing algorithm Sign , a confirmation protocol and a disavowal protocol. We consider undeniable signature schemes such that the confirmation protocol and the disavowal protocol are perfect zero-knowledge in the auxiliary-input model. Hence, we denote an undeniable signature scheme by $\Sigma = (\mathsf{G}_{sign}, \mathsf{Sign})$. G_{sign} is a PPT algorithm which generates (vk, sk), where vk is a verification key and sk is the signing key. Sign is a PPT algorithm which generates a signature σ on input a message m and the signing key sk. We say that (m, σ) is valid if σ is an output of $\mathsf{Sign}(sk, m)$.

An undeniable signature scheme must satisfy unforgeability and invisibility. Invisibility means that for a message m, the receiver cannot tell if σ is a valid signature or a random string. This implies that the receiver cannot verify the validity of (m, σ) by himself. Instead, the cooperation of the signer is needed to

prove the validity and invalidity of (m, σ) by running a confirmation protocol and a disavowal protocol with the receiver respectively.

Zero-knowledgeness means that the verifier can generate the communication transcript of the protocol by himself. Hence he cannot prove to the third party that (m, σ) is valid by showing the transcript of the ZK confirmation protocol. This is the central requirement for undeniable signature schemes.

We describe the formal definition of perfect auxiliary-input zero-knowledge below:

Definition 1. *[18,17] A proof system (P, V) is perfect auxiliary-input zero-knowledge on a language L if, for every PPT verifier V^* and every polynomial p, there exists a PPT algorithm M^* such that*

$$\{(P, V^*(y))(x)\}_{x \in L, y \in \{0,1\}^{p(|x|)}} \equiv \{M^*(x, y)\}_{x \in L, y \in \{0,1\}^{p(|x|)}}$$

where the first distribution ensemble denotes the output of V^* when having auxiliary-input y and interacting with prover P on common input $x \in L$; and the second distribution ensemble denotes the output of M^* on inputs $x \in L$ and $y \in \{0,1\}^{p(|x|)}$.

An alternative definition is to require M^* to simulate the *history* of V^*'s interaction with P [17, Remark 3.2].

As shown in [17], auxiliary-input zero-knowledge is preserved under sequential composition. Almost all known zero-knowledge proofs are in fact auxiliary-input zero-knowledge.

3 Definitions of Security

For each of unforgeability (UF) and invisibility (IV), we consider two different attacks, chosen message attack (CMA) and full attack (FULL). By combining two adversarial goals and two attacks, we have the following four notions of security, namely, UF-CMA, UF-FULL, IV-CMA and IV-FULL.

In each attack game, we say that a message-signature pair (m, σ) is unfresh if the adversary A has already queried m to the signing oracle and received σ. Otherwise, we say that (m, σ) is fresh.

3.1 Unforgeability

The unforgeability against CMA (UF-CMA) is defined as follows. Consider the following game between a challenger and an adversary A.

1. The challenger generates a key pair (vk, sk) randomly, and gives the verification key vk to A.
2. For $i = 1, \ldots, q$, A queries a message m_i to the signing oracle adaptively and receives a signature σ_i.
3. Eventually, A outputs a forgery (m^*, σ^*).

A wins the game if (m^*, σ^*) is valid and fresh.

Definition 2. *We say that Σ is unforgeable against CMA (UF-CMA) if* $\Pr(A \text{ wins})$ *is negligible for any PPT adversary A in the above game.*

To define the unforgeability against the full attack (UF-FULL), we modify the game against CMA as follows. We allow the adversary A to query (m, σ) to the confirmation/disavowal oracle adaptively at step 2. The confirmation/disavowal oracle responds as follows.

- If (m, σ) is a valid pair, then the oracle returns a bit $\mu = 1$ and proceeds with the execution of the confirmation protocol with A.
- Otherwise, the oracle returns a bit $\mu = 0$ and executes the disavowal protocol with A accordingly.

A wins the game if A outputs a valid and fresh pair (m^*, σ^*) or it queries a valid and fresh pair (m^*, σ^*) to the confirmation/disavowal oracle.

Definition 3. *We say that Σ is unforgeable against the full attack (UF-FULL) if* $\Pr[A \text{ wins}]$ *is negligible for any PPT adversary A in the above game.*

Remark 1. If the signing algorithm is probabilistic, there are many signatures σ for a fixed message m. In this case, we can consider weak forgery and strong forgery. In the weak forgery, an adversary wins if she can forge (m^*, σ^*) such that m^* has never been queried to the signing oracle by the adversary. In the strong forgery, an adversary wins if she can forge (m^*, σ^*) such that σ^* has never been returned by the signing oracle for a query m^*.

In the above definitions, we consider strong forgery. Note that strongly unforgeable undeniable signature schemes are more secure than weakly unforgeable ones.

If the signing algorithm is deterministic, the two types of forgery coincide.

3.2 Invisibility

The invisibility against CMA (IV-CMA) is defined by using the following game between a challenger and an adversary A.

1. The challenger generates a key pair (vk, sk) randomly, and gives the verification key vk to A.
2. A is permitted to issue a series of signing queries to the signing oracle adaptively and receives a signature σ_i.
3. At some point, A chooses a message m^* and sends it to the challenger.
4. The challenger chooses a random bit b. If $b = 1$, then he computes a signature σ^* on m^*. Otherwise, he chooses σ^* randomly from the signature space S. He then returns σ^* to A.
5. A performs some signing queries again[1].
6. At the end of this attack game, A outputs a guess b'.

[1] If the signing algorithm is deterministic, then A is not allowed to query m^* to the signing oracle.

Definition 4. *We say that Σ is invisible against CMA (IV-CMA) if* $|\Pr[b = b'] - 1/2|$ *is negligible for any PPT adversary A in the above game.*

Finally, to define the invisibility against full attack (IV-FULL), we modify the previous game (IV-CMA) as follows. We allow the adversary A to query (m, σ) to the confirmation/disavowal oracle adaptively at step 2 and at step 5, where A is not allowed to query the challenge (m^*, σ^*) to the confirmation/disavowal oracle at step 5. The confirmation/disavowal oracle responds as follows.

- If (m, σ) is a valid pair, then the oracle returns a bit $\mu = 1$ and proceeds with the execution of the confirmation protocol with A.
- Otherwise, the oracle returns a bit $\mu = 0$ and executes the disavowal protocol with A accordingly.

Definition 5. *We say that Σ is invisible against the full attack (IV-FULL) if* $|\Pr[b = b'] - 1/2|$ *is negligible for any PPT adversary A in the above game.*

We now say that

- Σ is CMA-secure if it is unforgeable against CMA attack (UF-CMA) and invisible against CMA attack (IV-CMA).
- Σ is fully secure if it is unforgeable against the full attack (UF-FULL) and invisible against the full attack (IV-FULL).

4 Relations Among Security Notions

We use the following notation.

- $X \Longrightarrow Y$: Any undeniable signature scheme Σ meets the security notion of Y if it meets the security notion of X. In this case, we say that X implies Y.
- $X \Longleftrightarrow Y$: Any undeniable signature scheme Σ meets the security notion of Y if and only if it meets the security notion of X. In this case, we say that X and Y are equivalent.

We first show that UF-CMA and UF-FULL are equivalent. That is,

$$\text{UF-CMA} \Longleftrightarrow \text{UF-FULL}.$$

Theorem 1. *UF-CMA and UF-FULL are equivalent if the confirmation protocol and the disavowal protocol are perfect auxiliary-input zero-knowledge.*[2]

Proof. It is clear that UF-FULL $\Longrightarrow$ UF-CMA. Therefore, we will show that UF-CMA $\Longrightarrow$ UF-FULL. Suppose that there exists an adversary A which breaks UF-FULL. We will construct an adversary A' which breaks UF-CMA by using A as a subroutine.

[2] We consider strong unforgeability as mentioned in Remark 1 of Section 3.1.

On input a verification key vk, A' starts running A by feeding A with vk. If A makes a signing query for a message m_i, then A' queries m_i to her signing oracle. A' receives a signature σ_i from the signing oracle, and returns σ_i to A.

Next, we consider the case when A makes a confirmation/disavowal query. Let q_v be the number of queries that A issues to the confirmation/disavowal oracle. For convenience, we consider that the final output of A is the $(q_v + 1)$-th query. We say that (m_i, σ'_i) is special if it is a valid and fresh message-signature pair queried by A to the confirmation/disavowal oracle. A' guesses the first special query. More precisely, A' guesses the first i such that the i-th query (m_i, σ'_i) is special. So, at the beginning, A' chooses $Guess \in \{1, 2, \cdots, q_v + 1\}$ randomly. There are two cases to be considered here, namely, $i < Guess$ and $i = Guess$. First suppose that $i < Guess$.

- If A has never made a signing query for m_i, then A' returns $\mu = 0$ and runs the disavowal protocol with A.
- Otherwise, A has already made a signing query for m_i, and A' answered with a valid signature σ_i. If $\sigma_i = \sigma'_i$ then A' returns $\mu = 1$ and runs the confirmation protocol with A. Otherwise, A' returns $\mu = 0$ and runs the disavowal protocol with A.

Notice that since the confirmation protocol and the disavowal protocol are perfect auxiliary-input zero-knowledge from our assumption, A' can simulate the confirmation/disavowal oracle perfectly (by using the proof technique of [17, Theorem 3.3]).

Now suppose that $i = Guess$. Let (m^*, σ^*) be the i-th query. If A has queried m^* to the signing oracle, then A' aborts. Otherwise, A outputs (m^*, σ^*) as a forgery.

A' guesses the first special query with probability $1/(q_v + 1)$. Therefore, if A wins the game of UF-FULL with non-negligible probability, then A' wins the game of UF-CMA with non-negligible probability too because q_v is polynomially bounded. This completes our proof. □

We next show that IV-CMA and IV-FULL are equivalent if Σ is UF-CMA. That is,

$$\text{IV-CMA} \Longleftrightarrow \text{IV-FULL}$$

as long as Σ is UF-CMA.

Theorem 2. *Suppose that an undeniable signature scheme Σ is UF-CMA. Then IV-CMA and IV-FULL are equivalent if the confirmation protocol and the disavowal protocol are perfect auxiliary-input zero-knowledge.*

Proof. It is clear that IV-FULL $\Longrightarrow$ IV-CMA. Therefore, we will show that IV-CMA $\Longrightarrow$ IV-FULL. Suppose that there exists an adversary A which breaks IV-FULL. We will construct an adversary A' which breaks IV-CMA by using A as a subroutine.

On input a verification key vk, A' starts running A by feeding A with the vk. If A makes a signing query for a message m_i, then A' queries m_i to her signing oracle. A' receives a signature σ_i from the signing oracle, and returns σ_i to A.

Next, we consider the case when A makes a confirmation/disavowal query (m_i, σ_i'). We say that (m_i, σ_i') is *special* if it is a valid and fresh message-signature pair queried by A to the confirmation/disavowal oracle.

Suppose that A makes a *special* confirmation/disavowal query (m_i, σ_i'). with non-negligible probability. Then A wins the game of UF-FULL. However, this is against our assumption because UF-FULL and UF-CMA are equivalent from Theorem 1.

Therefore, A makes a *special* confirmation/disavowal query (m_i, σ_i') only with negligible probability. Hence A' behaves as follows.

- If A has never made a signing query for m_i, then A' returns $\mu = 0$ and runs the disavowal protocol with A.
- Otherwise, A has already made a signing query for m_i, and A' answered with a valid signature σ_i. If $\sigma_i = \sigma_i'$ then A' returns $\mu = 1$ and runs the confirmation protocol with A. Otherwise, A' returns $\mu = 0$ and runs the disavowal protocol with A.

Notice that since the confirmation protocol and the disavowal protocol are perfect auxiliary-input zero-knowledge from our assumption, A' can simulate the confirmation/disavowal oracle (by using the proof technique of [17, Theorem 3.3]).

At some point, A chooses a message m^* which has never been queried, and sends it to A'. A' queries m^* to its challenger, and receives σ^* from the challenger. A' then returns σ^* to A.

At the end of the attack game, A outputs a guess b'. Then A' outputs $b'' = b'$. Now it is clear that $|\Pr[b = b'] - \Pr[b = b'']|$ is negligible, where b is the hidden bit chosen by the challenger. Hence M can break IV-CMA. □

We finally show that IV-CMA implies UF-CMA if the signing algorithm is deterministic. Note that UF-CMA does not imply IV-CMA: A digital signature scheme which is UF-CMA is not IV-CMA. Hence we cannot prove more than the following figure.

$$\begin{array}{ccc} \text{UF-CMA} & \Longleftrightarrow & \text{UF-FULL} \\ \Uparrow & & \\ \text{IV-CMA} & \Longleftrightarrow & \text{IV-FULL} \end{array}$$

Theorem 3. *IV-CMA implies UF-CMA if the signing algorithm is deterministic.*

Proof. Suppose that there exists an adversary A which breaks UF-CMA. We will construct an adversary A' which breaks IV-CMA by using A as a subroutine.

On input a verification key vk, A' starts running A by feeding A with vk. If A makes a signing query for a message m_i, then A queries m_i to her signing oracle. A' receives a signature σ_i from the signing oracle, and returns σ_i to A.

Eventually, A outputs a forgery (m^*, σ^*). Then A' sends m^* to her challenger. The challenger chooses a random bit b. If $b = 1$, then he computes a signature σ' on m^*. Otherwise, he chooses σ' randomly from the signature space S. The challenger returns σ'.

Finally, if $\sigma' = \sigma^*$, then A' outputs $b' = 1$. Otherwise, A' outputs a random bit b'. Suppose that (m^*, σ^*) is valid with probability ϵ. Then

$$\Pr[b = b'] = \epsilon + (1/2)(1 - \epsilon) = (1/2) + \epsilon/2$$

because the signing algorithm is deterministic. Hence if A outputs a valid forgery with non-negligible probability, then A' wins the game of IV-CMA with non-negligible probability too. □

Remark 2. The above proof shows that weak IV-CMA implies UF-CMA, where weak IV-CMA is exactly the IV-CMA except the step 5 in Section 3.2. Now we have IV-CMA → weak IV-CMA → IV-FULL.

5 Application to Factoring-Based Undeniable Signatures

Galbraith and Mao showed a factoring-based undeniable signature scheme [14] and proved its security for non-interactive, designated verifier version of confirmation/disavowal protocols [14, page 89, line -7].

Now by using our results, we can prove its security for the 4-move version of confirmation/disavowal protocols due to Chaum [7]. In this section, we present a better factoring-based undeniable signature scheme and prove its security by using our results.

5.1 Proposed Scheme

Galbraith and Mao used PSS-Rabin signature scheme [4]. Instead, we use a Rabin-type signature scheme presented in [22] which has much shorter signature size. Hence the size of our undeniable signatures is much shorter than that of [14].

The details of this new undeniable signature scheme are described as follows.

Definition 6. *Let $N = pq$, where p and q are primes. For $x \in Z_N^*$, let*

$$u = \left(\frac{x}{p}\right), \ v = \left(\frac{x}{q}\right).$$

Define

$$type(x) \triangleq \begin{cases} 0 & \text{if } u = v = 1 \\ 1 & \text{if } u = 1, v = -1 \\ 2 & \text{if } u = -1, v = 1 \\ 3 & \text{if } u = v = -1 \end{cases} \tag{1}$$

It is easy to see that $xy \in QR_N$ if and only if $type(x) = type(y)$.

Key Generation. On input 1^k, the system is set up by the signer as follows. Choose two k-bit safe primes p and q such that $p' = (p-1)/2$ and $q' = (q-1)/2$ are also primes. Then set $N = pq$ and select an element $e \in Z_{p'q'}^*$ such that $e > 1$.

Choose $g \in Z_N^*$ to be a generator of Z_p^* and Z_q^*, and compute $\beta = g^2 \bmod N$ and $w = \beta^e \bmod N$.
Next, choose α_1 and α_2 such that $type(\alpha_1) = 1$ and $type(\alpha_2) = 2$. Also, let $\alpha_0 \stackrel{\triangle}{=} 1$ and $\alpha_3 \stackrel{\triangle}{=} \alpha_1\alpha_2 \bmod N$. Note that $type(\alpha_i) = i$ for $i = 0, 1, 2, 3$.
Let $H : \{0,1\}^* \to Z_N^*$ be a hash function.
Finally, set the verification key as $(N, \beta, w, H, \alpha_0, \alpha_1, \alpha_2, \alpha_3)$ and the signing key as (p, q).

Notice that β is a generator of QR_N because $ord_p(\beta) = (p-1)/2 = p'$ and $ord_q(\beta) = (q-1)/2 = q'$, thus $ord_N(\beta) = lcm(p', q') = p'q' = |QR_N|$.

Signing. On input the verification key $(N, \beta, w, H, \alpha_0, \alpha_1, \alpha_2, \alpha_3)$, the signing key (p, q) and a message m , the signer executes the following steps.
Step 1: Compute i such that $type(H(m)) = i$.
Step 2: For this i, compute σ such that $0 < \sigma < N/2$ and

$$\alpha_i H(m) = \sigma^{2e} \bmod N \tag{2}$$

The signature is σ.

We say that (m, σ) is valid if $0 < \sigma < N/2$ and equation (2) is satisfied.

Definition 7. *We say that* $(\beta, \beta^x, \beta^y, \beta^{xy}) \in (QR_N)^4$ *is a composite Diffie-Hellman (CDH) tuple, where* $(x, y) \in Z_{p'q'}^2$.

In each of the confirmation/disavowal protocols, given a message-signature pair (m, σ), the verifier checks if $0 < \sigma < N/2$. If not, he rejects immediately. if so, he runs the following protocols with the signer.

Confirmation Protocol. The signer first sends i such that $type(H(m)) = i$. The signer next proves that $(\beta, w, \sigma^2, \alpha_i H(m))$ is a CDH-tuple in zero-knowledge.

Disavowal Protocol. The signer first sends i such that $type(H(m)) = i$. Next the signer proves that $(\beta, w, \sigma^2, \alpha_i H(m))$ is not a CDH-tuple in zero-knowledge.

For the confirmation and disavowal protocols, we can use the 4-move protocol due to Chaum [7]. Alternatively, we can use designated verifier proofs which are non-interactive zero-knowledge [20]. They are perfect zero-knowledge in the auxiliary-input model.

Remark 3.
1. It is not necessarily the case that $H(m) \in QR_N$. Therefore, we use the technique of [22]. That is, we have to include $(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$ in the verification key so that $\alpha_i H(m)$ in QR_N for some i.
2. Since the order of β is $p'q'$, Chaum's ZKIP protocols works well on the CDH-tuples and the non CDH-tuples in the group QR_N.

5.2 Security Analysis

Theorem 4. *The above undeniable signature scheme satisfies UF-CMA under the factoring assumption in the random oracle model.*

Proof. Let A be an adversary which breaks UF-CMA with non-negligible probability ϵ. Then we will construct the factoring algorithm M which factors N with non-negligible probability ϵ' by running A as a subroutine. The input of M is $N(=pq)$, where $p = 2p' + 1$ and $q = 2q' + 1$ are safe primes.

M constructs the verification key for A as follows. M chooses a random integer $e \in \{2, \cdots, \lfloor N/4 \rfloor\}$. Next, M chooses a random $g \in Z_N^*$ and defines $\beta = g^2 \bmod N$ and $w = \beta^e \bmod N$. It is easy to see that e is co-prime to $p'q'$ and β is a generator of QR_N with overwhelming probability because N is a product of two safe primes. M also chooses α_1, α_2 randomly in such a way that

$$\left(\frac{\alpha_1}{N}\right) = \left(\frac{\alpha_2}{N}\right) = -1.$$

With probability 1/4, it holds that $type(\alpha_1) = 1$ and $type(\alpha_2) = 2$. M sets $\alpha_0 = 1$ and $\alpha_3 = \alpha_1\alpha_2 \bmod N$

M then feeds A with the verification key $(N, \beta, w, H, \alpha_0, \alpha_1, \alpha_2, \alpha_3)$ where H is a random oracle that will be simulated by M. We assume that when A requests a signature on a message m_j, it has already made the corresponding H-query on m_j.

The factoring algorithm M must answer all the queries by itself. When A makes a H-query for a message m_j, A chooses $r_j \in Z_N^*$ and $i \in \{0, 1, 2, 3\}$ randomly, and returns $H(m_j) = {r_j}^{2e}/\alpha_i \bmod N$. M will maintain a H-query list (m_j, r_j, i).

Suppose that A makes a signing query for a message m_j. Since we have assumed that A has already made the corresponding H-query on m_j, then the H-query list includes (m_j, r_j, i) for some (r_j, i). M then returns $\sigma_j = r_j \bmod N$ as the corresponding signature. Notice that σ_j is a valid signature since

$$\alpha_i H(m_j) = r_j^{2e} \bmod N.$$

Now suppose that A forges (m^*, σ^*). Then

$$\alpha_i H(m^*) = (\sigma^*)^{2e} \bmod N. \tag{3}$$

Since we assumed that A has made the H-query on m^*, so $m^* = m_j$ for some j in the H-query list. Therefore, M can find the triple (m^*, r^*, i) from the H-query list where

$$\alpha_i H(m^*) = (r^*)^{2e} \bmod N. \tag{4}$$

From equation (3) and equation (4),

$$((r^*)^2)^e = ((\sigma^*)^2)^e \bmod N.$$

Since $\gcd(e, p'q')) = 1$ with overwhelming probability, it holds that

$$(r^*)^2 = (\sigma^*)^2 \bmod N$$

with overwhelming probability.

Case 1. Suppose that m^* has never been queried to the signing oracle. In this case, $\gcd(r^* - \sigma^*, N) = p$ or q with probability $1/2$ because r^* is randomly chosen. Hence M can factor N with probability almost $1/2 \times 1/4 = 1/8$.

Case 2. Suppose that m^* has been queried to the signing oracle which returned $\tilde{\sigma}$. In this case, we can see that $\gcd(\sigma^* - \tilde{\sigma}, N) = p$ or q because $0 < \sigma < N/2$. Hence M can factor N with probability almost $1/4$.

In any case, M can factor N with significant probability. □

Corollary 1. *The above undeniable signature scheme satisfies UF-FULL under the factoring assumption in the random oracle model.*

Proof. From Theorem 4 and Theorem 1. □

Next we prove the invisibility. It relies on the composite decision Diffie-Hellman (CDDH) assumption which is defined as follows.

We denote $\langle g_1, \ldots, g_m \rangle$ for the subgroup generated by $g_1, \ldots, g_m$. Let N be a product of two safe primes p and q such that $p' = (p-1)/2$ and $q' = (q-1)/2$ are also primes. Consider the two sets

$$\mathcal{T} = \{(N, g, w, u, v, \alpha_1, \alpha_2) : type(\alpha_1) = 1, type(\alpha_2) = 2,$$

$$ord_N(g) = ord_N(u) = 2p'q', \langle g, u \rangle = Z_N^*, (w, v) \in (QR_N)^2\}$$

and

$$\mathcal{T}_{CDDH} = \{(N, g, w, u, v, \alpha_1, \alpha_2) \in \mathcal{T} : w = g^{2e} \bmod N,$$

$$v = u^{2e} \bmod N \text{ for some } e \in Z_{p'q'}\}$$

with the uniform distribution on each. The CDDH problem is to distinguish these two distributions.

Theorem 5. *The above undeniable signature scheme satisfies IV-CMA under the CDDH assumption in the random oracle model.*

Proof. Let A be an adversary which breaks IV-CMA with non-negligible probability ϵ. Then we will construct a composite decision Diffie-Hellman algorithm M with non-negligible probability ϵ' by running A as a subroutine.

Let $(N, g, w, u, v, \alpha_1, \alpha_2)$ be the challenge CDDH problem input to M. M first computes $\beta = g^2 \bmod N$. Let $\alpha_0 = 1$ and $\alpha_3 = \alpha_1\alpha_2 \bmod N$. M runs A by feeding A with the verification key $(N, \beta, w, H, \alpha_0, \alpha_1, \alpha_2, \alpha_3)$ where H is a random oracle that will be simulated by M. We assume that when A requests a signature on a message m_j, it has already made the corresponding H-query on m_j.

When A makes a H-query for a message m_j, M chooses $x_j, y_j \in \{1, 2, \cdots, \lfloor N/2 \rfloor\}$ randomly and $i \in \{0, 1, 2, 3\}$ randomly, and returns $H(m_j) = (w^{x_j} v^{y_j})^2/\alpha_i \bmod N$. M will maintain a H-query list (m_j, x_j, y_j, i).

When A makes a signing query for a message m_j, since we have assumed that A has already made the corresponding H-query on m_j, then $H(m_j) = (w^{x_j} u^{y_j})^2/\alpha_i \bmod N$. M then computes $\sigma_j = g^{x_j} u^{y_j} \bmod N$ and returns σ_j as the corresponding signature.

Eventually, A outputs a message m^*. M then chooses a hidden bit b. If $b = 1$, M generates σ^* using the above signing process and returns σ^* as the signature. If $b = 0$, M chooses $\sigma^* \in Z_N^*$ randomly and returns σ^* as the signature.

Next, A performs some H queries and signing queries again with the restriction that no signing queries on m^* is allowed. Finally, A outputs a bit b' which it thinks is equal to the hidden bit b. If $b' = b$ then M outputs 1 as the answer and if $b' \neq b$ then M outputs 0 as the answer.

Notice that if $(N, g, w, u, v, \alpha_1, \alpha_2) \in \mathcal{T}_{CDDH}$, then the signing oracle behaves perfectly and the simulation is identical to a real attack. Thus we have

$$\Pr[M \text{ outputs } 1] = \Pr[b' = b] = \frac{1}{2} + \epsilon,$$

where ϵ is the advantage of algorithm A.

On the other hand, when the input is a random tuple of $\mathcal{T}$, the signatures generated by the signing oracle are with high probability invalid. The simulation is therefore not indistinguishable from a real attack. However, we can show as in [14, Appendix B] that the hidden bit b is independent of the simulation. That is,

$$\Pr[M \text{ outputs } 1] = \Pr[b' = b] = \frac{1}{2}.$$

It follows that the advantage of algorithm M

$$\epsilon' = \frac{1}{2} + \epsilon - \frac{1}{2} = \epsilon$$

which is non-negligible. □

Corollary 2. *The above undeniable signature scheme satisfies IV-FULL.*

Proof. From Theorem 5, Theorem 4 and Theorem 2 □

6 Conclusion

We have studied on the relationships among various notions of security of undeniable signature schemes, namely, UF-CMA, UF-FULL, IV-CMA and IV-FULL and shown some important relationships among them. We also proposed an undeniable signature scheme where its unforgeability is based on the factoring assumption and its invisibility is based on the CDDH assumption.

References

1. N. Attrapadung,Y. Cui, G. Hanaoka, H. Imai, K. Matsuura, P. Yang and R. Zhang. Relations among notions of security for identity based encryption schemes. *Cryptology ePrint Archive Report 2005/258*. Available from `http://eprint.iacr.org/2005/258`.
2. M. Bellare, A. Desai, D. Pointcheval and P. Rogaway. Relations among notions of security for public-key encryption schemes. *Advances in Cryptology — CRYPTO '98*, LNCS 1462, pp. 26–45, Springer-Verlag, 1998.

3. M. Bellare, O. Goldreich and A. Mityagin. The power of verification queries in message authentication and authenticated encryption. *Cryptology ePrint Archive Report 2004/309*. Available from `http://eprint.iacr.org/2004/309`.
4. M. Bellare and P. Rogaway. The exact security of digital signatures – how to sign with RSA and Rabin. *Advances in Cryptology — EUROCRYPT '96*, LNCS 1070, pp. 399–416, Springer-Verlag, 1996.
5. J. Boyar, D. Chaum, I. Damgård and T. Pedersen. Convertible undeniable signatures. *Advances in Cryptology — CRYPTO '90*, LNCS 537, pp. 189–208, Springer-Verlag, 1990.
6. J. Camenisch and M. Michels. Confirmer signature schemes secure against adaptive adversaries. *Advances in Cryptology — EUROCRYPT '00*, LNCS 1870, pp. 243–258, Springer-Verlag, 2000.
7. D. Chaum. Zero-knowledge undeniable signatures. *Advances in Cryptology — EUROCRYPT '90*, LNCS 473, pp. 458–464, Springer-Verlag, 1990.
8. D. Chaum. Designated confirmer signatures. *Advances in Cryptology — EUROCRYPT '94*, LNCS 950, pp. 86–91, Springer-Verlag, 1995.
9. T. Chaum and T. P. Pedersen. Wallet databases with observers. *Advances in Cryptology — CRYPTO '92*, LNCS 740, pp. 89–105, Springer-Verlag, 1993.
10. D. Chaum and H. van Antwerpen. Undeniable signatures. *Advances in Cryptology — CRYPTO '89*, LNCS 435, pp. 212–216, Springer-Verlag, 1989.
11. D. Chaum, E. van Heijst and B. Pfitzmann. Cryptographically strong undeniable signatures, unconditionally secure for the signer. *Advances in Cryptology — CRYPTO '91*, LNCS 576, pp. 470–484, Springer-Verlag, 1991.
12. I. Damgård and T. Pedersen. New convertible undeniable signature schemes. *Advances in Cryptology — EUROCRYPT '96*, LNCS 1070, pp. 372–386, Springer-Verlag, 1996.
13. A. Datta, R. Küsters, J.C. Mitchell and A. Ramanathan. On the relationships between notions of simulation-based security. *Theory of Cryptography Conference — TCC '05*, LNCS 3378, pp. 476–494, Springer-Verlag, 2005.
14. S. Galbraith and W. Mao. Invisibility and anonymity of undeniable and confirmer signatures. *Topics in Cryptology — CT-RSA '03*, LNCS 2612, pp. 80–97, Springer Verlag, 2003.
15. S. Galbraith, W. Mao and K. G. Paterson. RSA-based undeniable signatures for general moduli. *Topics in Cryptology — CT-RSA '02*, LNCS 2271, pp. 200–217, Springer Verlag, 2002.
16. R. Gennaro, H. Krawczyk and T. Rabin. RSA-based undeniable signatures. *Advances in Cryptology — CRYPTO '97*, LNCS 1294, pp. 132–149, Springer-Verlag, 1997.
17. O. Goldreich and Y. Oren. Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, vol. 7, no. 1, pp. 1–32, Springer-Verlag, 1994.
18. S. Goldwasser, S. Micali and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, vol. 18, pp. 186–208, 1989 (Preliminary version in 17th STOC, 1985).
19. S. Goldwasser, S. Micali and R. Rivest. A digital signature scheme secure against adaptative chosen-message attacks. *SIAM Journal on Computing*, vol. 17, no. 2, pp. 281–308, 1988.
20. M. Jakobsson, K. Sako and R. Impagliazzo. Designated verifier proofs and their applications. *Advances in Cryptology — EUROCRYPT '96*, LNCS 1070, pp. 143–154, Springer-Verlag, 1996.
21. K. Kurosawa and S.-H. Heng. 3-Move undeniable signature scheme. *Advances in Cryptology — EUROCRYPT '05*, LNCS 3494, pp. 181–197, Springer-Verlag, 2005.

22. K. Kurosawa and W. Ogata. Efficient Rabin-type digital signature scheme. *Design, Codes and Cryptography*, vol. 16, no. 1, pp. 53–64, 1999.
23. B. Libert and J.-J Quisquater. Identity based undeniable signatures. *Topics in Cryptology — CT-RSA '04*, LNCS 2964, pp. 112–125, Springer-Verlag, 2004.
24. J. Monnerat and S. Vaudenay. Undeniable signatures based on characters: how to sign with one bit. *Public Key Cryptography — PKC '04*, LNCS 2947, pp. 361–396, Springer-Verlag, 2004.
25. J. Monnerat and S. Vaudenay. Generic homomorphic undeniable signatures. *Advances in Cryptology — Asiacrypt '04*, LNCS 3329, pp. 354–371, Springer-Verlag, 2004.
26. W. Ogata, K. Kurosawa and S.-H. Heng. The security of the FDH variant of Chaum's undeniable scheme. *Public Key Cryptography — PKC '05*, LNCS 3386, pp. 328–345, Springer-Verlag, 2005.