On the Invisibility and Anonymity of Undeniable Signature Schemes*

Jia-Ch'ng Loh[1], Swee-Huay Heng[1†], Syh-Yuan Tan[2], and Kaoru Kurosawa[3]
[1]*Faculty of Information Science and Technology, Multimedia University, Melaka, Malaysia*
jasonlohjc@gmail.com, shheng@mmu.edu.my
[2]*School of Computing, Newcastle University, Newcastle upon Tyne, United Kingdom*
syh-yuan.tan@newcastle.ac.uk
[3]*Department of Computer and Information Sciences, Ibaraki University, Hitachi, Ibaraki 316-8511, Japan*
kaoru.kurosawa.kk@vc.ibaraki.ac.jp

Received: January 23, 2020; Accepted: March 6, 2020; Published: March 31, 2020

Abstract

Undeniable signature is a special featured digital signature which can only be verified with the help of the signer. Undeniable signature should satisfy invisibility which implies the inability of a user to determine the validity of a message and signature pair as introduced by Chaum et al. Galbraith and Mao later proposed the notion of anonymity which implies the infeasibility to determine which user has issued the signature. They also proved that the notions of invisibility and anonymity are equivalent when the signers possess the same signature space, such that if an undeniable signature possesses invisibility, then it also possesses anonymity, and vice versa. In this paper, we show that in contradiction to the equivalency result established by Galbraith and Mao, there exist some undeniable signature schemes that possess invisibility but not anonymity. This motivates us to find out whether there is a limitation on Galbraith and Mao's equivalency result or the schemes are actually flawed. Our analysis shows that the anonymity property requires all signers to possess the same signature space but the invisibility property does not. This conforms to the equivalency result and implies that an undeniable signature scheme can be invisible but not anonymous if the signers possess the different signature space. Our result invalidates two past cryptanalyses on undeniable signature schemes. We also provide a generic solution to solve the above problem.

Keywords: anonymity, invisibility, undeniable signature

1 Introduction

The notion of undeniable signature was introduced by Chaum and van Antwerpen [2]. Unlike ordinary digital signature, undeniable signature has a distinctive feature, i.e., without the help of the signer, the verifier will not be able to verify the validity of the undeniable signature. Since it was introduced, there are various applications using it such as licensing software [2], electronic cash [3], electronic voting and auctions [4, 5]. There are also some variants of undeniable signature proposed such as convertible undeniable signature [6], designated verifier signature [7], and designated confirmer signature [8, 9].

Convertible undeniable signature was proposed by Boyar et al. [6]. It is an extension of undeniable signature that allows the signer to transform an undeniable signature into an universally verifiable

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 11(1):18-34, Mar. 2020
DOI:*10.22667/JOWUA.2020.03.31.018*

[*] This paper is an extended version of our paper published in [1].

[†] Corresponding author: Faculty of Information Science and Technology, Multimedia University, Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia, Tel: +60-(0)6-2523600

ordinary digital signature. There are two types of convertible undeniable signature, namely, selectively convertible and universally convertible. Selectively convertible undeniable signature allows the signer to convert only a specific undeniable signature into an universally verifiable one by releasing a token. In universally convertible undeniable signature, the signer releases part of his secret to convert the undeniable signature into the ordinary digital signature. Designated confirmer signature was introduced by Chaum [8], where it allows an undeniable signature to be verified with the help of the signer or the designated confirmer. On the other hand, the designated verifier signature was introduced by Jakobsson et al. [7], where it allows an undeniable signature to be verified by the designated verifier or the signer only.

As previous works were all built in the paradigm of conventional public key cryptography, Libert et al. [10] introduced the paradigm of identity-based undeniable signature, where it addressed the certificate generation and management issues by deriving the signer's public key from the signer's publicly verifiable information, and the signer's private key is issued by a trusted third party called Private Key Generator (PKG). Identity-based undeniable signature was further enhanced by Duan [11] with the paradigm of certificateless undeniable signature in 2008 which addressed the issue of private key escrow problem in identity-based cryptography.

The notion of invisibility was introduced as the main security property for undeniable signature and designated confirmer signature by Chaum et al. [12]. Invisibility implies the inability of a user to determine whether a given message and signature pair is valid. It was later formalised by Camenisch and Michels [13] and generalised by Galbraith and Mao [14]. These two definitions of invisibility were also proven to be equivalent by Galbraith and Mao [14]. Galbraith and Mao [14] also introduced the notion of anonymity as the most relevant security property for undeniable signature and designated confirmer signature in multi-user settings. Anonymity implies that given an undeniable signature and public keys of two or more possible signers, it is infeasible to determine which user has issued the signature. They also claimed that the notions of invisibility and anonymity are equivalent if all signers are sharing the same signature space by providing a formal security proof. Huang et al. [15] later formalised invisibility and anonymity in convertible setting where the adversary has some additional accessible oracles and restrictions. They then provided the proof of equivalency between invisibility and anonymity using the same approach as Galbraith and Mao [14]. Since then, the notions of invisibility and anonymity have been regarded by researchers as equivalent, where one proves either of the security properties and the other security property follows [16, 10, 17, 18, 19].

The first provably secure convertible undeniable signature scheme based on RSA was proposed by Kurosawa and Takagi [20]. It was later revisited by Phong et al. [21] who showed that Kurosawa and Takagi's convertible undeniable signature scheme [20] did not satisfy anonymity, and thus invisibility is not satisfied too. Meanwhile, an identity-based convertible undeniable signature scheme based on pairings was proposed by Wu et al. [22]. It was later revisited by Behnia et al. [23] who showed that there exists an adversary who can break the invisibility and anonymity of the scheme. A convertible undeniable signature scheme without random oracle was later proposed by Huang and Wong [24]. However, it was pointed out by Schuldt and Matsuura [25] that their schemes did not satisfy anonymity. The full version [26] of Huang and Wong's convertible undeniable signature scheme [24] was later published and they remarked that their scheme possesses invisibility only. Besides, Huang et al. [27] proposed a designated confirmer signature scheme, and they later highlighted that it did not satisfy anonymity in the full version [28] as well.

1.1 Our Contributions

We revisit three cryptanalyses [21, 23, 25] on undeniable signature schemes and show that two [21, 23] of them did not make a correct conclusion for the cryptanalysed schemes [26, 29, 27] on the equivalency of anonymity and invisibility. We also revisit a designated confirmer signature scheme [28] and show that it faces the same issue as in the cryptanalysed schemes. More precisely, these four schemes do not possess anonymity but they are invisible as the validity of the message and signature pair are not revealed. These observations contradict to the well accepted fact that invisibility is equivalent to anonymity. It is thus interesting to find out whether this phenomenon is caused by a limitation on Galbraith and Mao's security model or the schemes are actually flawed. We first show that the equivalency result of invisibility and anonymity is not applicable in the four schemes due to the signature space for each signer is different as opposed to the requirement placed in Galbraith and Mao's equivalency result [14]. Next, we show that invisibility does not require signers to have a common signature space but anonymity does. Therefore, the four schemes [26, 29, 27, 28] are invisible but not anonymous and the two cryptanalyses [21, 23] inadequately applied Galbraith and Mao's equivalency theorem on them. In addition to our published version [1], we propose a generic solution to overcome the weaknesses in the three conventional schemes without requiring any modification to their security proof.

1.2 Organisation of the Paper

The organisation of the paper is as follows. In Section 2, we review some preliminaries and recall the definitions of undeniable signature, convertible undeniable signature, and designated confirmer signature. We also review the security model of invisibility and anonymity, and the equivalency between them. In Section 3, we review the past attacks on some existing undeniable signature schemes. In Section 4, we show that the past attacks are not entirely correct by providing a detailed discussion. In Section 5, we propose a generic solution to fix the discussed conventional schemes. Finally, we conclude this paper in Section 6.

2 Preliminaries

2.1 Bilinear Pairings

A brief review on the properties of bilinear pairings [30] is included here. Let $\mathbb{G}$ and $\mathbb{G}_T$ be cyclic groups of prime order p and a generator $g \in \mathbb{G}$. The map $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a bilinear map which satisfies the following properties:

- Bilinearity: for all $(x,y) \in \mathbb{G}$ and $(a,b) \in \mathbb{Z}_p$, we have $\hat{e}(x^a, y^b) = \hat{e}(x,y)^{ab}$.
- Non-degeneracy: if g is a generator of $\mathbb{G}$, then $\hat{e}(g,g)$ is a generator of $\mathbb{G}_T$ which also implies $\hat{e}(g,g) \neq 1$.
- Computability: there exists an efficient algorithm to compute $\hat{e}(x,y)$ for all $x, y \in \mathbb{G}$.

2.2 Proofs of Knowledge

A proof of knowledge (PoK) is a zero-knowledge protocol (ZK) that allows the signer to convince the verifier that he knows a secret without leaking it [31]. There are some variants of PoK protocols that applied in undeniable signature schemes [32], namely, the perfect zero-knowledge protocol (ZKIP), the honest verifier zero-knowledge protocol (HVZK), and the non-interactive zero-knowledge protocol (NIZK) with designated-verifier technique. In this paper, we describe HVZK in detail as we apply it in Section 5. The HVZK assumes there is an honest verifier who runs the ZK protocol with the prover. At the end of the protocol, the prover is able to generate a proof to either claim or deny a statement. The HVZK is defined as $HVZK\{(sk) : statement\}$ where sk is the secret to be proven and $statement$ is the condition to achieve true or false. A *statement* can also be a combination of two or more statements with the condition of either one of the statement is true "$\vee$" or all the statements are true "$\wedge$".

2.3 Undeniable Signature Scheme

An undeniable signature is a special featured digital signature which is only verifiable with the help of the signer. An undeniable signature scheme consists of the following algorithms and protocols [14]:

- *KeyGen*: On input a security parameter 1^k, it outputs a signer's public and private key pair (pk, sk).
- *Sign*: On input a message and a signer private key (m, sk), it outputs an undeniable signature σ.
- $Confirmation/Disavowal\,Protocol$: An interactive protocol that runs between the signer and the verifier on common input (pk, m, σ). The signer uses *sk* to check the validity of σ, the output is a non-transferable transcript ("*Accept*"/"*Deny*") that shows σ is valid/invalid on (m, pk).

Correctness. Every valid (invalid) undeniable signature can always be proven valid (invalid) with $Confirmation/\ Disavowal\,Protocol$.

2.4 Convertible Undeniable Signature Scheme

A convertible undeniable signature scheme allows the signer to transform an undeniable signature into a publicly verifiable one. It consists of the same algorithms and protocols as in undeniable signature scheme with the following additional algorithms which allow selectively conversion and universally conversion respectively [15]:

- *Selective-Convert*: On input (sk, m, σ), it computes a selective token π^S which can be used to publicly verify (m, σ) on *pk*.
- $Selective\text{-}Verify$: On input (pk, m, σ, π^S), it outputs $\perp$ if π^S is an invalid token on *pk*. Else, it outputs "1" if (m, σ, pk) is valid and outputs "0" otherwise.
- *Universal-Convert*: On input *sk*, it computes an universal token π^U which can be used to publicly verify every σ generated by *sk*.
- $Universal\text{-}Verify$: On input (pk, m, σ, π^U), it outputs $\perp$ if π^U is an invalid token on *pk*. Else, it outputs "1" if (m, σ, pk) is valid and outputs "0" otherwise.

Completeness and ***Soundness***. ***Completeness*** is defined as that a valid (invalid) undeniable signature can always be proven valid (invalid) and ***Soundness*** is defined as that a valid (invalid) undeniable signature cannot be proven as invalid (valid).

2.5 Designated Confirmer Signature Scheme

A designated confirmer signature scheme allows the signer to designate a third party (confirmer) to verify an undeniable signature. It consists of the same algorithms and protocols as in undeniable signature scheme with the additional algorithm, *DCKeyGen*, and an additional input, the confirmer's public key pk_c, into *Sign* and $Confirmation/Disavowal\,Protocol$ [8]:

- *DCKeyGen*: On input a security parameter 1^k, it outputs a confirmer's public and private key pair (pk_c, sk_c).

- *Sign*: On input (m, sk, pk_c), it outputs a designated confirmer signature σ.
- $Confirmation/Disavowal Protocol$: An interactive protocol that runs between the signer/confirmer and the verifier on common input (pk, pk_c, m, σ). The signature/confirmer uses sk/sk_c to check the validity of σ, the output is a non-transferable transcript ("*Accept*"/"*Deny*") that shows σ is valid/invalid on (m, pk, pk_c).

Correctness. Same as in Section 2.3.

2.6 The Notions of Invisibility and Anonymity

The notion of invisibility was first introduced by Chaum et al. [12]. It was later formalised by Camenisch and Michels [13] to distinguish whether a signature is corresponding to either message m_0 or m_1. Galbraith and Mao then generalised the notion of invisibility to distinguish a signature from a random element. Besides, Galbraith and Mao also proposed the notion of anonymity [14] to distinguish a signature which is either valid on public key pk_0 or pk_1, and they claimed that anonymity rather than invisibility should be considered as the main security property for undeniable signature in the multi-user setting, The notions of invisibility and anonymity were further studied by Huang et al. [15] in order to cover the convertible undeniable signature scheme.

2.6.1 Invisibility

This security property requires that given (m, σ) and a signer's public key pk, there is no computational way to decide whether (m, σ) is valid on pk or not without the help from the signer. Its security model is defined as the following game between an adversary $\mathscr{A}_I$ and a challenger $\mathscr{C}$ [14, 15].

- **Setup:** $\mathscr{C}$ first runs $KeyGen(1^k) \to (pk, sk)$ and sends pk to $\mathscr{A}_I$.
- **Queries I:** $\mathscr{A}_I$ is able to make queries to **Sign oracle** and **Confirmation/disavowal oracle**. $\mathscr{A}_I$ can also make query to selective convert oracle if the scheme is convertible.
- **Output I:** At some point, $\mathscr{A}_I$ outputs a challenge message $\hat{m}$ to request a challenge signature $\hat{\sigma}$. If the scheme is deterministic, $\hat{m}$ is restricted where it must not have been submitted to **Sign oracle** during **Queries I**. $\mathscr{A}_I$ submits a challenge message $\hat{m}$. $\mathscr{C}$ responds by randomly choosing a challenge bit $b \in \{0, 1\}$ and generates $\hat{\sigma} = Sign_{sk}(\hat{m})$ if $b = 0$. Otherwise, $\mathscr{C}$ returns a random element that is chosen from the same signature space as in $\hat{\sigma} = Sign_{sk}(\hat{m})$.
- **Queries II:** Once $\mathscr{A}_I$ obtains $\hat{\sigma}$, $\mathscr{A}_I$ can still make queries to the accessible oracles as in **Queries I**. The restrictions defined in **Output I** still hold with an additional restriction that any $(\hat{m}, \cdot)$ in the equivalence class of $(\hat{m}, \hat{\sigma})$ is not allowed to be submitted to **Confirmation/disavowal oracle** and selective convert oracle.
- **Output II:** $\mathscr{A}_I$ outputs a guess b' and wins the game if $b' = b$.

The advantage of $\mathscr{A}_I$ has in the above game is defined as Adv($\mathscr{A}_I$) $= |Pr[b = b'] - \frac{1}{2}|$.

Definition 1. *An undeniable signature, convertible undeniable signature, or designated confirmer signature scheme is (t, q, ε)-invisible if there is no probabilistic polynomial time (PPT) adversary $\mathscr{A}_I$ can have success probability more than ε in its game with at most q queries to its accessible oracles in time t.*

2.6.2 Anonymity

This security property requires that given a valid (m, σ) and two possible signers' public keys (pk_0, pk_1), there is no computational way to decide who the real signer is. Its security model is defined as the following game between an adversary $\mathscr{A}_A$ and a challenger $\mathscr{C}$ [14, 15].

- **Setup:** $\mathscr{C}$ first runs $KeyGen(1^k) \rightarrow (pk_0, sk_0)$ and $KeyGen(1^k) \rightarrow (pk_1, sk_1)$ and sends (pk_0, pk_1) to $\mathscr{A}_A$.
- **Queries I:** $\mathscr{A}_A$ is able to make queries to all the accessible oracles and the same restrictions as in Section 2.6.1.
- **Output I:** $\mathscr{A}_A$ outputs a challenge message $\hat{m}$ to request for a challenge signature $\hat{\sigma}$ with the same restriction as in Section 2.6.1. $\mathscr{C}$ responds by randomly choosing a challenge bit $b \in \{0, 1\}$ and generates a challenge signature $\hat{\sigma} = Sign_{sk_b}(\hat{m})$ that is valid on either pk_0 or pk_1. In either case, $\hat{\sigma}$ is returned to $\mathscr{A}_A$.
- **Queries II:** Same as in Section 2.6.1.
- **Output II:** $\mathscr{A}_A$ outputs a guess b' and wins the game if $b' = b$.

The advantage of $\mathscr{A}$ has in the above game is defined as Adv($\mathscr{A}_A$)= $|Pr[b = b'] - \frac{1}{2}|$.

Definition 2. *An undeniable signature, convertible undeniable signature, or designated confirmer signature scheme is (t, q, ε)-anonymous if there is no PPT adversary $\mathscr{A}_A$ can have success probability more than ε in its game with at most q queries to its accessible oracles in time t.*

2.6.3 The Equivalence of Invisibility and Anonymity

The equivalence of invisibility and anonymity in undeniable signature and designated confirmer signature schemes was introduced by Galbraith and Mao [14], and further studied by Huang et al. [15] for the convertible variant. The equivalency shows that if an undeniable signature possesses invisibility, then it also possesses anonymity, and vice versa. This is highlighted by Galbraith and Mao [14] and Phong et al. [21] that invisibility implies anonymity if and only if all signers are sharing the same signature space, especially in RSA based undeniable signature in order to ensure the signature length does not reveal the identity of the signer. We only include the proof of Theorem 1 as given by Galbraith and Mao [14]. We omit the proof of Theorem 2 as it is not referred in our subsequent discussion.

Theorem 1. [14, 15] *If an undeniable signature, convertible undeniable signature, or designated confirmer signature possesses invisibility, then it also possesses anonymity.*

Proof. Suppose there exists an adversary $\mathscr{A}_A$ who can reveal the signer's public key of the signature in the game of anonymity, then there is an adversary $\mathscr{A}_I$ who can use $\mathscr{A}_A$ to have the advantage in the game of invisibility and thus the scheme is not invisible.

- **Setup:** The input to $\mathscr{A}_I$ is pk_0, and we run $KeyGen(1^k) \rightarrow (pk_1, sk_1)$ to produce another public and private key pair (pk_1, sk_1). $\mathscr{A}_I$ keeps sk_1 and flips a coin $b' \in \{0, 1\}$. If $b' = 0$, the input to $\mathscr{A}_A$ is (pk_0, pk_1), otherwise the input is (pk_1, pk_0).
- **Queries I:** Queries made by $\mathscr{A}_A$ with respect to pk_0 are all passed on as $\mathscr{A}_I$ queries, and queries with respect to pk_1 are handled by $\mathscr{A}_I$ using knowledge of sk_1.

- **Output I:** At some point, $\mathscr{A}_A$ outputs a challenge message $\hat{m}$, $\mathscr{A}_I$ passes $\hat{m}$ as his own challenge as well. If the challenge bit $b=0$, $\mathscr{A}_I$ receives a challenge signature $\hat{\sigma} = Sign_{sk_0}(\hat{m})$, or $\hat{\sigma}$ which with negligible probability, is valid on an arbitrary message if $b=1$.
- **Queries II:** $\mathscr{A}_A$ can continue to make his queries to $\mathscr{A}_I$ as in **Queries I** with the restrictions covered in the adversaries' own challenges, such as $\hat{m}$ is not allowed to query for confirmation/disavowal.
- **Output II:** At the end, $\mathscr{A}_A$ outputs a guess b''. If $b''=b'$, $\mathscr{A}_I$ outputs 0 as his guess and 1 otherwise.

Note that in the case $b=0$, where $\hat{\sigma} = Sign_{sk_0}(\hat{m})$. Since $\mathscr{A}_A$ can reveal the signer, $\mathscr{A}_A$ outputs $b''=b'$ to $\mathscr{A}_I$ then $\mathscr{A}_I$ can always output 0. At this point, $\mathscr{A}_I$ wins the game with the help of $\mathscr{A}_A$ which denotes as:

$$\Pr[b''=b'|b=0] = \frac{1}{2} + \mathrm{Adv}(\mathscr{A}_A)$$

However, in the case $b=1$, $\hat{\sigma}$ is a random element which indicates an invalid signature (with the negligible chance that it is valid on $\hat{m}$). It follows by b' is independent of $\hat{\sigma}$, hence $\Pr[b'' \neq b'|b=1] \approx \frac{1}{2}$. Therefore, the advantage of $\mathscr{A}_I$ is defined as follows:

$$\begin{aligned}\mathrm{Adv}(\mathscr{A}_I) &= \Pr[b''=b'|b=0]\frac{1}{2} + \Pr[b'' \neq b'|b=1]\frac{1}{2} - \frac{1}{2} \\ &= (\frac{1}{2} + \mathrm{Adv}(\mathscr{A}_A))\frac{1}{2} + \frac{1}{2}\frac{1}{2} - \frac{1}{2} \\ &= \frac{1}{2}\mathrm{Adv}(\mathscr{A}_A)\end{aligned}$$

□

Theorem 2. [14, 15] *If an undeniable signature, convertible undeniable signature, or designated confirmer signature possesses anonymity, then it also possesses invisibility.*

3 Revisiting the Cryptanalysis on Some Undeniable Signature Schemes

In this section, we first briefly describe the attack mounted by Behnia et al. [23] on Wu et al.'s identity-based convertible undeniable signature scheme [22], followed by the attack by Phong et al. [21] on Kurosawa and Takagi's convertible undeniable signature scheme [20], and the attack by Schuldt and Matsuura [25] on Huang and Wong's convertible undeniable signature scheme [24]. Besides, we also briefly describe Huang et al.'s designated confirmer signature scheme [28] which possesses invisibility but not anonymity. We show that these schemes satisfy invisibility, but not anonymity.

3.1 Identity-based Convertible Undeniable Signature Scheme of Wu et al.

In the identity-based convertible undeniable signature scheme of Wu et al. [22], the public parameter $PM = (\hat{e}, g, P_{pub} = g^s, H_1, H_2, H_3)$ and the signer's private key $sk = (SK_{ID} = H_1(ID)^s$, $VK_{ID} = H_1(ID||\text{“}Undeniable\text{”})^s)$. The undeniable signature $\sigma = (U,V,W)$ is given by

$$\begin{aligned}U &= \hat{e}(VK_{ID}, H_2(m)) \\ V &= g^v \\ W &= SK_{ID} \cdot H_3(U,V)^v\end{aligned}$$

where v is the random salt.

Behnia et al. showed that this scheme did not satisfy anonymity [23]. Indeed, given $\sigma = (U,V,W)$, one can identify the signer by checking the validity of σ using the following equation (1) with the signer identity ID:

$$\hat{e}(W,g) = \hat{e}(H_1(ID),P_{pub}) \cdot \hat{e}(H_3(U,V),V) \tag{1}$$

They therefore concluded that invisibility in Wu et al.'s scheme is broken too following the equivalency result of Galbraith and Mao [14].

3.2 Undeniable Signature Scheme of Kurosawa and Takagi

In the undeniable signature scheme of Kurosawa and Takagi [20], the signer's public key $pk = (x,h_1,h_2,H,N_1,N_2)$ and the private key $sk = (d,p_2,q_2)$. The undeniable signature $\sigma = (e,y,x',\omega)$ is given by

$$y^e = x \cdot h_2^{H(x')} \mod N_2 \tag{2}$$

where e is a random exponent and (x',ω) are commitment values of a message m. Note that y must satisfy equation (2) with respect to the signer's public key $pk = (x,h_1,h_2,H,N_1,N_2)$.

Note that the signer randomly chooses $y' \in Z_{N_1}^*$, and $x' \in Z_{N_1}$ is computed such that

$$(y')^{N_1} = x'h_1^{H(m)} \mod N_1$$

and $N_1 \cdot d = 1 \mod lcm(p_1 - 1, q_1 - 1)$ with the signer private key $sk = d$ and $N_1 = p_1 \cdot q_1$.

Phong et al. showed that this scheme did not satisfy anonymity [21]. Indeed, given $\sigma = (e,y,x',\omega)$, one can identify the signer by checking the validity of (e,y) on x' using equation (2) and pk. Phong et al. [21] then claimed that Kurosawa and Takagi's scheme did not possess invisibility too following the equivalency result of Galbraith and Mao [14], even if the signers share a common signature space.

3.3 Convertible Undeniable Signature Scheme of Huang and Wong

In the undeniable signature scheme of Huang and Wong [24], The signer's public key $pk = (X = g^x, Y = g^{\frac{1}{y}}, u, \kappa)$ and the private key $sk = (x,y)$.

The undeniable signature $\sigma = (\delta,\gamma,\theta)$ is given by

$$\delta = H_\kappa(m)^{\frac{1}{(x+s)}} \tag{3}$$

$$\gamma = Y^s \tag{4}$$

$$\theta = u^s \tag{5}$$

where s is the random salt and H_κ is a programmable hash function with an input κ.

Schuldt and Matsuura showed that this scheme did not satisfy anonymity [25]. Indeed, given $\sigma = (\delta,\gamma,\theta)$, one can identify the signer by checking the validity of (γ,θ) using the following equation (6) with pk:

$$\hat{e}(\gamma,u) = \hat{e}(Y,\theta) \tag{6}$$

This issue was also highlighted in the full version [26] of the convertible undeniable signature scheme by Huang and Wong [24] but no solution is given.

3.4 Designated Confirmer Signature Scheme of Huang et al.

In the designated confirmer signature scheme of Huang et al., the same signature structure as in Section 3.3 was adopted. A slight difference is in the signer's public key $pk = u$ and there is confirmer's public key $pk_c = Y$. The undeniable signature $\sigma = (\delta, \gamma, \theta)$ is as in equations (3), (4), and (5) respectively.

Huang et al. highlighted in the full version of their paper that this scheme did not satisfy anonymity [28]. Indeed, given a designated confirmer signature $\sigma = (\delta, \gamma, \theta)$, one can identify the signer and the confirmer using the same equation (6) with (pk, pk_c). Huang et al. claimed that their scheme did not possess anonymity but is invisible.

3.5 Invisibility of the Above Schemes

On the other hand, we can show that all the above schemes satisfy invisibility. Let us recall the invisibility game in Section 2.6.1 where the adversary $\mathscr{A}_I$ is required to guess whether a given $\hat{\sigma}$ is valid on $\hat{m}$ or a random element (invalid on $\hat{m}$). Note that during **Output I**, $\mathscr{A}_I$ submits a challenge message $\hat{m}$ to request a challenge signature $\hat{\sigma}$, where $\hat{\sigma}$ is valid on $\hat{m}$ if the challenge bit $b = 0$ or a random element if $b = 1$. However, Wu et al.'s scheme [22] shows that when the challenge bit $b = 1$, only the signature element $\hat{U}$ is random while $(\hat{V}, \hat{W})$ are not, such that $\hat{V} = g^v$ and $\hat{W} = SK_{ID} \cdot H_3(\hat{U}, \hat{V})^v$ where $v \in \mathbb{Z}_q$.

$$\text{If } b = 0,\ \hat{\sigma} = (\hat{U}, \hat{V}, \hat{W})$$
$$\text{If } b = 1,\ \hat{\sigma} = (random, \hat{V}, \hat{W})$$

Therefore, when $b = 1$, $\hat{\sigma} = (\hat{U}, \hat{V}, \hat{W})$ can be partially verified with equation (1) using the signer's identity ID and $(\hat{V}, \hat{W})$. This observation agrees with the claim of Behnia et al. [23] that the scheme did not possess anonymity, but the claim on invisibility is wrong as equation (1) cannot verify the validity of the challenge signature. In precise, $\mathscr{A}_I$ receives $\hat{\sigma}$ from the challenger which is valid on $\hat{m}$ if $b = 0$ or a random element (invalid on $\hat{m}$) if $b = 1$. In either case, $\mathscr{A}_I$ always output 0 as equation (1) always holds.

The same issue lies in Kurosawa and Takagi's scheme. Even if the signature element $x' \in Z_{N_1}$ is a random element, a valid y can be generated such that $y^e = x \cdot h_2^{H(x')} \mod N_2$ where e is a randomly selected value. At the end, a challenge signature $\hat{\sigma} = (\hat{e}, \hat{y}, \hat{x}', \hat{\omega})$ can still be partially verified with equation (2) using the signer's public key $pk = x$ and $(\hat{e}, \hat{y}, \hat{x}')$ in either case of $b = 0$ or $b = 1$. Apparently, the validity of $(\hat{m}, \hat{\sigma})$ cannot be decided as $\hat{m}$ is perfectly bonded in $\hat{x}'$ which is only verifiable with the knowledge of random value y'. This shows that equation (2) only reveals the identity of the signer but then invisibility still holds.

Likewise, the same issue happens in the security proofs of Huang and Wong's scheme [26] and Huang et al.'s scheme [28]. Even though the signature element $\hat{\delta}$ is a random value, $\hat{\gamma} = Y^s$ and $\hat{\theta} = u^s$ are still correctly generated. At the end, a challenge signature $\hat{\sigma} = (\hat{\delta}, \hat{\gamma}, \hat{\theta})$ can always be partially verified with equation (6) using the signer's public key (Y, u) (and the confirmer's public key $pk_c = Y$ in Huang et al.'s scheme). Therefore, the invisibility is still intact as equation (6) reveals only the identity of the signer (and the confirmer in Huang et al.'s scheme).

4 Discussion

4.1 What is Lacking in the Above Schemes?

We observe that each signer in the above schemes has their own respective signature space because of the condition that a valid signature must satisfy equations (1), (2), and (6) respectively, depending on their respective public keys (signer identity).

More precisely, in the scheme of Wu et al. in Section 3.1, $\sigma = (U,V,W)$ must satisfy equation (1) which depends on ID. Therefore, the valid σ depends on ID. Hence the signature space is different if ID is different.

In the scheme of Kurosawa and Takagi in Section 3.2, $\sigma = (e,y,x',\omega)$ must satisfy equation (2) which depends on $pk = (x,h_1,h_2,H,N_1,N_2)$. Therefore, obviously the valid σ depends on $pk = (x,h_1,h_2,H,N_1,N_2)$. Hence the signature space is different if $pk = (x,h_1,h_2,H,N_1,N_2)$ is different.

Similarly, in the schemes of Huang and Wong and Huang et al. in Sections 3.3 and 3.4 respectively, $\sigma = (\delta,\gamma,\theta)$ must satisfy equation (6) which depends on $pk = (Y,u)$ and $(pk = u, pk_c = Y)$ respectively. Therefore, the valid σ depends on $pk = (Y,u)$ or $(pk = u, pk_c = Y)$. Hence the signature space is different if $pk = (Y,u)$ or $(pk = u, pk_c = Y)$ is different.

Let us now consider the proof of Theorem 1 which is given in Section 2.6.3. The following scenario may happen in the above schemes due to that the signers are having different signature space. We look at this in general without referring to a specific scheme. Suppose that $b = 1$. Then in Output I, $\mathscr{A}_I$ receives $\hat{\sigma}$ from his challenger, and sends it to $\mathscr{A}_A$, where $\hat{\sigma}$ is randomly chosen from the signature space Σ_0 of pk_0. Now if the signature space Σ_1 of pk_1 is different from Σ_0, then $\mathscr{A}_A$ would be able to see that $\hat{\sigma} \in \Sigma_0$ but $\hat{\sigma} \notin \Sigma_1$. This means that

$$\Pr[b'' = b' \mid b = 1] \neq 1/2.$$

This is the part where the one-way equivalency from invisibility to anonymity cannot be achieved in the above schemes, i.e. invisibility does not imply anonymity if the signature space of the signers is different.

Thus, we may conclude that invisibility is preserved in the above schemes even though anonymity is broken mainly due to the signature space issue, i.e., each signer in the above schemes has their own respective signature space which is different. We note that this observation does not contradict to Galbraith and Mao's equivalency result [14] which stated that invisibility implies anonymity and vice versa, if and only if all signers are sharing the same signature space.

5 How to Improve These Schemes?

The above problem in Section 4 does not occur if the signature space of each signer is the same. Therefore, in the design of a provably secure undeniable signature scheme which fulfils both invisibility and anonymity, the designer must take into serious consideration on the signature space of each signer such that the scheme design enables all signers to share the same signature space.

5.1 A Generic Solution

A workaround to invalidate the equations (2) and (6) is to hide the signer's public key. This results in signature space indistinguishability and subsequently preserves the anonymity of the undeniable signature σ. The confirmation protocol is thus an honest verifier zero-knowledge protocol (HVZK) on the hidden public key. In order to ensure the successful running of the disavowal protocol, a dummy signature σ' has to be added to the signer's public key. This allows the signer to generate a HVZK which shows that the same hidden public key is corresponding to the dummy signature σ' but not the signature σ requested by the verifier. Anyway, our generic solution is not applicable to the identity-based undeniable signature scheme, such as Wu et al.'s scheme due to the fact that the signer does not hold the secret of PKG, but the user private key which is a signature from the PKG. Particularly, applying the generic solution requires the signer to expose a witness of his user private key and results in a witness hiding protocol, instead of a zero-knowledge protocol. Since the transcript of a witness hiding protocol is unique, verifier can use this transcript as a proof to convince a third party on the validity of an undeniable signature.

5.1.1 Fix for Convertible Undeniable Signature Scheme of Huang and Wong and Designated Confirmer Signature Scheme of Huang et al.

We can remove $Y = g^{\frac{1}{y}}$ from the pk of Huang and Wong's convertible undeniable signature [24] scheme and add $z = \log_u(Y)$ to the private key such that $pk = (X = g^x, u, \kappa)$ and $sk = (x, y, z)$. The signer then executes the HVZK protocol with the verifier via the confirmation protocol on $\sigma = (\delta = H_\kappa(m)^{\frac{1}{(x+s)}}, \gamma = Y^s, \theta = u^s)$:

$$HVZK\{(z,y) : \gamma = \theta^z \wedge \hat{e}(\delta,\gamma)^y = \hat{e}(H_\kappa(m),g)\hat{e}(\delta,X)^{-1}\}$$

whose details are as follows:

1. The signer chooses random $\tilde{z}, \tilde{y} \in \mathbb{Z}_p^*$ and sends $\tilde{\gamma}_1 = \theta^{\tilde{z}}, \tilde{\gamma}_2 = \hat{e}(\delta,\gamma)^{\tilde{y}}$ to the verifier.

2. The verifier sends a challenge $c \in \mathbb{Z}_p^*$ to the signer.

3. The signer calculates $\hat{z} = \tilde{z} + cz, \hat{y} = \tilde{y} + cy$ and sends $(\hat{z}, \hat{y})$ to the verifier.

4. The verifier accepts if the following hold:

   (a) $\theta^{\hat{z}} = \tilde{\gamma}_1 \gamma^c$

   (b) $\hat{e}(\delta,\gamma)^{\hat{y}} = \tilde{\gamma}_2 \left(\hat{e}(H_\kappa(m),g)\hat{e}(\delta,X)^{-1}\right)^c$.

On the contrary, assume the dummy undeniable signature is a self-signed signature on the public key such that $\sigma' = (\delta', \gamma', \theta')$ and $m' = pk$. The new public key for Huang and Wong's convertible undeniable signature scheme is now $pk' = (pk, \sigma')$. The signer can make use of the inequality proof of discrete logarithm introduced by Camenisch and Shoup [33] to establish the disavowal protocol:

$$\begin{aligned} HVZK\{(z',y',r) :1 = \theta'^{z'}\left(\frac{1}{\gamma'}\right)^r \wedge 1 = \hat{e}(\delta',\gamma')^{y'}(\hat{e}(H_\kappa(pk),g)^{-1}\hat{e}(\delta',X))^r \wedge \\ C_1 = \theta^{z'}\left(\frac{1}{\gamma}\right)^r \wedge C_2 = \hat{e}(\delta,\gamma)^{y'}(\hat{e}(H_\kappa(m),g)^{-1}\hat{e}(\delta,X))^r\} \end{aligned}$$

whose details are as follows:

1. The signer chooses random $r, \tilde{z}', \tilde{y}', \tilde{r} \in \mathbb{Z}_p^*$ and computes $z' = zr \mod p, y' = yr \mod p$, $C_1 = \theta^{z'}\left(\frac{1}{\gamma}\right)^r, C_2 = \hat{e}(\delta,\gamma)^{y'}(\hat{e}(H_\kappa(m),g)^{-1}\hat{e}(\delta,X))^r$. The signer sends

   $$\tilde{B}_1 = \theta'^{\tilde{z}'}\left(\frac{1}{\gamma'}\right)^{\tilde{r}}, \tilde{B}_2 = \hat{e}(\delta',\gamma')^{\tilde{y}'}(\hat{e}(H_\kappa(pk),g)^{-1}\hat{e}(\delta',X))^{\tilde{r}},$$
   $$C_1, C_2, \tilde{C}_1 = \theta^{\tilde{z}'}\left(\frac{1}{\gamma}\right)^{\tilde{r}}, \tilde{C}_2 = \hat{e}(\delta,\gamma)^{\tilde{y}'}(\hat{e}(H_\kappa(m),g)^{-1}\hat{e}(\delta,X))^{\tilde{r}}$$

   to the verifier.

2. The verifier sends a challenge $c \in \mathbb{Z}_p^*$ to the signer.

3. The signer calculates $\hat{z}' = \tilde{z}' + cz', \hat{y}' = \tilde{y}' + cy', \hat{r} = \tilde{r} + cr$ and sends $(\hat{z}', \hat{y}', \hat{r})$ to the verifier.

4. The verifier accepts if the following hold:

   (a) $\theta'^{\hat{z}'}\left(\frac{1}{\gamma'}\right)^{\hat{r}} = \tilde{B}_1$

(b) $\hat{e}(\delta', \gamma')^{\hat{y}'}(\hat{e}(H_\kappa(pk), g)^{-1}\hat{e}(\delta', X))^{\hat{r}} = \tilde{B}_2$

(c) $\theta^{\hat{z}}\left(\frac{1}{\gamma}\right)^{\hat{r}} = \tilde{C}_1 C_1^c$

(d) $\hat{e}(\delta, \gamma)^{\hat{y}}(\hat{e}(H_\kappa(m), g)^{-1}\hat{e}(\delta, X))^{\hat{r}} = \tilde{C}_2 C_1^c$.

Notice that if the step (c) in the disavowal protocol does not hold, the verifier can reject the signer without proceeding to verify the remaining steps. This approach also works for Huang et al.'s [28] designated confirmer signature scheme since it shares the similar signature structure.

5.1.2 Fix for Undeniable Signature Scheme of Kurosawa and Takagi

Likewise, we can remove h_2 from, but add $\sigma_{pk} = (e_{pk}, y_{pk}, x'_{pk}, \omega_{pk})$ to the public key of Kurosawa and Takagi's [20] undeniable signature scheme such that $pk = (x, h_1, H, N_1, N_2, \sigma_{pk})$. Subsequently, the secret prime $s = \log_{h_2}(x)$ is added to the private key such that $sk = (d, p_2, q_2, s)$. The HVZK for the confirmation protocol is thus:

$$\begin{aligned} HVZK\{(s, y') : & y^e = x \cdot (x^{H(x')})^s \mod N_2 \wedge \\ & y'^{N_1} = x' h_1^{H(m)} + \omega N_1 \mod N_1^2\} \end{aligned}$$

whose details are as follows:

1. The signer chooses random $z \in \mathbb{Z}^*_{N_1^2}, \tilde{s} \in \mathbb{Z}^*_e$ and sends $\tilde{Z} = z^{N_1} \mod N_1^2, \tilde{\gamma} = (x^{H(x')})^{\tilde{s}} \mod N_2$ to the verifier.
2. The verifier sends a challenge $c \in \mathbb{Z}^*_e$ to the signer.
3. The signer calculates $\hat{Z} = zy'^c \mod N_1^2, \hat{s} = \tilde{s} + cs$ and sends $(\hat{Z}, \hat{s})$ to the verifier.
4. The verifier accepts if the following hold:

   (a) $\left(x^{H(x')}\right)^{\hat{s}} = \tilde{\gamma}\left(\frac{y^e}{x}\right)^c \mod N_2$

   (b) $\hat{Z}^{N_1} = \tilde{Z}(x' h_1^{H(m)} + \omega N_1)^c \mod N_1^2$.

On the other hand, the disavowal protocol can be constructed as such:

$$\begin{aligned} HVZK\{(s', y', r) : 1 = (x^{H(x'_{pk})})^{s'}\left(\frac{x}{y_{pk}^{e_{pk}}}\right)^r \mod N_2 \wedge y'^{N_1}_{pk} = x'_{pk} h_1^{H(pk)} + \omega_{pk} N_1 \mod N_1^2 \wedge \\ C = (x^{H(x')})^{s'}\left(\frac{x}{y^e}\right)^r \mod N_2 \wedge y'^{N_1} = x' h_1^{H(m)} + \omega N_1 \mod N_1^2\} \end{aligned}$$

to prove the signature element x', similar to its counterpart x'_{pk}, can be a valid element under N_1, but such x' does not yield a valid σ under the same pk. The details of the disavowal protocol are as follows:

1. The signer chooses random $z, z_{pk} \in \mathbb{Z}^*_{N_1^2}, \tilde{s}', r, \tilde{r} \in \mathbb{Z}^*_e$ and computes $s' = sr$, $C = (x^{H(x')})^{s'}\left(\frac{x}{y^e}\right)^r$ $\mod N_2$. The signer sends

   $$\tilde{B} = (x^{H(x'_{pk})})^{\tilde{s}'}\left(\frac{x}{y_{pk}^{e_{pk}}}\right)^{\tilde{r}}, \tilde{Z}_{pk} = z_{pk}^{N_1} \mod N_1^2,$$

   $$C, \tilde{C} = (x^{H(x')})^{\tilde{s}'}\left(\frac{x}{y^e}\right)^{\tilde{r}}, \tilde{Z} = z^{N_1} \mod N_1^2$$

   to the verifier.

2. The verifier sends a challenge $c \in \mathbb{Z}_e^*$ to the signer.
3. The signer calculates $\hat{Z}_{pk} = z_{pk}{y'}_{pk}^{c} \mod N_1^2, \hat{Z} = zy'^c \mod N_1^2, \hat{s}' = \tilde{s}' + cs', \hat{r} = \tilde{r} + cr$ and sends $(\hat{Z}_{pk}, \hat{Z}, \hat{s}', \hat{r})$ to the verifier.
4. The verifier accepts if the following hold:
   (a) $(x^{H(x'_{pk})})^{\hat{s}'} \left(\frac{x}{y_{pk}^{e_{pk}}}\right)^{\hat{r}} = \tilde{B} \mod N_2$
   (b) $\hat{Z}_{pk}^{N_1} = \tilde{Z}_{pk}(x'_{pk} h_1^{H(pk)} + \omega_{pk} N_1)^c \mod N_1^2$
   (c) $(x^{H(x')})^{\hat{s}'} \left(\frac{x}{y^e}\right)^{\hat{r}} = \tilde{C} C^c \mod N_2$
   (d) $\hat{Z}^{N_1} = \tilde{Z}(x' h_1^{H(m)} + \omega N_1)^c \mod N_1^2$

Notice that if the step (c) in the disavowal protocol does not hold, the verifier can reject the signer without proceeding to verify the remaining steps.

5.2 A Summary of the Fixes

These fixes remove the ability to reveal the identity of the signer and thus enable the schemes to achieve the anonymity of the undeniable signature. Since signature space is not an issue anymore, by Galbraith and Mao's equivalency result [14], these schemes possess invisibility as well. Furthermore, the unforgeability of each fixed scheme is preserved because no changes were made to the signature structure. However, as shown by Ogata et al. [32], when the confirmation and disavowal protocols are based on HVZK protocols, an undeniable signature scheme can be proven to be unforgeable as well as unforgeable-and-unimpersonation against the passive adversaries only but not the active adversaries. A ready solution for this issue is to apply the designated-verifier technique [32] on the non-interactive version of HVZK protocols in order to be secure against active adversaries. The resulted non-interactive proof proves either the (in)validity of the undeniable signature or the knowledge of the verifier's private key, whose knowledge is thus non-transferable as opposed to the normal non-interactive zero-knowledge proof. Our generic solution can adopt the designated-verifier technique to avoid the active adversaries but with assumption that every verifier has a public key, which is not always the case in practice. A more elegant solution to achieve security against active adversaries is to construct the confirmation and disavowal protocols using the perfect zero-knowledge protocol (ZKIP), such as the one proposed by Phong et al. [21] for Huang and Wong's convertible undeniable signature scheme [24] though the solution is not known to work on RSA-based undeniable signature schemes. We leave the ZKIP constructions for the schemes analysed in this work as an open problem for now.

6 Conclusion

In this paper, we discovered that the past attacks on some existing undeniable signature schemes are not entirely correct as the invisibility of these schemes is still intact although the anonymity is broken. Thus, we managed to partially falsify the previous cryptanalysis mounted on Wu et al.'s Scheme by Behnia et al. and Kurosawa and Takagi's Scheme by Phong et al. We further pointed out that Galbraith and Mao's equivalency theorem is not applicable on these schemes due to the different signature space owned by each signer. We also showed that Huang and Wong's as well as Huang et al.'s schemes faced the similar issue. Subsequently, we proposed a generic solution for the conventional or non-identity-based schemes using the honest verifier zero-knowledge proofs of knowledge protocols. Our finding can be viewed as a reminder to researchers to exercise extreme caution in the design of a provably secure undeniable signature scheme which fulfils both invisibility and anonymity.

Acknowledgments

The authors would like to acknowledge the Malaysia government's Fundamental Research Grant Scheme (FRGS/1/2018/ICT04/MMU/01/01) for supporting this work.

References

[1] J.-C. Loh, S.-H. Heng, S.-Y. Tan, and K. Kurosawa, "A note on the invisibility and anonymity of undeniable signature schemes," in *Proc. of the 20th International Workshop on Information Security Applications (WISA'19), Jeju Island, South Korea*, ser. Lecture Notes in Computer Science, vol. 11897. Springer, Cham, August 2019, pp. 112–125.

[2] D. Chaum and H. Van Antwerpen, "Undeniable signatures," in *Proc. of the 1989 Conference on the Theory and Application of Cryptology (Crypto'89), Santa Barbara, California, USA*, ser. Lecture Notes in Computer Science, vol. 435. Springer, New York, August 1989, pp. 212–216.

[3] D. Pointcheval, "Self-scrambling anonymizers," in *Proc. of the 4th International Conference on Financial Cryptography (FC'00), Anguilla, British West Indies*, ser. Lecture Notes in Computer Science, vol. 1962. Springer, Berlin, Heidelberg, February 2000, pp. 259–275.

[4] K. Sakurai, "A bulletin-board based digital auction scheme with bidding down strategy-towards an onymous electronic bidding without anonymous channels nor trusted centers in cryptographic techniques and e-commerce," in *Proc. of the 1999 International Workshop on Cryptographic Techiniques and E-Commerce (CryTEC'99)*, 1999.

[5] K. Sakurai and S. Miyazaki, "An anonymous electronic bidding protocol based on a new convertible group signature scheme," in *Proc. of the 5th Australasian Conference on Information Security and Privacy (ACISP'00), Brisbane, Australia*, ser. Lecture Notes in Computer Science, vol. 1841. Springer, Berlin, Heidelberg, July 2000, pp. 385–399.

[6] J. Boyar, D. Chaum, I. Damgård, and T. P. Pedersen, "Convertible undeniable signatures." in *Proc. of the 1990 Conference on the Theory and Application of Cryptography (Crypto'90), Santa Barbara, California, USA*, ser. Lecture Notes in Computer Science, vol. 537. Springer, Berlin, Heidelberg, 1990, pp. 189–205.

[7] M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated verifier proofs and their applications," in *Proc. of the 1996 International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'96), Saragossa, Spain*, ser. Lecture Notes in Computer Science, vol. 1070. Springer, Berlin, Heidelberg, May 1996, pp. 143–154.

[8] D. Chaum, "Designated confirmer signatures," in *Proc. of the 1994 Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy*, ser. Lecture Notes in Computer Science, vol. 950. Springer, Berlin, Heidelberg, May 1994, pp. 86–91.

[9] T. Okamoto, "Designated confirmer signatures and public-key encryption are equivalent," in *Proc. of the 14th Annual International Cryptology Conference (CRYPTO'94), Santa Barbara, California, USA*, ser. Lecture Notes in Computer Science, vol. 839. Springer, Berlin, Heidelberg, August 1994, pp. 61–74.

[10] B. Libert and J.-J. Quisquater, "Identity based undeniable signatures," in *Proc. of the 2004 Cryptographers' Track at the RSA Conference (CT-RSA'04), San Francisco, California, USA*, ser. Lecture Notes in Computer Science, vol. 2964. Springer, Berlin, Heidelberg, February 2004, pp. 112–125.

[11] S. Duan, "Certificateless undeniable signature scheme," *Information Sciences*, vol. 178, no. 3, pp. 742–755, February 2008.

[12] D. Chaum, E. van Heijst, and B. Pfitzmann, "Cryptographically strong undeniable signatures, unconditionally secure for the signer," in *Proc. of the 1991 Annual International Cryptology Conference (CRYPTO'91), Santa Barbara, California, USA*, ser. Lecture Notes in Computer Science, vol. 576. Springer, Berlin, Heidelberg, August 1991, pp. 470–484.

[13] J. Camenisch and M. Michels, "Confirmer signature schemes secure against adaptive adversaries," in *Proc. of the 2000 International Conference on the Theory and Applications of Cryptographic Techniques, Bruges, Belgium*, ser. Lecture Notes in Computer Science, vol. 1807. Springer, Berlin, Heidelberg, May 2000, pp. 243–258.

[14] S. D. Galbraith and W. Mao, "Invisibility and anonymity of undeniable and confirmer signatures," in *Proc. of the 2003 Cryptographers' Track at the RSA Conference (CT-RSA'03), San Francisco, California, USA*, ser. Lecture Notes in Computer Science, vol. 2612. Springer, Berlin, Heidelberg, April 2003, pp. 80–97.

[15] X. Huang, Y. Mu, W. Susilo, and W. Wu, "Provably secure pairing-based convertible undeniable signature with short signature length," in *Proc. of the 2007 International Conference on Pairing-Based Cryptography (Pairing'07), Tokyo, Japan*, ser. Lecture Notes in Computer Science, vol. 4575. Springer, Berlin, Heidelberg, July 2007, pp. 367–391.

[16] D. Galindo, J. Herranz, and E. Kiltz, "On the generic construction of identity-based signatures with additional properties," in *Proc. of the 12th Internatinoal Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt'06), Shanghai, China*, ser. Lecture Notes in Computer Science, vol. 4284. Springer, Berlin, Heidelberg, December 2006, pp. 178–193.

[17] K. Kurosawa and S.-H. Heng, "3-move undeniable signature scheme." in *Proc. of the 24th Annual International Conference on Theory and Application of Cryptographic Techniques (EUROCRYPT'05), Aarhus, Denmark*, ser. Lecture Notes in Computer Science, vol. 3494. Springer, Berlin, Heidelberg, May 2005, pp. 181–197.

[18] F. Laguillaumie and D. Vergnaud, "Time-selective convertible undeniable signatures," in *Proc. of the 2005 Cryptographers' Track at the RSA Conference (CT-RSA'05), San Francisco, California, USA*, ser. Lecture Notes in Computer Science, vol. 3376. Springer, Berlin, Heidelberg, February 2005, pp. 154–171.

[19] F. Laguillaumie and D. Vergnaud, "Short undeniable signatures without random oracles: The missing link," in *Proc. of the 6th International Conference on Cryptology in India (INDOCRYPT'05), Bangalore, India*, ser. Lecture Notes in Computer Science, vol. 3797. Springer, Berlin, Heidelberg, December 2005, pp. 283–296.

[20] K. Kurosawa and T. Takagi, "New approach for selectively convertible undeniable signature schemes," in *Proc. of the 12th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'06), Shanghai, China*, ser. Lecture Notes in Computer Science, vol. 4284. Springer, Berlin, Heidelberg, December 2006, pp. 428–443.

[21] L. T. Phong, K. Kurosawa, and W. Ogata, "New rsa-based (selectively) convertible undeniable signature schemes," in *Proc. of the 2nd International Conference on Cryptology in Africa (AFRICACRYPT'09), Gammarth, Tunisia*, ser. Lecture Notes in Computer Science, vol. 5580. Springer, Berlin, Heidelberg, June 2009, pp. 116–134.

[22] W. Wu, Y. Mu, W. Susilo, and X. Huang, "Provably secure identity-based undeniable signatures with selective and universal convertibility," in *Proc. of the 3rd International Conference on Information Security and Cryptology (Inscrypt'07), Xining, China*, ser. Lecture Notes in Computer Science, vol. 4990. Springer, Berlin, Heidelberg, August-September 2007, pp. 25–39.

[23] R. Behnia, S.-Y. Tan, and S.-H. Heng, "Cryptanalysis of an identity-based convertible undeniable signature scheme," in *Proc. of the 2nd International Conference on Paradigms in Cryptology (Mycrypt'16), Kuala Lumpur, Malaysia*, ser. Lecture Notes in Computer Science, vol. 10311, no. July. Springer, Cham, 2017, pp. 474–477.

[24] Q. Huang and D. S. Wong, "New constructions of convertible undeniable signature schemes without random oracles," https://eprint.iacr.org/2009/517 [Online; Accessed on March 25, 2020], 2009, cryptology ePrint Archive, Report 2009/517.

[25] J. Schuldt and K. Matsuura, "An efficient convertible undeniable signature scheme with delegatable verification," in *Proc. of the 6th International Conference on Information Security, Practice and Experience (ISPEC'10), Seoul, Korea*, ser. Lecture Notes in Computer Science, vol. 6047. Springer, Berlin, Heidelberg, May 2010, pp. 276–293.

[26] Q. Huang and D. S. Wong, "Short and efficient convertible undeniable signature schemes without random oracles," *Theoretical Computer Science*, vol. 476, pp. 67 – 83, March 2013.

[27] Q. Huang, D. S. Wong, and W. Susilo, "A new construction of designated confirmer signature and its appli-

cation to optimistic fair exchange," in *Proc. of the 2010 International Conference on Pairing-Based Cryptography (Pairing'10), Yamanaka Hot Spring, Japan*, ser. Lecture Notes in Computer Science, vol. 6487. Springer, Berlin, Heidelberg, December 2010, pp. 41–61.

[28] Q. Huang, D. S. Wong, and W. Susilo, "Efficient designated confirmer signature and dcs-based ambiguous optimistic fair exchange," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 4, pp. 1233–1247, December 2011.

[29] J. C. Schuldt and K. Matsuura, "Efficient convertible undeniable signatures with delegatable verification," *IEICE transactions on fundamentals of electronics, communications and computer sciences*, vol. E94.A, no. 1, pp. 71–83, 2011.

[30] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proc. of the 21st Annual International Cryptology Conference (CRYPTO'01), Santa Barbara, California, USA*, ser. Lecture Notes in Computer Science, vol. 2139. Springer, Berlin, Heidelberg, August 2001, pp. 213–229.

[31] R. Cramer, I. Damgård, and B. Schoenmakers, "Proofs of partial knowledge and simplified design of witness hiding protocols," in *Proc. of the 1994 Annual International Cryptology Conference (CRYPTO'94), Santa Barbara, California, USA*, ser. Lecture Notes in Computer Science, vol. 839. Springer Berlin Heidelberg, August 1994, pp. 174–187.

[32] W. Ogata, K. Kurosawa, and S.-H. Heng, "The security of the fdh variant of chaum's undeniable signature scheme," *IEEE Transactions on Information Theory*, vol. 52, no. 5, pp. 2006–2017, May 2006.

[33] J. Camenisch and V. Shoup, "Practical verifiable encryption and decryption of discrete logarithms," in *Proc. of the 2003 Annual International Cryptology Conference (CRYPTO'03), Santa Barbara, California, USA*, ser. Lecture Notes in Computer Science, vol. 2729. Springer, Berlin, Heidelberg, August 2003, pp. 126–144.

Author Biography

Jia-Ch'ng Loh received his Master of Science (Information Technology) in 2019 and Bachelor of Information Technology (Hons.) (Security Technology) in 2016 at Multimedia University. Currently he is a research assistant in the National University of Singapore. His research interests lie in Cryptography and Cybersecurity, and the ongoing research topics are focusing on the area of privacy-preserving in network security and biometrics systems.

Swee-Huay Heng received her Doctor of Engineering degree from the Tokyo Institute of Technology, Japan. She is currently a Professor in the Faculty of Information Science and Technology, Multimedia University, Malaysia. Her research interests are cryptography and information Security. She was the Programme Chair of ProvSec 2010, CANS 2010 and ISPEC 2019. She served as Technical Programme Committee of many international security conferences.

Syh-Yuan Tan received his Ph.D. degree in engineering from Universiti Tunku Abdul Rahman, Malaysia in 2015. He is currently with the School of Computing, Newcastle University UK as a post-doctoral researcher. He was a senior lecturer with Multimedia University, Malaysia, from 2012 to 2018. His current research interests include cryptography and information security, particularly on provable security techniques.

Kaoru Kurosawa received the B.E. and Dr. Eng. degrees in electrical engineering in 1976 and 1981, respectively, from Tokyo Institute of Technology. From 1997 to 2001, he was a Professor in Tokyo Institute of Technology. He is currently a Professor in the Department of Computer and Information Sciences at Ibaraki University. His current research interest is cryptography. He was Program Chair for Asiacrypt 2007, PKC 2013 and some other conferences. Dr. Kurosawa is a Fellow of IACR and IEICE, and a member of IEEE and ACM. He received the excellent paper award of IEICE in 1981, the young engineer award of IEICE in 1986, Telecom System Scientific Award of Telecommnucations Avdancement Foundation in 2006 and Achievement Award of IEICE in 2007.