Secure Convertible Undeniable Signature Scheme Using Extended Euclidean Algorithm without Random Oracles

Shi-Jinn Horng[1,2], Shiang-Feng Tzeng[2], Pingzhi Fan[1], Xian Wang[1], Tianrui Li[1], and Muhammad Khurram Khan[3]
[1]School of Information Science and Technology, Southwest Jiaotong University,
Chengdu 610031, China
[e-mail: horngsj@yahoo.com.tw, pingzhifan@gmail.com, drwangxian@gmail.com, trli@swjtu.edu.cn]
[2]Department of Computer Science and Information Engineering,
National Taiwan University of Science and Technology, Taipei 106, Taiwan
[e-mail: sftzeng@gmail.com]
[3]Center of Excellence in Information Assurance, King Saud University, Kingdom of Saudi Arabia
[e-mail: mkhurram@ksu.edu.sa]
*Corresponding author: Shi-Jinn Horng

Received February 25, 2013; revised April 27, 2013; revised May 19, 2013; accepted May 22, 2013; published June 26, 2013

Abstract

A convertible undeniable signature requires a verifier to interact with the signer to verify a signature and furthermore allows the signer to convert a valid one to publicly verifiable signature. In 2007, Yuen *et al*. proposed a convertible undeniable signature without random oracles in pairings. However, it is recently shown that Yuen *et al*.'s scheme is not invisible for the standard definition of invisibility. In this paper, we propose a new improvement by using extended Euclidean algorithm that can overcome the visibility attack. The proposed scheme has been evaluated based on computation and communication complexities and the performance comparisons of Yuen *et al*.'s scheme and various convertible undeniable signature schemes are provided. Moreover, it has been observed that the proposed algorithm reduces the computation and communication times significantly.

Keywords: Convertible, extended Euclidean algorithm, random oracle, undeniable signature.

This work was supported in part by the National Science Council under contract number NSC-99-2916-I-011-002-A1, and it was also partially supported by the 111 Project under the grant No. 111-2-1 and One Hundred Person Project 2012, Sichuan Province. The work of X. Wang was supported by the National Science Foundation of China under Grants 60902023 and 61171096, as well as by the Fundamental Research Funds for the Central Universities under the Grant SWJTU12CX093.

http://dx.doi.org/10.3837/tiis.2013.06.010

1. Introduction

The concept of undeniable signature was first introduced in 1989 by Chaum and van Antwerpen [1]. In this setting, one has to interact with the signer in order to be convinced of the validity or invalidity of a given signature. Undeniable signature has found various applications such as in licensing software [1], electronic cash [2] [3] [4], confidential business agreement [5], electronic voting and auction [6][7]. The popular application is in licensing software. For instance, software vendors might desire to sign on their products to provide authenticity to their paying customers. Nevertheless, they strictly disallow dishonest customers who have illegally duplicated their software to verify the validity of these signatures. Undeniable signature plays a significant role here as it allows only legitimate users to verify the validity of the signatures on the software. So far, many undeniable signature schemes were discussed.

In order to link undeniable signature to regular signature, Boyar *et al*. [8] introduced convertible undeniable signatures which allow the signer to convert his undeniable signatures into publicly verifiable signatures. Their signatures provide individual and universal conversions of the signatures. Two types of conversions were introduced: individual conversion which enables the signer to individually convert signatures, and universal conversion which enables the signer to convert all (existing and future) signatures. Unfortunately, the scheme was later broken and improved by Michel *et al*. in [9] with no security proof given.

Gennaro *et al*. [10] proposed the first RSA-based convertible undeniable signature and described several extensions of it. Their scheme was later shown to be visible in [11]. Kurosawa and Takagi [12] proposed a scheme which they claimed to be the RSA based scheme secure in the standard model, but it was shown by Phong *et al*. [13] that the scheme does not provide full invisibility. Furthermore, Phong *et al*. [13] proposed a new convertible RSA based scheme secure in the standard model.

Recently, Yuen *et al*. [14] presented the first convertible undeniable signature without random oracles in pairings. By using more standard assumptions in the security proofs, Yuen *et al*.'s scheme is better than the existing undeniable signature scheme without random oracles by Laguillaumie and Vergnaud [15]. Yuen *et al*. proposed variant of undeniable signature is proven unforgeable by the computational Diffie-Hellman (CDH) assumption and anonymous by the decision linear assumption. Therefore, by removing the protocol for convertible parts, their undeniable signature scheme is the first proven secure scheme without using random oracles and without using a new assumption in discrete logarithm settings.

However, Phong *et al*. [16] and Zhao [17] pointed out that the scheme of Yuen *et al*. [14] is not invisible for the standard definition of invisibility, respectively. The adversary can decide whether the challenge message-signature pair is valid or invalid by constructing and submitting another message-signature pair to the confirmation/disavowal oracle. In [16], Phong *et al*. showed that if the strong definition of invisibility is used, the scheme in [14] is totally insecure; while if the weaker definition is used, then the invisibility proof provided in [14] is incorrect. In [17], Zhao also thought how to define exactly the security model for cryptographic primitive is an important work. In the full version of [14], Yuen *et al*. have revised this visibility problem of their scheme in [18]. Yuen *et al*.'s scheme [18] uses two Waters hashes along with a strong one-time signature [19].

In addition, Phong *et al*. [16] proposed two efficient schemes which are claimed to be the first practical discrete logarithm based convertible undeniable signature schemes in the standard model. Later, Huang and Wong [20] presented a scheme with even shorter signatures than the schemes by Phong *et al*. [16], but only prove the scheme to be invisible according to a weaker definition of invisibility. Recently, Schuldt and Matsuura [21] proposed another convertible undeniable signature scheme in the standard model. Their scheme combines linear encryption and Waters signature, and has unforgeability based on CDH assumption and invisibility based on decision linear assumption.

In this article, we will propose a new improvement of convertible undeniable signature scheme that can overcome the weakness of invisibility. In the next section, we explain some knowledge and the security models of the undeniable signature scheme. In Section 3, we show the existing scheme and its weakness. In Section 4, our scheme will be presented in detail. The security proofs and the performance evaluation of our scheme will be shown in Section 5. Finally, the conclusion will be given in the last section.

2. Preliminaries

In this section, we describe the bilinear maps with certain properties, some hard problems and the concepts of mathematical tools. Further, we give precise definitions and security models for the undeniable signature scheme.

2.1 Pairings and Some Computational Problems

We briefly review the necessary facts about bilinear pairing. We consider two groups $\mathbb{G}$ and $\mathbb{G}_T$ of the same prime order p. Let g be a generator of $\mathbb{G}$. A bilinear map is a map $\hat{e}: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ satisfying the following properties [22].

1. Bilinear: We say that a map $\hat{e}: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is bilinear if $\hat{e}(x^a, y^b) = \hat{e}(x, y)^{ab}$ for all x, $y \in \mathbb{G}$ and all a, $b \in Z_p$.
2. Non-degenerate: The map does not send all pairs in $\mathbb{G} \times \mathbb{G}$ to the identity in $\mathbb{G}_T$. Observe that since $\mathbb{G}$, $\mathbb{G}_T$ are groups of prime order this implies that if g is a generator of $\mathbb{G}$ then $\hat{e}(g, g)$ is a generator of $\mathbb{G}_T$.
3. Computable: There exists a polynomial time algorithm to compute $\hat{e}$.

Definition 2.1 The computational Diffie-Hellman (CDH) problem is that, given g, g^x, $g^y \in \mathbb{G}$ for unknown x, $y \in Z_p^*$, to calculate g^{xy}. The CDH assumption states that it is computationally intractable to compute the value g^{xy}.

Definition 2.2 The Decision Linear [23] problem is that, given u, u^a, v, v^b, h, $h^c \in \mathbb{G}$ for unknown a, b, $c \in Z_p^*$ to output 1 if $c = a + b$ and output 0 otherwise. The Decision Linear assumption states that it is hard to distinguish $c = a + b$.

Definition 2.3 The discrete logarithm problem is that, given g, $g^a \in \mathbb{G}$, to calculate a.

2.2 The Extended Euclidean Algorithm

Let $a \in \mathbb{Z}_n$. The modular multiplicative inverse [24] of a modulo n is defined: it is the number x such that $ax = 1 \pmod{n}$. If such an x exists, then it is unique, and a is said to be invertible; the modular multiplicative inverse of a is denoted by a^{-1}. The extended Euclidean algorithm may be used to calculate it. We describe the concept of the extended Euclidean algorithm as follows.

The extended Euclidean algorithm [24] is an extension to the Euclidean algorithm. Let a and b be non-negative integers. Besides finding the greatest common divisor of integers a and b, as the Euclidean algorithm does, it also finds integers x and y satisfying $ax + by = d$, where $d = \gcd(a, b)$. If $d > 1$, then $a^{-1} \bmod n$ does not exist. The extended Euclidean algorithm is particularly useful when a and b are coprime, since x is the multiplicative inverse of a modulo b, and y is the multiplicative inverse of b modulo a. The concept of the extended Euclidean algorithm is very useful in our scheme construction.

2.3 Security Notions

The undeniable signature scheme consists of the following algorithms.

Setup. It is a probabilistic algorithm which takes as input k. The outputs are the common parameters which are shared by all the users in the system.

Key Generation. It is a probabilistic algorithm which takes as input the common parameters and generates a secret/public key pair (sk, pk) for a user in the system.

Sign. It is a probabilistic algorithm which takes as input a secret key sk, a message m and common parameters, generates the undeniable signature σ.

Confirmation/Disavowal. It is a protocol between the signer and a verifier which takes as input a message-signature pair (m, σ), a pair of keys (sk, pk) and common parameters. This protocol allows the signer to convince the verifier that the given message-signature pair is valid or invalid, with the knowledge of the corresponding secret key sk.

The following algorithms are only for the undeniable signature scheme with convertible property.

Individual Conversion. It is a deterministic algorithm which takes as input a secret key sk, a message-signature pair (m, σ) and common parameters, generates the individual receipt r.

Individual Verification. It is a deterministic algorithm which takes as input a public key pk, a message-signature pair (m, σ), an individual receipt r and common parameters, generates $\perp$ if r is an invalid individual receipt. Otherwise, outputs 1 if σ is a valid signature of m and outputs 0 otherwise.

Universal Conversion. It is a deterministic algorithm which takes as input a secret key sk and common parameters, generates the universal receipt R.

Universal Verification. It is a deterministic algorithm which takes as input a public key pk, any message-signature pair (m, σ), an universal receipt R and common parameters, generates $\perp$ if R is an invalid universal receipt. Otherwise, outputs 1 if σ is a valid signature of m and outputs 0 otherwise.

2.4 Unforgeability

The unforgeability is defined by using the following game between a simulator $\mathcal{S}$ and an adversary $\mathcal{A}$.

1. $\mathcal{S}$ sends the public keys and parameters to $\mathcal{A}$. (For convertible schemes, $\mathcal{S}$ also gives the universal receipt to $\mathcal{A}$.)
2. $\mathcal{A}$ performs a series of queries.
   - Signing queries. For $i = 1, 2, \cdots, q_s$ for some q_s, $\mathcal{A}$ queries a message m_i to the signing oracle adaptively and receives a signature σ_i.
   - Confirmation/disavowal queries. For $j = 1, 2, \cdots, q_c$ for some q_c, $\mathcal{A}$ queries a message-signature pair to the confirmation/disavowal oracle adaptively. If it is a

valid pair, then the oracle returns a bit $\mu = 1$ and proceeds with the execution of the confirmation protocol with $\mathcal{A}$. Otherwise, the oracle returns a bit $\mu = 0$ and proceeds with the execution of the disavowal protocol with $\mathcal{A}$.

3. $\mathcal{A}$ succeeds in strong forgery if (m^*, σ^*) is valid and (m^*, σ^*) is not among the pairs (m_i, σ_i) generated during the signing oracle queries.

$\mathcal{A}$ wins the game if σ^* is a valid undeniable signature for a message m^*.

Definition 2.4 A (convertible) undeniable signature scheme is said to be existential unforgeable under adaptive chosen message attack if no probabilistic polynomial time (PPT) $\mathcal{A}$ has a non-negligible advantage in the above game.

2.5 Invisibility

The invisibility is defined as follows. Consider the following game between a simulator $\mathcal{S}$ and an adversary $\mathcal{A}$.

1. $\mathcal{S}$ delivers the public keys and parameters to $\mathcal{A}$.
2. $\mathcal{A}$ executes a series of queries.
   - Signing queries, Confirmation/disavowal queries: the same as unforgeability.
   - (For convertible schemes only.) Receipt generating oracle. For $i = 1, 2, \cdots, q_r$ for some q_r, $\mathcal{A}$ queries a message-signature pair (m_i, σ_i) to the receipt generating oracle adaptively and receives an individual receipt r_i.
3. $\mathcal{A}$ chooses a message m^* which has never been queried to the signing oracle, and sends it to $\mathcal{S}$. $\mathcal{S}$ selects a hidden bit b. If $b = 1$, then $\mathcal{S}$ calculates σ^* using the signing oracle, otherwise $\mathcal{S}$ chooses σ^* uniformly at random from the signature space.
4. $\mathcal{A}$ is not allowed to query m^* to the signing oracle and the receipt generating oracle. In addition, $\mathcal{A}$ is not allowed to query (m^*, σ^*) to the confirmation/disavowal oracle.
5. At the end of this game, $\mathcal{A}$ outputs a guess b'.

$\mathcal{A}$ wins the game if $b = b'$. $\mathcal{A}$'s advantage is $\mathrm{Adv}(\mathcal{A}) = |Pr[b' = b] - \frac{1}{2}|$.

Definition 2.5 A (convertible) undeniable signature scheme is said to have the property of invisibility under adaptive chosen message attack if no PPT $\mathcal{A}$ has a non-negligible advantage in the above game.

2.6 Impersonation

The impersonation is defined by using the following game between a simulator $\mathcal{S}$ and an adversary $\mathcal{A}$.

1. $\mathcal{S}$ sends the public keys and parameters to $\mathcal{A}$.
2. $\mathcal{A}$ executes a series of Signing oracle and Confirmation/Disavowal oracle, which are the same as the one in unforgeability.
3. $\mathcal{A}$ outputs a bit b and a message-signature pair (m^*, σ^*). If $b = 1$, $\mathcal{A}$ performs the confirmation protocol with $\mathcal{S}$. Otherwise $\mathcal{A}$ executes the disavowal protocol with $\mathcal{S}$.

$\mathcal{A}$ wins the game if $\mathcal{S}$ is convinced that σ^* is a valid signature for the message m^* if $b = 1$, or is an invalid signature for the message m^* if $b = 0$.

Definition 2.6 A (convertible) undeniable signature scheme is said to be secure against impersonation under adaptive chosen message attack if no PPT $\mathcal{A}$ has a non-negligible advantage in the above game.

3. The Yuen-Au-Liu-Susilo Scheme and Its Weakness

In this section, we first review the Yuen-Au-Liu-Susilo scheme [14] in brief using the same notations, and then show a weakness [16][17] on invisibility of their scheme.

3.1 Review of the Yuen-Au-Liu-Susilo Scheme

The Yuen-Au-Liu-Susilo scheme consists of the following algorithms.

Setup. Let $\mathbb{G}$, $\mathbb{G}_T$ be groups of prime order p. Given a pairing: $\hat{e}: \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. Choose generators g, $g_2 \in \mathbb{G}$. Generator $u' \in \mathbb{G}$ is randomly selected, and a random n-length vector $\mathrm{U} = (u_i)$, whose elements are chosen at random from $\mathbb{G}$.

Next, choose an integer d as a system parameter. Denote $\ell = 2^d$ and $k = n/d$. Let $H_j: \{0,1\}^n \to Z_\ell^*$ be collision resistant hash functions, where $1 \le j \le k$.

Key Generation. Randomly choose α, β', $\beta_i \in Z_p^*$ for $1 \le i \le \ell$. Compute $g_1 = g^\alpha$, $v' = g^{\beta'}$ and $v_i = g^{\beta_i}$. The secret keys are $(\alpha, \beta', \beta_1, \beta_2, \cdots, \beta_\ell)$. The public keys are $(g_1, v', v_1, v_2, \cdots, v_\ell)$.

Sign. To sign a message $m = (m_1, m_2, \cdots, m_n) \in \{0,1\}^n$, denote $\bar{m}_j = H_j(m)$ for $1 \le j \le k$. The signer selects $r \in Z_p^*$, and calculates the signature

$$S_1 = g_2^\alpha \left(u' \prod_{i=1}^{n} u_i^{m_i}\right)^r,$$

$$S_{2,j} = \left(v' \prod_{i=1}^{\ell} v_i^{\bar{m}_j^i}\right)^r.$$

The undeniable signature of a message m is $(S_1, S_{2,1}, S_{2,2}, \cdots, S_{2,k})$.

Confirmation/Disavowal. On input $(S_1, S_{2,1}, S_{2,2}, \cdots, S_{2,k})$, the signer calculates for $1 \le j \le k$

$$L = \hat{e}(g, g_2),$$

$$M = \hat{e}(g_1, g_2),$$

$$N_j = \hat{e}\left(v' \prod_{i=1}^{\ell} v_i^{\bar{m}_j^i}, g_2\right),$$

$$O_j = \hat{e}\left(v' \prod_{i=1}^{\ell} v_i^{\bar{m}_j^i}, S_1\right) \Big/ \hat{e}\left(S_{2,j}, u' \prod_{i=1}^{n} u_i^{m_i}\right).$$

Then, the signer executes the 3-move WI protocols [25] of the equality or the inequality of discrete logarithm $\alpha = log_L M$ and $log_{N_j} O_j$ in $\mathbb{G}_T$.

Individual Conversion. Upon input the undeniable signature $(S_1, S_{2,1}, S_{2,2}, \cdots, S_{2,k})$ on the message m, the signer calculates $\bar{m}_1 = H_1(m)$ and

$$S_2' = S_{2,1}^{1/(\beta' + \sum_{i=1}^{\ell} \beta_i \bar{m}_1^i)}.$$

Output the individual receipt S_2' for the message m.

Individual Verification. Upon input the undeniable signature $(S_1, S_{2,1}, S_{2,2}, \cdots, S_{2,k})$ for the message m and the individual receipt S_2', calculate $\bar{m}_j = H_j(m)$ for $1 \le j \le k$ and check if

$$\hat{e}(g, S_{2,j}) = \hat{e}\left(S_2', v' \prod_{i=1}^{\ell} v_i^{\bar{m}_j^i}\right).$$

If they are not equal, output $\perp$. Otherwise compare if

$$\hat{e}(g, S_1) = \hat{e}(g_1, g_2) \cdot \hat{e}\left(S_2', u' \prod_{i=1}^{n} u_i^{m_i}\right).$$

Output 1 if the above holds. Otherwise output 0.

Universal Conversion. The signer publishes her/his universal receipt $(\beta', \beta_1, \beta_2, \cdots, \beta_\ell)$.

Universal Verification. Upon input the signature $(S_1, S_{2,1}, S_{2,2}, \cdots, S_{2,k})$ on the message m and the universal receipt $(\beta', \beta_1, \beta_2, \cdots, \beta_\ell)$, check if

$$v' = g^{\beta'},$$

$$v_i = g^{\beta_i},$$

for $1 \le i \le \ell$. If they are not equal, output $\perp$. Otherwise calculate $\bar{m}_j = H_j(m)$ for $1 \le j \le k$ and compare if

$$\hat{e}(g, S_1) = \hat{e}(g_1, g_2) \cdot \hat{e}\left(S_{2,j}^{1/\left(\beta' + \sum_{i=1}^{\ell} \beta_i \bar{m}_j^i\right)}, u' \prod_{i=1}^{n} u_i^{m_i}\right).$$

Output 1 if the above holds. Otherwise output 0.

3.2 The Weakness of the Yuen-Au-Liu-Susilo Scheme

In this subsection, we show a weakness [16][17] on the Yuen-Au-Liu-Susilo scheme [14] and point out that the Yuen-Au-Liu-Susilo scheme actually does not satisfy the security model of invisibility the authors presented [14].

Weakness. Let $\{m^*, \sigma^*\}$ be the challenge in the attacking phase of the security model for invisibility where $\sigma^* = (S_1^*, S_{2,1}^*, S_{2,2}^*, \cdots, S_{2,k}^*)$. After the adversary $\mathcal{A}$ obtains the challenge, not querying the signing oracle, she/he can pick $r' \in Z_p^*$ and calculate

$$\sigma' = \left(S_1^* \left(u' \prod_{i=1}^{n} u_i^{m_i}\right)^{r'}, S_{2,1}^* \left(v' \prod_{i=1}^{\ell} v_i^{\bar{m}_j^i}\right)^{r'}, \cdots, S_{2,k}^* \left(v' \prod_{i=1}^{\ell} v_i^{\bar{m}_j^i}\right)^{r'}\right)$$

$$= \left(g_2^{\alpha} \left(u' \prod_{i=1}^{n} u_i^{m_i} \right)^{r+r'}, \left(v' \prod_{i=1}^{\ell} v_i^{\overline{m}_j^i} \right)^{r+r'}, \cdots, \left(v' \prod_{i=1}^{\ell} v_i^{\overline{m}_j^i} \right)^{r+r'} \right).$$

Then, the adversary $\mathcal{A}$ sends σ' to the Confirmation/Disavowal oracle. It is obvious that if σ^* is valid, then σ' is valid, and vice verse. Therefore, the adversary $\mathcal{A}$ can decide whether σ^* is valid or invalid according to whether σ' is valid or invalid. That is to say, the adversary $\mathcal{A}$ can break the invisibility of the Yuen-Au-Liu-Susilo scheme.

4. Our Scheme Construction

We describe our convertible undeniable signature scheme. The scheme consists of the following algorithms.

Setup. Let $\mathbb{G}$, $\mathbb{G}_T$ be groups of prime order p. Choose generators g, $g_2 \in \mathbb{G}$. Generator $u' \in \mathbb{G}$ is randomly selected, and a random n-length vector $\mathrm{U} = (u_i)$, whose elements are chosen at random from $\mathbb{G}$. Given a bilinear pairing $\hat{e}: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$.

Next, choose an integer ℓ as a system parameter. Let $H: \{0,1\}^n \rightarrow Z_\ell^*$ be a collision resistant hash function. The system parameters are $(g\ , g_2, u', \mathrm{U}, H)$.

Key Generation. Randomly choose α, β', $\beta_i \in Z_p^*$ for $1 \le i \le \ell$. Compute $g_1 = g^{\alpha}$, $v' = g^{\beta'}$ and $v_i = g^{\beta_i}$. The secret keys are $(\alpha, \beta', \beta_1, \beta_2, \cdots, \beta_\ell)$ .The public keys are $(g_1, v', v_1, v_2, \cdots, v_\ell)$.

Sign. Suppose that a signer wants to sign a message $m = (m_1, m_2, \cdots, m_n) \in \{0,1\}^n$. The signer's secret keys are $(\alpha, \beta', \beta_1, \beta_2, \cdots, \beta_\ell)$ and the corresponding public keys are $(g_1, v', v_1, v_2, \cdots, v_\ell)$. The signer picks a random number $r \in Z_p^*$ such that $\gcd(\alpha, \gamma) = 1$ and calculates two integers x and y satisfying $x\alpha + y\gamma = 1$ by extended Euclidean algorithm [24]. The signer calculates S as

$$S = g_2^{y\alpha},$$

and $\overline{m}$ as $\overline{m} = H(S, m)$. Next, the signer computes

$$S_1 = g_2^{x\alpha^2} \left(u' \prod_{i=1}^{n} u_i^{m_i} \right)^{r},$$

$$S_2 = \left(v' \prod_{i=1}^{\ell} v_i^{\overline{m}^i} \right)^{r}.$$

Finally, the undeniable signature σ of the message m is (S, S_1, S_2).

Confirmation/Disavowal. Upon input the undeniable signature $\sigma = (S, S_1, S_2)$ on the message m, the signer calculates

$$L = \hat{e}(g, g_2),$$

$$M = \hat{e}(g_1, g_2),$$

$$N = \hat{e}\left(v' \prod_{i=1}^{\ell} v_i^{\overline{m}^i}, g_2\right),$$

$$O = \hat{e}(S_2, S) \cdot \hat{e}\left(v' \prod_{i=1}^{\ell} v_i^{\overline{m}^i}, S_1\right) \Big/ \hat{e}\left(S_2, u' \prod_{i=1}^{n} u_i^{m_i}\right). \quad (1)$$

The signer performs the 4-move proof of knowledge of discrete logarithm or the non-interactive zero-knowledge proof system for bilinear groups by Groth and Sahai [26] of the equality or the inequality of the knowledge $\alpha = log_L M$ and $log_N O$.

Individual Conversion. Upon input the undeniable signature $\sigma = (S, S_1, S_2)$ on the message m, the signer calculates $\overline{m} = H(S, m)$ and

$$S_2' = S_2^{1/(\beta' + \sum_{i=1}^{\ell} \beta_i \overline{m}^i)}.$$

Output the individual receipt S_2' for the message m.

Individual Verification. Upon input the undeniable signature $\sigma = (S, S_1, S_2)$ for the message m and the individual receipt S_2', calculate $\overline{m} = H(S, m)$ and verify if

$$\hat{e}(g, S_2) = \hat{e}\left(S_2', v' \prod_{i=1}^{\ell} v_i^{\overline{m}^i}\right).$$

If they are not equal, output $\perp$. Otherwise check if

$$\hat{e}(S_2', S) \cdot \hat{e}(g, S_1) = \hat{e}(g_1, g_2) \cdot \hat{e}\left(S_2', u' \prod_{i=1}^{n} u_i^{m_i}\right).$$

Output 1 if the above holds. Otherwise output 0.

Universal Conversion. The signer publishes her/his universal receipt $R = (\beta', \beta_1, \beta_2, \cdots, \beta_\ell)$.

Universal Verification. Upon input the undeniable signature $\sigma = (S, S_1, S_2)$ on the message m and the universal receipt $R = (\beta', \beta_1, \beta_2, \cdots, \beta_\ell)$, verify if

$$v' = g^{\beta'},$$

$$v_i = g^{\beta_i},$$

for $1 \le i \le \ell$. If they are not equal, output $\perp$. Otherwise calculate $\overline{m} = H(S, m)$ and check if

$$\hat{e}\left(S_2^{1/(\beta' + \sum_{i=1}^{\ell} \beta_i \overline{m}^i)}, S\right) \cdot \hat{e}(g, S_1) = \hat{e}(g_1, g_2) \cdot \hat{e}\left(S_2^{1/(\beta' + \sum_{i=1}^{\ell} \beta_i \overline{m}^i)}, u' \prod_{i=1}^{n} u_i^{m_i}\right).$$

Output 1 if the above holds. Otherwise output 0.

5. Discussion

In this section, the security analysis of our proposed scheme is given first and then the performance evaluation is given.

5.1 Cryptanalysis Result

The security analysis of the proposed scheme is examined as follows. As with Yuen *et al*.'s scheme [14], the level of security is quite desirable. The related proofs of our scheme are similar to that of Yuen *et al*.'s proofs. Moreover, our scheme can satisfy the security model of invisibility.

Theorem 5.1 (Unforgeability.) *Our proposed scheme is secure against forgeability without random oracle model if and only if the CDH problem is hard.*

Proof. Let $\mathcal{A}$ be a (ϵ, t, q_s)-adversary. Using $\mathcal{A}$, we shall construct another probabilistic polynomial time (PPT) $\mathcal{B}$ to solve the CDH problem.

$\mathcal{B}$ will take a CDH challenge (g, g^a, g^b). In order to use $\mathcal{A}$ to solve for the CDH problem, $\mathcal{B}$ needs to simulate a challenger and the oracles for $\mathcal{A}$. $\mathcal{B}$ runs $\mathcal{A}$ executing the following steps.

Setup. Let $l_p = 2q_s$. $\mathcal{B}$ randomly chooses an integer κ such that $0 \le \kappa \le n$. Also, suppose that $l_p(n+1) < p$ for the given values of q_s and n. It chooses the following integers at random.

$$x' \in Z_{l_p}.$$

$$y' \in Z_p$$

$$d_t \in Z_p, \text{for } t = 1,2,\cdots,l_p.$$

$$x_i \in Z_{l_p}, \text{for } i = 1,2,\cdots,n. \text{ Let } \hat{X} = \{x_i\}.$$

$$y_i \in Z_p, \text{for } i = 1,2,\cdots,n. \text{ Let } \hat{Y} = \{y_i\}.$$

We further define the following functions for binary strings $m_t = (m_{t,1}, m_{t,2}, \cdots, m_{t,n})$ as follows

$$F(m_t) = x' + \sum_{i=1}^{n} x_i m_{t,i} - l_p \kappa,$$

$$J(m_t) = y' + \sum_{i=1}^{n} y_i m_{t,i}.$$

$\mathcal{B}$ randomly selects $\beta', \beta_i \in Z_p^*$ for $1 \le i \le \ell$. Let $v' = g^{\beta'}$ and $v_i = g^{\beta_i}$. $\mathcal{B}$ makes a set of common parameters as follows: g, $g_2 = g^b$, $u' = g_2^{-l_p\kappa + x'} g^{y'}$, $u_i = g_2^{x_i} g^{y_i}$ for $1 \le i \le n$. The signer's public keys are $(g_1 = g^a, v', v_1, v_2, \cdots, v_\ell)$.

Denote $G(m_t) = \beta' + \sum_{i=1}^{\ell} \beta_i \bar{m}_t^i$ where $\bar{m}_t = H(g^{-d_t F(m_t)}, m_t)$. Note that we have the following equations

$$u'\prod_{i=1}^{n} u_i^{m_{t,i}} = g_2^{F(m_t)} g^{J(m_t)},$$

$$v'\prod_{i=1}^{\ell} v_i^{\overline{m}_t^i} = g^{G(m_t)}.$$

All common parameters and the universal receipt $(\beta', \beta_1, \beta_2, \cdots, \beta_\ell)$ are passed to $\mathcal{A}$.

Oracles Simulation. $\mathcal{B}$ simulates the oracles as follow.

(*Signing oracle.*) Upon receiving the t-th signing oracle query for message $m_t = (m_{t,1}, m_{t,2}, \cdots, m_{t,n})$, although $\mathcal{B}$ does not know the secret key, it still can construct the signature by assuming $F(m_t) \neq 0 \bmod p$. It selects $r_t \in Z_p$ at random. Then, calculate the signature as

$$S = g^{-d_t F(m_t)},$$

$$S_1 = g_1^{\left(-\frac{J(m_t)}{F(m_t)} - d_t\right)} \left(g_2^{F(m_t)} g^{J(m_t)} g^{d_t F(m_t)}\right)^{r_t},$$

$$S_2 = \left(g_1^{-\frac{1}{F(m_t)}} g^{r_t}\right)^{G(m_t)},$$

where $\overline{m}_t = H(S, m_t)$.

By letting $\widetilde{r_t} = r_t - \frac{a}{F(m_t)}$, it can be checked that (S, S_1, S_2) is a signature, shown as follow:

$$S = g^{-d_t F(m_t)},$$

$$S_1 = g_1^{\left(-\frac{J(m_t)}{F(m_t)} - d_t\right)} \left(g_2^{F(m_t)} g^{J(m_t)} g^{d_t F(m_t)}\right)^{r_t}$$

$$= g^{\left(-a\frac{J(m_t)}{F(m_t)} - a d_t\right)} \left(g_2^{F(m_t)} g^{J(m_t)} g^{d_t F(m_t)}\right)^{\frac{a}{F(m_t)}} \left(g_2^{F(m_t)} g^{J(m_t)} g^{d_t F(m_t)}\right)^{-\frac{a}{F(m_t)}} \cdot \left(g_2^{F(m_t)} g^{J(m_t)} g^{d_t F(m_t)}\right)^{r_t}$$

$$= \left(g^{-a\frac{J(m_t)}{F(m_t)}} g^{-a d_t}\right) \left(g_2^a g^{a\frac{J(m_t)}{F(m_t)}} g^{a d_t}\right) \left(g_2^{F(m_t)} g^{J(m_t)} g^{d_t F(m_t)}\right)^{\widetilde{r_t}}$$

$$= g_2^a g^{d_t F(m_t)\widetilde{r_t}} \left(g_2^{F(m_t)} g^{J(m_t)}\right)^{\widetilde{r_t}}$$

$$= g_2^a g^{d_t F(m_t)\widetilde{r_t}} \left(u'\prod_{j=1}^{n} u_j^{m_{t,j}}\right)^{\widetilde{r_t}}$$

$$S_2 = \left(g_1^{-\frac{1}{F(m_t)}} g^{r_t} \right)^{G(m_t)}$$

$$= \left(g^{r_t - \frac{a}{F(m_t)}} g^{r_t} \right)^{G(m_t)}$$

$$= g^{G(m_t)\tilde{r}_t}$$

$$= \left(v' \prod_{w=1}^{\ell} v_w^{\overline{m}_t^w} \right)^{\tilde{r}_t}.$$

$\mathcal{B}$ outputs the undeniable signature (S, S_1, S_2). To the adversary, all undeniable signatures given by $\mathcal{B}$ are indistinguishable from the signatures produced by the signer.

Output. Finally, $\mathcal{A}$ sends the undeniable signature (S^*, S_1^*, S_2^*) for the message m_*. $\mathcal{B}$ checks if $F(m_*) = 0 \bmod p$. If not, $\mathcal{B}$ aborts. Otherwise $\mathcal{B}$ calculates $\overline{m}_* = H(S^*, m_*)$ and outputs

$$\frac{S_1^*}{{S_{2,1}^*}^{J(m_*)/G(m_*)}} = \frac{g_2^a g^{d_* F(m_*)\tilde{r}} (u' \prod_{i=1}^{n} u_i^{m_{*,i}})^{\tilde{r}}}{\left(v' \prod_{i=1}^{\ell} v_i^{\overline{m}_*^i} \right)^{\tilde{r} J(m_*)/G(m_*)}}$$

$$= \frac{g_2^a \left(g^{J(m_*)} \right)^{\tilde{r}}}{g^{\tilde{r} J(m_*)}}$$

$$= g^{ab}$$

which is the solution to the CDH problem instance.

Theorem 5.2 (Invisibility.) *The invisibility of the proposed scheme holds under decision linear assumption without random oracle model*.

Proof. Let $\mathcal{A}$ be a $(\epsilon, t, q_c, q_r, q_s)$-adversary. We construct another PPT $\mathcal{B}$ that makes use of $\mathcal{A}$ to solve the decision linear problem.

$\mathcal{B}$ is given a decision linear problem instance (u, v, h, u^a, v^b, h^c). In order to use $\mathcal{A}$ to solve for the decision linear problem, $\mathcal{B}$ needs to simulate the oracles for $\mathcal{A}$. $\mathcal{B}$ does it in the following steps.

Setup. Let $l_p = 2(q_s + 1)$. $\mathcal{B}$ chooses an integer κ randomly such that $0 \le \kappa \le n$. Also, assume that $l_p(n+1) < p$ for the given values of q_c, q_r, q_s and n. It randomly chooses the following integers.

$$x' \in Z_{l_p}.$$

$$y' \in Z_p.$$

$$d_t \in Z_p, \text{for } t = 1,2,\cdots,l_p.$$

$$x_i \in Z_{l_p}, \text{for } i = 1,2,\cdots,n. \text{ Let } \hat{X} = \{x_i\}.$$

$$y_i \in Z_p, \text{for } i = 1,2,\cdots,n. \text{ Let } \hat{Y} = \{y_i\}.$$

We further define the following functions for binary strings $m_t = (m_{t,1}, m_{t,2}, \cdots, m_{t,n})$ as follows:

$$F(m_t) = x' + \sum_{i=1}^{n} x_i m_{t,i} - l_p \kappa,$$

$$J(m_t) = y' + \sum_{i=1}^{n} y_i m_{t,i} - l_p \kappa.$$

Then, $\mathcal{B}$ randomly selects a set of distinct numbers $C = \{c_1^*, c_2^*, \cdots, c_s^*\} \in \{Z_\ell^*\}^s$. We further define the following functions for any binary string m

$$G(m_t) = \prod_{i \in C} (\bar{m}_t - i) = \sum_{i=0}^{s} \gamma_i \bar{m}_t^i \quad \text{and}$$

$$K(m_t) = \prod_{i=1, i \notin C}^{\ell} (\bar{m}_t - i) = \sum_{i=0}^{\ell - s} \alpha_i \bar{m}_t^i$$

for some $\gamma_i, \alpha_i \in Z_p^*$, where $\bar{m}_t = H(g^{-d_t F(m_t)}, m_t)$.

$\mathcal{B}$ generates a set of common parameters as follow: $g = u$, $g_2 = h$, $u' = g_2^{-l_p\kappa + x'} g^{-l_p\kappa + y'}$, $u_i = g_2^{x_i} g^{y_i}$ for $1 \leq i \leq n$. The signer's public keys are: $g_1 = u^a$, $v' = v^{\alpha_0} g^{\gamma_0}$, $v_i = v^{\alpha_i} g^{\gamma_i}$ for $1 \leq i \leq s$ and $v_j = v^{\alpha_i}$ for $s + 1 \leq i \leq \ell$.

Note that we have the following equation:

$$u' \prod_{i=1}^{n} u_i^{m_{t,i}} = g_2^{F(m_t)} g^{J(m_t)},$$

$$v' \prod_{i=1}^{\ell - 1} v_i^{\bar{m}_t^i} = g^{G(m_t)} v^{K(m_t)},$$

where $\bar{m}_t = H(g^{-d_t F(m_t)}, m_t)$. All common parameters are passed to $\mathcal{A}$. $\mathcal{B}$ also maintains an empty list $\mathcal{L}$.

Oracles Simulation. $\mathcal{B}$ simulates the oracles as follows.

(*Signing oracle.*) Upon receiving the i-th signing oracle query for the message $m_t = (m_{t,1}, m_{t,2}, \cdots, m_{t,n})$, although $\mathcal{B}$ does not know the secret key, it still can generate the undeniable signature by assuming $F(m_t) \neq 0 \bmod p$ and $K(m_t) = 0 \bmod p$. It selects $r_t \in Z_p$ at random and calculates the undeniable signature as

$$S = g^{-d_t F(m_t)},$$

$$S_1 = g_1^{\left(-\frac{J(m_t)}{F(m_t)}-d_t\right)}\left(g_2^{F(m_t)} g^{J(m_t)} g^{d_t F(m_t)}\right)^{r_t},$$

$$S_2 = \left(g_1^{-\frac{1}{F(m_t)}} g^{r_t}\right)^{G(m_t)}.$$

Same as the above proof, (S, S_1, S_2) is a valid undeniable signature. $\mathcal{B}$ stores (m_t, S, S_1, S_2) into the list $\mathcal{L}$ and then outputs the undeniable signature (S, S_1, S_2). To the adversary, all undeniable signatures given by $\mathcal{B}$ are indistinguishable from the signature generated by the signer.

(*Confirmation/Disavowal oracle.*) Upon receiving a undeniable signature (S, S_1, S_2) for the message m, $\mathcal{B}$ compares whether(m_t, S, S_1, S_2) is in $\mathcal{L}$ or not. If so, $\mathcal{B}$ outputs **Valid** and performs the confirmation protocol with $\mathcal{A}$, to show that (L, M, N, O) in Equation 1 are Diffie-Hellman (DH) tuples. It can simulate the interactive proof perfectly, because $\mathcal{B}$ knows the discrete logarithm of N with base L.

If the undeniable signature is not in $\mathcal{L}$, $\mathcal{B}$ outputs **Invalid** and executes the disavowal protocol with $\mathcal{A}$. By Theorem 1, the undeniable signature is unforgeable if the CDH assumption holds. $\mathcal{B}$ performs the oracle incorrectly only if $\mathcal{A}$ can forge a undeniable signature. However, if one can solve the CDH problem, it can also solve the decision linear problem.

(*Receipt generating oracle.*) Upon receiving a undeniable signature (S, S_1, S_2) for the message m, $\mathcal{B}$ calculates $\overline{m} = H(S, m)$. If $K(m) \neq 0 \bmod p$, $\mathcal{B}$ aborts. Otherwise, $\mathcal{B}$ calculates $S_2' = S_2^{1/G(m)}$, which is the valid individual receipt for the undeniable signature.

Challenge. $\mathcal{A}$ sends $m_* = (m_{*,1}, m_{*,2}, \cdots, m_{*,n})$ to $\mathcal{B}$ as the challenge message. $\mathcal{B}$ randomly selects an integer $d_* \in Z_p$. Denote $\overline{m}_* = H(g_2^{-d_*}, m_*)$. If $F(m_*) = 0 \bmod p$, $J(m_*) \neq 0 \bmod p$ or $G(m_*) \neq 0 \bmod p$, $\mathcal{B}$ aborts.

Otherwise, $\mathcal{B}$ computes

$$S^* = g_2^{-d_*},$$

$$S_1^* = h^c,$$

$$S_2^* = v^{bK(m_*)/(F(m_*)+d_*)},$$

and returns (S^*, S_1^*, S_2^*) to $\mathcal{A}$.

Output. Finally, $\mathcal{A}$ outputs a bit b'. $\mathcal{B}$ returns b' as the solution to the decision linear problem. Notice that if $c = a + b$, then

$$S^* = g_2^{-d_*},$$

$$S_1^* = g_2^{a+b}$$

$$= g_2^a \left(g_2^{F(m_*)+d_*}\right)^{b/(F(m_*)+d_*)}$$

$$= g_2^a \left(u' \prod_{i=1}^{n} u_i^{m_{*,i}} \right)^{b/(F(m_*)+d_*)} \quad g_2^{d_* b/(F(m_*)+d_*)},$$

$$S_2^* = v^{bK(m_*)/(F(m_*)+d_*)}$$

$$= \left(v' \prod_{i=0}^{\ell} v_i^{\bar{m}_*^i} \right)^{b/(F(m_*)+d_*)}.$$

Theorem 5.3 (Impersonation.) *Our proposed scheme is secure against impersonation without random oracle model if and only if the discrete logarithm problem is hard.*

Proof. Let $\mathcal{A}$ be a $(\varepsilon, t, q_c, q_s)$-adversary. We construct another PPT $\mathcal{B}$ that makes use of $\mathcal{A}$ to solve the discrete logarithm problem. $\mathcal{B}$ is given a discrete logarithm problem instance (g, g^a). The remaining analysis is similar as the proof of Theorem 1 and Yuen *et al*.'s scheme [14], so we omit the proof here.

5.2 Performance Evaluation

In this subsection, we show the results of the comparison between Yuen *et al*.'s scheme and our scheme in terms of computational complexity and communication cost. In the full version [18] of [14], Yuen *et al*. have totally revised their scheme. Yuen *et al*. use the generic construction of strongly unforgeable signatures in [19] to solve the security problem mentioned in [16]. In [19], we consider the Schnorr-based one-time scheme to create the one-time scheme. Key generation in the Schnorr-based one-time scheme requires two exponentiations. Signing requires only one hash computation and an multiplication, and verification requires two exponentiations and one multiplication. The comparison results are given in **Table 1** and **Table 2**.

Table 1 shows the comparison on computational complexity between Yuen *et al*.'s scheme [18] and our scheme. The scheme [18] is the revised version which does not suffer from the visibility attack in [16][17]. The performance evaluation notations are defined as follows. T_{EXP}: time for a modular exponentiation computation, T_{PAR}: time for a pairing computation, T_{MUL}: time for a modular multiplication computation, T_H: time for computing a one-way hash function $H(\cdot)$, T_{EEA}: time for an extended Euclidean algorithm computation. As introduced in [27][28], we also learn a relationship as follows. $T_{EXP} \cong 2T_{PAR}$, $T_{EXP} \cong 240T_{MUL}$ and $T_{EXP} \cong 600T_H$. Moreover, $T_{MUL} = 0.5\, ms$ and $T_{INV} \cong 19T_{MUL}$ in [29][30] where T_{INV} denotes the time for an inverse operation computation. We assume that $T_{EEA} \cong T_{INV}$. **Fig. 1** shows the relationship between the computation time and process algorithms if we set $n = 160$ and $\ell = 160$.

Table 2 shows the comparison on communication cost between our scheme and the recently proposed convertible undeniable signature schemes [13][16][18][20][21]. All schemes are instantiated to provide approximately 80-bits of security. The RSA-based schemes are assumed to be instantiated with an RSA group with a 1024 bit modulus and the pairing-based schemes are assumed to use an elliptic curve group equipped with an asymmetric pairing using group elements of size 170 bits. The Yuen *et al*.'s revised scheme [18] in **Table 2** fixes a flaw in the proof of invisibility [14]. Moreover, the scheme [18] requires both a verification key and a signature of a one-time signature scheme to be included as part of an undeniable signature, which leads to a slightly larger signature size.

In the assumptions column in **Table 2**, the abbreviations CDH, DLIN, OMDL, tdm-RSA, SRSA, DNR, DIV, q-SDH, q-HSDH, q-DHSDH and ψ-CDH stands for computational Diffie-Hellman assumption, decisional linear assumption, one more discrete logarithm assumption, decisional two moduli RSA assumption, strong RSA assumption, decisional N-th residuosity assumption, division intractability assumption, q strong Diffie-Hellman, q hidden strong Diffie-Hellman assumption, q decisional hidden strong Diffie-Hellman assumption and computational ψ-Diffie-Hellman assumption. **Fig. 2** shows the relationship between the size of signature and some existing convertible undeniable signatures.

Hence, our proposed scheme provides the smallest signature size of the convertible undeniable signature schemes which provably satisfies all desired security requirements. Furthermore, the security of our scheme rests more natural security assumptions compared to all of them.

Table 1. The comparison on computational complexity

Algorithm	Yuen *et al.*'s scheme [18]	Our proposed scheme
Sign	$5T_{EXP}+(n+\ell+2)T_{MUL}+T_H$ $\cong (n+\ell+1204.4)T_{MUL}$	$4T_{EXP}+(n+\ell+4)T_{MUL}+T_H+T_{EEA}$ $\cong (n+\ell+983.4)T_{MUL}$
Confirmation/Disavowal	$5T_{PAR}$ $\cong 600T_{MUL}$	$6T_{PAR}$ $\cong 720T_{MUL}$
Individual Conversion	$T_{EXP}+T_H$ $\cong 240.4T_{MUL}$	$T_{EXP}+T_H$ $\cong 240.4T_{MUL}$
Individual Verification	$2T_{EXP}+5T_{PAR}+(n+\ell+1)T_{MUL}+T_H$ $\cong (n+\ell+1081.4)T_{MUL}$	$6T_{PAR}+(n+\ell)T_{MUL}+T_H$ $\cong (n+\ell+720.4)T_{MUL}$
Universal Verification	$5T_{EXP}+3T_{PAR}+(n+1)T_{MUL}+T_H$ $\cong (n+1561.4)T_{MUL}$	$3T_{EXP}+4T_{PAR}+nT_{MUL}+T_H$ $\cong (n+1200.4)T_{MUL}$

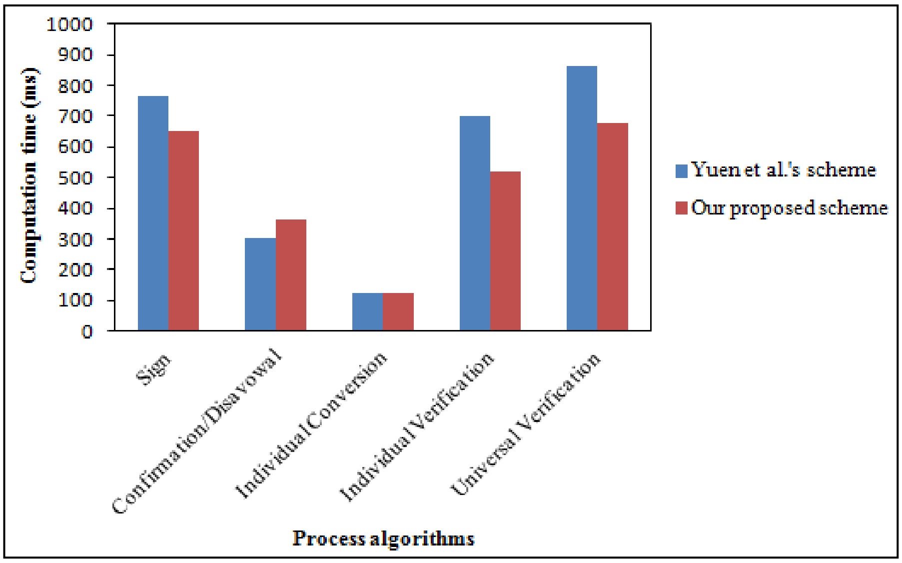

Fig. 1. Computation time evaluation in process algorithms

Table 2. The comparison on on communication cost

Scheme	Signature size	Assumptions
Yuen *et al.*'s revised scheme [18]	1020	CDH+DLIN+OMDL
Phong *et al.*'s $SCUS_0$ scheme [13]	1024	RSA+dtm-RSA
Phong *et al.*'s $SCUS_1$ scheme [13]	2128	SRSA+DNR
Phong *et al.*'s $SCUS_2$ scheme [13]	2048	SRSA+DIV+DNR
Phong *et al.*'s $SCUS_1$ scheme [16]	580	q-SDH+DLN
Phong *et al.*'s $SCUS_2$ scheme [16]	680	q-SDH+DLN
Huang-Wong's scheme [20]	510	q-HSDH+q-DHSDH
Schuldt-Matsuura's scheme [21]	680	ψ-CDH+DLIN
Our proposed scheme	510	CDH+DLIN

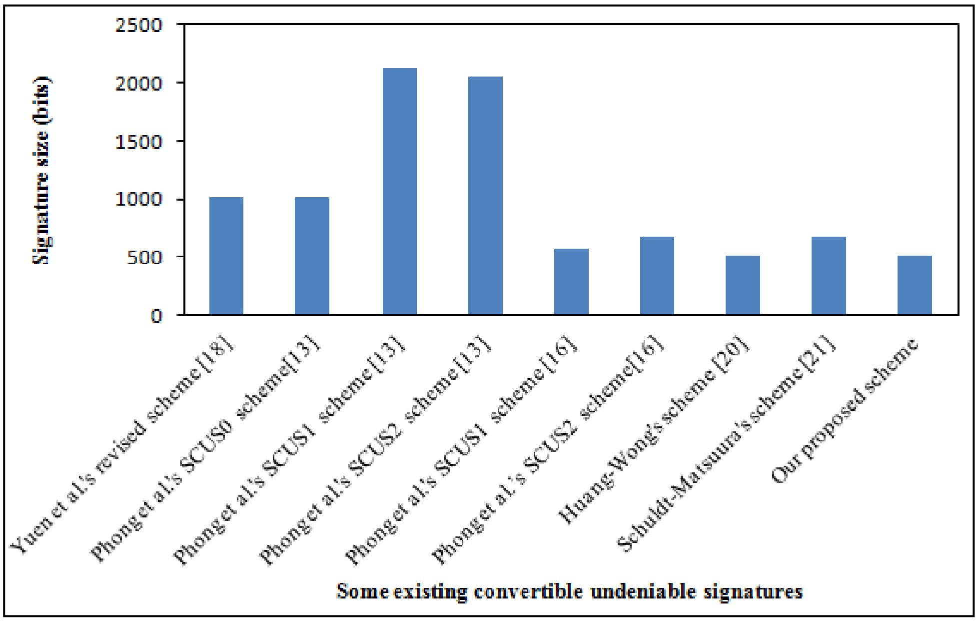

Fig. 2. Signature size evaluation in some existing convertible undeniable signatures

6. Conclusion

In this paper, we have proposed a new convertible undeniable signature scheme using extended Euclidean algorithm that can overcome the visibility attack by Phong *et al*. [16] and Zhao [15] presented. The security proofs of our scheme are equivalent to those of Yuen *et al*.'s scheme without random oracles by using more standard assumptions such as the computational Diffie-Hellman assumption and the decision linear assumption. We show the results of the comparison between Yuen *et al*.'s scheme and our scheme in terms of the computational complexity and the communication cost. The computational complexity for the most algorithms and the communication cost in our scheme are better than that of Yuen *et al*.'s scheme. Moreover, our scheme has the shortest signature size to the best of our knowledge.

Acknowledgements

The authors would like to thank the anonymous reviewers for the valuable comments on this work.

References

[1] D. Chaum and H. van Antwerpen, "Undeniable signatures," in *Proc. of Int. Conference on Cryptology-CRYPTO 1989*, LNCS 435, pp. 212-216, 1989. Article (CrossRef Link)
[2] T. Chaum and T. P. Pedersen, "Wallet databases with observers," in *Proc. of Int. Conference on Cryptology-CRYPTO 1992*, LNCS 740, pp. 89-105, 1993. http://dl.acm.org/citation.cfm?id=705670
[3] C. Boyd and E. Foo, "Off-line fair payment protocols using convertible signatures," in *Proc. of Int. Conference on the Theory and Application of Cryptology and Information Security-ASIACRYPT 1998*, LNCS 1541, pp. 271-285, 1998. http://dl.acm.org/citation.cfm?id=647094.716583
[4] D. Pointcheval, "Self-scrambling anonymizers," in *Proc. of Int. Conference on Financial Cryptography-FC 2000*, LNCS 1962, pp. 259-275, 2000. Article (CrossRef Link)
[5] I. Damgard and T. P. Pedersen, "New convertible undeniable signature schemes," in *Proc. of Int. Conference on the Theory and Applications of Cryptographic Techniques-EUROCRYPT 1996*, LNCS 1070, pp. 372-386, 1996. Article (CrossRef Link)
[6] K. Sakurai and S. Miyazaki, "A bulletin-board based digital auction scheme with bidding down strategy-towards anonymous electronic bidding without anonymous channels nor trusted centers," in *Proc. of Int. Workshop on Cryptographic Techniques and E-Commerce*, pp. 180-187, 1999. http://libra.msra.cn/Publication/2121146/a-bulletin-board-based-digital-auction-scheme-with-bidding-down-strategy-towards-anonymous
[7] K. Sakurai and S. Miyazaki, "An anonymous electronic bidding protocol based on a new convertible group signature scheme," in *Proc. of 5th Australasian Conference on Information Security and Privacy-ACISP 2000*, LNCS 1841, pp. 385-399, 2000. Article (CrossRef Link)
[8] J. Boyar, D. Chaum, I. Damgard and T. P. Pedersen, "Convertible undeniable signatures," in *Proc. of Int. Conference on Cryptology-CRYPTO 1990*, LNCS 537, pp. 189-205, 1991. Article (CrossRef Link)
[9] M. Michels, H. Petersen, and P. Horster, "Breaking and repairing a convertible undeniable signature scheme," in *Proc. of the 3rd ACM conference on Computer and Communications Security*, pp. 148-152, 1996. http://dl.acm.org/citation.cfm?id=238207
[10] R. Gennaro, H. Krawczyk and T. Rabin, "RSA-based undeniable signatures," in *Proc. of Int. Conference on Cryptology-CRYPTO 1997*, LNCS 1294, pp. 132-149, 1997. Article (CrossRef Link)
[11] S. D. Galbraith and W. Mao, "Invisibility and anonymity of undeniable and confirmer signatures," in *Proc. of the RSA Conference on the Cryptographers' Track-CT-RSA 2003*, LNCS 2612, pp. 80-97, 2003. Article (CrossRef Link)
[12] K. Kurosawa and T. Takagi, "New approach for selectively convertible undeniable signature schemes," in *Proc. of Int. Conference on the Theory and Application of Cryptology and Information Security-ASIACRYPT 2006*, LNCS 4284, pp. 428-443, 2006. Article (CrossRef Link)
[13] L. T. Phong, K. Kurosawa and W. Ogata, "New RSA-based (Selectively) convertible undeniable signature schemes," in *Proc. of Int. Conference on Cryptology-AFRICACRYPT 2009*, LNCS 5580, pp. 116-134, 2009. Article (CrossRef Link)
[14] T. H. Yuen, M. H. Au, J. K. Liu, and W. Susilo, "(Convertible) undeniable signatures without random oracles," in *Proc. of Int. Conference on Information and Communications Security-ICICS 2007*, LNCS 4861, pp. 83-97, 2007. Article (CrossRef Link)

[15] F. Laguillaumie and D. Vergnaud, "Short undeniable signatures without random oracles: the missing link," in *Proc. of Int. Conference on Cryptology-INDOCRYPT 2005*, LNCS 3797, pp. 283-296, 2005. Article (CrossRef Link)
[16] L. T. Phong, K. Kurosawa and W. Ogata, "Provably secure convertible undeniable signatures with unambiguity," in *Proc. of Int. Conference on Security and Cryptography for Network-SCN 2010*, LNCS 6280, pp. 291-308, 2010. Article (CrossRef Link)
[17] W. Zhao, "On the security of yuan *et al*.'s undeniable signature scheme," *International Journal of Network Security*, vol. 11, no. 2, pp. 87-90, 2010.
http://ijns.femto.com.tw/contents/ijns-v11-n3/ijns-2010-v11-n3-p179-182.pdf
[18] T. H. Yuen, M. H. Au, J. K. Liu and W. Susilo, "(Convertible) undeniable signatures without random oracles," in *Cryptology ePrint Archive*, Report 2007/386, 2007. Article (CrossRef Link)
[19] M. Bellare and S. Shoup, "Two-Tier Signatures, Strongly Unforgeable Signatures, and Fiat-Shamir without Random Oracles," in *Proc. of 10th Int. Conference on Practice and Theory in Public-Key Cryptography-PKC 2007*, LNCS 4450, pp. 201-216, 2007. Article (CrossRef Link)
[20] Q. Huang and D. S. Wong, "New constructions of convertible undeniable signature schemes without random oracles," in *Cryptology ePrint Archive*, Report 2009/517, 2009.
https://eprint.iacr.org/2009/517.pdf
[21] J. C. N. Schuldt and K. Matsuura, "An efficient convertible undeniable signature scheme with delegatable verification," in *Proc. of 6th Int. Conference on Information Security Practice and Experience-ISPEC 2010*, LNCS 6047, pp. 276-293, 2010. Article (CrossRef Link)
[22] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *Journal of Computing*, vol. 32, no. 3, pp. 586-615, 2003. Article (CrossRef Link)
[23] D. Boneh, X. Boyen and H. Shacham, "Short group signatures," in *Proc. of Int. Conference on Cryptology -CRYPTO 2004*, LNCS 3152, pp. 41-55, 2004. Article (CrossRef Link)
[24] A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996. Article (CrossRef Link)
[25] K. Kurosawa and S. H. Heng, "3-move undeniable signature scheme," in *Proc. of 24th Int. Conference on the Theory and Applications of Cryptographic Techniques-EUROCRYPT 2005*, LNCS 3494, pp. 181-197, 2005. Article (CrossRef Link)
[26] J. Groth and A. Sahai, "Efficient Non-interactive Proof Systems for Bilinear Groups," in *Proc. of 27th Int. Conference on the Theory and Applications of Cryptographic Techniques-EUROCRYPT 2008*, LNCS 4965, pp. 415--432, 2008. Article (CrossRef Link)
[27] Z. Li, J. Higgins and M. Clement, "Performance of finite field arithmetic in an elliptic curve cryptosystem", in *Proc. of 9th Int. Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems-MASCOT 2001*, pp. 249-256, 2001. Article (CrossRef Link)
[28] B. Schneier, *Applied cryptography*, 2nd edition, John Wiley & Sons Inc., 1996.
http://www.amazon.com/Applied-Cryptography-Protocols-Algorithms-Source/dp/0471117099
[29] K. Xue, P. Hong and X. Tie, "Using Security Context PreTransfer to Provide Security Handover Optimization for Vehicular Ad Hoc Networks", in *Proc. of IEEE 72nd Vehicular Technology Conference Fall* (*VTC 2010-Fall*), pp. 1-5, 2010. Article (CrossRef Link)
[30] S. Atay, A. Koltuksuz, H. Hisil and S. Eren, "Computational Cost Analysis of Elliptic Curve Arithmetic", in *Proc. of Int. Conference on Hybrid Information Technology-ICHIT 2006*, pp. 578-582, 2006. Article (CrossRef Link)

Shi-Jinn Horng received the B.S. degree in electronics engineering from the National Taiwan Institute of Technology, in 1980, the M.S. degree in information engineering from the National Central University, in 1984, and the Ph.D. degree in computer science from the National Tsing Hua University in 1989. He was a Professor and Dean of the College of Electrical Engineering and Computer Science, National United University, Miaoli, Taiwan, from 2006 to 2009. Currently, he is a Professor in the Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology. He was promoted to the Chair Professor in 2008. His research interests include VLSI design, multiprocessing systems, and parallel algorithms. He has published more than 170 research papers. Dr. Horng has received many awards including the Distinguished Research Award, from 2004 and 2006, from the National Science Council in Taiwan; Outstanding I.T. Elite Award, in 2005; Outstanding EE Prof. Award, the Chinese Institute of Electrical Engineering; and the Outstanding Research and Invention Award, from 2006 and 2008, from National Taiwan University of Science and Technology.

Shiang-Feng Tzeng is currently pursuing his Ph.D. degree in Computer Science and Information Engineering from National Taiwan University of Science and Technology. His current research interests include applied cryptography and information security.

Pingzhi Fan Ph.D. (UK), IEE Fellow, SMIEEE. He is currently a professor and director of the Institute of Mobile Communications, Southwest Jiaotong University, P.R. China, a guest professor of Leeds University, UK (1997–), chairman of the IEEE China VT Chapter, and Chair-elect of IEEE Chengdu Section. He was a recipient of the UK ORS Award (1992), and the National Science Foundation of China for Outstanding Young Scientist (1998). He served as general chair of IWSDA'07, IEEE-ITW'06, SETA'06, IWSDA'05, WSN'05, PDCAT'03 and IWSDA'01, and TPC chair or TPC member of more than 20 international conferences. He serves as the guest editor-in-chief of the IEICE Transactions on Fundamentals, IEICE Transactions on Information and Systems (Japan), Journal of High Performance Computing and Networking (Inderscience Publishers, USA), Wireless Communications and Mobile Computing (USA), Chinese Journal of Electronics (CIE), Communications and Mobile Computing, and Journal of Radio Science, etc. He is the inventor of 20 patents, and the author of over 300 research papers and 8 books, including six books published by John Wiley & Sons Ltd, RSP (1996), IEEE Press (2003, 2006), Springer (2004), and Nova Science, respectively. Recent and Current on-going research projects led by Dr. Fan are funded by RFBR (Russia), Royal Society (UK), DAAD (Germany), MEXT/JSPS (Japan), RGC (Hong Kong), IITA/KOSEF (South Korea), NSFC(China), National 863 project (MoST), industrial companies and other sources. His research interests include CDMA theory and technology, information theory and coding, sequence design and applications, radio resource management, cellular radio positioning, etc.

Xian Wang is a postdoctoral researcher in the Department of Computer Science and Information Engineering at the National Taiwan University of Science and Technology, Taiwan. His research interests include mobility management and performance modeling for personal communications service networks. Wang has a PhD in communication and information systems from Southwest Jiaotong University, Chengdu, China.

Tianrui Li received the BS, MS, and PhD degrees from the Southwest Jiaotong University, Chengdu, China, in 1992, 1995, and 2002, respectively. He was a postdoctoral researcher at the Belgian Nuclear Research Centre (SCK.CEN), Belgium from 2005-2006, a visiting professor at Hasselt University, Belgium, in 2008 and the University of Technology, Sydney, Australia in 2009. Currently, he is a professor and the director of the Key Lab of Cloud Computing and Intelligent Technology, Southwest Jiaotong University, China. His research interests include data mining and knowledge discovery, granular computing and rough sets, cloud computing. Since 2000, he has coedited two textbooks, six proceedings, three special issues of international journal and published more than 90 research papers in refereed journals and conferences. He is the vice chair of IEEE CIS Chengdu Chapter and the area editor of the International Journal of Computational Intelligence Systems (IJCIS). He has served as ISKE2007, ISKE2008, ISKE2009, ISKE2010, ISKE2011 program chairs, IEEE GrC 2009 program vice chair and RSKT2008, FLINS2010 organizing chairs and has been a reviewer for several leading academic journals. He is a senior member of the IEEE.

Muhammad Khurram Khan is currently working as associate professor and R&D Manager at Center of Excellence in Information Assurance (CoEIA), King Saud University, Kingdom of Saudi Arabia. He is the Founding Editor of 'Bahria University Journal of Information & Communication Technology (BUJICT)'. He is on the editorial board of several international journals e.g. Journal of Network & Computer Applications (Elsevier), Journal of Security & Communication Networks (Wiley), Telecommunication Systems (Springer), Computers & Electrical Engineering (Elsevier), Journal of Information Hiding and Multimedia Signal Processing (JIHMSP), International Journal of Biometrics (Interscience), Journal of Physical & Information Sciences, and Journal of Independent Studies and Research-Computing (JISR). He has also played role of the guest editor of several international journals of Springer-Verlag and Elsevier Science, etc. Furthermore, he is on the organizing and technical committees of dozens of international conferences. In addition, he is an active reviewer of many international journals. Dr. Khurram is an honorary Professor at IIIRC, Shenzhen Graduate School, China. He has been included in the Marquis Who's Who in the World 2010 edition. He was recently awarded a Gold Medal for the best invention & innovation award at 10th Malaysian Technology Expo that was held in Feb. 2011 at Kuala Lumpur, Malaysia. Besides, he has received a certificate of appreciation for outstanding contributions in Biometrics & Information Security Research, AIT Conference, June 2010 at Japan. He has also secured an outstanding leadership award at IEEE international conference on Networks and Systems Security 2009, Australia. Dr. Khurram has published/accepted more than 100 research papers in the journals and conferences of international repute and has two US/PCT patents pending. He has edited 4 books/proceedings published by Springer-Verlag and IEEE. His areas of interest are biometrics, multimedia security, digital data hiding, and authentication protocols.