The Insecurity of a Certificateless Undeniable Signature Scheme

Rouzbeh Behnia and Swee-Huay Heng
Faculty of Information Science and Technology
Multimedia University
Melaka, Malaysia
Email: {rouzbeh.behnia, shheng@mmu.edu.my}

***Abstract*—Duan proposed the first certificateless undeniable signature scheme in 2008. Later in 2012, Zhao and Ye proffered an efficient scheme which enjoys from a pairing-free sign algorithm. In this paper, we prove the insecurity of their efficient scheme by mounting two attacks on its invisibility and non-impersonation. In addition, we propose an improved scheme that addresses both of the above attacks while providing better flexibility and additional features for the signer.**

***Keywords*—Undeniable signature, non-impersonation, designated verifier, invisibility**

I. Introduction

In traditional public key cryptography, the authenticity of the user public key is delivered by means of certificates. However, the cost of issuing and managing certificates would become a major issue in large systems. To address the issue, Shamir [23] proposed the concept of identity-based cryptography. In identity-based systems, the public key of the users can be derived from their publicly available information (e.g. passport number, email address, etc.). The private key of the user, however, needs to be computed by a fully-trusted third party called the Private Key Generator (PKG). The knowledge of the PKG over the user private keys introduces the private key escrow problem and creates a repudiable environment. Hence, the employment of identity-based cryptography is limited to the small systems where the PKG has complete knowledge over all the information that is being communicated.

In contemplation of bridging the gap between the traditional public key cryptography and identity-based cryptography, Al-Riyami and Paterson [1] introduced the concept of certificateless cryptography. The main objective in certificateless paradigm is to eliminate the need of certificates in traditional public key cryptography, while addressing the private key escrow problem in identity-based cryptography. The underlying idea in such systems is to compute the user private key from two independent secrets, an identity-based private key (partial private key) which is generated by the Key Generation Center (KGC), and a random value (secret value) which is chosen by the user. The corresponding public key has to be computed (based on the secret value), and made available in the system by the user herself. Since there is no certificate to provide authentication on public keys, we always consider two adversary types when defining the security models of certificateless systems. A Type I adversary is a normal adversary which can replace the public key of any user with any public key of his choice and a Type II adversary who plays the role of a malicious KGC.

Ordinary digital signatures provide authentication, integrity and non-repudiation while being publicly verifiable. Put it differently, any user in the system with knowledge of the signer's public key is able to verify the validity of all the signatures generated by that signer. This nice feature however, may not be suitable in some situations (e.g., when two parties sign a confidential document). Chaum and van Antwerpen [8] introduced the notion of undeniable signature scheme with the aim of limiting the public verifiability of ordinary digital signatures. Verifying an undeniable signature is only possible with the direct help of its signer via the confirmation or disavowal protocol. Therefore, in addition to the advantages of ordinary digital signatures, undeniable signatures provide privacy for signers by limiting the public verifiability of signatures. The notion of invisibility, as introduced in [9], distinguishes undeniable signatures from ordinary digital signatures. It implies the inability of the users to verify the validity or invalidity of any message-signature pair without the consent and cooperation of its signer. In 2005, Kurosawa and Heng [19] introduced the property of non-impersonation to the context of undeniable signature schemes. This new property is to prevent the adversary from impersonating the signer by initiating either the confirmation or disavowal protocol with any third party. Among the main applications of undeniable signature schemes, we can name software licensing [8], e-cash [22] and e-voting [4].

Duan [14] proffered the first provably secure certificateless undeniable signature scheme to the literature. The scheme requires two expensive pairing computations in its sign algorithm which leads to a longer signature length. With the aim of proposing a more efficient scheme, Zhao and Ye [26] proposed a new provable secure certificateless undeniable signature scheme which does not require any pairing evaluations in its sign algorithm and has a considerably smaller signature size. Zhao and Ye relied the unforgeability and invisibility of their scheme on the hardness of the Computational Diffie-Hellman and the 3-Decisional Diffie-Hellman[1] problems respectively.

A. Our Contribution

In this paper, we point out two weaknesses of the efficient certificateless undeniable signature scheme proposed by Zhao

[1] In [26], the authors stated that their scheme is invisible under the Decisional Diffie-Hellman problem. However, the assumption they used is called the 3-Decisional Diffie-Hellman (it is also called the Decisional Diffie-Hellman problem in $\mathbb{G}$ by [6]). Comparing to the Decisional Diffie-Hellman problem which has been widely studied and used, the hardness of the 3-Decisional Diffie-Hellman problem has not been formally proven.

and Ye [26]. We then exploit these weaknesses in order to mount two attacks on the proposed scheme. In our first attack, we target the invisibility of the scheme and show how a Type I adversary can verify the validity/invalidity of a message-signature pair without the help of its signer. In our second attack, we show that the confirmation and disavowal protocols of the proposed scheme do not possess the property of non-impersonation and a Type I adversary is able to impersonate the signer by initiating these protocols with any third party on her behalf. Next, we put forth an improved scheme which addresses both of the aforementioned weaknesses of Zhao and Ye's scheme. While the Sign algorithm of the improved scheme is as efficient as the one in the original scheme, it also provides more flexibility for the signer by enabling her to selectively convert her undeniable signatures to ordinary digital signatures.

This paper is organized as follows. In Section 2, we review some useful definitions that are going to be used throughout this paper and define the adversarial model in certificateless systems. In Section 3, we describe the structure of Zhao and Ye's scheme in detail. In Section 4, we point out the weaknesses of Zhao and Ye's scheme and show our attacks on its invisibility and non-impersonation. In Section 5, we propose the improved scheme and discuss about its features and security. We conclude our paper in Section 6.

II. Preliminaries

A. Bilinear Pairing

We let $\mathbb{G}$ be a cyclic group of prime order q with g as its generator, and $\mathbb{G}_1$ be another cyclic group of the same order. An admissible bilinear pairing $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$ is given which is to satisfy the following properties:

1) **Bilinearity:** For every $g \in \mathbb{G}$ and $a, b \in \mathbb{Z}_q$ we have $e(g^a, g^b) = e(g, g)^{ab}$.
2) **Non-degeneracy:** There exists $g \in \mathbb{G}$ such that $e(g, g) \neq 1$.
3) **Computability:** e is efficiently computable.

Computational Diffie–Hellman (CDH) problem: Given $g^a, g^b \in \mathbb{G}$, for g as a generator of $\mathbb{G}$ and the random choice of $a, b \in \mathbb{Z}_q$, the CDH problem is to compute g^{ab}.

3-Decisional Diffie-Hellman (3-DDH) problem: Given $g^a, g^b, g^c, h \in \mathbb{G}$, for g as a generator of $\mathbb{G}$, and the random choice of $a, b, c \in \mathbb{Z}_q$, the 3-DDH problem is to decide whether $h = g^{abc}$.

The CDH problem is believed to be as hard as the Discrete Logarithm problem [24]. The conventional Decisional Diffie-Hellman (DDH) problem can be easily solved in pairing-based schemes. The 3-DDH problem [20] is definitely not harder than the DDH problem, but it seems intractable and can be used to achieve the privacy required in undeniable signatures.

B. Certificateless Undeniable Signature Scheme

A certificateless undeniable signature scheme consists of six algorithms and two protocols as follows.

Setup: A probabilistic algorithm that is run by the KGC and takes as input a security parameter k, and returns the KGC's key pair (s, P_{Pub}). Where, s is the master secret key and P_{Pub} is the respective public key. It outputs the system public parameters $params$ which is shared in the system. For the sake of brevity, we omit the inclusion of $params$ as the input of the remaining algorithms/protocols.

Set-User-Key: This algorithm is run by the user and takes as input the user identity ID in order to generate the secret value s_{ID} and the corresponding public key PK_{ID}.

Partial-Private-Key-Extract: Provided a user identity ID, the KGC uses the master secret key s to compute the user partial private key D_{ID}. The KGC is responsible to deliver D_{ID} to the user in a secure manner.

Set-Private-Key: After running the above algorithms, a user with identity ID and public key PK_{ID} uses her secret value s_{ID} and partial private key D_{ID} to form her private key as SK_{ID}.

Sign: This algorithm takes as input a message m to be signed, the signer's identity ID and public key PK_{ID}, along with her private key SK_{ID} and outputs a certificateless undeniable signature σ.

Verify: This algorithm takes as input a message-signature pair (m, σ), the alleged signer's identity ID (and public key PK_{ID}), and private key SK_{ID}. It outputs $valid$ if the signature is valid, and $invalid$ otherwise.

Confirmation/Disavowal: A protocol (conceivably non-interactive) that takes as input a valid/invalid message-signature pair (m, σ), the alleged signer's identity ID (and public key PK_{ID}), and private key SK_{ID} and outputs a non-transferable proof which can convince the verifier about the validity/invalidity of the signature σ.

C. Adversarial Model

Due to the lack of the infrastructure to authenticate users public keys in certificateless systems, it is vital to consider an adversary who is able to replace the user public key with any public key of his choice. Therefore, in the security model of certificateless systems, we always consider two types of adversary as follows.

Type I Adversary $\mathcal{A}_I$: This type of adversary simulates a third party adversary who has no possible knowledge on the master secret key s. However, due to the aforementioned characteristic of certificateless systems, $\mathcal{A}_I$ is allowed to replace the public key of any user with the public key of his choice.

Type II Adversary $\mathcal{A}_{II}$: This type of adversary simulates a malicious KGC. Therefore, $\mathcal{A}_{II}$ is assumed to have knowledge over the master secret key s which enables him to compute the partial private key of any user in the system. Nonetheless, $\mathcal{A}_{II}$ is not permitted to replace the user public key.

As it has been depicted in the security model of many certificateless schemes, a Type I adversary can gain knowledge on the secret value of users by either querying the secret value extract oracle [2], [15], [10], [16], [14] or by replacing the public key of the users with public keys of his choice (where he may know the corresponding secret value) [16], [14], [25], [1]. Moreover, we know that a Type II adversary can easily compute the users partial private keys since he has complete

knowledge over the master secret key. Therefore, the security model of certificateless systems should be formulated in a way to prevent the adversary $\mathcal{A} \in \{\mathcal{A}_I, \mathcal{A}_{II}\}$ to use the portion of the user private key that he may have knowledge on (i.e. secret value or partial private key) in initiating cryptographic operations on behalf of the user. For instance, in the case of certificateless undeniable signature schemes, the security model should be formulated in such a way to prevent the adversary $\mathcal{A} \in \{\mathcal{A}_I, \mathcal{A}_{II}\}$ from violating any of the security notions of such schemes (i.e. unforgeability, invisibility, etc.).

III. Zhao and Ye's Scheme

In this section, we review the efficient certificateless undeniable signature scheme of Zhao and Ye in detail. The proposed scheme consists of seven algorithms and two protocols as follows. In order to avoid confusion, we use the same notations as in [26].

Setup: By choosing $k \in \mathbb{Z}_q$ as a security parameter, the KGC runs this algorithm by generating two cyclic groups $\mathbb{G}$ and $\mathbb{G}_1$ of prime order $p \geqslant 2^k$, selecting an arbitrary generator $g \in \mathbb{G}$ and an admissible bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$. Next, it chooses two cryptographic hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{G}$ and $H_2 : \{0,1\}^* \rightarrow \mathbb{G}$, and generates its key pair by selecting $s \in \mathbb{Z}_q$ as the master secret key and computing $P_{Pub} = g^s$ as the respective public key. Lastly, it publishes the system public parameters as $params = (\mathbb{G}, \mathbb{G}_1, p, g, e(.,.), H_1, H_2, P_{Pub})$.

Partial-Private-Key-Extract: Provided the user's identity ID and the system public parameters $params$, the KGC computes $Q_{ID} = H_1(ID)$ and sets the partial private key of the user as $D_{ID} = Q_{ID}^s$ and transmits it to the user in a secure manner.

Set-Secret-Value: The user with identity ID chooses $s_{ID} \in \mathbb{Z}_q$ at random as her secret value.

Set-Private-Key: After the user received her partial private key D_{ID} and selected her secret value s_{ID}, she can form her private key as $SK_{ID} = (D_{ID}, s_{ID})$.

Set-Public-Key: The user with identity ID uses her secret value s_{ID} to compute her public key as $PK_{ID} = (PK_1, PK_2) = (g^{s_{ID}}, Q_{ID}^{s_{ID}})$.

Sign: Provided a message $m \in \{0,1\}^*$ to be signed, the user with identity ID chooses $r \in \mathbb{Z}_q$ at random, computes $U = g^r$ and $V = H_2(m||ID||PK_{ID} ||U)^{r s_{ID}} D_{ID}$ and forms the signature as $\sigma = (U, V)$.

Verify: Provided a message-signature pair $(m, \sigma = (U, V))$, the alleged signer (with identity ID) checks $e(V, g) = e(H_2(m||ID||PK_{ID}||U), U)^{s_{ID}} e(Q_{ID}, P_{Pub})$ and outputs $valid$ of it holds, and $invalid$ otherwise.

Confirmation: Given a valid message-signature pair (m, σ), the alleged signer (with identity ID) uses Chaum's [7] zero-knowledge interactive proofs (ZKIP) to prove that $(e(g,g), e(g, PK_1), e(H_2(m||ID||PK_{ID}||U), U), {}^{e(V,g)}/_{e(Q_{ID}, P_{Pub})})$ is a valid Diffie-Hellman (DH) tuple as follows:

1) The verifier chooses $a, b \in \mathbb{Z}_q$ at random, computes $c = e(g,g)^a e(H_2(m||ID ||PK_{ID}||U), U)^b$, and sends c to the signer.
2) The signer chooses $r \in \mathbb{Z}_q$ at random, computes $z_1 = ce(g,g)^r$ and $z_2 = z_1^{s_{ID}}$, and sends (z_1, z_2) to the verifier.
3) The verifier sends (a, b) to the signer.
4) The signer checks if $c = e(g,g)^a e(H_2(m||ID||PK_{ID}||U), U)^b$ holds, she sends r to the verifier.
5) The verifier checks if $z_1 = e(g,g)^{a+r} e(H_2(m||ID||PK_{ID}||U), U)^b$ and $z_2 = e(g, PK_1)^{a+r} {}^{(e(V,g)/e(Q_{ID}, P_{Pub}))^b}$ hold, he will accept the proof, and reject otherwise.

Disavowal: Given an invalid message-signature pair $(m, \sigma = (U, V))$, the alleged signer (with identity ID) uses Chaum's [7] zero-knowledge interactive proofs in order to prove that $(e(g,g), e(g, PK_1^{'}), e(H_2(m||ID|| PK_{ID}||U), U), {}^{e(V,g)}/_{e(Q_{ID}, P_{Pub})})$ is a non-DH-tuple. For the details of the protocol, we refer the reader to [7], [26].

IV. Attacks on Zhao and Ye's Scheme

In this section, we point out the weaknesses of Zhao and Ye's scheme [26] and mount our attacks. In our first attack, we target the invisbility of the proposed scheme and show that a Type I adversary $\mathcal{A}_I$ is able to verify the validity/invalidity of a message-signature pair without the help of its signer. Next, we exploit the second weakness of the proposed scheme to mount our attack which enables the same adversary (i.e. $\mathcal{A}_I$) to impersonate the signer by initiating the confirmation or disavowal protocol with any third party. The main goal in undeniable signature schemes is to protect the signer's privacy while providing authentication. Our attacks are important as they enable a Type I adversary $\mathcal{A}_I$ to not only breach the privacy of the signer by verifying her signatures without her consent, but also transfer this knowledge to any third party by impersonating the signer.

A. Attack on the Invisibility

As aforementioned, the security models of certificateless schemes have to be formulated in such a way to prevent both adversary types (i.e. Type I and Type II) to violate any of the security notions related to such schemes. In order to ensure security, the security models of certificateless schemes allows a Type I adversary $\mathcal{A}_I$ to get access to the user secret values by either querying the secret value extract oracle [2], [15], [10], [16], [14] or the public key replacement oracle [16], [14], [25], [1] which enables the adversary to replace the public key of the users with any public key of his choice (that he may know the corresponding secret value).

As it is clearly stated in the security models of Zhao and Ye's scheme [26, see Section 3.2], in addition to having access to the secret value extract oracle, $\mathcal{A}_I$ has access to a Sign oracle which is able to return valid signatures under the replaced public keys. In the following attack, we consider the latter approach where the adversary replaces the target signer's public key and requests for a valid signature[2]. The details of the attack are as follows.

[2]The same attack could be mounted if the secret value of the signer is queried from the secret value extract oracle defined in the security model of [26].

The adversary $\mathcal{A}_I$ picks $s_{ID}^{'} \in \mathbb{Z}_p$ and computes the corresponding public key $PK_{ID}^{'} = (PK_1^{'}, PK_2^{'}) = (g^{s_{ID}^{'}}, Q_{ID}^{s_{ID}^{'}})$. Then, he requests for a valid signature under the replaced public key $PK_{ID}^{'}$ (note that the replaced public key $PK_{ID}^{'}$ is valid since $e(PK_2^{'}, g) = e(Q_{ID}, PK_1^{'})$). Upon receiving such a request, the signer picks $r \in \mathbb{Z}_q$ at random and forms $U = g^r$ and $V = H_2(m||ID||PK_{ID}^{'}||U)^{r s_{ID}^{'}} D_{ID}$ to output the signature as $\sigma = (U, V)$.

It can be easily observed that $\mathcal{A}_I$ can verify the validity or invalidity of the signature by checking if $e(V, g) = e(H_2(m||ID||PK_{ID}^{'}||U), U)^{s_{ID}^{'}} e(Q_{ID}, P_{Pub})$ holds, and therefore, violating the invisibility property of the proposed scheme.

A flaw in the signature structure of the proposed scheme leads to the above attack. As it is shown above, the adversary $\mathcal{A}_I$ with knowledge of only the secret value of the signer is able to verify the validity or invalidity of any of the signer's signatures without the signer's help. This results in violating one of the vital security notions of undeniable signature schemes which distinguishes such schemes from ordinary digital signatures.

B. Attack on the Non-Impersonation

Following the above attack, we show how the same adversary $\mathcal{A}_I$ can impersonate the signer by only having knowledge on her secret value. More specifically, the attack enables the adversary to initiate the confirmation or disavowal protocol with any third party on behalf of the signer.

Here, we only demonstrate the attack on the confirmation protocol (the same attack can be mounted on the disavowal protocol) and show its identicality with the original protocol initiated by the signer (in Section 3).

For a valid message-signature pair $(m, \sigma = (U, V))$, the adversary $\mathcal{A}_I$ has to prove to the third party that $(e(g, g), e(g, PK_1^{'}), e(H_2(m||ID||PK_{ID}^{'}||U), U), {}^{e(V,g)}/_{e(Q_{ID}, P_{Pub})})$ is a valid DH-tuple using the ZKIP as follows:

1) The verifier chooses $a, b \in \mathbb{Z}_q$ at random, computes $c = e(g, g)^a e(H_2(m||ID||PK_{ID}^{'}||U), U)^b$ and sends c to $\mathcal{A}_I$.
2) $\mathcal{A}_I$ chooses $r \in \mathbb{Z}_q$ at random, computes $z_1 = c e(g, g)^r$ and $z_2 = z_1^{s_{ID}^{'}}$, and sends (z_1, z_2) to the verifier.
3) The verifier sends (a, b) to $\mathcal{A}_I$.
4) $\mathcal{A}_I$ checks if $c = e(g, g)^a e(H_2(m||ID||PK_{ID}^{'}||U), U)^b$ holds, he sends r to the verifier.
5) The verifier checks if $z_1 = e(g, g)^{a+r} e(H_2(m||ID||PK_{ID}^{'}||U), U)^b$ and $z_2 = e(g, PK_1^{'})^{a+r\left({}^{e(V,g)}/_{e(Q_{ID}, P_{Pub})}\right)^b}$ hold, he will accept the proof, and rejects otherwise.

The second attack is resulted from the poorly structured confirmation and disavowal protocols of the proposed scheme. The authors made use of the ZKIP in the confirmation and disavowal protocols. However, the only private input of the signer to these protocols is her secret value. This is against the fundamental security requirements of certificateless schemes where the users are required to provide their whole private key (consisted of the secret value and the partial private key) in order to prevent the adversary $\mathcal{A} \in \{\mathcal{A}_I, \mathcal{A}_{II}\}$ from initiating any cryptographic operations on their behalf.

V. The Improved Scheme

In this section, we propose an improved scheme that addresses the above weaknesses and prevents the attacks in the previous section. From the efficiency point of view, the Sign algorithm of the improved scheme is as efficient as the original scheme with the same signature length. In order to overcome the second attack and provide more efficiency and additional security, we employed the non-interactive designated verifier (NIDV) proofs of Jakobsson et al. [18] in the confirmation and disavowal protocols of the improved scheme. The primary objective of introducing NIDV proofs is to address the man-in-the-middle [11] and blackmailing attacks [17], [12] on undeniable signature schemes. NIDV proofs are also more efficient since they reduce the number of interactions between the signer and the verifier to only one move. While the Partial-Private-Key-Extract algorithm of our scheme is identical to the original scheme, we need to include two new hash fucntions $H_3, H_4 : \mathbb{G}_1 \times \ldots \times \mathbb{Z}_q \rightarrow \mathbb{Z}_q$ in the public parameters of the new scheme's Setup algorithm. The rest of the algorithms and protocols of the improved scheme are as follows.

Set-User-Key: The user with identity ID chooses $s_{ID} \in \mathbb{Z}_q$ at random as her secret value and computes her public key as $PK_{ID} = g^{s_{ID}}$.

Set-Private-Key: After the user received her partial private key D_{ID} and selected her secret value s_{ID}, she can form her private key as $SK_{ID} = (D_{ID}, s_{ID})$.

Sign: Provided a message $m \in \{0,1\}^*$ to be signed, the user with identity ID chooses $r \in \mathbb{Z}_q$ at random, computes $U = g^r$ and $V = (H_2(m||ID||PK_{ID}||U)^{s_{ID}} D_{ID})^r$ and forms the signature as $\sigma = (U, V)$.

Verify: Provided a message-signature pair $(m, \sigma = (U, V))$, the alleged signer (with identity ID) uses her private key SK_{ID} and checks if $e(V, g) = e(H_2(m||ID||PK_{ID}||U), U)^{s_{ID}} e(D_{ID}, U)$ holds, it outputs $valid$, and $invalid$ otherwise.

Confirmation: Given a valid message-signature (m, σ) pair to be confirmed, the signer (with identity ID_A and public key PK_A) works as follows in order to generate a non-interactive confirmation proof transcript for the designated verifier (with identity ID_B and public key PK_B). Compute $Q_B = H_1(ID_B)$ and pick at random $J, W \in \mathbb{G}$ and $\beta, \tau, v \in \mathbb{Z}_q$ to compute $n_1 = e(g, J) e(P_{Pub}, Q_B)^{\nu} \in \mathbb{G}_1$, $n_2 = PK_B^v + g^{\tau} \in \mathbb{G}, p_1 = e(g, W) \in \mathbb{G}_1$, $p_2 = e(g, g)^{\beta} \in \mathbb{G}_1, p_3 = e(H_2(m||ID_A||PK_A||U), U)^{\beta} e(W, U) \in \mathbb{G}_1$. Set the value of $h_C = H_3(n_1, n_2, p_1, p_2, p_3, \sigma) \in \mathbb{Z}_q$, $I = W - D_A^{(h_C + \nu)}$ and $u = \beta - (h_C + \nu) s_A$ and send the confirmation proof transcript as (J, v, τ, I, u, h_C).

In order to verify the veracity of the confirmation proof transcript (J, v, τ, I, u, h_C), the designated verifier computes $n_1^{'} = e(g, J) e(P_{Pub}, Q_B)^{\nu}$, $n_2^{'} = PK_B^v + g^{\tau}, p_1^{'} = e(g, I) e(P_{Pub}, Q_A)^{(h_C + \nu)}, p_2^{'} = e(g, g)^u e(g, PK_A)^{(h_C + \nu)}$, and, $p_3^{'} =$

$e(H_2(m||ID_A||PK_A||U),U)^u e(U,I)e(g,V)^{(h_C+\nu)}$
and will only accept the proof if and only if $h_C = H_3(n_1^{'}, n_2^{'}, p_1^{'}, p_2^{'}, p_3^{'}, \sigma)$.

Disavowal: Given an invalid message-signature pair (m, σ), the signer (with identity ID_A and public key PK_A) works as follows in order to generate a non-interactive confirmation proof transcript for the designated verifier (with identity ID_B and public key PK_B). She parses σ into (U, V), compute $Q_B = H_1(ID_B)$ and pick $J \in \mathbb{G}$ and $\tau, v, \gamma \in \mathbb{Z}_q$ at random in order to compute the values of $n_1 = e(g, J)e(P_{Pub}, Q_B)^{\nu}$, $n_2 = PK_B^v + g^{\tau}$ and $C = (\frac{e(H_2(m||ID_A||PK_A||U),U)^{s_A} e(D_A,U)}{e(g,V)})^{\gamma}$. The signer has to prove her knowledge of a tuple $(T, \gamma, \omega) \in \mathbb{G} \times \mathbb{Z}_q \times \mathbb{Z}_q$ where $C = \frac{e(H_2(m||ID_A||PK_A||U),U)^{\omega} e(T,U)}{e(g,V)^{\gamma}}$, $\frac{e(T,g)}{e(Q_A,P_{Pub})^{\gamma}} = 1$ and $\frac{g^{\omega}}{PK_A^{\gamma}} = 1$. In order to do so, the signer picks $X \in \mathbb{G}$ and $a, i \in \mathbb{Z}_q$ at random and computes $j_1 = \frac{e(g,X)}{e(Q_A,P_{Pub})^a}$, $j_2 = \frac{e(g,g)^i}{e(g,PK_A)^a}$, and $j_3 = \frac{e(H_2(m||ID_A||PK_A||U),U)^i e(U,X)}{e(g,V)^a}$. Next, she sets the values of $h_D = H_4(C, n_1, n_2, j_1, j_2, j_3, \sigma) \in \mathbb{Z}_q$, $w_1 = i - (h_D + \nu)\omega$, $w_2 = a - (h_D + \nu)\gamma$, and $Y = X - (h_D + v)T$ to form the proof as $(C, J, v, \tau, h_D, Y, w_1, w_2)$.

Upon receiving the disavowal proof transcript $(C, J, v, \tau, h_D, Y, w_1, w_2)$, the designated verifier first checks if $C = 1$, he rejects and outputs $\perp$. Otherwise, he verifies the proof by computing $n_1^{'} = e(g, J)e(P_{Pub}, Q_B)^{\nu}$, $n_2^{'} = vPK_B + g^{\tau}, j_1^{'} = \frac{e(g,Y)}{e(Q_A,P_{Pub})^{w_2}}$, $j_2^{'} = \frac{e(g,g)^{w_1}}{e(g,PK_A)^{w_2}}, j_3^{'} = \frac{e(H_2(m||ID_A||PK_A||U),U)^{w_1} e(U,Y)}{e(V,g)^{w_2}} C^{(h_D+\nu)}$, and will only accept the proof if and only if $h_D = H_4(C, n_1^{'}, n_2^{'}, j_1^{'}, j_2^{'}, j_3^{'}, \sigma)$.

A. Efficiency

As mentioned above, the Sign algorithm of the improved scheme is as efficient as the one in Zhao and Ye's scheme. While the confirmation and disavowal protocols of our scheme are more efficient in communication (since they are non-interactive) and provide more flexibility for the signer, they require more pairing evaluations. The structure of our scheme is more compact and less complex as we combined the Set-Secret-Value and Set-Public-Key algorithms into a single algorithm (i.e. Set-User-Key) and the public key of users in our scheme is consisted of only a single point in $\mathbb{G}$. Therefore, the verify algorithm of our scheme is more efficient as the signer is not required to run the validity check on the public key.

B. Convertibility

Boyar, Chaum, Damgard and Pedersen [5] proffered the notion of convertible undeniable signatures which enables the signer of an undeniable signature to convert her signatures to conventional digital signatures. This feature becomes favorable in situations where the signed data lose their sensitivity and the signer decides to make them publicly verifiable. The conversion can take place in two forms: selective conversion which allows the signer to convert a single signature, and universal conversion which enables the signer to convert all her signatures to publicly verifiable ones.

Our scheme provides the signer with the option to selectively convert her undeniable signatures to ordinary digital signatures by omitting the trapdoor commitments from the the proof of the confirmation and disavowal protocols. To generate a selective token on a valid message-signature pair $(m, \sigma = (U, V))$, the signer with identity ID_A (and public key PK_A) chooses $T \in \mathbb{G}$ and $y \in \mathbb{Z}_q$ at random to form $c_1 = e(g, T) \in \mathbb{G}_1$, $c_2 = e(g, g)^y \in \mathbb{G}_1$, and $c_3 = e(H_2(m||ID_A||PK_A||U), U)^y e(T, U) \in \mathbb{G}_1$ and sets $h_{SC} = H_3(c_1, c_2, c_3, \sigma)$, $I = T - D_A^{h_C}$ and $i = y - (h_{SC})s_A$ and outputs the proof as (I, i, h_{SC}). Upon receiving the selective token (I, i, h_{SC}), any user in the system can check the validity of the message-signature pair $(m, \sigma = (U, V))$ by computing $c_1^{'} = e(g, I)e(g, P_{Pub})$, $c_2^{'} = e(g, g)^i e(g, PK_A)$, and $c_3^{'} = e(H_2(m||ID_A||PK_A||U), U)^i e(I, U)e(g, V)$ and checking if $h_{SC} = H_3(c_1^{'}, c_2^{'}, c_3^{'}, \sigma)$ holds. Note that the same method can be applied in the disavowal protocol of the new scheme.

C. Security

We ensured the security of the new scheme against the aforementioned attacks by enforcing the signer to use her whole private key in order to verify signatures in the Verify algorithm and also when generating proofs in the confirmation and disavowal protocols. Using the same reduction technique as in [26], we can also relate the unforgeability and invisibility of our scheme to the hardness of the Computational Diffie-Hellman problem and the 3-Decisional Diffie-Hellman problem respectively.

It is trivial to show the completeness of both the confirmation and disavowal protocols of the improved scheme. In the following, we show that the confirmation and disavowal protocols of the improved scheme are sound and non-transferable.

Soundness: We prove the soundness of the confirmation/disavowal protocols of the improved scheme in order to make sure that the signer is unable to generate fraudulent proofs. Soundness is an indispensable property of undeniable signature schemes since only the signer of the signature should be able to generate proofs on the validity or invalidity of her signatures. This vital property ensures that if an uncorrupted designated verifier (where his private key was never compromised or stolen) receives a valid pairing-based non-interactive proof, it was created using the signer private key SK_A. Therefore, given a commitment $(n_1, n_2, p_1, p_2, p_3)$ and two challenges h_C and $h_C^{'}$, if the signer (with identity ID_A and public key PK_A) can produce two tuples (I, u) and $(I^{'}, u^{'})$ then we can compute $e(g, I - I^{'}) = e(P_{Pub}, Q_A)^{(h_C - h_C^{'})}, e(g, g)^{(u-u^{'})} = e(g, PK_A)^{(h_C - h_C^{'})}, e(H_2(m||ID_A||PK_A||U), U)^{u-u^{'}} e(U, I - I^{'}) = e(g, V)$. Therefore, $\sigma = (U, V)$ could have only been generated using the signer private key SK_A on message m. We note that the same approach can be used to prove the soundness of the disavowal protocol of our scheme.

Non-transferability: Non-transferability is a weaker assumption than zero-knowledgeness. A pairing-based non-interactive designated verifier proof system is non-transferable if there exists a polynomial time algorithm that on input of a tuple (σ, SK_B, ID_A) where SK_B is the private key of the designated verifier, ID_A is the identity of the signer, but σ is not essentially a valid signature, produces a proof transcript which is indistinguishable from the one generated by using the signer private key SK_A.

Here, we prove the non-transferability of the confirmation protocol of our scheme by showing that the designated verifier (with identity ID_B and public key PK_B) is able to generate proofs which are indistinguishable from the ones generated by the signer. In order to simulate the confirmation proof transcript for a message-signature pair (m, σ), the designated verifier picks $u, \tau^{'}, v^{'} \in \mathbb{Z}_q$ and $I, J^{'} \in \mathbb{G}$ at random and computes $n_1 = e(g, J^{'})$, $n_2 = g^{\tau^{'}}$, $p_1 = e(g, I)e(P_{Pub}, Q_A)^{h_C^{'}}$, $p_2^{'} = e(g, g)^u e(g, PK_A)^{h_C^{'}}$, and $p_3^{'} = e(H_2(m||ID_A||PK_A||U), U)^u e(U, I)e(g, V)^{h_C^{'}}$. Then, it forms the values of $h_C = H_4(n_1, n_2, p_1, p_2, p_3, \sigma)$, $v = h_C^{'} - h_C$, $\tau = \tau^{'} - vs_B$ and $J = J^{'} - vD_B$ and outputs the proof as (J, v, τ, I, u, h_C). It can be easily shown that the simulated proof (J, v, τ, I, u, h_C) can be verified similar to the one generated by the true signer. We note that the same method can be used to show the non-transferability of the disavowal protocol of the improved scheme.

VI. Conclusion

In this paper, we pointed out the weaknesses of Zhao and Ye's certificateless undeniable signature scheme and mounted two attacks on their scheme. The first attack was resulted from a flaw in the signature structure of the proposed scheme and the second attack was due to the poorly structured confirmation and disavowal protocols. In our first attack, we targeted the invisibility of the scheme and in the second attack, we showed that the scheme does not possess the non-impersonation property and the adversary is able to impersonate the signer by initiating the confirmation/disavowal protocol on her behalf.

We then proposed an improved scheme which overcomes the aforementioned weaknesses while enjoying from the same efficient Sign algorithm. Our scheme employs a completely different method in its confirmation and disavowal protocols. Although the employment of the pairing-based version of Jakobsson et al.'s [18] NIDV proof systems requires more pairing computations in the confirmation and disavowal protocols of the improved scheme, it is secure against the second attack (i.e. attack on the non-impersonation) and provides the signer with better security and additional features.

Acknowledgment

This research was supported by the FRGS grants (FRGS/1/2015/ICT04/MMU/03/5) and (FRGS/2/2013/ICT04/MMU/01/1).

References

[1] Al-Riyami, S., and Paterson, K., Certificateless Public Key Cryptography, Advances in Cryptology - ASIACRYPT 2003, Springer Berlin / Heidelberg, (2003), pp. 452-473.

[2] Au, M.H., Mu, Y., Chen, J., Wong, D.S., Liu, J.K., and Yang, G., Malicious KGC attacks in certificateless cryptography. Proceedings of the 2nd ACM symposium on Information, computer and communications security, (2007), pp. 302-311.

[3] Boneh, D., and Franklin, M., Identity-Based Encryption from the Weil Pairing, Advances in Cryptology - CRYPTO 2001, Springer Berlin / Heidelberg, (2001), pp. 213-229.

[4] Boyd, C., and Foo, E., Off-line Fair Payment Protocols using Convertible Signatures, Advances in Cryptology - ASIACRYPT '98, Springer Berlin / Heidelberg, (1998), pp. 271-285.

[5] Boyar, J., Chaum, D., Damgard, I., and Pedersen, T., Convertible Undeniable Signatures, Advances in Cryptology - CRYPTO '90, Springer Berlin / Heidelberg, (1991), pp. 189-205.

[6] Chabanne, H., Phan, D., and Pointcheval, D., Public Traceability in Traitor Tracing Schemes, Advances in Cryptology EUROCRYPT 2005, Springer Berlin Heidelberg, (2005), pp. 542-558.

[7] Chaum, D., Zero-Knowledge Undeniable Signatures Advances in Cryptology - EUROCRYPT 90, Springer Berlin / Heidelberg, (1991), pp. 458-464.

[8] Chaum, D., and van Antwerpen, H., Undeniable Signatures, Advances in Cryptology - CRYPTO '89 Springer Berlin / Heidelberg, (1989), pp. 212-216.

[9] Chaum, D., van Heijst, E., and Pfitzmann, B., Cryptographically Strong Undeniable Signatures, Unconditionally Secure for the Signer, Advances in Cryptology - CRYPTO 91, Springer Berlin / Heidelberg, (1992), pp. 470-484.

[10] Choi, K.Y., Park, J.H., and Lee, D.H., A new provably secure certificateless short signature scheme, Computers & Mathematics with Applications, 61: 7, (2011), 1760-1768.

[11] Desmedt, Y., Goutier, C., and Bengio, S., Special uses and abuses of the Fiat-Shamir passport protocol, Advances in Cryptology - CRYPTO 87, Springer Berlin / Heidelberg, (1987), pp. 21-39.

[12] Desmedt, Y., and Yung, M., Weaknesses of Undeniable Signature Schemes, Advances in Cryptology - EUROCRYPT 91, Springer Berlin / Heidelberg, (1991), pp. 205-220.

[13] Diffie, W., and Hellman, M., New directions in cryptography, Information Theory, IEEE Transactions on, 22: 6, (1976), 644-654.

[14] Duan, S.S., Certificateless Undeniable Signature Scheme, Inform Sciences, 178: 3, (2008), 742-755.

[15] Hu, B., Wong, D., Zhang, Z., and Deng, X., Certificateless signature: a new security model and an improved generic construction, Designs, Codes and Cryptography, 42: 2, (2007), 109-126.

[16] Huang, X., Mu, Y., Susilo, W., Wong, D., and Wu, W., Certificateless Signature Revisited, Information Security and Privacy, Springer Berlin / Heidelberg, (2007), pp. 308-322.

[17] Jakobsson, M., Blackmailing using undeniable signatures, Advances in Cryptology - EUROCRYPT' 94, Springer Berlin / Heidelberg, (1995), pp. 425-427.

[18] Jakobsson, M., Sako, K., and Impagliazzo, R., Designated Verifier Proofs and Their Applications, Advances in Cryptology - EUROCRYPT 96, Springer Berlin / Heidelberg, (1996), pp. 143-154.

[19] Kurosawa, K., and Heng, S.-H., 3-Move Undeniable Signature Scheme, Advances in Cryptology - EUROCRYPT 2005, Springer Berlin / Heidelberg, (2005), pp. 181-197.

[20] Laguillaumie, F., and Vergnaud, D., Time-Selective Convertible Undeniable Signatures, Topics in Cryptology - CT-RSA 2005, Springer Berlin Heidelberg, (2005), pp. 154-171.

[21] Libert, B., and Quisquater, J.-J., Identity Based Undeniable Signatures, Topics in Cryptology - CT-RSA 2004, Springer Berlin / Heidelberg, (2004), pp. 112-125.

[22] Sakurai, K., and Miyazaki, S., An Anonymous Electronic Bidding Protocol Based on a New Convertible Group Signature Scheme, Information Security and Privacy, Springer Berlin / Heidelberg, (2000), pp. 385-399.

[23] Shamir, A., Identity-Based Cryptosystems and Signature Schemes, Advances in Cryptology, Springer Berlin / Heidelberg, (1985), pp. 47-53.

[24] Shoup, V., Lower Bounds for Discrete Logarithms and Related Problems, Advances in Cryptology - EUROCRYPT 97, Springer Berlin / Heidelberg, (1997), pp. 256-266.

[25] Tso, R., Huang, X., and Susilo, W., Strongly secure certificateless short signatures, Journal of Systems and Software, 85: 6, (2012), 1409-1417.

[26] Zhao, W., and Ye, D., Certificateless undeniable signatures from bilinear maps, Inform Sciences, 199: 0, (2012), 204-215.