International Journal of Cryptology Research 3(1): 48-67 (2011)

Development of Undeniable Signature Schemes without Certificates

[1] Rouzbeh Behnia, [1] Swee-Huay Heng and [2] Che-Sheng Gan

[1] Faculty of Information Science and Technology, Multimedia University

[2]Faculty of Engineering and Technology, Multimedia University

Email: rouzbeh.behnia@mmu.edu.my, shheng@mmu.edu.my and csgan@mmu.edu.my

ABSTRACT

The notion of undeniable signature schemes was proposed by Chaum and Antwerpen in order to provide the signer with the ability to control the privacy of her signatures. Undeniable signature schemes without certificates that have been proposed to this day are either in identity-based paradigm or certificateless paradigm. In this paper, we provide a complete review on the development course of undeniable signature schemes without certificates. This paper reviews all of the undeniable signature schemes without certificates proposed so far.

Keywords: Undeniable signatures, identity-based, certificateless, designated verifiers, convertibility.

INTRODUCTION

Public key cryptography was first designed to address the issues associated with key distribution related to symmetric systems. The development of public key cryptography was a breakthrough in modern cryptography. In public key cryptography, the authenticity of a user's public key is delivered in the form of certificates which are generated by the trusted third party (i.e. certificate authority). However, costly issues of public key cryptography (e.g. certificate generation, certificate management, etc.) were incentives of developing other systems which do not require certificates (i.e. implicit certification) to deliver the authenticity of user's public key.

The idea of identity-based cryptography was first mentioned by Shamir (1985) to address the issues inherited in public key cryptography. In identity-based systems, a user's public key is directly computed from his publicity available information (i.e. email address, IP address, etc.). Hence, the need to issue and manage signed certificates for each user's public key is completely eliminated. The idea of implicit certification is enforced in user's private key generation, whereby the trusted third party called *private key generator* (PKG) uses its secret information (master secret) on user's identity information to calculate the private key that corresponds to a particular public key. The first successful implementation of identity-based systems was until the noble work of Boneh and Franklin (2001). They developed their system using bilinear pairing on modified elliptic curves.

The idea of certificateless cryptography was first proposed in Al-Riyami and Paterson (2003). In certificateless system, the private key of the user is composed of two elements. Consequently, user chooses a part of her private key and calculates her public key. The second element of the private key is then generated by the trusted third party called *key generation center* (KGC), based on its secret information, the hash value of the user's identity information and her respective public key. Therefore, it addresses the inherited private key escrow problem of identity-based system, while eliminating the feature of easy public key.

Chaum and Antwerpen (1990) introduced the concept of undeniable signature schemes by which the validity/invalidity of the signature can only be verified with the direct help of the signer (via confirmation and disavowal protocol) in either an interactive or non interactive manner. Mainly, an undeniable signature protects signer's rights to the privacy of the signed document. Software licensing is one of the main applications of undeniable signatures; software vendor can incorporate an undeniable signature into the software and validate the software correctness and authenticity only to the paying customers. Therefore, the software will be protected from piracy since the pirate is not able to prove the correctness of the software. Various extensions of undeniable signatures such as convertible undeniable signatures (Boyar, Chaum, Damgård and Pedersen (1991)), designated verifier signatures (Jakobsson, Sako and Impagliazzo (1996)) and designated confirmer signatures (Chaum (1995)), have been proposed in literature.

Convertibility (Boyar *et al.* (1991)) and designation of verifier (Jakobsson *et al.* (1996)) are two of the important added features to undeniable signatures. The former enables the signer to convert her undeniable signatures to universally verifiable signatures (i.e., ordinary digital signatures). Basically, the signer can choose to convert a single signature (selective conversion) or all of her signatures (universal conversion) to universally verifiable signatures. The latter implies the ability of the signer to decide by whom her signature is being verified.

Practically, designation of verifier solves the conflict between authentication and privacy of the signer.

The purpose of this paper is to map out and discuss the development course of undeniable signatures without certificates. To the best of our knowledge, undeniable signature schemes without certificates that have been proposed in the literature to this day are developed in either identity-based system or certificateless system. In this paper, we first provide a brief overview on definitions that are going to be used throughout the paper. Then, we outline and explain the notion of undeniable signature and its security notions. And lastly, we will discuss the emerge and development course of undeniable signature schemes without certificates.

PRELIMINARIES

We let $\mathbb{G}_1$ be an additive cyclic group of prime order q with P as its generator, and $\mathbb{G}_2$ be and multiplicative cyclic group of the same cyclic group. An admissible bilinear pairing $\hat{e}$: $\mathbb{G}_1 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_2$ is given which is to satisfy the following properties:

Bilinearity: for $P, Q, R \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_q^*$ we have:

- $\hat{e}(P + Q, R) = \hat{e}(P, R)\, \hat{e}(Q, R)$
  and $\hat{e}(P, Q + R) = \hat{e}(P, Q)\, \hat{e}(P, R)$.

- $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$and $\hat{e}(aP, bQ) = \hat{e}(abP, Q)$.

Non-degeneracy: there exits P and $Q \in \mathbb{G}_1$ such that $\hat{e}(P, Q) \neq 1$.

Computability: for every P and $Q \in \mathbb{G}_{1\,,}$ $\hat{e}(P, Q)$ is computable.

The *Computational Diffie-Hellman problem* (CDH) is, given P, aP, bP for unknown $a, b \in \mathbb{Z}_q^*$, to compute abP.

The *Bilinear Diffie-Hellman problem* (BDH) is, given P as a generator of $\mathbb{G}_1$ and $aP, bP, cP \in \mathbb{G}_1$ for unknown a, b, $c \in \mathbb{Z}_q^*$, to compute $\hat{e}(P, P)^{abc}$.

The *Decisional Bilinear Diffie-Hellman problem* (DBDH) is, given P as a generator of $\mathbb{G}_1$, $aP, bP, cP \in \mathbb{G}_1$ and $h \in \mathbb{G}_2$ for unknown $a, b, c \in \mathbb{Z}_q^*$, to decide whether $h = \hat{e}(P, P)^{abc}$ or not.

The *Gap Bilinear Diffie-Hellman problem* is to solve a BDH problem by making use of a DBDH oracle. A prime group $\mathbb{G}$ is called a Gap Diffie-Hellman group if DBDH is easy in $\mathbb{G}$ but BDH is hard.

OUTLINE OF UNDENIABLE SIGNATURE SCHEME

Generally, the structure of an undeniable signature scheme consists of two probabilistic polynomial time (PPT) algorithms (key generation and sign) and two protocols (confirmation and disavowal).

Key Generation: A probabilistic algorithm that on the input of security parameter(s) generates private and public key pair for users in the system.

Sign: A probabilistic/deterministic algorithm which generates an undeniable signature on the input of secret key, public parameters and a message.

Confirmation: A protocol between the signer/designated confirmer and the verifier to convince the verifier about the validity of message-signature pair issued by the signer.

Disavowal: A protocol between the signer/designated confirmer and the verifier to convince the verifier about the invalidity of the message-signature pair.

SECURITY NOTIONS

The following subsection is dedicated to briefly mention and explain the security notions that are defined in the context of undeniable signature schemes.

Unforgeability: The notion of unforgeability of undeniable signature scheme is quite similar to the notion of existential unforgeability in ordinary digital signatures. The only variation in defining this notion in the context of undeniable signature schemes is that in addition to the sign oracle, the adversary has access to the confirmation and disavowal oracles as well.

Invisibility: The notion of invisibility was first introduced by Chaum *et al.* (1992). Essentially, this notion implies the inability to decide whether a given message-signature pair (m, σ) is valid. Invisibility is the distinguishing factor of undeniable signatures from ordinary digital signatures; if the verifier is able to determine the validity of a message-signature pair without the help of the signer then the signature is not any different than the ordinary digital signature.

The notion of anonymity was first introduced by Galbraith and Mao (2003) and it is considered as a variation of indivisibility. Without loss of generality, the notion of anonymity implies; given a message-signature pair (m, σ), and two identities of possible signers ID_1, ID_2; one should be unable to distinguish which identity has produced the signature.

Non-transferability: Non-transferability is a security notion which is driven from zero-knowledgeness property of both the confirmation and disavowal protocols in undeniable signature schemes. Intuitively, non-transferability refers to the inability of the verifier to transfer the proof of validity or invalidity of a message-signature pair to a third party. Informally, information that the verifier obtains from the confirmation/disavowal oracles should only be enough to convince the verifier about the validity/invalidity of a particular message-signature pair; and not to enable him to transfer the proof to a third party.

Un-Impersonation: Security notion against impersonation attack is yet another security notion introduced by Kurosawa and Heng (2005). The definition of impersonation attack in the context of undeniable signature can be interpreted as a two phase attack. In the first phase, the attacker generates a forged message-signature pair, the difference of this forgery with the one introduced in the notion of unforgeability is that an additional bit is generated along with the forged pair which indicates the validity and invalidity of the generated message-signature pair produced. In the second phase, the adversary engages in either the confirmation or disavowal protocol (based on the indicator bit) to convince the verifier about the validity/invalidity of the forged message-signature pair.

UNDENIABLE SIGNATURE SCHEMES WITHOUT CERTIFICATES

Successful implementation of identity-based system by Boneh and Franklin (2001) gave rise to the development of many different cryptographic schemes. Two years later, Al-Riyami and Paterson (2003) used the same method (Weil pairing) to propose the concept of certificateless cryptography to address the inherited key escrow problem in identity-based system. In both of the systems mentioned above, implicit certification takes place where the trusted third party (either PKG or KGC) calculates a part of (in certificateless cryptography) or the whole secret key (identity-based cryptography) of the user. Table below lists the undeniable signature schemes without certificates that are proposed to this day.

TABLE 1: Undeniable signature without certificates

Scheme	Security	Underlying Assumption	Model	Designated Verifier	Paradigm	Security Notions
Han *et al.* (2003)	Broken by Zhang *et al.* (2005)	-	-	-	Identity-based	-
Chow (2005)	No security proof	-	-	-	Identity-based	-
Libert and Quisquater (2004)	Broken by Li *et al.* (2008)	BDH	RO	Yes	Identity-based	Unforgeability, invisibility, anonymity
Galindo *et al.* (2006)	Indirect proof (generic construction)	RSA	-	-	Identity-based	-
Duan (2008)	Pairing related assumptions	BDH	RO	Yes	Certificateless	Unforgeability, invisibility
Wu *et al.* (2008)	Pairing related assumptions	CDH	RO	Yes	Identity-based	Unforgeability, invisibility, anonymity, un-impersonation

In the rest of the paper, A will denote the signer and B will denote the verifier.

IDENTITY-BASED UNDENIABLE SIGNATURE SCHEMES

To explain the basic ideas underlying identity-based undeniable signature schemes, we illustrate the following general structure of such schemes.

Remark: It is evident that schemes with various security level and additional features (e.g., convertibility) may have various numbers of algorithms in their structure.

Setup: This algorithm will generate PKG's secret and public key pair as well as the system's public parameters.

Extract: The private key of the user will be generated based on the hash value of her identity information (ID) and delivered to the user in a secure way.

Sign: Through this algorithm, user will generate the signature.

Confirmation/Disavowal: Using these protocols, the signer will prove the validity/invalidity of the message-signature pair.

EARLY SCHEMES (WITHOUT SECURITY PROOF)

In 2003, Han *et al.* (2003) proposed the first identity-based undeniable signature scheme which provided the feature of designation of confirmer. Their scheme has an identical *setup* step to Boneh and Franklin's scheme (2001). In their *extract* algorithm, PKG generates two keys for each user, namely the signing key and the verifying key; whereby, the latter is used for the verifying process (i.e. could be passed to a designated confirmer). Even though signature generation using Han *et al.*'s scheme was quiet efficient (since they did not use any pairing evaluation in their sign algorithm) the weak structure of their scheme led to the attack mounted by Zhang *et al.* (2005).

Zhang *et al.* (2005) mounted two attacks (denial attack and forge attack) on Han *et al.*'s scheme. The former is initiated by the signer, where she would be able to misuse the disavowal protocol in order to deny a valid signature. The attack takes place due to a flaw in the disavowal protocol where the signer is not obligated to prove the veracity of her secret keys in the disavowal protocol. The latter refers to the ability of an adversary to generate a signature for a given message on behalf of a particular signer and engage in the confirmation protocol with the verifier.

The imperfect structure of Han et al.'s scheme and the attacks mounted by Zhang *et al.* were good incentives for Chow (2005) to incorporate the concept of *verifiable pairing* in the structure of confirmation and disavowal protocol of Han *et al.*'s scheme.

Verifiable pairing is used to prove the existence of the link between the signer's public key and the signature without leaking the value of the private key. Basically, it proves the validity of the signature by enabling the verifier to solve an instance (only for the message that the signer has generated the signature) of BDH problem. In fact, verifiable pairing is employed in order to enable the verifier to compute the response of the challenged value himself (of course it is only possible with the direct help of the signer in an interactive manner).

The *extract* and *sign* algorithms of Chow's modified scheme were identical to the original scheme of Han *et al.* However, in the *setup* algorithm, PKG generates and publishes one additional public key in the form of $P_{inv} = s^{-1}P$. P_{inv} is necessary in order to incorporate the concept of verifiable pairing in the structure of Han *et al.*'s confirmation and disavowal protocols. The author illustrates that both of the Zhang *et al.*'s attacks could be prevented by employing the concept of verifiable pairing in the confirmation and disavowal protocol. Nonetheless, no security proof was provided to prove the security of the newly proposed scheme.

PROVABLY SECURE IDENTITY-BASED UNDENIABLE SIGNATURE SCHEMES

Provable security is a detachable part of developing secure signature schemes. This subsection of the paper is dedicated to review and discuss provably secure identity-based undeniable signature schemes. Table 2 depicts the efficiency differences of the two provably secure identity-based undeniable signature schemes (Libert and Quisquater (2004); Wu *et al.* (2008)) in the literature. (S denotes the signer, and V denotes the verifier).

TABLE 2: Efficiency of provably secure identity-based undeniable signature schemes

		Pairing Evaluation		**Exponentiation in $\mathbb{G}_2$**		**Computation of form $\alpha P + \beta Q$**	
		S	V	S	V	S	V
Libert and Quisquater (2004)	Signature	1	-	-	-	-	-
	Confirmation	4	5	1	3	1	-
	Disavowal	6	4	4	4	1	-
Wu *et al.* (2008)	Signature	1	-	2	-	1	-
	Confirmation	4	8	1	3	1	-
	Disavowal	6	8	6	4	1	-

Libert and Quisquater's Scheme

Libert and Quisquater (2004) proposed the first provably secure undeniable signature scheme in an identity-based system. Their scheme is inspired by the signature scheme proposed by Boneh and Franklin (2001). Libert *et al.*'s scheme consists of 3 algorithms and 2 protocols as follows:

Setup: Providing the security parameters k and l, generates $\mathbb{G}_1$and $\mathbb{G}_2$of prime order $q \geq 2^k$, a generator P of $\mathbb{G}_1$ and an admissible bilinear map $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_2$; the algorithm also chooses 4 cryptographic hash functions. PKG sets $s \longleftarrow_R \mathbb{Z}_q$ randomly as its secret key and calculates $P_{pub} = sP$ as its public key. PKG's public key and system parameters $(params)$ will be available to all system users.

$$params = \left(q, \mathbb{G}_1, \mathbb{G}_2, P, P_{pub}, H_1, H_2, H_3, H_4\right)$$

Extract: Given a user identity ID, PKG will compute the private key for the user based on his/her identity ID and its' secret key s. $d_{ID} = sQ_{ID} = sH_1(ID)$.

Sign: Provided a message m, the signer A chooses a random salt $r \longleftarrow_R \{0,1\}^l$ and computes the value of $\gamma = \hat{e}\left(H_2(m, r, ID_A),\ d_{ID_A}\right)$ to form the signature as $\sigma\ = (r,\ \gamma\ )\ = (r, \hat{e}\left(H_2(m, r, ID_A),\ d_{ID_A}\right))$.

Confirmation: Figure 1 illustrates the steps taken in the confirmation protocol to produce a proof transcript for the designated verifier B.

Signer		Verifier
$Q_{ID_B} = H_1(ID_B)$ $U, R \longleftarrow_R \mathbb{G}_1$ $v \longleftarrow_R \mathbb{Z}_q^*$ $c = \hat{e}(P, U)\hat{e}\left(P_{pub}, Q_{ID_B}\right)^v$ $g_1 = \hat{e}(P, R)$ $g_2 = \hat{e}(H_2(m, r, ID_A), R)$ $h = H_3(c, g_1, g_2\ )$ $S = R + (h + v)\ d_{ID_A}$	$\xrightarrow{(U, v, h, S)}$	$c^{'} =\ \hat{e}(P, U)\hat{e}\left(P_{pub}, Q_{ID_B}\right)^v$ $g_1^{'} =\ \hat{e}(P, S)\hat{e}\left(P_{pub}, Q_{ID_A}\right)^{h+v}$ $g_2^{'} =\ \ \hat{e}\ (H_2(m, r, ID_A), S)\ \gamma^{h+v}$

Figure 1: Confirmation protocol of Libert and Quisquater's scheme

At the end of the protocol, the verifier performs the consistency check and accepts the proof if $h^{'} = h$ where $h' = H_3(c^{'}, g_1^{'}, g_2^{'})$. The confirmation protocol is non-transferable. More precisely, the verifier is able to simulate the identical transcript by computing the commitment collisions (U, v), using his secret key d_{ID_B}.

Disavowal: Figure 2 below shows the steps in the disavowal protocol of Libert and Quisquater's scheme.

Signer		Verifier
$Q_{ID_B} = H_1(ID_B)$		
$U, R \longleftarrow_R \mathbb{G}_1$		
$v \longleftarrow_R \mathbb{Z}_q^*$		
$\omega \longleftarrow_R \mathbb{Z}_q^*$		
$c = \hat{e}(P, U)\hat{e}\left(P_{pub}, Q_{ID_B}\right)^v$		
$C = \dfrac{\hat{e}\left(H_2(m, r, ID_A),\ d_{ID_A}\right)^{\omega}}{\gamma}$		
$V \longleftarrow_R \mathbb{G}_1$		
$y = \hat{e}\left(P_{pub}, Q_{ID_A}\right)$		
$\rho_1 = \hat{e}(H_2(m, r, ID_A), V)\, \gamma^{-v}$		
$\rho_2 = \hat{e}(P, V)\, y^{-v}$		
$h = H_4(\mathrm{C}, \mathrm{c}, \rho_1, \rho_2)$	(C, U, v, h, S, s)	If $(C = 1) \longrightarrow \perp$, else:
$S = V + (h + v)R$	$\xrightarrow{\qquad\qquad}$	$c^{'} = \hat{e}(P, U)\hat{e}\left(P_{pub}, Q_{ID_B}\right)^v$
$s = v + (h + v) \propto$		$\rho_1^{'} = \hat{e}(H_2(m, r, ID_A), S)\, \gamma^{-s} C^{-(h+v)}$
		$\rho_2^{'} = \hat{e}(P, S)\, y^{-s}$

Figure 2: Disavowal protocol of Libert and Quisquater's scheme

The signer has to prove her knowledge of the pair $(R = \omega\, d_{ID_A}, \propto = \omega)$ such that, $C = \frac{\hat{e}(H_2(m,r,ID_A),R)^{\omega}}{\gamma^{\propto}}$ and $\frac{\hat{e}(P,R)}{\hat{e}\left(P_{pub},Q_{ID_A}\right)^{\propto}} = 1$. At the end of the protocol, the verifier will perform a consistency check so that $h = h'$ where $h' = H_4(C, c^{'}, \rho_1^{'}, \rho_2^{'})$.

Li *et al.*'s Attack

Li *et al.* (2008) mounted a forgery attack on Libert and Quisquater's scheme by exploiting the bilinear property of pairing. The attack enables the adversary to forge a signature for any message m^* on behalf of any victim signer which he has obtained a valid message-signature pair from. The attack violates the existential unforgeability notion defined for the scheme as the victim signer is unable to deny the forged message-signature pair. The implementation detail of the attack could be found in Li *et al.* (2008).

Discussion

Libert and Quisquater's scheme is the first provably secure identity-based undeniable signature scheme proposed in the literature. Even after Li et al.'s attack, the general structure of the scheme is considered as a comprehensive sample of provable secure identity-based undeniable signature scheme. The signature generation algorithm of Libert *et al.*'s scheme is inspired by the work of Goh and Jarecki's (2003). Libert and Quisquater employed the method of designated verifier proof of Jakobsson *et al.* (1996) in the confirmation protocol and the method of Camenisch and Shoup (2003) to prove the inequality of two discrete logarithms in the disavowal protocol. The security model designed by Libert and Quisquater for undeniable signature schemes in identity-based setting is later employed by other schemes such as Wu *et al.* (2008).

Wu *et al.*'s Scheme

In 2008, Wu *et al.* proposed a provably secure convertible identity-based undeniable signature scheme. Their proposed scheme was quite similar to that of Libert and Quisquater in many aspects. Informally, it could be considered as the secured version of Libert and Quisquater's scheme with the additional feature of convertibility. In the following, we demonstrate Wu et al.'s scheme and mention the implementation differences of the new scheme with that of Libert and Quisquater (2004).

Setup: The setup algorithm is identical to Libert and Quisquater's scheme.

Extract: In the extract algorithm of the Wu et al.'s scheme, PKG has to calculate two secret keys for each user $SK_{ID} = sH_1(ID)$ and $VK_{ID} = sH_1(ID \parallel undeniable)$. Namely the signing key and the verifying key, the latter will be released if the signer intends to convert all her undeniable signatures to universally verifiable signatures (i.e., universal convert).

Sign: The convertible identity-based undeniable signature of Wu et al. is formed as a tuple $\sigma = (U, V, W)$, where $U = \hat{e}\big(VK_{ID}, H_2(m)\big)$, $V = vP$ where $v \longleftarrow_R \mathbb{Z}_q^*$ and $W = SK_{ID} + vH_3(U \parallel V)$.

Undeniable Verify: This protocol is for the signer to decide the validity of the provided message-signature pair by the verifier $\{True, False\} \longleftarrow verify\,(\sigma, m)$. Based on the output of this algorithm, the signer will produce the transcript of the confirmation or disavowal protocol.

Confirmation/Disavowal Protocol: The approach used in the confirmation/disavowal protocol is quite similar to the confirmation protocol of Libert and Quisquater's scheme. Therefore, we skip explaining these two protocols in our paper.

Selective Convert: The prover is able to generate a selective proof for either a valid or an invalid signature. On input of a valid message-signature pair by the verifier the signer generates the selective proof as shown in Figure 3-(a) and if the provided message-signature pair is identified invalid by the signer she will produce the selective proof as in Figure 3-(b).

Signer		Verifier
$v \longleftarrow_R \mathbb{Z}_p$	$\xrightarrow{(c, C)}$	$R_1' = \hat{e}(C, P)\hat{e}(H(ID \parallel undeniable), P_{pub})^c$
$R_1 = \hat{e}(P, P)^r$		$R_2' = \hat{e}(C, H(m))U^c$
$R_2 = \hat{e}(P, H(m))^r$		$c' = H(ID_S \parallel R'_1 \parallel R'_2 \parallel m \parallel \sigma)$
$c = H(ID_S \parallel R_1 \parallel R_2 \parallel m \parallel \sigma)$		$if\ (c = c') \Rightarrow accept$
$C = rP - cVK_{ID_S}$		else $\Rightarrow \perp$

a) Selective proof for a valid message-signature pair

Signer		Verifier
$z, \alpha, \beta \longleftarrow_R \mathbb{Z}_p$		
$A = (\frac{\hat{e}(VK_{ID_S},\ H(m))}{U})^z$		
$B = \frac{\hat{e}(P, H(m))^\alpha}{U^\beta}$		
$C = \frac{\hat{e}(P, P)^\alpha}{\hat{e}(H(ID \parallel undeniable), P_{pub})^\beta}$		$B' = \frac{\hat{e}(D_S, H(m))}{U^{K_s}\, A^d}$
$d = H(ID_S \parallel A \parallel B \parallel C \parallel m \parallel \sigma)$	$\xrightarrow{(A, d, D_S, K_s)}$	$C' = \frac{\hat{e}(D_S, P)}{\hat{e}(H(ID \parallel undeniable), P_{pub})^{K_s}}$
$D_S = \alpha P + dzVK_{ID_S}$		$d' = H(ID_S \parallel A \parallel B \parallel C \parallel m \parallel \sigma)$
$K_s = \beta + dz$		$if\ (d = d') \Rightarrow accept$
$c = H(ID_S \parallel R_1 \parallel R_2 \parallel m \parallel \sigma)$		else $\Rightarrow \perp$
$C = rP - cVK_{ID_S}$		

b) Selective proof for an invalid message-signature pair

Figure 3: Selective proof of Wu *et al.*'s scheme

Universal Convert: The signer is also able to convert all of her signatures to universally verifiable signatures by releasing the universal proof VK_{ID} as it is the signer's verifying key.

Discussion

Wu *et al.* proposed the security model of identity-based convertible undeniable signature schemes for the first time. Even though the cost of signature generation in Wu *et al.*'s scheme is slightly higher than that of Libert and Quisquater's, it is completely secure against attacks that exploit the bilinear property of pairing (attack mounted by Li *et al.* on Libert and Quisquater's scheme). Practically, the scheme proposed by Wu *et al.* is able to enjoy the benefits of designated confirmer signatures. The signer can simply designate a confirmer by passing him the verifying key VK_{ID}. Clearly, the designated verifier will not be able to forge signatures since he does not have access to the signing key SK_{ID}.

CERTIFICATELESS UNDENIABLE SIGNATURE SCHEMES

Certificateless cryptography was developed to address the key escrow issue in identity-based systems. Unfortunately, the research on certificateless undeniable signature scheme has been very slow as we only have one provably secure certificateless undeniable signature scheme proposed so far. Following the work of Al-Riyami and Paterson (2003), Duan (2008) proposed the first certificateless undeniable signature scheme. Duan's scheme is designed with five algorithms and two protocols. Table 3 below illustrates the efficiency of Duan's proposed certificateless scheme (S denotes the signer, and V denotes the verifier).

TABLE 3: Efficiency of Duan's scheme

		Pairing Evaluation		**Exponentiation in $\mathbb{G}_2$**		**Computation of form $\alpha P + \beta Q$**	
		S	V	S	V	S	V
Duan (2008)	Signature	2	-	1	-	-	-
	Confirmation	6	8	3	6	2	1
	Disavowal	11	8	7	7	2	1

Setup: The setup algorithm takes place quite similar to Libert and Quisquater's scheme (except that Duan uses five cryptographic hash functions in the proposed scheme).

Set Secret Value and Public Key: $t \in Z_q$ will be chosen randomly by user as his secret value and $T = tP$ is computed as the corresponding public key.

Partial Private Key Extraction: Providing user's identity ID and public key T, the KGC computes $d_{ID} = sQ_{ID} = sH_1(ID, T)$ and sends it to the user in a secure way.

Set Private Key: After user received his partial private key, he will form his private key as a pair consisting of his secret value and partial private key (t, d_{ID}).

Sign: To issue a signature on message m, Alice chooses a random string $r \leftarrow_R \{0,1\}^k$ and forms $h_2 = H_2(m, r, ID_A)$ and $h_3 = H_3(m, r, ID_A,\ T_A) \in \mathbb{G}_1$. Alice uses her private key pair (t, d_{ID}) to compute $\rho = \hat{e}\left(h_2, d_{ID_A}\right) \hat{e}(Q_{ID_A}, h_3)^{t_A}$. The signature on the message m is given as $\sigma = (r, \rho, T_A)$.

Confirmation: Figure 4 below illustrates the details of the confirmation protocol.

Signer		Verifier
$U, Y \longleftarrow_R \mathbb{G}_1$		
$v, u, a \longleftarrow_R \mathbb{Z}_q^*$		
$c_1 = \hat{e}(P, U)\hat{e}\left(P_{pub}, Q_{ID_B}\right)^v$		
$c_2 = uP + vT_B$		
$M = \hat{e}(P, P)^a$		
$N = \hat{e}(P, Y)$		
$O = \hat{e}(H_2(m, r, ID_A), Y)$		
$\hat{e}\left(Q_{ID_A}, H_3(m, r, ID_A, T_A)\right)^a$		$c'_1 = \hat{e}(P, U)\hat{e}\left(P_{pub}, Q_{ID_B}\right)^v$
$h = H_4(c_1, c_2, M, N, O, m, r, \rho)$		$c'_2 = uP + vT_B$
$B = Y - (h + v)\, d_{ID_A}$	$\xrightarrow{(U, u, v, h, b, B)}$	$M' = \hat{e}(P, P)^b \hat{e}(P, T_A)^{h+v}$
$b = a - (h + v)\, t_A$		$N' = \hat{e}(P, B)\hat{e}\left(P_{pub}, Q_{ID_A}\right)^{h+v}$
		$O' = \rho^{h+v}\hat{e}(H_2(m, r, ID_A), B)$
		$\hat{e}\left(Q_{ID_A}, H_3(m, r, ID_A, T_A)\right)^b$

Figure 4: Confirmation protocol of Duan's scheme

At the end of the protocol, the verifier will perform the consistency check by checking if $h = h'$ where $h' = H_4(c'_1, c'_2, M', N', O', m, r, \rho)$ and will accept the proof if the equation holds.

Disavowal: Figure 5 depicts the implementation details of the disavowal protocol.

Signer

$U \longleftarrow_R \mathbb{G}_1$

$v, u, \alpha \longleftarrow_R \mathbb{Z}_q^*$

$c_1 = \hat{e}(P, U)\hat{e}\left(P_{pub}, Q_{ID_B}\right)^v$

$c_2 = uP + vT_B$

$h_2 = H_2(m, r, ID_A)$

$h_3 = H_3(m, r, ID_A, T_A)$

$C = (\frac{\hat{e}(h_2, d_{ID})\hat{e}(Q_{ID_A}, h_3)^{t_A}}{\rho})^\alpha$

$I \longleftarrow_R \mathbb{G}_1$

$\beta \longleftarrow_R \mathbb{Z}_q^*$

$y = \hat{e}\left(P_{pub}, Q_{ID_A}\right)$

$P_1 = \hat{e}(P, I)\ \hat{e}(P_{pub}, Q_{ID_A})^{-v}$

$P_2 = \hat{e}(P, P)^\beta\ \hat{e}(P, T_A)^{-v}$

$P_3 = \hat{e}(h_2, I)\ \hat{e}(Q_{ID_A}, h_3)^\beta \rho^{-v}$

$h = H_5\ (C, c_1, c_2, P_1, P_2, P_3, \mathrm{m}, \mathrm{r}, \rho)$

$Q = I + (h + v)J$

$\mu_1 = v + (h + v)\alpha$

$\mu_2 = \beta + (h + v)j$

$$\xrightarrow{(C, U, u, v, h, Q, \mu_1, \mu_2)}$$

Verifier

If $C = 1$ proof will be rejected, else:

$c'_1 = \hat{e}(P, U)\hat{e}\left(P_{pub}, Q_{ID_B}\right)^v$

$c'_2 = uP + vT_B$

$h_2 = H_2(m, r, ID_A)$

$h_3 = H_3(m, r, ID_A, T_A)$

$P'_1 = \hat{e}(P, Q)\ \hat{e}(P_{pub}, Q_{ID_A})^{\mu_1}$

$P'_2 = \hat{e}(P, P)^{\mu_2}\ \hat{e}(P, T_A)^{-\mu_1}$

$P'_3 = \hat{e}(h_2, Q)\ \hat{e}(Q_{ID_A}, h_3)^{\mu_2} \rho^{-\mu_1} C^{-(h+v)}$

Figure 5: Disavowal protocol of Duan's scheme

The protocol is for the signer to prove her knowledge of the tuple (J, j, α) such that, $C = \frac{\hat{e}(h_2, J)\hat{e}(Q_{ID_A},\ h_3)^j}{\rho^\alpha}$, $\hat{e}(P, J) = \hat{e}\left(P_{pub}, Q_{ID_A}\right)^\rho$ and $jP = \alpha T_A$. Finally, the verifier will undergo the consistency check by checking if $h = h'$ where $h' = H_4(c'_1, c'_2, P'_1, P'_2, P'_3, m, r, \rho)$ and will accept the proof if the equation holds.

Note: The method that was employed in confirmation and disavowal protocol of Duan's scheme is similar to that of Libert and Quisquater's scheme. The main difference here is that because of the nature of certificateless systems the signer has to prove the linkage between the signature and both components of her private key (t, d_{ID}).

Discussion

Duan's certificateless scheme is the first undeniable signature scheme developed in a certificateless setting. Duan modeled the security of undeniable signature schemes in certificateless system for the first time. The proposed certificateless scheme took advantage of the same techniques used in Libert and Quisquater's confirmation and disavowal protocol in order to provide non interactive designated verifier proofs. Following the original proposal of certificateless systems (Al-Riyami and Paterson (2003)), Duan modeled the security of the proposed scheme based on two type attackers. Namely type 1 and type 2 attackers. Where the earlier considers attackers who have no access the system wide master key but are able to replace user's public keys and former defines attackers who has access to the system wide master key (i.e., malicious KGC) but is not permitted to replace user's public keys.

GENERIC CONSTRUCTION OF UNDENIABLE SIGNATURE SCHEMES

Galindo *et al.* (2006) proposed a generic construction of identity-based schemes by employing two quite similar ordinary digital signature schemes. The nature of their work was to extend the work of Bellare *et al.* (2004) to develop a method of generic construction of identity-based signature schemes with additional properties. Following is the structure of the ordinary digital signature scheme that is used to develop identity-based signature schemes with additional properties.

Key generation algorithm: On the input of the security parameter k, the secret key SK and the public key PK are generated $(SK, PK) \leftarrow KG(1^k)$.

Signing algorithm: Upon inputting signer's secret key SK and a message m, the signature will be generated $sig_{SK}\ (m) \leftarrow Sign(SK, m)$.

Verification algorithm: This algorithm is to decide whether a message-signature pair is valid. Providing user's public key PK, and a message signature pair, it will output true or false $\{0,1\} \leftarrow Vfy\ (PK, m, sig)$.
The algorithms above are formed as below to construct the identity-based undeniable signature scheme of Galindo *et al.* (2006).

Setup $IB_{\mathbf{US}}.\mathbf{KG}(\mathbf{1^k})$: This algorithm is simulated to generate the master secret key msk and the public parameters mpk of the trusted third party (i.e. PKG) $(msk, mpk) \leftarrow KG(1^k)$.

Extract $IB_{\mathbf{US}}.\mathbf{Extr}(\mathbf{msk}, \mathbf{id_i})$: On inputting the user's ID and system wide secret key, PKG will simulate $\mathrm{KG}'(1^k)$ to generate a random key pair (pk_s, sk_s) for the user. The secret key of the user will be in the form of $sk[id_s] = (sig_s, pk_s, sk_s)$ where $sig_s \leftarrow Sign(msk, id_s||pk_s)$

Sign $IB_{\mathbf{US}}.\mathbf{Sign}(\ \mathbf{sk}[\mathbf{id_i}], \mathbf{m})$: On inputting user's secret key $sk[id_i]$ and the message to be signed, the algorithm first parses the secret key $sk[id_s] \longrightarrow (sig_s, pk_s, sk_s)$ and then forms the signature as $sig_{\ us} \longleftarrow \mathrm{Sign}'(\ sk_s, \mathrm{m})$.

Confirmation: To perform the confirmation protocol, the prover parses $sk[id_s] \longrightarrow (sig_s, pk_s, sk_s)$ and sends (sig_s, pk_s) to the verifier. The verifier checks the validity of signer's secret key $sk[id_s]$, by running $Vfy(mpk, id_s||pk_s, sig_s\ )$. The verifier will initiate the confirmation protocol if and only if Vfy returns true, otherwise the verifier will reject.

Disavowal: The same validity check on sig_s will be performed and the disavowal protocol will be initiated if $S.Vfy(mpk, id_s||pk_s, sig_s\ )$ returns true.

Discussion

Galindo *et al.* proposed other identity-based signature schemes with additional properties (e.g. verifiably encrypted signatures, blind signatures, etc.) in their paper. They claimed that their scheme is secure in the standard model by providing indirect proofs (i.e. if the underlying ordinary signature schemes are secure then the resulted identity-based undeniable signature scheme is secure.). Following the work of Damgård and Pedersen (1996), they fabricated a simulator algorithm which on the input of the user's public key and a message produces a simulated signature which is indistinguishable from a real undeniable signature. The simulator algorithm is to provide simulatability; simulatability is treated as a special form of standard notion of invisibility.

CONCLUSION

In this paper, we reviewed the development of undeniable signature schemes without certificates which were practically proposed after the successful implementation of Boneh and Franklin. We highlighted the similarities and differences of the proposed schemes in the literature. Furthermore, we stressed on the common successful methods of some proposed schemes which would be beneficial to be incorporated in future schemes. Among all the schemes that are proposed to this day, there exist only two secure schemes (Duan (2008); Wu *et al.* (2008)) with security proofs in the literature of undeniable signature schemes without certificates which makes the research in this field more challenging.

ACKNOWLEDGEMENT

This research was supported by the FRGS grant (FRGS/2/2010/TK/MMU/02/03) and Multimedia University Graduate Research Assistant Scheme.

REFERENCES

Al-Riyami, S. and Paterson, K. 2003. Certificateless Public Key Cryptography *Advances in Cryptology - ASIACRYPT 2003*, Springer Berlin / Heidelberg. **537**: 189-205.

Bellare, M., Namprempre, C. and Neven, G. 2004. Security Proofs for Identity-Based Identification and Signature Schemes. *Journal of Cryptology*. **22**: 1-61.

Boneh, D. and Franklin, M. 2001. Identity-Based Encryption from the Weil Pairing. In J. Kilian (Ed.). *Advances in Cryptology — CRYPTO 2001* , Springer Berlin / Heidelberg. **2139**: 213-229.

Boyar, J., Chaum, D., Damgård, I. and Pedersen, T. 1991. Convertible Undeniable Signatures. In A. Menezes & S. Vanstone (Eds.). *Advances in Cryptology-CRYPT0' 90,* Springer Berlin/ Heidelberg. **537**: 189-205.

Camenisch, J. and Shoup, V. 2003. Practical verifiable encryption and decryption of discrete logarithms *Advances in Cryptology-Crypto 2003*. 2729: 126-144.

Chaum, D. 1995. Designated Confirmer Signatures. In A. De Santis (Ed.), *Advances in Cryptology — EUROCRYPT'94*, Springer Berlin/ Heidelberg. **950**: 86-91.

Chaum, D. and van Antwerpen, H. 1990. Undeniable Signatures. In G. Brassard (Ed.), *Advances in Cryptology — CRYPTO' 89*, Springer Berlin / Heidelberg. 372-386.

Chaum, D., van Heijst, E. and Pfitzmann, B. 1992. Cryptographically Strong Undeniable Signatures, Unconditionally Secure for the Signer. In J. Feigenbaum (Ed.). *Advances in Cryptology — CRYPTO '91*, Springer Berlin / Heidelberg. 372-386.

Chow, S. S. M. 2005. Verifiable pairing and its applications *Information Security Applications*. **3325**: 170-187.

Damgård, I. and Pedersen, T. 1996. New convertible undeniable signature schemes. *Proceedings of the 15th annual international conference on Theory and application of cryptographic techniques*. Saragossa, Spain: Springer-Verlag. 372-386.

Duan, S. S. 2008. Certificateless undeniable signature scheme. *Information Sciences*. **178**: 742-755.

Galbraith, S. D. and Mao, W. B. 2003. Invisibility and anonymity of undeniable and confirmer signatures. *Topics in Cryptology - Ct-Rsa 2003*. **2612**:80-97.

Galindo, D., Herranz, J. and Kiltz, E. 2006. On the generic construction of identity-based signatures with additional properties. *Advances in Cryptology - ASIACRYPT 2006*. **4284**:178-193.

Goh, E. J. and Jarecki, S. 2003. A signature scheme as secure as the Diffle-Hellman problem. *Advances in Cryptology-Eurocrypt 2003*. **2656**: 401-415.

Han, S., Yeung, W. K. Y. and Wang, J. 2003. Identity-based confirmer signatures from pairings over elliptic curves. *Proceedings of the 4th ACM conference on Electronic commerce*. San Diego, CA, USA: ACM, 262-263.

Jakobsson, M., Sako, K. and Impagliazzo, R. 1996. Designated verifier proofs and their applications. *Proceedings of the 15th annual international conference on Theory and application of cryptographic techniques.* Saragossa, Spain: Springer-Verlag, 143-154.

Kurosawa, K. and Heng, S.-H. 2005. 3-Move Undeniable Signature Scheme. In R. Cramer (Ed.). *Advances in Cryptology – EUROCRYPT 2005.* Springer Berlin / Heidelberg. **3494**: 561-561.

Li, Z. C., Yan, Y. S. and Zhang, J. M. 2008. Attack on Libert *et al.*'s ID-Based Undeniable Signature Scheme. *Chinese Journal of Electronics*. **17**: 748-750.

Libert, B. and Quisquater, J. J. 2004. Identity based undeniable signatures. *Topics in Cryptology - Ct-Rsa 2004.* **2964**: 112-125.

Shamir, A. 1985. Identity-Based Cryptosystems and Signature Schemes. In G. Blakley and D. Chaum (Eds.). *Advances in Cryptology*, Springer Berlin / Heidelberg. **196**: 47-53.

Wu, W., Mu, Y., Susilo, W. and Huang, X. Y. 2008. Provably secure identity-based undeniable signatures with selective and universal convertibility. *Information Security and Cryptology.* **4990**: 25-39.

Zhang, F., Safavi-Naini, R. and Susilo, W. 2005. Attack on Han *et al.*'s ID-based confirmer (undeniable) signature. *ACM-EC'03 Applied Mathematics and Computation.* **170**: 1166-1169.