International Journal of Cryptology Research 3(1): 34-47 (2011)

The Applications of DH-Tuple Witness Indistinguishable Protocols

[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 concept of *witness indistinguishable* and *witness hiding* was introduced by Feige and Shamir. *A witness hiding proof system is* an achievable substitute of zero knowledge proof systems in many cryptographic protocols, and is weaker requirements than zero knowledge. Kurosawa and Heng introduced the concept of *witness indistinguishability* and *witness hiding* to confirmation and disavowal protocols of undeniable signature schemes, their 3-move protocol is used to prove the validity/invalidity of DH-tuples and non DH-tuples. In this paper, we review the applications and of the 3-move protocol of Kurosawa and Heng, and discuss its use in various extensions of undeniable signature schemes.

Keywords: undeniable signatures, witness indistinguishability, selective/universal conversion, nominative signatures, designated confirmer.

INTRODUCTION

The concept of interactive zero knowledge proof systems was introduced by Goldwasser *et al.* (1985). Zero knowledge protocols have a great number of applications in modern cryptography. Informally, zero-knowledge (ZK) assures that the verifier V will not gain any information other than the veracity of the proof after interaction with the prover P. In a zero knowledge proof system, there exists a simulator S for each V; and S does not have any access to P, yet it can simulate the interaction between P and V. Consequently, it can be intuitively extracted that V did not gain any knowledge from his interaction with P since the same output could have been produced even without interaction with P (i.e., output generated by S).

Triviality of ZK under parallel composition of protocols was the main incentive for Feige and Shamir (1990) to propose the idea of witness indistinguishability and witness hiding. A proof system (P, V) is witness indistinguishable (WI) if V cannot distinguish between two (or more) executions of a proof system, in which, P uses different witnesses for each. A witness indistinguishable protocol is non-trivial if every input to the proof system has at least two computationally independent witnesses. Witness hiding (WH) can be obtained from any non-trivial witness indistinguishable protocol and assures that no information about P's witnesses will leak in executions of any WH protocols. Under the assumption that one way functions exist, it is proven in Feige and Shamir (1990) that any ZK protocol is also WI.

Chaum and Antwerpen (1990) introduced the concept of undeniable signature schemes in which the validity/invalidity of the signature can only be verified with the direct help of the signer (via confirmation and disavowal protocol). Later in 1991, Chaum deployed his scheme by employing the concept of zero-knowledge to confirmation and disavowal protocols of the original scheme. Zero-knowledgeness of confirmation and disavowal protocols of undeniable signature scheme makes sure that that no adversary in role of a cheating verifier is able to compute or gain any knowledge about the prover's secret information (i.e. secret key).

In 2005, Kurosawa and Heng (2005) incorporated the concept of witness indistinguishability in the confirmation and disavowal protocols of undeniable signature scheme. The basic idea of Kurosawa and Heng is based on the fact that each DH-tuple has two witnesses, and the prover, whom is in possession of either one of the witnesses, can prove that the tuple is DH or non-DH using a simple 3-move interactive protocol. Since there exist two witnesses for every DH tuple, the protocol is also WH based on the results of Feige and Shamir (1990). Since then, the technique of employing WI protocols to prove the validity/invalidity of a DH-tuple has incorporated in many other extensions of undeniable signatures. 3-move protocol of Kurosawa and Heng had noticeable effect on development of many extensions of undeniable signature, especially in development of nominative signature schemes. However, its application is not only limited to nominative signature as it is well employed to the structure of other signature schemes such as convertible undeniable signature schemes (Yuen *et al.* (2007)) and designated confirmer signature schemes (Wang and Xia, (2009)). The motivation of this paper is to point out and discuss the applications of Kurosawa and Heng's 3-move WI protocol, and illustrate its role in developing undeniable signature schemes with additional properties.

NOTATIONS AND DEFINITIONS

This section is to recall the definitions and notations that are going to be used throughout this paper. Since most of the schemes that made use of the applications of WI protocols on DH-tuple are pairing based, here we provide a quick review on bilinear pairing and its related hard assumptions.

We let $\mathbb{G}_1$ be an additive cyclic group of prime order q with P as its generator, and $\mathbb{G}_2$ be multiplicative 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:

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

Non-degeneracy: there exists 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.

A tuple (P, aP, bP, cP, z) is called a DH-tuple if $z = \hat{e}(P, P)^{abc}$ and is called a non DH-tuple if $\neq \hat{e}(P, P)^{abc}$.

The *Decisional Linear Problem* (DLP) is, given $u, u^a, v, v^b, h, h^c \in \mathbb{G}_1$ for unknown $a, b, c \in \mathbb{Z}_q^*$, to decide whether $c = a + b$.

NOMINATIVE SIGNATURES

The notion of nominative signature (NS) was first initiated by Kim *et al.* (1996). But not only their paper did not provide an opposite definition for nominative signature; it also lacked proposing a suitable application for the proposed scheme. Nominative signatures are similar to undeniable signatures in many ways (i.e. NS is considered as a dual scheme of undeniable signatures). The main common feature of undeniable signatures and nominative signatures is that the public verifiability of the signature is limited in both of the schemes (i.e. the validity of a message-signature pair can only be verified with the direct help of the signer and/or nominee.).

Basically, the concept of nominative signature is very similar to undeniable designated confirmer signature. Their key difference is, in nominative signature, when the *nominator* nominates a signature to the *nominee,* he/she transfers the proving ability of the signature to the nominee as well. In fact, the main point of NS is that the signer should not be able to verify the signature.

Employing the WI method introduced by Heng and Kurosawa (2005) in NS, Liu *et al.* (2007) proposed the first practical nominative signatures scheme. The work of Liu *et al.* nominated NS schemes as one of the best candidates for user certification systems. Specification details and a short literature review on NS can be found in Liu *et al.* (2007).

Nominative Signature Scheme Structure

A nominative signature consists of three polynomial time algorithms (Setup, KeyGen and Ver$^{\text{nominee}}$) and three protocols (SigGen, Confirmation and Disavowal).

Setup: Given the security parameter $k,$ it generates the system wide master secret and public parameters ($params$).

KeyGen: Providing system public parameters, it generates a public/private key pair for entities in the system.

Ver$^{\text{nominee}}$: Verify the validity of the given message-signature pair. Provided system's public parameters, a message m and a nominative signature σ, a public key (nominator's public key) and a private key (nominee's private key); it returns valid or invalid.

SigGen: Signature generation protocol in NS schemes can take place either interactively (Liu *et al.* (2007)), or non-interactively (Huang *et al.* (2008)) between the nominator and the nominee.

Without loss of generality, following are the steps taken to undergo an interactive SigGen protocol.

- The common inputs of the nominator A and nominee B are m and $params$.
- A inputs pk_B stating that A is nominating B as the nominee.
- B inputs pk_A stating that A is the nominator.

At the end of the protocol, either A or B outputs a nominative signature σ upon successful completion of the protocol or outputs $\perp$ upon failure.

Confirmation/Disavowal Protocol: Upon inputting the tuple $(m, \sigma, pk_A$, $pk_B)$ by the verifier C, B checks if the message-signature is valid. He will initiate the confirmation protocol with the verifier C if the pair is valid, otherwise he will initiate the disavowal protocol.

Applications of DH-Tuple WI Proof in Nominative Signatures

Multi-Round (Interactive) Nominative Signatures

In the interactive (multi-round) nominative signatures (Liu *et al.* (2007)), they used WI protocols on DH-tuple twice:

1. In SigGen protocol, to help the nominee B to prove the validity of his signature to nominator A for his further cooperation (issuing $\sigma^{standard} = Sig_A$ on B's valid undeniable signature). After B chooses a message $m \in \{1, 0\}^*$, he forms an undeniable signature $\sigma^{undeniable} = H(m \parallel pk_A)^{x_B}$ (given H is a collision free hash function and x_B is B's private key). B then has to prove to A that $\left(g, g^{x_B},\ H(m \parallel pk_A), \sigma^{undeniable}\right)$ is a DH-tuple, using WI method introduced by Kurosawa and Heng (2005). A issues the signature $\sigma^{standard} = Sig_A\ (\sigma^{undeniable})$ (nominates B) on B's undeniable signature, only after he is convinced with B's WI protocol on the validity of the DH-tuple. A nominative signature is formed as $(\sigma^{undeniable}, \sigma^{standard})$.

2. In the confirmation/disavowal protocol, to convince the verifier C of the validity/invalidity of the signature. After C verifies $\sigma^{standard}$ (i.e., nominator's signature on nominee's signature $\sigma^{undeniable}$ $(valid \leftarrow Verify_{A}\left(\sigma^{undeniable}\right))$), the only way to verify the validity of $\sigma^{undeniable}$ is to initiate the confirmation/disavowal protocol with the nominee. In confirmation/disavowal protocols using WI protocols of Kurosawa and Heng (2005), the nominee proves the validity/invalidity of a DH-tuple. B uses his secret knowledge on his private x_B to prove that $\left(g, g^{x_B},\ H(m \parallel pk_A), \sigma^{undeniable}\right)$ is a DH/non-DH tuple.

One-Move (Non-Interactive) Nominative Signatures

A nominative signature is called one-move (non-interactive) when the procedure of generating the signature takes place in a single move between the nominator and the nominee. The first one-move nominative signature was proposed in Huang *et al.* (2008).

SigGen protocol in a one-move nominative signature is initiated by the nominator by sending the signature $s = H(m \parallel y_A \parallel y_B)^{x_A}$ (where y_A and $y_B$are public keys of the nominee and the nominator respectively) to the nominee. After checking the validity of the signature s, nominee B generates the nominative signature as follows:

B computes $\sigma_1 = s^{x_B^2 r}, \sigma_2 = y_A^r,\ \sigma_3 = y_B^r$, and $\sigma_4 = g^r$ and forms the signature as $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$. In the confirmation/disavowal protocol B has to prove that $(e(\sigma_4, g), e(H(m \parallel y_A \parallel y_B), \sigma_2), e(\sigma_3, y_B), e(\sigma_1, g))$ is a DH-tuple/non DH-tuple using the WI technique of Kurosawa and Heng (2005).

Application of WI protocol in nominative is not limited only to the mentioned nominative signature schemes, Liu *et al.* (2007) and Zhao *et al.* (2009) also employed WI protocol in their nominative signature scheme.

Discussion

Witness indistinguishable protocols that were introduced by Kurosawa and Heng (2005) had revolutionary effects in the development of nominative signatures. Employing WI techniques enabled nominative signatures to become one of the best candidates in user certification systems along with universal designated-verifier signature and designated confirmer signature.

DESIGNATED CONFIRMER SCHEMES

As it mentioned before the validity/invalidity of an undeniable signature can only be verified with the help of the signer. Informally, both the verifier and the signer should be online at the same time to verify the validity/invalidity of an undeniable signature. The problem arises when the signer is unavailable. Chaum (1995) introduced the concept of designated confirmer scheme as an extension to undeniable signatures to solve the aforementioned issue. In designated confirmer scheme, both the signer of the signature and the nominated confirmer can verify the validity of the signature via the confirmation protocol.

Many designated confirmer schemes have been proposed in the literature (Camenisch and Michels (2000); Gentry, Molnar and Ramzan, (2005); Michels and Stadler (1998); Okamoto (1994)). However, none of them provide the signer of the signature with the ability to disavow the validity of a signature (i.e. run the disavowal protocol) and yet different (in structure) confirmation protocols had to be used for the signer and the designated confirmer to prove the validity of a signature. Wang and Xia (2009) proposed their designated confirmer signature (DCS) scheme which possesses a complete set of interesting features for DCS. In their proposed DCS scheme, the signer is able to initiate both the confirmation and disavowal protocol, using the same protocol the designated verifier uses (i.e., *unified verification*). Based on Wang and Xia's claim, their scheme is the first DCS scheme which provides the property of unified verification. The security of Wang and Xia's scheme is based on the security of co-GDH signature proposed by Boneh, Lynn and Shacham (2004).

Structure of Wang and Xia's Scheme

Key Generation: The same ElGamal like key generation algorithm is used to generate the key pairs for both the signer and the designated confirmer. Therefore $x \leftarrow_R \mathbb{Z}_q$ will be chosen randomly as private key and $y = g^x mod\, q$ will be computed as public key; $(x_S,\ y_S)$and $(x_C,\ y_C)$ represent private-public key pairs for the signer and the designated confirmer respectively.

Sign: Provided signer's private key x_S, and a message $m \in \{0,1\}^*$; the signer computes the basic signature $\sigma = H(m)^{x_S}\ mod\, p$.

Verify: Given a message-signature pair (m, σ), the signer checks if $(g, y_S, H(m), \sigma)$ is a DH-tuple. For this purpose the signer has to check if $e(g, \sigma) = e\big(y, H(m)\big)$ holds.

ConfirmedSign: The signer generates a DCS from the basic signature σ; an ElGamal encryption of a basic signature is used to form a DCS as follows:

He picks $r \leftarrow_R \mathbb{Z}_p$ and computes $l = g^r$, $\sigma_2 = y_c^r$, and $\omega = \sigma . l \; mod \; p$ and he forms DCS as $\sigma_{DCS} = (\omega, \sigma_2)$.

Extraction: Provided a DCS (ω, σ_2), the designated confirmer checks if $e(\omega, g) = e(H(m), y_S). e(\sigma_2, g)^{x_C{}^{-1}}$ holds then he extracts the basic signature using his private key $\sigma = \omega / \sigma_2{}^{x_C{}^{-1}}$, otherwise he outputs $\perp$.

Confirmation: Provided a message-signature pair (m, σ_{DCS}), the validity of DCS on message m can be confirmed by the designated confirmer using his knowledge of x_C such that if $e(\omega, g) = e(H(m), y_S). e(\sigma_2, g)^{x_C{}^{-1}}$ is held or not. In addition, the signer can respectively use his knowledge of his private key x_S to check if $e(\omega, y_c) = e(\sigma_2, g). e(H(m), y_c)^{x_s}$ holds or not; if both of the equations are held then either the signer or the designated verifier will engage in the confirmation protocol with the verifier. The confirmation protocol employs the WI technique of Kurosawa and Heng (2005). Using this technique, the designated confirmer or the signer can perform the confirmation protocol without revealing their role in the scheme (i.e. the verifier is not able to decide whether he is interacting with the designated confirmer or the signer). In general the proof of knowledge system of the confirmation protocol is as follows:

$$PK\,\{(x_S \vee x_C): [e(\omega, y_c) = e(\sigma_2, g). e(H(m), y_c)^{x_s} \wedge y_S = g^{x_S}]$$
$$\vee\, [e(\omega, g) = e(H(m), y_S). e(\sigma_2, g)^{x_C{}^{-1}} \wedge y_C = g^{x_C}]\}$$

The complete details of this WI protocol could be viewed in (Wang and Xia (2009).

Disavowal: Provided a message-signature pair (m, σ_{DCS}), the signer and the designated confirmer are able to prove the invalidity of the message-signature pair. The signature σ_{DCS} is invalid if the inequalities, $e(\omega, g) \neq e(H(m), y_S). e(\sigma_2, g)^{x_C{}^{-1}}$ and $e(\omega, y_c) \neq e(\sigma_2, g). e(H(m), y_c)^{x_s}$ are held for the designated confirmer and the signer respectively; either the designated confirmer or the signer can undertake the disavowal protocol and run the following proof of knowledge system with the verifier.

$$PK\,\{(x_S \vee x_C): [e(\omega, y_c) \neq e(\sigma_2, g).e(H(m), y_c)^{x_s} \wedge y_S = g^{x_S}]\} \\ \vee \left[e(\omega, g) \neq e(H(m), y_S).e(\sigma_2, g)^{x_C{}^{-1}} \wedge y_C = g^{x_C}\right]\}$$

Anonymity of the confirmer in disavowal is held using the same technique that is used in developing the confirmation protocol of the scheme.

Discussion

To the best of our knowledge, Wang and Xia's scheme is the first DCS scheme which incorporated WI technique of Kurosawa and Heng (2005) in DCS schemes. As observed, both vital and interesting features are obtained using WI protocols on validity/invalidity of DH-tuple. Both the designated confirmer and the signer use the same confirmation/disavowal protocol (i.e. unified verification) in an anonymous way (i.e. verifier cannot decide if he is interacting with the signer or the designated confirmer, this is because of the WI property that the verifier cannot distinguish which witness does the prover use to run the proof system).

CONVERTIBLE UNDENIABLE SIGNATURES WITHOUT RANDOM ORACLES

The first convertible undeniable signature was proposed by Boyar *et al.* (1991). Convertibility is an extension of undeniable signatures which enables the signer to convert her undeniable signatures into ordinary signatures. Convertibility of undeniable signatures takes in account in two forms, selective convert and universal convert. More precisely, the signer can convert one of her signatures into publicly verifiable signature using selective convert and convert all of her signatures using universal convert.

Yuen *et al.* (2007) proposed the first convertible undeniable signature scheme and provided the security proofs in the standard model. Using bilinear pairing, the security of their scheme is based on CDH and Decision Linear assumptions. Their scheme is built based on Waters' signature scheme (Waters (2005)) and they incorporated the concept of WI protocol of Kurosawa and Heng (2005) in order to develop a 3-move convertible undeniable signature scheme.

Phong *et al.* (2010) showed that Yuen *et al.*'s scheme does not satisfy the security model of invisibility presented by the authors. However, Yuen et al. revised their paper later in 2010, and fixed the mentioned fault in their invisibility proof. Here, we show the original scheme of Yuen *et al.* proposed in 2007. However, the method of applying the WI protocol in both the revised and the original scheme is identical.

Structure of Yuen *et al.*'s Scheme

Setup: After choosing an admissible mapping function $\hat{e}\colon \mathbb{G}_1 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_2$, generators $g, g_2, u' \in \mathbb{G}_1$ will be selected at random, and finally an n-length vector $U = (u_i)$, which elements are chosen randomly from $\mathbb{G}_1$ is selected. An integer d is selected as the system parameter and $l = 2^d$ and $k = n/d$. $H\colon \{0,1\}^n \longrightarrow \mathbb{Z}_l^*$ is a collision resistant hash function.

Key Generation: α, β', β_i are selected randomly from $\mathbb{Z}_p^*$ for $1 < i < l$. Public key will be formed as $\left(g_1,\ v', v_1, \ldots, v_l\right)$ where $g_1 = g^{\alpha}$, $v' = g^{\beta'}$ and $v_i = g^{\beta_i}$. The secret keys are $(\alpha, \beta', \beta_1, \ldots, \beta_l)$.

Sign: To sign a message m $(m_1, \ldots, m_n) \in \{0,1\}^n$, denoted by $\bar{m} = H_j(m)$ where $1 < j < k$, the signer chooses $r \leftarrow_R \mathbb{Z}_p^*$ and generates the signature as follow:

$$S_1 = g_2^{\alpha}\left(u' \textstyle\prod_{i=1}^{n} u_i^{m_i}\right)^r \text{And } S_{2,j} = \left(v' \textstyle\prod_{i=1}^{l} v_i^{\bar{m}_j^i}\right)^r$$

The convertible undeniable signature will be in the form of $(S_1, S_{2,1}, \ldots, S_{2,k})$.

Confirmation/Disavowal: On inputting the signature $(S_1, S_{2,1}, \ldots, S_{2,k})$, the signer initiates the 3-move WI protocol by computing:

$$L = \hat{e}(g, g_2)$$
$$M = \hat{e}(g_1, g_2)$$
$$N_j = \hat{e}\left(v' \textstyle\prod_{i=1}^{l} v_i^{\bar{m}_j^i}, g_2\right)$$
$$O_j = \hat{e}\left(v' \textstyle\prod_{i=1}^{l} v_i^{\bar{m}_j^i}, S_1\right) / \hat{e}\left(S_{2,j}, u' \textstyle\prod_{i=1}^{n} u_i^{m_i}\right)$$

Using the 3-move WI protocol of Kurosawa and Heng (2005), the signer proves the equality/inequality of discrete logarithm of $\log_L M$ and $\log_{N_j} O_j$.

Selective Convert: On inputting the signature $(S_1, S_{2,1}, \dots, S_{2,k})$, the signer computes $\bar{m} = H_j(m)$ and generates the selective receipt S_2' as follows:

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

Selective Verification: On inputting the message-signature pair $((S_1, S_{2,1}, \dots, S_{2,k}),\ m)$ and the selective receipt S_2' ,verifier computes $\bar{m} = H_j(m)$ and checks if:

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

If the condition is satisfied he checks if:

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

If all the equalities hold, he will be convinced about the validity of the signature; otherwise, he will output 0.

Universal Convert: The signer publishes $(\beta', \beta_1, \dots, \beta_l)$ as her universal receipt.

Universal Verification: On inputting the message-signature pair $((S_1, S_{2,1}, \dots, S_{2,k}),$ m) and the universal receipt $(\beta', \beta_1, \dots, \beta_l)$, the verifier checks if:

$$v' = g^{\beta'} \text{ And } v_i = g^{\beta_i}$$

If the above equalities hold, the verifier computes $\bar{m} = H_j(m)$ and checks whether the below equalities hold:

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

The verifier will be convinced about the validity of the signature if and only if the above quality is held, otherwise he will output 0.

Discussion

To the best of our knowledge, all the convertible undeniable signatures without random oracles proposed to this day are based on RSA. Yuen et al.'s scheme is the first proven to be unforgeable based on the CDH assumption and to be invisible and anonymous under the Decision Linear assumption.

They claimed that their scheme is the first provable secure undeniable signature scheme without random oracles which uses well-known assumptions.

CONCLUSION

We observed that how employing 3-move WI protocol of Kurosawa and Heng gave rise to deployment of some schemes (i.e. nominative signatures), and how it has been employed to provide some other schemes with additional interesting features. A very distinctive application of WI protocols is in schemes which the signer and the confirmer could be two distinct entities; where there are two or more possible witnesses incorporated in the structure of the signature, and each witness (in this situation secret key) belongs to one entity (similar method is used in designated confirmer signature of Wang and Xia (2009)).

However, Ogata *et al.* (2006) stated that the non-impersonation property of 3-move WI protocol of Kurosawa and Heng does not hold under active attacks. In their attack, a cheating verifier is able to transfer the validity of a message-signature pair to a third party. Therefore, pre-caution or minor amendments should be taken in account when employing the 3-move WI protocols.

ACKNOWLEDGEMENT

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

REFERENCES

Boneh, D., Lynn, B. and Shacham, H. (2004). Short Signatures from the Weil Pairing. *Journal of Cryptology.* **17**(4): 297-319.

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

Camenisch, J. and Michels, M. (2000). Confirmer Signature Schemes Secure against Adaptive Adversaries. In B. Preneel (Ed.). *Advances in Cryptology — EUROCRYPT 2000,* Springer Berlin / Heidelberg. **1807**: 243-258.

Chaum, D. (1991). Zero-Knowledge Undeniable Signatures In I. Damgård (Ed.). *Advances in Cryptology — EUROCRYPT '90,* Springer Berlin / Heidelberg. **473**: 458-464.

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. **435**: 212-216.

Feige, U. and Shamir, A. (1990). Zero Knowledge Proofs of Knowledge in Two Rounds. In G. Brassard (Ed.). *Advances in Cryptology — CRYPTO' 89,* Springer Berlin / Heidelberg. **435**: 526-544.

Gentry, C., Molnar, D. and Ramzan, Z. (2005). Efficient Designated Confirmer Signatures Without Random Oracles or General Zero-Knowledge Proofs. In B. Roy (Ed.). *Advances in Cryptology - ASIACRYPT 2005*, Springer Berlin / Heidelberg. **435**: 526-544.

Goldwasser, S., Micali, S. and Rackoff, C. (1985). The knowledge complexity of interactive proof-systems. *The seventeenth annual ACM symposium on Theory of computing*. 291-304.

Huang, Q., Liu, D. Y. W. and Wong, D. S. (2008). An efficient one-move Nominative Signature scheme. *Int. J. Appl. Cryptol.* **1**(2): 133-143.

Kim, S.J., Park, S.J. and Won, D.H. (1996). Zero-knowledge nominative signatures. *PragoCrypt, International Conference on the Theory and Applications of Cryptology*. 380–392.

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**: 181-197.

Liu, D. Y. W., Chang, S., Wong, D. S. and Mu, Y. (2007). Nominative signature from ring signature. *2nd international conference on Advances in information and computer security*. 396-41.

Liu, D. Y. W., Wong, D. S., Huang, X. Y., Wang, G. L., Huang, Q. and Mu, Y. (2007). Formal definition and construction of nominative signature. In S. Qing, H. Imai and G. Wang (Eds.). *Information and Communications Security*. **4681**: 57-68

Michels, M. and Stadler, M. (1998). Generic Constructions for Secure and Efficient Confirmer Signature Schemes (Extended Abstract). In K. Nyberg (Ed.). *Advances in Cryptology — EUROCRYPT'98*, Springer Berlin / Heidelberg. **3494**: 181-197.

Okamoto, T. (1994). Designated Confirmer Signatures and Public-Key Encryption are Equivalent. In Y. Desmedt (Ed.). *Advances in Cryptology — CRYPTO '94*, Springer Berlin / Heidelberg. **3494**: 181-197.

Phong, L., Kurosawa, K. and Ogata, W. (2010). Provably Secure Convertible Undeniable Signatures with Unambiguity. In J. Garay & R. De Prisco (Eds.). *Security and Cryptography for Networks*, Springer Berlin / Heidelberg. **3494**: 181-197.

Waters, B. (2005). Efficient Identity-Based Encryption Without Random Oracles. In R. Cramer (Ed.). *Advances in Cryptology – EUROCRYPT 2005,* Springer Berlin / Heidelberg. **3494**: 114-127.

Yuen, T., Au, M., Liu, J. and Susilo, W. (2007). (Convertible) Undeniable Signatures Without Random Oracles. In S. Qing, H. Imai and G. Wang (Eds.). *Information and Communications Security* Springer Berlin / Heidelberg. **4861**: 83-97.

Zhao, W., Lin, C. and Ye, D. (2009). Provably Secure Convertible Nominative Signature Scheme. In M. Yung, P. Liu and D. Lin (Eds.). *Information Security and Cryptology*, Springer Berlin / Heidelberg. **4861**: 83-97.