Short Convertible Undeniable Signature From Pairing

Fei Li
Department of Mathematics and Informatics, Ludong University, Yantai, China
Email: miss_lifei@163.com
Wei Gao
Department of Mathematics and Informatics, Ludong University, Yantai, China
Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China
Email:sdgaowei@gmail.com
Yilei Wang
School of Information and Electrical Engineering, Ludong University, Yantai, China
Email: wangyilei2000@163.com
Xueli Wang
School of Mathematics, South China Normal University, Guangzhou, China
Email: wangxuyuyan@gmail.com

***Abstract*—Undeniable signatures, introduced by Chaum and van Antwerpen, require a verifier to interact with the signer to verify a signature, and hence allow the signer to control the verifiability of his signatures. Convertible undeniable signatures allow the signer to convert undeniable signatures into ordinary signatures. In this paper we propose some extended variants of the famous Diffie-Hellman assumption on bilinear group system, then design a new convertible undeniable signature scheme and provide proofs for all relevant security properties based on the new assumption in the random oracle model. The advantages of our scheme are the short length of the signatures, the low computational cost of the signature, the receipt generation and the provable security.**

***Index Terms*—convertible undeniable signature, provable security, bilinear pairing**

I. Introduction

The two most important properties of ordinary digital signatures are nonrepudiation and universal verifiability. Non-repudiation guarantees that a signer cannot deny his or her commitment to a message or a contract at a later time, and the property of universal verifiability allows everybody to check the correctness of a signature. For privacy reasons, it is preferable, in many applications, that the verification of signatures be controlled or (at least) limited by the signer. Therefore, the concept of undeniable signatures was introduced by Chaum and van Antwerpen [1]. In this setting, the verification (and the denial) of a signature requires the cooperation of the signer. And non-repudiation is still guaranteed, since the signer cannot convince the verifier that a correct signature is invalid or that an incorrect signature is valid.

The security of the protocol in [1] relies on the discrete logarithm problem, but suffers from the fact that the interactive protocols were not zero-knowledge. One year later, Chaum improved significantly the initial proposal by providing a zero-knowledge version in [2]. In 1991, the concept has been refined by giving the possibility to transform an undeniable signature into a self-authenticating signature. These convertible undeniable signatures, proposed in [3] by Boyar, Chaum, Damgard and Pedersen, provide individual and universal conversions of the signatures. Unfortunately, this ElGamal like scheme has been broken in 1996 by Michels, Petersen, and Horster [5] who proposed a repaired version with heuristic security. Since then, many schemes have then been proposed, based upon classical signatures, such as Schnorr [6], ElGamal [7] and RSA [8]–[10]. In 2004, Monnerat and Vaudenay [11] proposed short undeniable signatures based on the computation of characters which do not provide the conversion property. In 2005, Laguillaumie and Vergnaud [12] presented a new efficient convertible undeniable signature scheme based on bilinear maps. Its unforgeability is tightly related, in the random oracle model, to the computational Diffie-Hellman problem and its anonymity to a non-standard decisional assumption. Convertible undeniable signatures have given rise to many applications in cryptography [3], [13], [14]. In 2006, Kurosawa and Takagi [15] proposed a new approach for selectively convertible undeniable signature Schemes, and presented two efficient schemes based on RSA. In 2007, Yue et al. [16] constructed a new convertible signature without random oracles based Waters signature scheme. In 2008, Aimani et al. [17] gave two specific approaches for building universally convertible undeniable signatures from a large class of pairing-based signatures. In 2009, Huang and Wong [18] proposed a new efficient construction of fully functional convertible undeniable signature, which supports both selective conversion and universal conversion, and is immune to the claimability attacks. In 2010, Phong et al. [19] proposed two convertible undeniable

This work is partially supported by National Natural Science Foundation of China (No.61202475) and Humanities and Social Science Research Project of the Ministry of Education (11YJCZH039). Corresponding Author, Fei Li.

doi:10.4304/jsw.8.12.2983-2990

signature schemes satisfying anonymity in the standard model. In 2010, Kikuchi et al. [20] proposed a framework for constructing convertible undeniable signatures from weakly-secure standard signatures, and presented a concrete instantiation employing a standard signature scheme proposed at Eurocrypt'09. In 2011, Schuldt and Matsuura [21] presented an updated definition and security model for schemes allowing delegation, and highlight a new essential security property, token soundness and proposed a new convertible undeniable signature scheme satisfying this security. In 2012, Zhao and Ye [22] proposed a certificateless undeniable signature scheme based on bilinear maps.

From the above survey, it is obvious that the designing of provably secure convertible undeniable signature scheme with high efficiency and short length has been a cryptographic task full of challenge. Motivated by this challenge, we propose a new convertible undeniable signature scheme which can be seen as the natural extension of the BLS short signature scheme [23] and the undeniable signature in [1]. Like the convertible undeniable signature scheme in [12], our scheme also use nonstandard computational number theory assumption relative to the so-called xyz-Diffie-Hellman problem. However, our generalization and extension of the Diffie-Hellman assumption on bilinear groups seems more natural and the resulting convertible undeniable scheme is more compatible to the atomic digital signature (BLS short signature) and more efficient in computation and size. Additionally, our proving technique is also different from that of [12]. In all, our scheme has the following advantages over its counterparts : short length, computational efficiency, both universally and individually convertibility, and provable security in the random oracle model [24].

The rest is organized as follows. In Section 2, we review some mathematical background including bilinear maps, the number-theoretic problems underlying our scheme and designated-verifier noninteractive zero-knowledge proof system. Specially, we gradually extend the famous Diffie-Hellman assumption to a new but less standard one — one-more tripartite-Diffie-Hellman problem — for the provable security. We recall the formalization of convertible undeniable signature scheme and its security model in Section 3. In Section 4, we describe our new convertible undeniable signature scheme. And then we prove its security in the random oracle model in Section 5. At last, we give the conclusion.

II. Preliminary

A. Bilinear Map

Recently, bilinear pairings have found various applications in cryptography and have allowed us to construct many new cryptographic schemes [25]–[28]. Our convertible undeniable signature scheme are also based on such generally applied cryptographic primitive — bilinear map. We now recall some definition relative to the bilinear group systems.

Definition 1. *(Bilinear group system). A bilinear group system is a tuple $(q, P_1, P_2, g_T, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \psi)$ where q is a prime number, $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are groups of order q with efficiently computable inner laws, $\mathbb{G}_1 = \langle P_1\rangle$, $\mathbb{G}_2 = \langle P_2\rangle$, $\mathbb{G}_T = \langle g_T\rangle$, the bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is an efficiently computable map such that for all $x, y \in \mathbb{Z}_q^*$, $e(xP_1, yP_2) = e(P_1, P_2)^{xy}$ holds and $e(P_1, P_2) \neq 1$ and $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ is an efficiently computable isomorphism with $\psi(P_2) = P_1$.*

Definition 2. *(Bilinear group system generator). A bilinear group system generator is a probabilistic algorithm BGSG that takes as input a security parameter 1^k and outputs a bilinear group system $(q, P_1, P_2, g_T, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \psi) \xleftarrow{R} BGSG(1^k)$ such that q is a k-bit prime number.*

B. Computational Problems in Bilinear Group Systems

We now give the description of some complexity assumptions.

Computational Co-Diffie-Hellman (Co-CDH) Given a tuple of $(xP_2, V) \in \mathbb{G}_2 \times \mathbb{G}_1$, compute $xV \in \mathbb{G}_1$.

Computational Co-Tripartite-Diffie-Hellman (CCTD-H) Given group elements $(xP_2,\ yP_2, V) \in \mathbb{G}_2^2 \times \mathbb{G}_1$, compute $xyV \in \mathbb{G}_1$.

Decisional Co-Tripartite-Diffie-Hellman (DCTDH) Given a tuple of group elements $(xP_2, yP_2, V, V') \in \mathbb{G}_2^2 \times \mathbb{G}_1^2$, decide whether $V' = xyV$.

The designing of our new undeniable signature is mainly based upon the observation on the above pair of problems (CCTDH and DCTDH) which just correspond to the authenticity and the privacy of our scheme. However, for provable security of our scheme, we need more formal and stronger assumption than the above "naked" ones. In [12], the so-called xyz-Diffie-Hellman (computational and decisional) problems similar to the above problems are proposed. They discussed the corresponding assumptions and proposed a new protocol of undeniable signature according to the similar idea to us. However, in this paper, we propose a seemingly more common extension of DCTDH and hence get more efficient, more compact and shorter undeniable signature.

For provable security of some cryptographic primitives and more efficiency, we often turn to some stronger assumption. The "one-more" variants of some standard assumption have been applied to prove the security of many cryptographic primitives which have only heuristic security before. For example, these one-more variants, including one-more RSA, one-more discrete logarithm, one-more Diffie-Hellman, have been used to prove the security of a series of transitive signature schemes [29] and identification schemes [30]. So we can see that one-more variants of some standard assumption are becoming very natural extension and forceful cryptographic tools in the field of provable security. Similarly, to attain the provable security (here the invisibility) instead of heuristic security and more efficiency, we naturally extend the above DCTDH assumption to the one-more variant formally defined as follows.

Definition 3 (**One-more Decisional Co-Tripartite-Diffie-Hellman (1m-DCTDH)).** *Let the bilinear group system* $(q, P_1, P_2, g_T, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \psi) \xleftarrow{R} BGSG(1^k)$ *be public parameters. Let* x, y *be two random element of* $\mathbb{Z}_q^*$ *and let* $X = xP_2, Y = yP_2$*. In addition to* X, Y*, the adversary A has access to two oracles:*

- **Target oracle** $\mathcal{TG}$ *$\mathcal{TG}$ first gets a random bit b by tossing a coin. If* $b = 0$*,* $\mathcal{TG}$ *selects and returns two random and independent points* $(V, V') \in_R \mathbb{G}_1^2$ *; otherwise, it first selects a random point* $V \in \mathbb{G}_1$ *and then return* (V, V') *with* $V' = xyV$*.*
- **Helper oracle** $\mathcal{HO}$ *On a query of* $V \in \mathbb{G}_1$*,* $\mathcal{HO}$ *return* $(xyV, yV) \in \mathbb{G}_1^2$*.*

Let q_T*, (resp.* q_H*) be the number of queries A made to the target (resp. helper) oracles. The advantage of the adversary attacking 1m-DCTDH is defined as*

$$Adv_{BGSG,A}^{1m-DCTDH} = |Adv_0 - 1/2|$$

where Adv_0 *is defined as the probability of A to output a set W of, say, l tuples* $((V_1, V_1', b_1), \cdots, (V_l, V_l', b_l))$ *such that for all* $1 \le i \le l$*,* (V_i, V_i') *is the output of the target oracle* $\mathcal{TG}$*,* $b_i = 1$ *if* $V_i' = xyV_i$ *and* $b_i = 0$ *otherwise, all* V_i *are distinct and* $(l-1) = q_H < q_T$*.*

The 1m-DCTDH assumption states that there is no polynomial-time adversary A with non-negligible $Adv_{BGSG,A}^{1m-DCTDH}$*.*

Informally, the above assumption states that it is computationally infeasible for an adversary without the secret keys to present all right answers to even 1 more random challenges (whether a target output (V, V') satisfies $V' = xyV$) than the times of the accesses to the helper oracle.

C. Proof of equality or inequality of two discrete logarithms

Let $(\mathbb{G}, +)$ and $(\mathbb{H}, \cdot)$ be two groups of the same prime order q and let P and g be generators of $\mathbb{G}$ and $\mathbb{H}$ (respectively). What we need in this paper are the non-interactive proof of equality (resp. inequality) of the discrete logarithm of $Y \in \mathbb{G}$ in base P and the one of $y \in \mathbb{H}$ in base g denoted by $NIPK(a : y = g^a \bigwedge Y = aP)$ (resp. $NIPK(a : y \neq g^a \bigwedge Y = aP)$). In [33], two efficient non-interactive zero-knowledge (in the random oracle model) proof systems of equality and inequality of two discrete logarithms are presented where $\mathbb{G} = \mathbb{H}$. However, it is trivial to extend both protocols to the more general case of $\mathbb{G} \neq \mathbb{H}$.

In general, a 3-move honest-verifier zero-knowledge (HVZK) protocol can be transformed to a more efficient noninteractive protocol by using the Fiat-Shamir transformation [4]. Such noninteractive protocols for proof of equality or inequality of two discrete logarithms are as follows [33] (H' is abused to denote some random oracle corresponding to the context and note that if the oracle H' can be controlled, the valid transcript can be simulated for any pair (y, Y)):

$$\underline{NIPK(a : y = g^a \bigwedge Y = aP)}$$

P : $r \xleftarrow{R} \mathbb{Z}_q$,
$z = g^r$,
$Z = rP$,
$c = H'(z, Z)$,
$d = r + ca \mod q$

V : Given z, Z, d, checks whether
$g^d = zy^c$,
$dP = Z + cY$.

$$\underline{NIPK(a : y \neq g^a \bigwedge Y = aP)} \text{ [31]}$$

P : $s,\ r,\ r' \xleftarrow{R} \mathbb{Z}_q$,
$w = (g^a/y)^s$,
$Z = rP - r'Y$,
$z = g^r/(y^{r'})$
$c = H'(w, z, Z)$,
$d = r + cas \mod q$,
$d' = r' + cs \mod q$

V : Given w, z, Z, d, d', checks whether
$w \neq 1$,
$g^d/(y^{d'}) = zw^c$,
$dP - d'Y = Z$.

To overcome universal verifiability of the above protocols, designated-verifier technique was introduced in [32] by Jakobsson et al. In a designated-verifier confirmation proof, the signer proves that "$NIPK(a : y = g^a \bigwedge Y = aP)$" or "he knows the verifier's secret key". In other words, the verifier is able to produce such a valid proof himself using his secret key. By using the designated-verifier technique, one can thereby prevent illegal copies of the proof. Using the technique shown in [34], a designated-verifier proof can be constructed for a public-secret key pair of any well-known public key system. The obtained NIPK proof is zero-knowledge in the random oracle model. And we denote such designated-verifier variants of the above two protocols as $DVPK(a : y = g^a \bigwedge Y = aP)$ and $DVPK(a : y \neq g^a \bigwedge Y = aP)$ respectively.

We do not give the concrete NIZK designated-verifier confirmation and disavowal protocols since different protocols are associated with different public key systems used by the verifier.

III. Formal definition and security model

In this section, we follow [12] to present the formal definition and security model for convertible undeniable signature schemes.

A. Definition

Definition 4 (**Convertible Undeniable Signature** [12]). *Given an integer k, a convertible undeniable signature scheme CUS with security parameter k is defined by the following:*

1) **common parameter generation algorithm** $CUS.Setup$*: it is a probabilistic algorithm which takes as input* 1^k *and outputs the public parameters;*
2) **key generation algorithm** $CUS.KeyGen$*: it is a probabilistic algorithm which takes as inputs*

the public parameters and outputs a pair of keys (pk, sk)*;*

3) **signing algorithm** $CUS.Sign$*: it is a probabilistic algorithm which takes as inputs a message* m*, a secret key* sk*, and the public parameters. The output* σ *is a convertible undeniable signature on* m *;*
4) **confirming/denying protocols** $CUS.\{Confirm$**,** $Deny\}$*: they are protocols which take as inputs a message* m*, a bit string* σ*, a pair of keys* (pk, sk) *and the public parameters. The output is a (possibly non-interactive) non-transferable proof that* σ *is actually a valid/invalid convertible undeniable signature on* m *with respect to the key* pk*. Note that we will use designated verifier NIZK proof system in our scheme;*
5) **individual receipt generation algorithm** $CUS.IReceipt$*: it is an algorithm which takes as inputs, a message* m*, a bit string* σ*, a secret key* sk *and the public parameters. It outputs an individual receipt* $\widetilde{\sigma}$ *which makes it possible to universally verify whether* σ *is valid or not;*
6) **verifying algorithm for individually converted signature** $CUS.IVerify$*: it is a deterministic algorithm which takes as inputs, a message* m*, a bit string* σ*, a bit string* $\widetilde{\sigma}$*, the signer's public key* pk*, and the public parameters. It tests whether* $\widetilde{\sigma}$ *is a valid individual receipt with respect to* σ *and the public key* pk*. If it does, the algorithm states whether* σ *is a valid convertible undeniable signature on* m *with respect to the key* pk *or not, else it outputs Error;*
7) **universal receipt generation algorithm** $CUS.UReceipt$*: it is a deterministic algorithm which takes as inputs, a secret key* sk*, and the public parameters and outputs a universal receipt* I *which makes it possible to universally verify all convertible undeniable signature* σ *with respect to* pk*;*
8) **verifying algorithm for universally converted signature** $CUS.UVerify$*: it is a deterministic algorithm which takes as inputs, a message* m*, a bit string* σ*, a public key* pk*, a bit string* I *and the public parameters. It tests whether* I *is a valid universal receipt with respect to the key* pk*. If it does, it states whether* σ *is a valid convertible undeniable signature on* m *with respect to the key* pk *or not, else it outputs Error;*

and must satisfy the following properties :

1) *completeness and soundness: the confirming and denying protocols and the verifying algorithms are complete and sound, where completeness means that valid (invalid) signatures can always be proved valid (invalid), and soundness means that no valid (invalid) signature can be proved invalid (valid);*
2) *unforgeability: given a public key* pk*, it is computationally infeasible, without the knowledge of the corresponding secret key to produce a convertible undeniable signature which is accepted by the verification algorithms or by the confirming protocols;*
3) *Invisibility: It is computationally infeasible to determine whether a given message-signature pair is valid for a given user without the help of the signer.*
4) *non-transferability: a verifier participating in an execution of the confirming/denying protocols does not obtain information that could be used to convince a third party about the validity/invalidity of a signature.*

B. Security model

In the following definition, we assume that the adversary (A or D) is allowed to query a receipt generating oracle Υ and a confirming/denying oracle Ξ on any couple message/ signature of his choice, in addition to the classical access to the signing oracle Σ and to the random oracle H. For more description, we refer reader to [12]. For one standard signature scheme, the adaptive chosen-message attack is the most powerful attack possible for an enemy who is restricted to using the signature scheme in a natural manner. The following definition 5 for CUS signatures is one variant of the chosen message attack for the standard signatures.

Definition 5 (Unforgability [12])**.** *Let CUS be a convertible undeniable signature scheme and let A be an EF-CMA-adversary against CUS. We consider the following random experiment, where* k *is a security parameter:*

$$\begin{aligned}
&params \xleftarrow{R} \text{CUS.Setup(k)},\\
&(pk, sk) \xleftarrow{R} \text{CUS.KeyGen(params)}\\
&(m^*, \sigma^*) \leftarrow A^{H,\Sigma,\Upsilon,\Xi}(params, pk),\\
&\text{Return } b \leftarrow CUS.UVerify(params, pk, m^*, \sigma^*, I)
\end{aligned}$$

We define the success of the adversary A, via $Suc^{cef-cma}_{CUS,A}(k) = Pr[b = \text{“}valid\text{”}]$*. (Note that it is trivial to require that* Σ *is not queried on* m^**).*

Given $k \in \mathbb{N}$ *and* $\epsilon \in [0, 1]$*, the scheme CUS is said to be* ϵ*-EF-CMA secure, if no EF-CMA-adversary A has a success probability* $Suc^{cef-cma}_{CUS,A}(k) \geq \epsilon(k)$*.*

Definition 6 (Invisibility [12])**.** *Let CUS be a convertible undeniable signature scheme and let D be an Inv-CMA-adversary against CUS. We consider the following random experiment, where* k *is a security parameter:*

$$\begin{aligned}
&params \xleftarrow{R} \text{CUS.Setup(k)},\\
&(pk, sk) \xleftarrow{R} \text{CUS.KeyGen(params)}\\
&m^* \xleftarrow{R} D^{H,\Sigma,\Upsilon,\Xi}(params, pk),\\
&b \xleftarrow{R} \{0, 1\}\\
&\text{If } b = 1,\ \sigma^* \leftarrow CUS.Sign(sk, m^*),\\
&\text{else } \sigma^* \xleftarrow{R} S \text{ where } S \text{ is the signature space}\\
&\text{return } b' \leftarrow D^{H,\Sigma,\Upsilon,\Xi}(params, pk, m^*, \sigma^*)\\
&\text{where no query of } m^* \text{ to } \Sigma \text{ or } (m^*, \sigma^*) \text{ to } \Upsilon \text{ or } \Xi\\
&\text{is allowed.}
\end{aligned}$$

The distinguisher D wins the game if $b' = b$*. D's advantage in this game is defined to be* $Adv^{Inv-cma}_{CUS,D}(k) = |Pr[b' = b] - \frac{1}{2}|$

Given $k \in \mathbb{N}$ and $\epsilon \in [0,1]$, the scheme CUS is said to be ϵ-Inv-CMA secure, if no Inv-CMA-adversary D has a success $Adv_{CUS,D}^{Inv-cma}(k) \geq \epsilon(k)$

IV. New convertible undeniable signature scheme

In this section, we present a new convertible undeniable signature scheme based on bilinear paring. This scheme consists of the following polynomial time algorithms.

- Setup: Let k be a security parameter, $BGSG$ be a bilinear group system generator and $param = (q, P_1, P_2, g_T, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \psi)$ be some output of $BGSG(k)$. Let $H : \{0,1\}^* \to \mathbb{G}_1$ be a cryptographic hash function. And let H' be another cryptographic hash function which will be used in Fiat-Shamir transformation for constructing designated-verifier noninteractive zero knowledge protocols of Confirming/denying in the later.
- KeyGen: Alice picks randomly two integers $x, y \in \mathbb{Z}_q^*$ and computes the points $X = xP_2$ and $Y = yP_2$. Alice's public key is the pair (X, Y) and her secret key is (x, y).
- Sign: Given a message $m \in \{0,1\}^*$, Alice computes the undeniable signature $\sigma = xyH(m)$.
- Confirm / Deny: Given a message m and a signature σ, Alice can confirm or deny σ with the following designated-verifier noninteractive zero-knowledge proof of knowledge:
$$DVPK(y : e(\sigma, P_2) = e(H(m), X)^y \bigwedge Y = yP_2)$$
or
$$DVPK(y : e(\sigma, P) \neq e(H(m), X)^y \bigwedge Y = yP_2)$$
- IReceipt: Given a message $m \in \{0,1\}^*$ and a putative signature σ on m, Alice computes the point $\sigma_2 = yH(m) \in \mathbb{G}_1$. The individual receipt with respect to σ is σ_2.
- IVerify: Given a message $m \in \{0,1\}^*$, a putative signature σ on m and a putative individual receipt σ_2 on σ, the validity of the receipt is decided by checking whether $e(\sigma_2, P_2) = e(H(m), Y)$ or not. If σ_2 is valid, then the validity of σ is decided by checking whether $e(\sigma, P_2) = e(\sigma_2, X)$ or not.
- UReceipt: Alice publishes the point $I = xyP_2$.
- UVerify: The validity of the universal receipt I is decided by verifying that $e(\psi(X), Y) = e(\psi(I), P_2)$. If it is valid, given a signature σ on a message $m \in \{0,1\}^*$ and I, everyone checks the validity of this signature by verifying that $e(\sigma, P_2) = e(H(m), I)$.

Efficiency considerations. Compared with other convertible undeniable signature schemes, our scheme has a number of advantages. As a natural extension of the shortest signature scheme BLS signature [23], our signature scheme inherited the shortest length and only consists in an element of $\mathbb{G}_1$. Therefore, the size of the signature is only 160 bits. Furthermore, a receipt (individual and universal) is also an element of $\mathbb{G}_2$ or $\mathbb{G}_1$. From an efficiency point of view, the signature generation and the individual and universal receipts generation algorithms require only one exponentiation as the most expensive operation. Unfortunately, it turns out that the signature verification is slightly more time consuming, as it requires some pairing evaluations.

V. Security Proof

Since the protocols of confirmation and denying are designated-verifier noninteractive zero-knowledge, it is obvious that our convertible undeniable signature satisfies the completeness, soundness and non-transferability. Now, it remains to prove the security of unforgeability and invisibility.

On one hand our convertible undeniable signature scheme is more efficient, shorter than the state-of-the-art convertible undeniable signature in [12]. On the other hand, our proving technique is also different from that of them. With respect to the proving of unforgeability, the different technique makes us to avoid the random salt in the scheme at the price of a slightly less reduction efficiency. When it comes to the proving of invisibility, our reduction between invisibility and the 1m-DCTCD is perfect and our method to extend the standard assumption are more commonly used in literature.

Theorem 1 (**Unforgeability).** *The new convertible undeniable scheme is EF-CMA-secure in the random oracle model if the Co-CDH problem is hard.*

Proof. In this proof, we will follow the security proof [33] which deals with the security of the FDH variant of Chaum's undeniable signature scheme, since our scheme also use the full domain hash function (FDH) as the random oracle.

We assume implicitly that all parties have access to the public parameter $param = (q, P_1, P_2, g_T, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \psi)$. Assume $H : \{0,1\}^* \to \mathbb{G}_1$ to be a cryptographic hash function. Assume H' to be another cryptographic hash function which are used in designated-verifier NIZK protocols of confirming/denying and not explicitly mentioned in above description of our scheme for simplicity. And note that by manipulating the random oracle H', a valid transcript of the NIZK proof can be easily simulated.

First, if there exists a forger F who can forge a signature with advantage ϵ_F, then we will construct an algorithm M which can solve the Co-CDH problem with advantage ϵ_M, with F as a subroutine. Assueme the input to M is (X, R) where $X = xP_2, R = rP_1$. M then runs F by giving F with the public key $(X, Y(= yP_2))$ and (H, H') where H and H' are random oracles that will be simulated by M and $y \in_R \mathbb{Z}_q$ is chosen and held by M. M simulates the signing oracle Σ, receipt generating oracle Υ and the confirmation/disavowal Ξ oracle itself. Let q_S and q_H denote the number of signing queries and H queries that F issues respectively. Assume that when F requests a signature on a message m_i, it has already made the corresponding H query on m_i.

When F request $H(m_i)$, M answers $R_i = H(m_i) = \alpha_i P_1$ with probability δ and $R_i = H(m_i) = \alpha_i R$ with probability $1-\delta$, where α_i is random in $\mathbb{Z}_q$ and δ is a fixed probability to be determined later.

When F makes a Υ-query for some pair of (m_i, σ_i), M can successfully return the universal receipt xyP_2 or the individual receipt $yH(m_i)$ since M holds the partial secret key y.

Suppose that F makes a signing query for a message m_i. If M has responded with $R_i = \alpha_i P_1$ to the H query for a message m_i, then M returns $\sigma_i = (y \cdot \alpha_i)\psi(X)$ as the valid signature. Otherwise, M aborts and it fails to solve the Co-CDH problem.

When F makes a H'-query for a new str, where str is the string that F would like to know its H' value, M always responds with a random number. In fact, M assigns some values to $H'(str)$ for some str such that he can simulate the confirmation/disavowal oracle Ξ. When F makes a H'-query for such str, M returns $H'(str)$ to F.

Next, we consider the case when F makes a confima-tion/disavowal query. Let q_v be the number of queries that F issues to the confirmation/disavowal oracle. For convenience, we consider that the final output of F is the (q_v+1)-th query (i.e. the forged signature pair (m^*, σ^*). We say that (m_i, σ_i) is special if it is a valid message-signature pair queried by F to the confirmation/disavowal oracle such that m_i has never been queried to the signing oracle. M guesses the first special query. More precisely, M guesses the first i such that the i-th query (m_i, σ_i) is special. So, at the beginning, M chooses $Guess \in \{1, 2, \cdots, q_v+1\}$ randomly. There are two cases to be considered here, namely, $i < Guess$ and $i = Guess$. First suppose that $i < Guess$.

- If F has never made a signing query for m_i, then M returns "no" and the transcript of the disavowal protocol.
- Otherwise, F has already made a signing query for m_i, and M answered with a valid signature σ_i' with probability δ (with probability $(1-\delta)$, M aborts). If $\sigma_i = \sigma_i'$ then M returns "yes" and the transcript of the confirmation protocol. Otherwise, M returns "no" and the transcript of the disavowal protocol.

As mentioned before, M can manipulate the H'-oracle and thus it can generate a transcript of the confirmation or disavowal protocol.

Now suppose that $i = Guess$. Let (m^*, σ^*) be the i-th query. If F has queried m^* to the signing oracle, then M aborts. Otherwise, we assume that F has queried the H oracle on m^* and so $m^* = m_j$ for some j. If $V_j = H(m^*) = \alpha_j R$, then we have $\sigma^* = xyV_j = (xy\alpha_j)R$. Consequently, M outputs xR since he knows α_j, y, where y is the partial secret key held by M and y is the parameter chosen and stored by M during the simulation of the random oracle H. Hence, M can solve the Co-CDH problem. Otherwise, M aborts and it fails to solve the Co-CDH problem.

Now it remains to compute the probability that M does not abort. M guesses the first special query with probability $1/(q_v+1)$. M answers to all the signing queries with property δ^{q_S} and M outputs xR with probability $1-\delta$. Hence, the probability that M does not abort during the simulation is $\delta^{q_S}(1-\delta)/(q_v+1)$. It is less than $\delta_{opt} = 1 - 1/(q_S+1)$. Hence, M's advantage ϵ_M is more than $\frac{1}{e(1+q_S)} \cdot \frac{1}{(q_v+1)}\epsilon_F$. Here, e is the natural logarithm base. In fact, the value $(1-1/(q_S+1))^{q_S}$ approaches $1/e$ for large q_S. □

Theorem 2 (Invisibility). *The invisibility of the above convertible undeniable signature scheme holds if one-more DCTDH problem is hard*

Proof. For simplicity, we assume implicitly that all parties can access to the public parameter $param = (q, P_1, P_2, g_T, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \psi)$. Let $H : \{0,1\}^* \rightarrow \mathbb{G}_1$ be a cryptographic hash function. And let H' be another cryptographic hash function which will be used in the protocols of confirming/denying. And note that by manipulating the the random oracle H', a valid transcript of the designated NIZK proof can be easily simulated.

We show that if there exists a distinguisher D with advantage ϵ_D for the convertible deniable signature scheme, then one can construct a 1m-DCTDH distinguisher D' with advantage $\epsilon_{D'}$, by running D as a subroutine. Suppose the input to D' is the public key $(X, Y) \in \mathbb{G}_2^2$ and D' has the access to the target oracle and helper oracle. D' then starts running D by feeding D with the public key $(X = xP_2, Y = yP_2)$ and H, H' which are random oracles that will be simulated by D'. D' also simulates the signing oracle, receipt generating oracle and the confirmation/disavowal oracle itself. Let q_S and q_H be the number of signing queries and H queries that D issues respectively. We assume that when D requests a signature on a message m_i, it has already made the corresponding H query on m_i.

Let m_i be some message. When D makes a H query for m_i, D' responds with $H(m_i) = V_i$ where (V_i, V_i') is the answer that D' gets from its own target oracle $\mathcal{TG}$. If D makes a signing query for m_i, D' responds with R_i where $(R_i, R_i') = (xyH(m_i), yH(m_i))$ is the answer that D' gets from its own the helper oracle $\mathcal{HO}$ on query $H(m_i)$. If $R_i = V_i'$, D' set $b_i = 1$ else $b_i = 0$. When D makes a query of (m_i, σ_i) on the individual receipt generating oracle Υ, D' responds with $R_i' = yH(m_i)$.

When D makes a H'-query for a new str, where str is the string that D would like to know its H' value, D' always responds with a random number. In fact, D' assigns some values to $H'(str)$ for some str such that he can simulate the confirmation/disavowal oracle. When D makes a H'-query for such str, D' returns $H'(str)$ to F.

At some time, D outputs a challenge query m^*. As assumed, $H(m^*)$ has been queried by D. Let $V^* = H(m^*)$ where $(V^*, V^{*\prime})$ is the answer that D' gets from the target oracle $\mathcal{TG}$ when he simulates the H-oracle query on m^*. Now, D' presents the challenge with $V^{*\prime}$ for D with respect to the query m^*.

In the next step, D adaptively performs some H-queries, H'-queries, signing queries, receipt generating queries and confirmation /disavowal queries again with the restriction that no signing queries on m^* should be allowed, and no confirmation/disavowal query or receipt generating query on the challenge message-signature pair $(m^*, V^{*\prime})$ is allowed.

Eventually, D outputs $b^* = 1$, if it thinks that $(m^*, V^{*\prime})$ is a valid message-signature pair, i.e.

$$V^{*\prime} = xyH(m^*) = xyV^*.$$

And it outputs $b^{*\prime} = 0$ if it thinks that $V^{*\prime}$ is chosen uniformly at random from the signature space S. Let $m_{j_1}, m_{j_2}, \cdots, m_{j_{q_s}}$ be all the messages which D has got the corresponding signatures $R_{j_1}, R_{j_2}, \cdots, R_{j_{q_s}}$ simulated by D'. Now, D' output $q_s + 1$ triples

$$(V_{j_1}, V'_{j_1}, b_{j_1}), (V_{j_2}, V'_{j_2}, b_{j_2}), \cdots, \\ (V_{j_{q_s}}, V'_{j_{q_s}}, b_{j_{q_s}}), (V^*, V^{*\prime}, b^*).$$

From previous description of D''s behavior on V_i, V'_i, R_i, b_i, it is obvious that for any $i \in \{j_1, \cdots, j_{q_s}\}$, b_i just denote whether $V'_i = xyV_i$. Note that the times of D''s signing queries q_s is just the times of D's accesses to its helper oracle. So it is obvious that the advantage of D' attacking 1m-DCTDH is just the advantage of D attacking the invisibility of our convertible deniable signature scheme, i.e. $\epsilon_{D'} = \epsilon_D$.

At last, we show how to simulate the confirmation/disavowal oracle. Suppose that 1m-DCTDH problem is hard. Then D cannot forge with non-negligible probability because forgery is equivalent to Co-CDH problem from above theorem. Now assume that D queries (m_i, σ_i) to the confirmation/disavowal oracle.

- If D has never made a signing query for m_i, then D' returns "no" and a transcript of the disavowal protocol. This is justified because D cannot forge as mentioned above.
- Otherwise, D has already made a signing query for m_i, and D' has answered with a valid signature σ_i. If $\sigma_i = \sigma'_i$ then D' returns "yes" and a transcript of the confirmation protocol. Otherwise, D' returns "no" and a transcript of the disavowal protocol.

D' can generate a transcript of the confirmation/disavowal protocol as shown in since he can control the random oracle of H' which is used in the NIZK proof systems—confirmation/denial protocol. □

VI. CONCLUSION

In this paper, we first propose computational and decisional Co-tripartite-Diffie-Hellman assumptions and extend the decisional tripartite-Diffie-Hellman assumption to the one-more variant based on the bilinear group system. Then we designed a new short convertible undeniable signature scheme which is proven to be secure under the assumption of computational Diffie-Hellman (unforgeable) and one-more decisional tripartite-Diffie-Hellman (invisible). This new convertible undeniable signature is based on the most popular short signature from pairing, and specially suitable some resource restricted settings such as smartcard.

REFERENCES

[1] D.Chaum, H. van Antwerpen, Undeniable Signatures, Proceedings of Crypto '89, Springer LNCS Vol.435, 212-216, 1990.

[2] D. Chaum, Zero-Knowledge undeniable signatures. Proceedings of Eurocrypt90, Springer LNCS Vol. 473, pp. 458-464, 1991.

[3] J. Boyar, D. Chaum, I. B. Damgard, T.P. Pedersen: Convertible undeniable signatures. Proc. of Crypto90, Springer LNCS Vol. 537, 189-205, 1991

[4] M. Abdalla, J. An, M. Bellare and C. Namprempre. From identification to signatures via the Fiat-Shamir transform: minimizing assumptions for security and forward-security. Proc. of Eurocrypt02, Springer LNCS Vol.2332, 418-433, 2002.

[5] M. Michels, H. Petersen, P. Horster: Breaking and repairing a convertible undeniable signature scheme. Proc. of ACM Conference on Computer and Communications Security 1996, 148-152, ACM Press (1996)

[6] M. Michels, M. Stadler: Efficient Convertible Undeniable Signature Schemes. Proc. of SAC97, 231-244 (1997)

[7] I. Damgard, T.P. Pedersen: New convertible undeniable signature schemes. Proc. of Eurocrypt96, Springer LNCS Vol. 1070, 372ł386, 1996

[8] S. Galbraith, W. Mao: Invisibility and anonymity of undeniable and confirmer signatures. Proc. of CT-RSA 2003, Springer LNCS Vol. 2612 80-97, 2003

[9] S. Galbraith, W. Mao, K.G. Paterson: RSA-based undeniable signatures for general moduli. Proc. of CT-RSA 2002, Springer LNCS Vol. 2271, 200-217, 2002

[10] R. Gennaro, H. Krawczyk, T. Rabin: RSA-based undeniable signatures. Proc. of Crypto97, Springer LNCS Vol. 1294, 132-149, 1997

[11] J. Monnerat, S. Vaudenay: Undeniable Signatures Based on Characters: How to Sign with One Bit. Proc. of PKC 2004, Springer LNCS Vol. 2947, 69-85, 2004

[12] F. Laguillaumie, D. Vergnaud. Time-Selective Convertible Undeniable Signatures. In: Topics in Cryptology - CT-RSA 2005, Springer LNCS Vol.3376, 154-171. 2005

[13] D. Chaum, T.P. Pedersen: Wallet Databases with Observers. Proc. of Crypto92, Springer LNCS Vol. 740, 89-105, 1993

[14] C. Boyd, E. Foo: Off-line Fair Payment Protocols using Convertible Signatures. Proc. of Asiacrypt98, Springer LNCS Vol. 1514, 271-285, 1998

[15] K. Kurosawa, T. Takagi. New Approach for Selectively Convertible Undeniable Signature Schemes. Proc. of ASIACRYPT 2006, Springer LNCS 4284, pp.428-443

[16] T.H. Yuen, M.H. Au, J. K. Liu, Willy Susilo. (Convertible) Undeniable Signatures Without Random Oracles. Proc. of ICICS 2007, Springer LNCS 4861, pp.83-97.

[17] L.E. Aimani. Toward a Generic Construction of Universally Convertible Undeniable Signatures from Pairing-Based Signatures. Proc. of INDOCRYPT 2008, Springer LNCS 5365 pp.145-157

[18] Q. Huang, D.S. Wong. New Constructions of Convertible Undeniable Signature Schemes without Random Oracles. IACR Cryptology ePrint Archive 2009: 517 (2009)

[19] L.T. Phong, K. Kurosawa, W. Ogata. Provably Secure Convertible Unameniable Signatures with Unambiguity. Proc. of SCN 2010, Springer LNCS 6280, pp.291-308

[20] R. Kikuchi, L.T. Phong, W. Ogata. A Framework for Constructing Convertible Undeniable Signatures. Proc. of ProvSec 2010, Springer LNCS 6402, pp.70-86

[21] J. C. N. Schuldt, K. Matsuura. Efficient Convertible Undeniable Signatures with Delegatable Verification. IEICE Transactions 94-A(1): 71-83 (2011)

[22] W. Zhao, D. Ye. Certificateless undeniablesignatures from bilinear maps. Information Sciences. 2012, volume 199: pp.204-215

[23] D. Boneh, B. Lynn, H. Shacham: Short signatures from the Weil pairing. Proc. of Asiacrypt01, Springer LNCS Vol. 2248, 514-532, 2001

[24] M. Bellare and P. Rogaway, Random oracles are practical: A paradigm for designing efficient protocols. Proceedings First Annual Conference on Computer and Communications Security, ACM, 1993.

[25] R. Dutta, R. Barua, P. Sarkar, "Pairing-Based Cryptography : A Survey," Cryptology ePrint Archive, Report 2004/064

[26] X. Cheng, S., J. Yu, X. Li, H. Ma. A Practical ID-Based Group Signature Scheme. Journal of Computers, Vol 7, No 11 (2012), 2650-2654, Nov 2012

[27] F. Li, W. Gao, Y. Wang, X. Wang. An Efficient Certificateless Threshold Decryption Schemes Based On Pairings. Journal of Computers, Vol 7, No 12 (2012), 2987-2996, Dec 2012
[28] W. Gao, G. Wang, X. Wang, D. Xie. Controllable Ring Signatures and Its Application to E-Prosecution. Journal of Computers, Vol 8, No 4 (2013), 833-841, Apr 2013
[29] M. Bellare and G. Neven. Transitive Signatures based on Factoring and RSA. Proc. of Asiacrypt'02, Springer LNCS Vol. 2501, 397-414, 2002.
[30] M. Bellare, C. Namprempre, G. Neven, Security Proofs for Identity-Based Identification and Signature Schemes. Proc. of Eurocrypt'2004, Springer LNCS Vol.3027, 268–286, 2004.
[31] J. Camenisch, V. Shoup: Practical Verifiable Encryption and Decryption of Discrete Logarithms. Proc. of Crypto03, Springer LNCS Vol. 2729, 126-144, 2003
[32] M. Jakobsson, K. Sako and R. Impagliazzo. Designated verifier proofs and their applications. Proc. of Eurocrypt'96, Springer LNCS Vol.1070, 143-154, 1996.
[33] W. Ogata, K. Kurosawa, S.H. Heng. The Security of the FDH Variant of Chaum's Undeniable Signature Scheme. In: Public Key Cryptography - PKC 2005, LNCS 3386, pp. 328-345. Springer-Verlag, 2005
[34] R. Cramer, I. Damgoard and B. Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. Proc. of Crypto'94, Springer LNCS Vol.839, 174-187, 1994

Fei Li received her MS degree in applied mathematics, Guangzhou University, China, in 2008. She is currently a lecturer in Ludong University, China. Her research interests include cryptography and algebra.

Wei Gao received his Ph.D., MS and BS degrees in applied mathematics from Hunan University in 2006, Guangzhou University 2003, and Ludong University in 2000, respectively. He is a lecturer in Ludong University from 2007. His research interests include security, cryptography and number theory.

Yilei Wang received her MS degree in computer science, Shandong Normal University, China, in 2004. She is currently a lecturer in Ludong University, China. Her research interests include cryptography and information security.

Xueli Wang received his PhD degree in mathematics from the Academy of China in 1991, his MS degree in mathematics from Shannxi Normal University in 1987. He is currently Professor of Computer Science at South China Normal University. His current research interests include cryptography, number theory and elliptic curves.