Identity-Based Universal Designated Verifier Signature Proof System

Xiaofeng Chen[1], Guomin Chen[1], Fangguo Zhang[1], Baodian Wei[1], and Yi Mu[2]
(Corresponding author: Xiaofeng Chen)
School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510275, P. R. China[1]
School of Computer Science and Software Engineering, University of Wollongong, Australia[2]
(Received Sept. 06, 2007; revised and accepted May 9, 2008)

Abstract

The notion of Universal Designated Verifier Signature (UDVS), introduced by Steinfeld *et al.* in Asiacrypt 2003, allows any holder of a signature to convince any designated verifier that the signer indeed generated the signature without revealing the signature itself, while the verifier cannot transfer the proof to convince anyone else of this fact. Such signature schemes can protect the privacy of signature holders and have applications in certification systems. Very recently, as pointed out by Baek *et al.* in Asiacrypt 2005, one significant inconvenience of all existing UDVS schemes is that they require the designated verifier to create a public key using the signer's public key parameter and have it certified to ensure the resulting public key is compatible with the setting that the signer provided. This is unrealistic in some situations where the verifier is not willing to go through such setup process. Baek *et al.* introduced the concept of Universal Designated Verifier Signature Proof (UDVSP) to solve this problem. In this paper, we first introduce the idea of identity-based (ID-based) UDVSP system. Furthermore, we point out that the algorithm "Signature Transformation $\mathcal{ST}$" of the UDVSP defined by Baek *et al.* can be eliminated, which results in a more efficient UDVSP system. We present two ID-based UDVSP systems based on bilinear pairings, and provide the security proofs of our systems in the random oracle model.

Keywords: Bilinear pairings, identity-based systems, universal designated verifier signature proof

1 Introduction

There are a plenty of researches on the conflict between authenticity (non-repudiation) and privacy (controlled verifiability) in the digital signatures. Undeniable signature, introduced by Chaum and van Antwerpen [5], is such a kind of digital signature which enables the signer to decide *when* his/her signature can be verified. In some applications, it is important for the signer to decide not only *when* but also *by whom* her signature can be verified. For example, the voting center presents a proof to convince a certain voter that his vote was counted without letting him to convince others (e.g., a coercer) of his vote, which is important to design a receipt-free electronic voting scheme preventing vote buying and coercion. This is the motivation of the concept of Designated Verifier Signature (DVS) [10]. The signer can provide a proof to convince the designated verifier that he indeed signed a message. However, the designated verifier cannot present the proof to convince any third party because he is fully capable of generating the same proof by himself.

Steinfeld *et al.* [14] introduced the concept of Universal Designated Verifier Signature (UDVS), which can be viewed as an extended notion of DVS. UDVS allows any holder of the signature (not necessarily the signer) to designate the signature to any desired designated verifier. The verifier can be convinced that the signer indeed generated the signature, but cannot transfer the proof to convince any third party of this fact. UDVS can protect the privacy of signature holders and have applications in certification systems. Recently, Lipmaa *et al.* [11] pointed out some security flaws of some DVS schemes and presented a new stronger security notion for DVS.

Very recently, as pointed out by Baek *et al.* [4] in Asiacrypt 2005, one significant inconvenience of all existing UDVS schemes is that they require the designated verifier to create private/public key pairs using the same public key parameter that has been set by the signer and have been certified. This is unrealistic in some situations, for example, the verifier have created his/her certified private/public key pairs using the public key parameter different from that of the signer. We argue that the verifier will be less likely to create another certified private/public key pairs using the public key parameter set by the signer just only to verify a signature of the signer because this key setup involving Public Key Infrastructure (PKI) may incur significant cost. Baek *et al.* introduced the concept of Universal Designated Verifier Signature Proof (UDVSP) to solve this problem. UDVSP also achieves all the properties of UDVS. The main difference between UDVS and UDVSP is that in UDVS the signature holder himself

provides a proof using the verifier's public key to convince the verifier that the signer indeed generated the signature, while in UDVSP the signature holder performs an interactive protocol together with the verifier to convince him of the fact. The verifier's key pair will not be involved in such a proof, even the verifier need not have a key pair in UDVSP. Therefore, UDVSP is a good substitute for UDVS in some applications.

Steinfeld *et al.*'s UDVS schemes [14, 15] were constructed under certificate-based (CA-based) public key systems. Identity-based (ID-based) systems [13] simplify key management procedure and can be a good alternative for CA-based systems, especially when efficient key management and moderate security are required. Zhang *et al.* [16] proposed the concept of ID-based UDVS, where the public key of the user is his/her identity. However, it is also required that the designated verifier creates the certified public/private key pair using the same public key parameter as that of the signer. That is to say, the signature holder uses the verifier's public key (identity) to generate a proof to convince that the signer indeed generated a signature, which can be verified by the signer's identity and the verifier's private key.

Our Contribution. In this paper, we first introduce the concept of ID-based UDVSP. Our contribution is two folds: 1. We provide a formal model and security notions for ID-based UDVSP and then propose a concrete construction of ID-based UDVSP based on Hess signature. We prove our construction achieves the desired security notions in the random oracle model. 2. We point out that the algorithm "Signature Transformation $\mathcal{ST}$" of the UDVSP defined by Baek *et al.* [4] can be eliminated, *i.e.*, we can present a more efficient UDVSP system. We then present an efficient ID-based UDVSP system based on Cha-Cheon signature scheme and provide the formal security proof.

The rest of this paper is organized as follows: Some preliminaries are given in Section 2. The formal definition and security notions for ID-based UDVSP are given in Section 3. The proposed ID-based UDVSP system based on Hess signature and its security analysis are given in Section 4. In Section 5, we propose a more efficient UDVSP system and extend it to ID-based one. Finally, conclusions will be made in Section 6.

2 Preliminaries

2.1 Bilinear Pairings

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_2 be a cyclic multiplicative group of the same order q. Let a and b be elements of $\mathbb{Z}_q^*$. We assume that the discrete logarithm problems (DLP) in both G_1 and G_2 are hard. A bilinear pairing is a map $e : G_1 \times G_1 \rightarrow G_2$ with the following properties:

1) Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1, a, b \in \mathbb{Z}_q$.
2) Non-degenerate: There exists P and $Q \in G_1$ such that $e(P, Q) \neq 1$.
3) Computable: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

Definition 1. Computational Diffie-Hellman Problem (CDHP): *Given a randomly chosen $P \in G_1$, as well as aP, bP (for unknown randomly chosen $a, b \in \mathbb{Z}_q$), compute abP.*

Definition 2. Decisional Diffie-Hellman Problem (DDHP): *Given a randomly chosen $P \in G_1$, as well as aP, bP, cP (for unknown randomly chosen $a, b, c \in \mathbb{Z}_q$), to decide whether $c \equiv ab \bmod q$.*

We call G a gap Diffie-Hellman group if DDHP can be solved in polynomial time but there is no polynomial time algorithm to solve CDHP with non-negligible probability. Such groups can be found in supersingular elliptic curve or hyperelliptic curve over finite field, and the bilinear pairings can be derived from the Weil or Tate pairings. For more details, see [1, 6, 8].

Throughout the rest of this paper we define G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_2 be a cyclic multiplicative group of the same order q. A bilinear pairing $e : G_1 \times G_1 \rightarrow G_2$. Define three cryptographic secure hash functions $H : \{0,1\}^* \rightarrow G_1$, $H_1 : G_1 \times \{0,1\}^* \rightarrow \mathbb{Z}_q^*$ and $h : \{0,1\}^* \times G_2 \rightarrow \mathbb{Z}_q^* \times \mathbb{Z}_q^*$.

Definition 3. One More Discrete Logarithm Problem: *The definition of "One More Discrete Logarithm" (OMDL) problem is introduced by Bellare [3]. Formally, the experiment for this problem can be described as follows [4]:*

- **Experiment:** *Let $SP = (q, P, e, G_1, G_2, k)$ be the system parameters. A polynomial-time attacker $\mathcal{A}$ makes m queries to the challenge oracle $\mathcal{C}()$ and n queries to the DL oracle $\mathcal{DL}_{q,P}()$. Let $(s_1, s_2, \cdots, s_n) \longleftarrow \mathcal{A}^{\mathcal{C}(), \mathcal{DL}_{q,P}()}(SP)$.*
- **Output:** *If $(g^{s_1} = h_1) \wedge \cdots \wedge (g^{s_m} = h_m)$, where $h_1, \cdots h_m$ are random points in G_1 output by the challenge oracle $\mathcal{C}()$, and $n < m$, where n denotes the number of queries to the DL oracle, then return 1. Otherwise, return 0.*

We say that OMDL problem is hard if the advantage of $\mathcal{A}$ in the above experiment is negligible in k.

2.2 ID-based Setting from Pairings

The ID-based public key cryptosystems allow some public information of the user such as name, address and email *etc.*, rather than an arbitrary string to be used as his public key. The private key of the user is calculated by PKG (Private Key Generator) and sent to the user via a secure channel.

ID-based public key setting from bilinear pairings can be implemented as follows:

- **Setup:** PKG chooses a random number $s \in \mathbb{Z}_q^*$ and set $P_{pub} = sP$. The center publishes systems parameters $params = \{G_1, G_2, e, q, P, P_{pub}, H\}$, and keep s as the *master-key*, which is known only by himself.
- **Extract:** A user submits his/her identity information ID to PKG. PKG computes $Q_{ID} = H(ID)$, and returns $S_{ID} = sQ_{ID}$ to the user as his/her private key.

3 ID-based Universal Designated Verifier Signature Proof

3.1 Definitions

There are four parties involved in the ID-based UDVSP system: a PKG, a signer, a designator (signature holder), a designated verifier. The PKG first generates the private key for the signer. The signer then signs a message and securely transmits the resulting signature together with the message to the designator. After obtained the valid signature from the signer, the designator creates a transformed signature by generating a random mask and hiding the original signature using it. The designator then convinces the designated verifier via an interactive protocol that the transformed signature has been generated from the valid signature obtained from the signer.

Definition 4. ***(ID-based UDVSP:)*** *An ID-based UDVSP system consists of the following five polynomial-time algorithms and a proof:*

- **System Parameters Generation $\mathcal{PG}$:** *On input a security parameter k, outputs the common system parameters Params and the master-key mk of PKG.*
- **Key Extraction $\mathcal{KE}$:** *On input Params, master-key mk, and a user's identity information ID as the public key pk, outputs the corresponding private key sk.*
- **Signature Generation $\mathcal{SG}$:** *On input the secret key sk_s of the signer S and a message m, outputs a signature σ on m.*
- **Signature Verification $\mathcal{SV}$:** *On input the public key $pk_s = ID_s$, the message m and the signature σ, outputs either accept or reject.*
- **Signature Transformation $\mathcal{ST}$:** *On input the public key pk_s of S, the signature σ and a secret mask $\tilde{sk}$, outputs a transformed signature $\tilde{\sigma}$ using $\tilde{sk}$.*
- **Interactive Verification Protocol $\mathcal{VP}$:** *This is an interactive verification protocol between a signature holder SH and a designated verifier DV. Common inputs for SH and DV are the signer's public key pk_s, a transformed signature $\tilde{\sigma}$ and the message m. SH's private input is the secret mask $\tilde{sk}$ used to create $\tilde{\sigma}$. DV does not have any private input. In this protocol, SH tries to convince DV that $\tilde{\sigma}$ has been generated from the valid signature σ obtained from the signer, with the knowledge of $\tilde{sk}$. The output of the protocol is either accept or reject.*

3.2 Security Requirements

There are two essential requirements for ID-based UDVSP system. One is that a signature created by the signer should be existentially unforgeable under adaptive chosen message attack and ID attack. This is similar to the property of "PV-Unforgeability" in UDVS scheme [14]. The other is resistance against impersonation attack. That is, UDVSP system should prevent an attacker who does not hold a valid signature created by the signer from impersonating the honest designator who holds a valid signature created by the signer [4].

This impersonation attack can be divided into two categories, "Type-1" and "Type-2" attacks. In Type-1 attack, an attacker who has obtained a transformed signature participates in the $\mathcal{VP}$ protocol as a cheating designated verifier and interacts with an honest designator a number of times. The attacker then tries to impersonate the honest designator to other honest designated verifier. In Type-2 attack, the attacker simply ignores the transformed signature that he has obtained before but tries to create a new transformed signature on his own and use this to impersonate the honest designator to an honest designated verifier in the $\mathcal{VP}$ protocol. About the formal definition for security against the Type-1 and Type-2 attacks, please refer to [4].

In UDVSP system, the property of "DV-Unforgeability" [14] is not considered, which requires that it is difficult for an attacker to forge a DV-signature $\tilde{\sigma}^*$ by the signer on a new message m^*, such that the pair $(m^*, \tilde{\sigma}^*)$ passes the DV-verification test. This prevents attacks to fool the designated verifier, possibly mounted by a dishonest designator. However, we remark that this attack can be included in the Type-2 attack, if we think the dishonest designator (attacker) impersonates himself to fool the honest designated verifier.

4 ID-based UDVSP System Based on Hess Signature

4.1 The Proposed System

Our proposed ID-based UDVSP system is based on Hess signature scheme [9]. Each sub-algorithm and protocol of this system can be described as follows:

- **System Parameters Generation $\mathcal{PG}$:** On input a security parameter k, outputs the system parameters $\mathsf{Params} = \{G_1, G_2, e, q, P, P_{pub} = xP, H, H_1\}$ and the PKG's master-key $\mathsf{mk} = x$.
- **Key Extraction $\mathcal{KE}$:** On input Params, the master-key x, and an identity information ID, outputs the corresponding private key $S_{ID} = xH(ID)$.

- **Signature Generation $\mathcal{SG}$:** On input the secret key S_{ID_s} of the signer, a message m and a random element $Q \in_R G_1$, the signer computes $r = e(Q, P)$, $(\lambda, \mu) = h(m, r)$, and $V = \lambda S_{ID_s} + \mu Q$. Outputs a signature $\sigma = (r, V)$ on m.
- **Signature Verification $\mathcal{SV}$:** On input the public key ID_s, the message m and the signature σ. Let $(\lambda, \mu) = h(m, r)$, if the equation $e(V, P) = e(H(ID_s), P_{pub})^{\lambda} r^{\mu}$ holds, outputs accept; otherwise, output reject.
- **Signature Transformation $\mathcal{ST}$:** On input the signer's public key ID_s, the signature σ and a random integer $z \in_R \mathbb{Z}_q^*$, outputs a transformed signature $\tilde{\sigma} = (r, V' = zV)$ and the secret mask $\tilde{sk} = z$.
- **Interactive Verification Protocol $\mathcal{VP}$:** Both SH and DV firstly compute $(\lambda, \mu) = h(m, r)$, $\omega_1 = e(V', P)$, and $\omega_2 = e(H(ID_s), P_{pub})^{\lambda} r^{\mu}$. They then perform the following interactive protocol:
  1) SH chooses a random integer $\alpha \in_R \mathbb{Z}_q^*$ and sends $a = \omega_2^{\alpha}$ to DV.
  2) DV chooses $c \in_R \mathbb{Z}_q^*$ and sends it to SH.
  3) SH computes $t = \alpha + cz \mod q$ and sends t to DV.
  4) DV checks $\omega_2^t \stackrel{?}{=} a\omega_1^c$. If the equation holds, outputs accept; otherwise, outputs reject.

The underlying signature scheme in the above ID-based UDVSP system is a standard Hess signature, so $e(V, P) = e(H(ID_s), P_{pub})^{\lambda} r^{\mu}$ holds. Also, in the protocol $\mathcal{VP}$, note that $\omega_1 = e(V', P) = e(V, P)^z = \omega_2^z$, therefore the equation $\omega_2^t = \omega_2^{\alpha + cz} = a\omega_1^c$ holds.

4.2 Security Analysis

We prove that our proposed ID-based UDVSP system achieves the desired security properties. Since the unforgeability of the Hess signature scheme [9] was proven under the assumption that CDHP in G_1 is hard, we only analyze the security of the UDVSP system under the impersonation attacks.

Theorem 1. *The ID-based UDVSP system based on Hess signature is secure against impersonation under Type-1 attack in the random oracle model [2] assuming that OMDL problem is hard in G_1.*

Proof. Let $\mathcal{A} = (\tilde{V}, \tilde{P})$ be an impersonator that tries to break the UDVSP system based on the Hess signature and $\mathcal{B}$ be an OMDL attacker. Suppose $\mathcal{B}$ is given the system parameters $\{G_1, G_2, e, q\}$. First, $\mathcal{B}$ queries its challenge oracle $\mathcal{C}$ to obtain a challenge point $S_0 = s_0 P$ for some unknown $s_0 \in_R \mathbb{Z}_q$. $\mathcal{B}$ then randomly chooses an integer $x \in_R \mathbb{Z}_q$ and outputs the signer's public key $pk = \{G_1, G_2, e, q, P, P_{pub} = xP, ID_s, H, h\}$, where $H : \{0,1\}^* \to G_1^*$ and $h : \{0,1\}^* \times G_2 \to \mathbb{Z}_q^* \times \mathbb{Z}_q^*$ are hash functions viewed as random oracles.

Let the signed message is m, $\mathcal{B}$ randomly chooses four integers $d, e, \lambda, \mu \in_R \mathbb{Z}_q$ and sets $H(ID_s) = dP$, $r = e(P, P)^e$, and $h(m, r) = (\lambda, \mu)$. $\mathcal{B}$ then computes $V' = (\lambda x d + \mu e) S_0$ and sends $\mathcal{A}$ a transformed signature $\tilde{\sigma} = (r, V')$.

$\mathcal{B}$ proceeds to simulate n times of the execution of the $\mathcal{VP}$ protocol between $\tilde{V}$ and an honest designator P as follows:

Make a query to $\mathcal{C}$ and get the response S_i, here $i \in \{1, 2, \cdots, n\}$. Compute $a_i = e((\lambda x d + \mu e)P, S_i)$ and send it to $\tilde{V}$. When $\tilde{V}$ sends c_i, make query $S_i + c_i S_0$ to $\mathcal{DL}_{q,P}()$ to get the response t_i. $\tilde{V}$ checks $(e(H(ID_s), P_{pub})^{\lambda} r^{\mu})^{t_i} \stackrel{?}{=} a_i e(V', P)^{c_i}$.

Note that $a_i = (e(dP, P_{pub})^{\lambda} e(P, P)^{\mu e})^{s_i} = (e(H(ID_s), P_{pub})^{\lambda} r^{\mu})^{s_i}$, and $t_i = s_i + c_i s_0 \mod q$, we have

$$\begin{aligned}(e(H(ID_s), P_{pub})^{\lambda} r^{\mu})^{t_i} &= (e(H(ID_s), P_{pub})^{\lambda} r^{\mu})^{s_i + c_i s_0} \\ &= a_i (e(H(ID_s), P_{pub})^{\lambda} r^{\mu})^{c_i s_0} \\ &= a_i e((\lambda x d + \mu e) S_0, P)^{c_i} \\ &= a_i e(V', P)^{c_i}\end{aligned}$$

After performing the above simulation n times, $\mathcal{B}$ now attempts to extract s_0. To do so, $\mathcal{B}$ runs $\tilde{P}$ to get a in Step 1 of $\mathcal{VP}$ protocol, selects $c \in_R \mathbb{Z}_q$ and runs $\tilde{P}$ to obtain its response t and checks $(e(H(ID_s), P_{pub})^{\lambda} r^{\mu})^t \stackrel{?}{=} a e(V', P)^c$. If so, $\mathcal{B}$ runs $\tilde{P}$ again with the same state as before but with different challenge $c' \in_R \mathbb{Z}_q$, obtains its response t' and checks $(e(H(ID_s), P_{pub})^{\lambda} r^{\mu})^{t'} \stackrel{?}{=} a e(V', P)^{c'}$. If so, we have $(e(H(ID_s), P_{pub})^{\lambda} r^{\mu})^{t - t'} = e(V', P)^{c - c'}$, that is $e(P, P)^{(\lambda x d + \mu e)(t - t')} = e(P, P)^{(\lambda x d + \mu e) s_0 (c - c')}$. Then we obtain $s_0 = \frac{t - t'}{c - c'} \mod q$. With s_0, we can compute all s_i for $i \in \{1, 2, \cdots, n\}$. □

Theorem 2. *The ID-based UDVSP system based on Hess signature is secure against impersonation under Type-2 attack in the random oracle model assuming that CDHP is hard in G_1.*

Proof. Let $\mathcal{A}$ be an impersonator that tries to break the ID-based UDVSP system based on Hess signature under Type-2 attack. Let $\mathcal{B}$ be a forger that tries to break the Cha-Cheon signature scheme under chosen message attack. Suppose the $\mathcal{B}$ is given a public key $\{G_1, G_2, e, q, P, P_{pub} = xP, H, h\}$, where $H : \{0,1\}^* \to G_1^*$ and $h : \{0,1\}^* \times G_2 \to \mathbb{Z}_q^* \times \mathbb{Z}_q^*$ are hash functions viewed as random oracles. Firstly, $\mathcal{B}$ outputs $pk = \{G_1, G_2, e, q, P, P_{pub} = xP, H, h\}$ as the signer's public key. $\mathcal{B}$ then chooses an arbitrary string $m \in \{0,1\}^*$.

$\mathcal{B}$ now runs $\mathcal{A}$ to get $\tilde{\sigma} = (r, V')$, continues to run $\mathcal{A}$ to get a in step 1 of $\mathcal{VP}$. Upon receiving a, $\mathcal{B}$ picks $c \in_R \mathbb{Z}_q^*$, runs $\mathcal{A}$ to obtain its response t and checks $(e(H(ID_s), P_{pub})^{\lambda} r^{\mu})^t \stackrel{?}{=} a e(V', P)^c$. If the equation holds, $\mathcal{B}$ runs $\mathcal{A}$ again with same state as before but with difference challenge c', obtains its response t' and

checks $(e(H(ID_s), P_{pub})^{\lambda} r^{\mu})^{t'} \stackrel{?}{=} ae(V', P)^{c'}$. If the equation holds, $\mathcal{B}$ outputs $(r, V'^{\frac{c-c'}{t-t'}})$ as a forgery.

Note that $e(V', P)^{c-c'} = (e(H(ID_s), P_{pub})^{\lambda} r^{\mu})^{t-t'}$, we have

$$e(V'^{\frac{c-c'}{t-t'}}, P) = e(H(ID_s), P_{pub})^{\lambda} r^{\mu}.$$

Therefore, $(r, V'^{\frac{c-c'}{t-t'}})$ is a valid Hess signature on message m. □

5 More Efficient ID-based UDVSP System

We observe that the algorithm "Signature Transformation $\mathcal{ST}$" defined in [4] can be eliminated, *i.e.*, we can present a more efficient UDVSP system. In this section, we first present the definition and the security notions for the new more efficient UDVSP system, and then extend it to ID-based one.

5.1 The New Definition and Security Notions

The new efficient UDVSP system only consists of three polynomial algorithms and a proof: $\mathcal{PG}$, $\mathcal{SG}$, $\mathcal{SV}$, and $\mathcal{VP}$. As an example, we present the following UDVSP system based on BLS signature scheme [1]:

- **System Parameters Generation $\mathcal{PG}$:** On input a security parameter k, outputs the system parameters $\mathsf{Params} = \{G_1, G_2, e, q, P, H\}$. Let the signer's private/public key pair be $(x, y = xP)$.
- **Signature Generation $\mathcal{SG}$:** On input the secret key x of the signer, and a message m, outputs the signature $\sigma = xH(m)$ on m.
- **Signature Verification $\mathcal{SV}$:** On input the public key y, the message m and the signature σ. If the equation $e(\sigma, P) = e(H(m), y)$ holds, outputs accept; otherwise, output reject.
- **Interactive Verification Protocol $\mathcal{VP}$:** The designator (SH) performs an interactive protocol with the designated verifier as follows:
  1) SH chooses a random element $R \in_R G_1$ and sends $a = e(R, P)$ to DV.
  2) DV chooses $c \in_R \mathbb{Z}_q^*$ and sends it to SH.
  3) SH computes $T = R + c\sigma$ and sends T to DV.
  4) DV checks $e(T, P) = ae(H(m), y)^c$. If the equation holds, outputs accept; otherwise, output reject.

Compare with Baek *et al.*'s UDVSP system based on BLS signature scheme, our UDVSP system not only eliminates the algorithm of $\mathcal{ST}$, but also improves the efficiency of $\mathcal{VP}$.

For the secure requirements, we still consider the two type of impersonation attacks. In Type-1 attack, an attacker participates in the $\mathcal{VP}$ protocol as a cheating designated verifier and interacts with an honest designator a number of times. The attacker then tries to impersonate the honest designator to other honest designated verifier. In Type-2 attack, the attacker just create a new proof to impersonate the honest designator to an honest designated verifier in the $\mathcal{VP}$ protocol.

Note that $\mathcal{VP}$ in our system is indeed a pairing-based honest verifier zero-knowledge proof [7] derived from Schnorr signature scheme [12], which ensures DV that SH knows the information of σ. Furthermore, due to the property of pairings, σ must be the form of $xH(m)$. Therefore, even the Type-1 attacker interacts with an honest designator a number of times, he can not know any useful information to impersonate the honest designator to cheat an honest designated verifier. It means that the advantage for Type-1 attacker to impersonate the honest designator is same to that of Type-2 attacker. So, in the following, we just consider the Type-2 attacker.

5.2 Efficient ID-based UDVSP System Based on Cha-Cheon Signature

In the following we follow the above definition to present a new ID-based UDVSP system based on Cha-Cheon signature scheme [6]. We argue that we can give such a system based on other ID-based signature schemes. Each sub-algorithm and protocol of this system can be described as follows:

- **System Parameters Generation $\mathcal{PG}$:** On input a security parameter k, outputs the system parameters $\mathsf{Params} = \{G_1, G_2, e, q, P, P_{pub} = xP, H, H_1\}$ and the PKG's master-key $\mathsf{mk} = x$.
- **Key Extraction $\mathcal{KE}$:** On input Params, the master-key x, and an identity information ID, outputs the corresponding private key $S_{ID} = xH(ID)$.
- **Signature Generation $\mathcal{SG}$:** On input the secret key S_{ID_s} of the signer, a message m, and a random integer $r \in_R \mathbb{Z}_q^*$, the signer computes $U = rH(ID_s)$, $V = (r + H_1(U||m))S_{ID_s}$. Outputs a signature $\sigma = (U, V)$ on m.
- **Signature Verification $\mathcal{SV}$:** On input the public key ID_s, the message m and the signature σ, if the equation $e(V, P) = e(U + H_1(U||m)H(ID_s), P_{pub})$ holds, outputs accept; otherwise, outputs reject.
- **Interactive Verification Protocol $\mathcal{VP}$:** Both SH and DV perform the following interactive protocol:
  1) SH chooses a random integer $Q \in_R G_1$ and then sends $a = e(Q, P)$, U to DV.
  2) DV chooses $c \in_R \mathbb{Z}_q^*$ and sends it to SH.
  3) SH computes $T = Q + cV$ and sends T to DV.

4) *DV* checks $e(T,P) \stackrel{?}{=} ae(U+H_1(U||m)H(ID_s), P_{pub})^c$. If the equation holds, outputs accept; otherwise, output reject.

The underlying signature scheme in the above ID-based UDVSP system is a standard Cha-Cheon signature, so $e(V,P) = e(U + H_1(U||m)H(ID_s), P_{pub})$ holds. Also, in the protocol $\mathcal{VP}$, note that $e(T,P) = e(Q + cV, P) = ae(V,P)^c$, therefore the equation $e(T,P) = ae(U + H_1(U||m)H(ID_s), P_{pub})^c$ holds.

5.3 Security Analysis

Theorem 3. *The ID-based UDVSP system based on Cha-Cheon signature is secure against impersonation under Type-2 attack in the random oracle model assuming that CDHP is hard in G_1.*

Proof. Let $\mathcal{A}$ be an impersonator that tries to break the ID-based UDVSP system based on Cha-Cheon signature under Type-2 attack. Let $\mathcal{B}$ be a forger that tries to break the Cha-Cheon signature scheme under chosen message attack. Suppose the $\mathcal{B}$ is given a public key $\{G_1, G_2, e, q, P, P_{pub} = xP, H, H_1\}$, where $H : \{0,1\}^* \rightarrow G_1^*$ and $H_1 : G_1 \times \{0,1\}^* \rightarrow \mathbb{Z}_q^*$ are hash functions viewed as random oracles [2]. Firstly, $\mathcal{B}$ outputs $pk = \{G_1, G_2, e, q, P, P_{pub} = xP, H, H_1\}$ as the signer's public key. $\mathcal{B}$ then chooses an arbitrary string $m \in \{0,1\}^*$.

$\mathcal{B}$ now runs $\mathcal{A}$ to get (a, U) in step 1 of $\mathcal{VP}$. Upon receiving a, $\mathcal{B}$ picks $c \in_R \mathbb{Z}_q^*$, runs $\mathcal{A}$ to obtain its response T and checks $e(T,P) \stackrel{?}{=} ae(U+H_1(U||m)H(ID_s), P_{pub})^c$. If the equation holds, $\mathcal{B}$ runs $\mathcal{A}$ again with same state as before but with difference challenge c', obtains its response t' and checks $e(T',P) \stackrel{?}{=} ae(U + H_1(U||m)H(ID_s), P_{pub})^{c'}$. If the equation holds, $\mathcal{B}$ outputs $(U, \frac{1}{c-c'}(T - T'))$ as a forgery.

Note that $e(T - T', P) = e(U + H_1(U||m)H(ID_s), P_{pub})^{c-c'}$, we have $e((c-c')^{-1}(T-T'), P) = e(U + H_1(U||m)H(ID_s), P_{pub})$. Therefore, $(U, \frac{1}{c-c'}(T - T'))$ is a valid Cha-Cheon signature on message m. □

6 Conclusion

In this paper, we first provide a formal model and security notions for ID-based UDVSP and present a concrete construction based on Hess signature. Meanwhile, we argue that the algorithm "Signature Transformation $\mathcal{ST}$" of the UDVSP defined by Baek *et al.* can be eliminated, which results in a more efficient UDVSP system. We then present an efficient ID-based UDVSP based on Cha-Cheon signature scheme. Also, we prove our constructions achieve the desired security notions in the random oracle model.

Acknowledgements

This work is supported by National Natural Science Foundation of China (No. 60503006 and No. 60773202), NSFC-KOSEF Joint Research Project (No. 60611140543), and 973 Program (No. 2006CB303104). The authors are grateful to the anonymous reviewers for their valuable comments.

References

[1] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairings," *Advances in Cryptology-Asiacrypt 2001*, LNCS 2248, pp. 514-532, Springer-Verlag, 2001.

[2] M. Bellare, and P. Rogaway, "Random oracles are practical: a paradium for designing efficient protocols," *ACM Conference on Computer and Communications Security-CCS 1993*, pp.62-73, 1993.

[3] M. Bellare, C. Namprempre, D. Pointcheval, and M. Semanko, "The power of RSA inversion oracles and the security of Chaum's RSA-based blind signature scheme," *FC 2001*, LNCS 2339, pp. 319-338, Springer-Verlag, 2002.

[4] J. Baek, R. Safavi-Naini, and W. Susilo, "Universal designated verifier signature proof (or How to efficiently prove knowledge of a signature)," *Advances in Cryptology-Asiacrypt 2005*, LNCS 3788, pp. 644-661, Springer-Verlag, 2005.

[5] D. Chaum, and H. V. Antwerpen, "Undeniable signatures," *Advances in Cryptology-Crypto 1989*, LNCS 435, pp. 212-216, Springer-Verlag, 1989.

[6] J. C. Cha, and J. H. Cheon, "An identity-based signature from gap Diffie-Hellman groups," *PKC 2003*, LNCS 2567, pp. 18-30, Springer-Verlag, 2003.

[7] R. Cramer, I. Damgard, and B. Schoenmakers, "Proofs of partial knowledge and simplified design of witness hiding protocols," *Advances in Cryptology-Crypto 1994*, LNCS 893, pp. 174-187, Springer-Verlag, 1995.

[8] S. D. Galbraith, K. Harrison, and D. Soldera, "Implementing the tate pairings," *ANTS 2002*, LNCS 2369, pp. 324-337, Springer-Verlag, 2002.

[9] F. Hess, "Efficient identity based signature schemes based on pairings," *SAC 2002*, LNCS 2595, pp. 310-324, Springer-Verlag, 2002.

[10] M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated verifier proofs and their applications," *Advances in Cryptology-Eurocrypt 1996*, LNCS 1070, pp. 143-154, Springer-Verlag, 1996.

[11] H. Lipmaa, G. Wang, and F. Bao, "Designated verifier signature schemes: attacks, new security notions and a new construction," *ICALP 2005*, LNCS 3580, pp. 459-471, Springer-Verlag, 2005.

[12] C. P. Schnorr, "Efficient signature generation for smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 239-252, Springer-Verlag, 1991.

[13] A. Shamir, "Identity-based cryptosystems and signature schemes," *Advances in Cryptology-Crypto 1984*, LNCS 196, pp. 47-53, Springer-Verlag, 1984.
[14] R. Steinfeld, L. Bull, H. Wang, and J. Pieprzyk, "Universal designated-verifier signatures," *Advances in Cryptology-Asiacrypt 2003*, LNCS 2894, pp. 523-542, Springer-Verlag, 2003.
[15] R. Steinfeld, H. Wang, and J. Pieprzyk, "Efficient extension of standard Schnorr/RSA signatures into universal designated-verifier signatures," *Public Key Cryptography-PKC 2004*, LNCS 2947, pp. 86-100, Springer-Verlag, 2004.
[16] F. Zhang, W. Susilo, Y. Mu, and X. Chen, "ID-based universal designated verifier signatures," *EUC Workshops 2005*, LNCS 3823, pp. 825-834, Springer-Verlag, 2005.

Xiaofeng Chen is an Associate Professor in the School of Information Science and Technology at Sun Yan-sen University, Guangzhou, China. He obtained his Ph.D degree in Cryptography from School of Communication Engineering, Xidian University in 2003. His main research interests include public key cryptography and its applications. (Email: isschxf@mail.sysu.edu.cn)

Guomin Chen is currently a student in the School of Information Science and Technology at Sun Yan-sen University, Guangzhou, China. His main research interests include cryptology and its applications. (Email: chengmin@mail2.sysu.edu.cn)

Fangguo Zhang is a Professor in the School of Information Science and Technology at Sun Yan-sen University in Guangzhou, China. He obtained his Ph.D degree in Cryptography from School of Communication Engineering, Xidian University in 2001. His main research interests include elliptic curve cryptography, pairing-based cryptosystem, anonymity and privacy. (Email: isszhfg@mail.sysu.edu.cn)

Baodian Wei is an Associate Professor in the School of Information Science and Technology at Sun Yan-sen University, Guangzhou, China. He obtained his Ph.D degree from School of Information and Communication Engineering, Xidian University in 2004. His research interests include cryptology and its applications. (Email: weibd@mail.sysu.edu.cn)

Yi Mu received his PhD from the Australian National University in 1994. He currently is an associate professor in School of Computer Science and Software Engineering and the director of Centre for Computer and Information Security Research, University of Wollongong. Prior to joining University of Wollongong, he was a lecturer in the School of Computing and IT, University of Western Sydney, and a senior lecturer in the Department of Computing, Macquarie University. His current research interests include network security, computer security, and cryptography. He is the editor-in-chief of International Journal of Applied Cryptography and serves as editor for seven other international journals. He has served as a member of program committees for more than 80 international conferences. He is a senior member of the IEEE and a member of the IACR. (Email: ymu@uow.edu.au)