Universal Designated Verifier Ring Signature (Proof) Without Random Oracles*

Jin Li[1] and Yanming Wang[1,2]

[1] School of Mathematics and Computational Science,
Sun Yat-sen University
Guangzhou, 510275, P.R. China
sysjinli@yahoo.com.cn
[2] Lingnan College, Sun Yat-sen University,
Guangzhou, 510275, P.R. China
stswym@mail.sysu.edu.cn

Abstract. This paper first introduces the concept of universal designated verifier ring signature (UDVRS), which not only allows members of a group to sign messages on behalf of the group without revealing their identities, but also allows any holder of the signature (not necessary the signer) to designate the signature to any designated verifier. According to whether the designator has a registered public key, two kinds of UDVRS are proposed. In order to distinguish the two types of UDVRS, we call it UDVRS Proof (UDVRSP) if the designator has not a registered public key, and this protocol is interactive. We give the formal security definitions and notions of UDVRS and UDVRSP. Then, we propose a UDVRS and a UDVRSP scheme, with rigorous security proofs without random oracles.

Keywords: Ring signature, Universal Designated verifier, Bilinear Pairings.

1 Introduction

A ring signature scheme [10] allows members of a group to sign messages on behalf of the group without revealing their identities. Different from a group signature scheme (for example, [3]), the group formation is spontaneous and there is no group manager to revoke the identity of the signer.

Ring signature schemes could be used for whistle blowing [10], anonymous membership authentication for ad hoc groups [1,6] to keep the anonymity of the signer and can be publicly verifiable. However, consider a situation, where an authority, who has got a secret as well as a ring signature of the secret from a whistleblower of a group, would like to confirm validity of the secret by seeking help from a third party. In this situation, the authority sends the secret to the

* This work is supported by the National Natural Science Foundation of China (No. 60403007 and No. 10571181) and Natural Science Foundation of Guangdong Province, China (No. 04205407).

X. Zhou et al. (Eds.): EUC Workshops 2006, LNCS 4097, pp. 332–341, 2006.

third party, and wants to convince the third party that he indeed holds a ring signature on the secret from a whistleblower of the group. However, he does not want to send the signature away. A normal ring signature will not reveal the identity of signer, however, cannot satisfy the scenario. So, we present a new notion UDVRS to solve this problem. The UDVRS allows the signature holder to designate a verifier and generate a designated verifier ring signature such that it can only be verified by the designator.

1.1 Related Work

Ring signature scheme was first formalized by Rivest [10] and the first practical ring signature [14] without random oracles was proposed by Xu, Zhang, and Feng. Very recently, Chow et al. [7] gave a formal security proof to [14]. The concept of designated verifier signature (DVS) was introduced by Jakobsson et al. [9]. These signatures are intended to a specific verifier, who is the only one able to check their validity. The notion of universal designated verifier signature (UDVS) was given by Steinfeld et al. [11]. These are ordinary signatures with the additional functionality that any holder of a signature is able to convert it into a designated verifier specified to any designated verifier of his choice. The first UDVS scheme without random oracles was proposed by Zhang et al. [16]. Very recently, a new notion called universal designated verifier signature proof (UDVS Proof) was proposed by Baek et al. [2] at AsiaCrypt'05. What is the difference between UDVS and UDVS Proof is that the designator does not need a registered public key in UDVS Proof, which is required in UDVS. In order to protect the privacy of signer, the notion of ring signature was combined with deniable authentication [9]. The result is called deniable ring authentication. In deniable ring authentication, only the signer can designate a verifier such that the signature can only be verified by the designator.

1.2 Contribution

In this paper, we first present formally the security model of UDVRS and also construct a UDVRS scheme. Meanwhile, we first present the security definitions and notions of UDVRSP, and construct a UDVRSP scheme in the standard model.

2 Security Model

SYNTAX of UDVRS. A UDVRS consists of 8-tuple of probabilistic polynomial time (PPT) algorithms (CPG, SKG, VKG, RS, RV, DRS, DRV, KR) defined as follows:

CPG- The common parameter generation algorithm, on input security parameter 1^k, outputs a string params consisting of common parameters of the scheme.
SKG- The signer key generation algorithm, on input params, outputs a public key pk_i and a secret key sk_i for the user i.

VKG- The verifier key generation algorithm, on input params, outputs a public key pk_v and a secret key sk_v.
RS- The ring signature generation algorithm, that takes as input a secret key sk_i, a message m and a set of public keys $\mathcal{L}$ including the one that corresponds to the private key sk_i, returns the signature σ.
RV- The ring signature verification algorithm, takes as input a set of $\mathcal{L}$, a message m and σ, returns 1 or 0 for accept or reject, respectively.
DRS- The designation algorithm, on input a set of public key set $\mathcal{L}$ including the one that correspond to the private key sk_i, designated verifier's public key pk_v, and a message/signature pair (m, σ), output designated verifier ring signature σ'.
DRV- The designated ring signature verification algorithm, on input σ', designated verifier's secret key sk_v and a message m, outputs 1 or 0 for accept or reject, respectively.
KR- The key registration algorithm, on input pk_v, and proof knowledge of corresponding secret key sk_v, output a pair $(pk_v, \mathsf{acc/rej})$, where acc/rej denotes the public key is valid or not, respectively.

The Oracles

- $\mathcal{RS}$: The ring signature oracle, on input message m, $\mathcal{L}$, returns a ring signature $\sigma \leftarrow \mathsf{RS}(sk_i, \mathcal{L}, m)$ such that $\mathsf{RV}(\mathcal{L}, m, \sigma) = 1$.
- $\mathcal{DRS}$: The designation oracle, on input any message m, $\mathcal{L}$, designated verifier public key pk_v, first computes $\sigma = \mathsf{RS}(sk_i, m, L)$, and returns a designated ring signature $\sigma' \leftarrow \mathsf{DRS}(\sigma, \mathcal{L}, m, pk_v)$ such that $\mathsf{DRV}(\mathcal{L}, m, \sigma', sk_v) = 1$.
- $\mathcal{DRV}$: The designated verifier ring signature verification oracle, on input $\mathcal{L}, m, \sigma', pk_v$, returns a bit 1 or 0 by running the algorithm DRV.
- $\mathcal{KR}$: Key registration oracle, on input $(sk_{v_i}, pk_{v_i}) \leftarrow \mathsf{KeyGen}(1^k)$, stores (sk_{v_i}, pk_{v_i}) as a registered key pair.

The correctness requires that valid signatures can always be proved valid. So, we present our detailed security notions for unforgeability, non-transferability, and signer ambiguity for UDVRS in the following.

2.1 Unforgeability

There are two types of unforgeability to consider: Publicly verifiable ring signature unforgeability (PV-unforgeability) and designated verifier ring signature unforgeability (DV-unforgeability). Meanwhile, we also consider the strong version of security model for existential unforgeability [7]. DV-unforgeability always implies PV-unforgeability, because anyone able to forge a normal ring signature can transform it into a designated verifier ring signature. Thus it is enough to consider only DV-unforgeability. DV-unforgeability for UDVRS against adaptive chosen public key attack and message attack is defined as in the following game involving an adversary $\mathcal{A}$.

- Let $\mathcal{L} = \{P_1, \cdots, P_n\}$ be the set of n public keys in which each key is generated as $(pk_i, sk_i) \leftarrow \mathsf{SKG}(1^k)$. $\mathcal{A}$ is given $\mathcal{L}$ and the public parameters.
- $\mathcal{A}$ accesses to $\mathcal{RS}$, $\mathcal{DRS}$, $\mathcal{DRV}$, and $\mathcal{KR}$ oracles.

The adversary $\mathcal{A}$ wins the game if he can output $(\mathcal{L}, m^*, pk_v^*, \sigma'^*)$, such that $(\mathcal{L}, m^*, \sigma'^*)$ and $(\mathcal{L}, m^*, pk_v^*, \sigma'^*)$ are not equal to any answer of $\mathcal{RS}$ oracle and $\mathcal{DRS}$ oracle, respectively. The advantage of the adversary is the probability that he wins the game.

Definition 1. *(DV-unforgeability) A UDVRS scheme is DV-unforgeability secure if no PPT adversary has a non-negligible advantage in the above DV-unforgeability game.*

2.2 Non-transferability

Non-transferability is defined through the following game involving $\mathcal{A}$, $\mathcal{S}$, and $\mathcal{D}$. $\mathcal{A}$ is an attacker that tries to brag about its interaction with the signature holder. $\mathcal{S}$ is a simulator that simulates the output of $\mathcal{A}$. $\mathcal{S}$ is able to access $\mathcal{A}$ as a black-box. $\mathcal{D}$ is a distinguisher that tries to distinguish whether a given output is of $\mathcal{A}$ or of $\mathcal{S}$.

- Let $\mathcal{L} = \{P_1, \cdots, P_n\}$ be the set of n public keys in which each key is generated as $(pk_i, sk_i) \leftarrow \mathsf{SPG}(1^k)$. $\mathcal{A}$ and $\mathcal{S}$ are allowed to access $\mathcal{RS}$ oracle. However, after the challenge message m is output, they may not access to $\mathcal{RS}$ oracle with respect to this challenge message.
- $\mathcal{A}$ and $\mathcal{S}$ are allowed to access $\mathcal{KR}$ oracle and $\mathcal{DRV}$ oracle. $\mathcal{A}$ is also allowed to access to $\mathcal{DRS}$, which $\mathcal{S}$ is not allowed.

  Finally, $\mathcal{A}$ and $\mathcal{S}$ return to $\mathcal{D}$ their outputs with respect to m. $\mathcal{D}$ decides whether this output is of $\mathcal{A}$ or of $\mathcal{S}$. The advantage of $\mathcal{D}$ is the probability that it guess correctly over $\frac{1}{2}$.

Definition 2. *(Non-transferability) A UDVRS scheme is Non-transferability secure against adaptive chosen public key attack and chosen message attack, if there exists $\mathcal{S}$ to every $\mathcal{A}$, such that the advantage of every computationally unbounded $\mathcal{D}$ is only negligible.*

2.3 Signer Ambiguity

In UDVRS, signer ambiguity means that it is hard to tell which signer out of the n possible signers who actually generates a ring signature or a designated verifier ring signature.

- Let $\mathcal{L} = \{P_1, \cdots, P_n\}$ be the set of n public keys in which each key is generated as $(pk_i, sk_i) \leftarrow \mathsf{SKG}(1^k)$. Meanwhile, $(pk_{v_i}, sk_{v_i}) \leftarrow \mathsf{VKG}(1^k)$ is also generated. (pk_i, sk_i), (pk_{v_i}, sk_{v_i}) are provided to adversary.
- Pick a random $1 \leq t \leq n$, output a valid ring signature $\sigma \leftarrow \mathsf{RS}(sk_t, \mathcal{L}, m)$ such that $\mathsf{RV}\ (\mathcal{L},m,\sigma) = 1$.

– Any unbounded adversary accepts as inputs σ.

The adversary wins the game if he can output t' such that $t' = t$ who signs the signature. The advantage of the adversary is the probability that he wins the game, over $\frac{1}{n}$, that he can guess t accurately.

Definition 3. *(Signer Ambiguity) A UDVRS scheme is said to be unconditionally signer ambiguous if any unbound adversary has a negligible advantage in the above signer ambiguity game.*

3 A UDVRS Without Random Oracles

3.1 Preliminaries

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two (multiplicative) cyclic groups of prime order p. Let g_1 be a generator of $\mathbb{G}_1$ and g_2 be a generator of $\mathbb{G}_2$. We also let ψ be an isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$, with $\psi(g_2) = g_1$, and $\hat{e}$ be a bilinear map such that $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ with the following properties:

1. *Bilinearity*: For all $u \in \mathbb{G}_1$, $v \in \mathbb{G}_2$ and $a, b \in \mathbb{Z}$, $\hat{e}(u^a, v^b) = \hat{e}(u, v)^{ab}$.
2. *Non-degeneracy*: $\hat{e}(g_1, g_2) \neq 1$.
3. *Computability*: There exists an efficient algorithm to compute $\hat{e}(u, v)$.

We introduce the following problem used in [7]:

Definition 4 ((q, n)-DsjSDH). *The (q, n)-Disjunctive Strong Diffie-Hellman Problem in $(\mathbb{G}_1, \mathbb{G}_2)$ is defined as follow: Given $h \in \mathbb{G}_1$, g, $g^x \in \mathbb{G}_2$, distinct $a_i \in Z_p$ and Universal One-Way Hash Functions (UOWHF) $H_i(\cdot)$ for $1 \leq i \leq n$, distinct nonzero m_τ for $1 \leq \tau \leq q$ and $\sigma_{i,\tau}$ for $1 \leq i \leq n$, $1 \leq \tau \leq q$, satisfying: $\prod_{i=1}^{n} \sigma_{i,\tau}^{(xa_i + H_i(m_\tau))} = h$ for all τ, output m^* and (σ_i^*, γ_i), for $1 \leq i \leq n$ such that they satisfy: $\prod_{i=1}^{n} \sigma_i^{*(xa_i + H_i(m^*) + \gamma_i)} = h$ and $H_i(m^*) + \gamma_i \neq H_i(m_\tau)$ for all i and τ. We say that the (q, n, t, ϵ)-DsjSDH assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$ if no t-time algorithm has advantage at least ϵ in solving the (q, n)-DsjSDH problem in $(\mathbb{G}_1, \mathbb{G}_2)$.*

3.2 The UDVRS Scheme

We construct a UDVRS scheme without random oracles.

1. **CPG.** Choose bilinear groups $(\mathbb{G}_1, \mathbb{G}_2)$ where $|\mathbb{G}_1| = |\mathbb{G}_2| = p$. Define a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ with an isomorphism $\psi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$. g_2 is the generator of $\mathbb{G}_2$, and $g_1 = \psi(g_2)$. h is also a random generator of $\mathbb{G}_1$. Let H_i be universal one-way hash function such that $H_i : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$. Then $\mathsf{params} = (\mathbb{G}_1, \mathbb{G}_2, \hat{e}, g_1, g_2, h, H_1, \cdots, H_n)$.
2. **SKG.** For signer i, it picks $(x_i, y_i) \in (\mathbb{Z}_p)^2$ and outputs $(x_i, y_i, X_i = g_2^{x_i}, Y_i = g_2^{y_i})$ as its key pair. The secret key is (x_i, y_i) and the public key is $(X_i, Y_i) \in (\mathbb{G}_2)^2$.

3. **VKG.** For verifier, it picks $(x_v, y_v) \in (Z_p)^2$ and outputs $(x_v, y_v, X_v = g_2^{x_v}, Y_v = g_2^{y_v})$ as its key pair. The verifier's secret key is (x_v, y_v) and the public key is (X_v, Y_v).
4. **RS.** Assume the signer wants to form a ring signature on message m of n users $\{(X_1, Y_1), \cdots, (X_n, Y_n)\}$ with his own public key at index t, he signs as follows:
   a. For $i \in \{1, \cdots, n\} \backslash t$, he picks $z_i \in_R \mathbb{Z}_p^*$ and computes $\sigma_i = g_1^{z_i}$.
   b. For $i \in \{1, \cdots, n\}$, he picks $r_i \in \mathbb{Z}_p^*$. Then he computes
   $\omega = h/(\prod_{i \in \{1,\ldots,n\} \backslash t} \psi(X_i \cdot g_2^{r_i} \cdot Y_i^{H_i(m)})^{z_i}$.
   c. He computes $\sigma_t = \omega^{1/(x_t + r_t + y_t H_t(m))}$ with his secret keys (x_t, y_t).
   The signature is $\sigma = \{(\sigma_1, r_1), \cdots, (\sigma_n, r_n)\}$.
5. **RV.** On input a set of $\mathcal{L} = \{(X_1, Y_1), \cdots, (X_n, Y_n)\}$, a message m and $\sigma = \{(\sigma_1, r_1), \cdots, (\sigma_n, r_n)\}$, accept if $\prod_{i=1}^n [\hat{e}(\sigma_i, (X_i \cdot g_2^{r_i} \cdot Y_i^{H_i(m)}))] = \hat{e}(h, g_2)$.
6. **DRS.** On input the signature $\sigma = \{(\sigma_1, r_1), \cdots, (\sigma_n, r_n)\}$ on message m, the signature holder generates the designated verifier ring signature $\sigma' = \{(\sigma_1, A_1), \cdots, (\sigma_n, A_n), B_1, \cdots, B_n\}$, where $A_i = g_2^{r_i}$ and $B_i = \hat{e}(\psi(X_v), Y_v)^{r_i}$ if the designated verifier public key is (X_v, Y_v).
7. **DRV.** On input $\sigma' = \{(\sigma_1, A_1), \cdots, (\sigma_n, A_n), B_1, \cdots, B_n\}$, designated verifier's secret key (x_v, y_v) and a message m, accept if $\prod_{i=1}^n [\hat{e}(\sigma_i, (X_i \cdot A_i \cdot Y_i^{H_i(m)}))] = \hat{e}(h, g_2)$ and $\hat{e}(\psi(X_v), A_i)^{y_v} = B_i$.

4 Security Analysis

The correctness of the scheme is straightforward. Before prove the DV-unforgeability of the UDVRS, we first derive a new ring signature without random oracles from above UDVRS scheme.

The system parameters are also $\{\mathbb{G}_1, \mathbb{G}_2, \hat{e}, g_1, g_2, h, H_1, \cdots, H_n\}$ as defined in section 3.

1. **KeyGen.** For user i, on input security parameter 1^k, outputs $(x_i, y_i, X_i = g_2^{x_i}, Y_i = g_2^{y_i})$, where $(x_i, y_i) \in (\mathbb{Z}_p)^2$ and $(X_i, Y_i) \in (\mathbb{G}_2)^2$ are the secret key and public key of user i, respectively.
2. **RS.** On input a secret key (x_t, y_t), a message m and a set of public keys $\mathcal{L}$ including the one that corresponds to the private key (x_t, y_t), it signs as follows:
   a. For $i \in \{1, \cdots, n\} \backslash t$, he picks $z_i \in_R \mathbb{Z}_p^*$ and computes $\sigma_i = g_1^{z_i}$.
   b. For $i \in \{1, \cdots, n\}$, he picks $r_i \in \mathbb{Z}_p^*$. Then he computes
   $\omega = h/(\prod_{i \in \{1,\ldots,n\} \backslash t} \psi(X_i \cdot g_2^{r_i} \cdot Y_i^{H_i(m)})^{z_i}$.
   c. He computes $\sigma_t = \omega^{1/(x_t + r_t + y_t H_t(m))}$ with his secret keys (x_t, y_t).
   The signature is $\sigma = \{(\sigma_1, r_1), \cdots, (\sigma_n, r_n)\}$.
3. **RV.** On input a set of $\mathcal{L} = \{(X_1, Y_1), \cdots, (X_n, Y_n)\}$, a message m and $\sigma = \{(\sigma_1, r_1), \cdots, (\sigma_n, r_n)\}$, return 1 if $\prod_{i=1}^n [\hat{e}(\sigma_i, (X_i \cdot g_2^{r_i} \cdot Y_i^{H_i(m)}))] = \hat{e}(h, g_2)$. Otherwise, output 0.

Theorem 1. *The new ring signature scheme is existentially unforgeable if* (q, n)*-DsjSDH assumption holds in bilinear groups, and it also achieves signer-ambiguity against unconditional adversary.*

The new ring signature is a variant of [7,14]. However, if directly use the ring signature [7,14], it is hard to construct a UDVRS by using the construction method in our paper. The new ring signature without random oracles is different from [7,14] in RS and RV. However, it can also easily be proved to be secure without random oracles from the proof of [7].

Definition 5. *(Knowledge of Exponent Assumption*[4,16]*) Suppose that an adversary is given a pair* (g, h) *which is randomly chosen from uniform distribution of* $\mathbb{G}^2$ *and if the adversary is able to generate a pair* $(x, y) \in \mathbb{G}^2$ *such that* $log_g x = log_h y$*, then there exists an extractor that extracts* $log_g x$*.*

We can get the following security results. For the page limitation, reader can contact the author for full version of this paper if needed.

Theorem 2. *The UDVRS scheme achieves DV-unforgeability provided that the underlying ring signature is secure and knowledge of exponent assumption holds in bilinear groups.*

Theorem 3. *The UDVRS scheme achieves signer-ambiguity against unconditional adversary.*

Theorem 4. *The UDVRS scheme achieves non-transferability against unconditional adversary.*

5 UDVRSP

SYNTAX of UDVRSP. A UDVRSP consists of 6-tuple of poly-time algorithms (CPG, SKG, RS, RV, Transform, IVerify) defined as follows:

CPG- The common parameter generation algorithm, on input security parameter 1^k, outputs a string params consisting of common parameters of the scheme.
SKG- The signer key generation algorithm, on input params, outputs a public key pk_i and a secret key sk_i for the user.
RS- The ring signature generation algorithm, that takes as input a secret key sk_i, a message m and a set of public keys $\mathcal{L}$ including the one that corresponds to the private key sk_i, returns the signature σ.
RV- The ring signature verification algorithm, takes as input a set of $\mathcal{L}$, a message m and σ, returns 1 or 0 for accept or reject, respectively.
Transform- On input signature σ, it picks a secret mask sk' and generates a transformed signature σ'.
IVerify- This is an interactive verification protocol between a designator P and a designated verifier V. Common input for P and V are a set of public key $\mathcal{L}$, a transformed signature σ' and a message m. P's private input is sk'. V does not have any input. The output of this protocol is 1 or 0 depending V accepts or rejects.

The UDVRSP should satisfy correctness, unforgeability, and signer ambiguity. Definitions of unforgeability and signer ambiguity are the same with the ring signature.

Another essential security requirement is resistance against impersonation attack. This 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 IVerify protocol as a cheating designated verifier and interacts with an honest designator a number of times. The target of the attacker is 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 IVerify protocol. For more details, please refer to [2].

5.1 The UDVRSP Scheme

The algorithms CPG, SKG, RS, RV are the same with their corresponding algorithms in section 3.

- Algorithms **CPG, SKG, RS,** and **RV** are the same with corresponding algorithms in section 3.
- **Transform.** On input the signature $\sigma = \{(\sigma_1, r_1), \cdots, (\sigma_n, r_n)\}$ on message m, the signature holder chooses $z \in \mathbb{Z}_p^*$ and generates the transformed ring signature $\sigma' = \{(\sigma'_1, r_1), \cdots, (\sigma'_n, r_n)\}$, where $\sigma'_i = \sigma_i^z$ for $1 \leq i \leq n$.
- **IVerify.** On input $\sigma' = \{(\sigma'_1, r_1), \cdots, (\sigma'_n, r_n)\}$, both the designator P and designated verifier V compute $R_1 = \prod_{i=1}^{n} [\hat{e}(\sigma'_i, (X_i \cdot g_2^{r_i} \cdot Y_i^{H_i(m)}))] (= (\hat{e}(h, g_2))^z)$, and $R_2 = \hat{e}(h, g_2)$. Then they interactive as follows:
  a. P picks $s \in_R \mathbb{Z}_p^*$ and sends $U = R_2^s$ to V.
  b. V chooses $c \in_R \mathbb{Z}_p^*$. and sends it to P.
  c. P computes $t = s + cz \ mod \ p$ and sends t to V.
  d. V checks that if $R_2^t = U \cdot R_1^c$.

  If it holds, output 1. Otherwise, output 0.

As mentioned above, the UDVRSP scheme achieves signer-ambiguity and unforgeability from the corresponding properties in the standard ring signature.

Definition 6. *One More Discrete Logarithm Problem (OMDL Problem[2]): on input n+1 challenge elements* $y_1 = g_1^{x_1}, \cdots, h_{n+1} = g_1^{x_{n+1}} \in (\mathbb{G}_1)^{n+1}$, *provided to the discrete logarithm oracle at most n times, it is hard to output* $x_1, \cdots, x_{n+1}$ *for any PPT algorithm.*

Theorem 5. *The UDVRSP scheme is secure against impersonation under Type-1 attack assuming the OMDL problem is hard.*

Theorem 6. *The UDVRSP scheme is secure against impersonation under Type-2 attack assuming the underlying ring signature is secure.*

6 A Short DVS Without Random Oracles

A DVS consists of three algorithms: the key generation algorithm KeyGen, the designated verifier signature generation algorithm Sign, and the designated verification algorithm Verify.

The security requirements of DVS [8] are unforgeability and non-transferability.

It is known that DVS can be converted from ring signatures just by setting the size of the ring signature to two-user [8]. So, we construct the first DVS without relying on random oracles from the two-user ring signature in section 4.

The system parameters are the same with section 4.

1. **KeyGen.** For signer, it generates $(x_s, y_s, X_s = g_2^{x_s}, Y_s = g_2^{y_s})$, where $(x_s, y_s) \in (\mathbb{Z}_p)^2$ and $(X_s, Y_s) \in (\mathbb{G}_2)^2$ are the secret key and public key, respectively. For verifier, it generates $(x_v, y_v, X_v = g_2^{x_v}, Y_v = g_2^{y_v})$, where $(x_v, y_v) \in (\mathbb{Z}_p)^2$ and $(X_v, Y_v) \in (\mathbb{G}_2)^2$ are its secret key and public key, respectively.
2. **Sign.** The signer generates a designated verifier signature on message m for the specific verifier as follows: The signer takes a secret key (x_s, y_s), then
   a. The signer picks $z \in_R \mathbb{Z}_p^*$ and computes $\sigma_2 = g_1^z$.
   b. He also picks $r_1, r_2 \in \mathbb{Z}_p^*$ and computes $\omega = h/(\psi(X_v \cdot g_2^{r_2} \cdot Y_v^{H_2(m)})^z$.
   c. He computes $\sigma_1 = \omega^{1/(x_s + r_1 + y_s H_1(m))}$.

   The signature is $\sigma = \{(\sigma_1, r_1), (\sigma_2, r_2)\}$.
3. **Verify.** On input (X_s, Y_s), (X_v, Y_v), a message m and $\sigma = \{(\sigma_1, r_1), (\sigma_2, r_2)\}$, return 1 if $\hat{e}(\sigma_1, X_s \cdot g_2^{r_1} \cdot Y_s^{H_1(m)}) \cdot \hat{e}(\sigma_2, X_v \cdot g_2^{r_2} \cdot Y_v^{H_2(m)}) = \hat{e}(h, g_2)$. Otherwise, output 0.

From the existentially unforgeability and non-transferability of the underlying two-user ring signature, we can easily get the following results:

Theorem 7. *The DVS is existentially unforgeable if (q, n)-DsjSDH assumption holds in bilinear groups.*

Theorem 8. *The DVS achieves unconditional non-transferability.*

7 Conclusion

We first propose the notion of UDVRS. It not only allows members of a group to sign messages on behalf of the group without revealing their identities, but also allows the signature holder to designate a verifier. We give a formal and strong UDVRS security model. Then, a provably secure UDVRS scheme without random oracles is proposed in this paper, with rigorous proofs under the security model. To achieve our goal, we also present a variant ring signature scheme of [7,14]. Meanwhile, we also propose the concept of UDVRSP and construct a secure UDVRSP scheme in the standard model. Finally, a DVS without random oracles is first given in this paper.

References

1. M. Abe, M. Ohkubo, and K. Suzuki. 1-*out-of-n Signatures from a Variety of Keys*. AsiaCrypt 2002, LNCS 2501, pp. 415-432, Springer-Verlag, 2002.
2. J.Baek, R.S. Naini, and W. Susilo. *Universal designated verifier signature proof (or how to efficiently prove knowledge of a signature)*. AsiaCrypt'05, LNCS 3788, pp. 644-661, Springer-Verlag, 2005.
3. M. Bellare, D. Micciancio, and B. Warinschi. *Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions*. EuroCrypt 2003, LNCS 2656, pp. 614-629, Springer-Verlag, 2003.
4. M. Bellare and A. Palacio. *The Knowledge-of-Exponent Assumptions and 3-Round Zero-Knowledge Protocols*. In Crypt 2004, LNCS 3152, Springer-Verlag, 2004.
5. D.Boneh and X. Boyen. *Short Signatures Without Random Oracles*. In Eurocrypt 2004, LNCS 3027, pp. 56-73, Springer-Verlag, 2004.
6. E. Bresson, J. Stern, and M. Szydlo. *Threshold Ring Signatures and Applications to Ad-hoc Groups*. CRYPTO 2002, LNCS 2442, pp. 465-480, Springer-Verlag, 2002.
7. Sherman S. M. Chow, Joseph K. Liu, Victor K. Wei, Tsz H. Yuen. *Ring Signatures without Random Oracles*. To be appeared at AsiaCCS'06. Available at http://eprint.iacr.org/2005/317.
8. M. Jakobsson, K. Sako, and R. Impagliazzo. *Designated Verifier Proofs and Their Applications*. EuroCrypt 1996, LNCS 1070, pp. 143-154, Springer-Verlag, 1996.
9. M. Naor. *Deniable ring authentication*. Crypto 2002, LNCS 2442, pp. 481-498, Springer-Verlag, 2002.
10. R. L. Rivest, A. Shamir, and Y. Tauman. *How to Leak a Secret*. AsiaCrypt 2001, LNCS 2248, pp. 552-565, Springer-Verlag, 2001.
11. R. Steinfeld, L. Bull, H. Wang, and J. Pieprzyk. *Universal designated-verifier signatures*. AsiaCrypt 2003, LNCS 2894, pp. 523-542, Springer-Verlag, 2003.
12. R. Steinfeld, H. Wang, and J. Pieprzyk. *Efficient Extension of Standard Schnorr/RSA Signatures into Universal Designated-Verifier Signatures*. PKC 2004, LNCS 2947, pp. 86-100, Springer-Verlag, 2004.
13. W. Susilo and Y. Mu. *Non-Interactive Deniable Ring Authentication*. ICISC 2003, LNCS 2971, pp. 386-401, Springer-Verlag, 2004.
14. J. Xu, Z. Zhang, and D. Feng. *A Ring Signature Scheme Using Bilinear Pairings*. WISA 2004, LNCS 3325, pp. 163-172, Springer-Verlag, 2004.
15. F. Zhang and K. Kim, *ID-based blind signature and ring signature from pairings*, AsiaCrpt 2002, LNCS 2501, pp. 533-547, Springer-Verlag, 2002.
16. R. Zhang, J. Furukawa, and H. Imai. *Short Signature and Universal Designated Verifier Signature Without Random Oracles*. ACNS 2005, LNCS 3531, pp. 483-498, 2005.