A Novel Ring Signature Scheme with Multi-designated Verifiers

Jianhong Zhang
College of Sciences
North China University of Technology
Beijing, 100144 China
jhzhangs@163.com

Jianjun Xie
College of Mathematics and Information Science
Hebei Normal University,
Shijiazhuang 050016,China
jj_xie@sohu.com

***Abstract*—Ring signature is an anonymous signature which allows a user to anonymously sign on behalf of a group. In some cases, we only hope that our signatures were anonymously verified by the designated users, such as hospital records. In this works, by combining ring signature and designated verifier signature scheme, a ring signature scheme with Multi-designated verifiers are proposed to satisfy the multi-user setting. And by analyzing the security of scheme, we show that the proposed scheme is secure in a novel assumption: the Chosen-Target-Inverse-CDH problem under the random oracle model, and the corresponding security proof is given.**

***Index Terms*—ring signature, Chosen-Target-Inverse-CDH problem, designated verifier signature**

I. Introduction

Ring signature is an anonymous signature which allows a user to anonymously sign on behalf of a group, yet no one can know which the actual signer is. When verifying, the verifier only knows that the signature has been produced by some member of this ring, but he has no information about who is the actual author of the signature. The idea was first proposed in by Cramer *et al* [5] and the notion was formalized by Rivest *et al*[6]. After that, many proposals of ring signature schemes have been publish[7,8,9], for both PKI and ID-based scenarios. To adapt to different requirement, many variants of ring signature [10,11,12] were put forward, such as ring blind signature, linkable ring signature.

Ring signature scheme could be used for whistle blowing[16], anonymous membership authentication for ad hoc group [14,15] to keep the anonymity of the signer and can be publicly verifiable. However, in some cases, we wish to control the verification of signature, and make that only the member of the designated verifier group can verify signature valid.

Anonymity is an important property of ring signature, which makes ring signature play very important roles in electronic commerce. Generally speaking, a ring signature is able to provide full anonymity, which produces such a case, even if a member of the ring produces a signature δ, he also cannot prove that the signature δ was produced by himself. To address the problem above, we proposed a ring signature scheme with self-verification. If necessary, a member of the ring can verify the message-signature δ which was indeed produced by himself. The kind of ring signature is able to be applied to electronic auction. For example, in an anonymous electronic auction, when the bidder bids, he applies ring signature to produce an anonymous signature on his bidding to hide his identity. After the auction ends, the highest bidder wins. However, it gives us to bring up a problem: how does the a bidder prove that he is the highest one? The problem can been solved by our proposed ring signature scheme with self-verification.

By combining ID-based cryptography and ring signature, Zhang and Kim [14] proposed the first ID-based ring signature scheme. Subsequently, J.Herranz *et al* proposed a provable secure ID-based ring signature scheme [15]. Until now, many ID-based ring signature schemes and variants appear. The state-of-the-art can achieved a constant number of pairing computations [16,17] and also a constant size signature [8]. At present, in the existing ID-based ring signature scheme, a special hash function call *MapToPoint* function [3], which is used to map an identity information into a point on elliptic curve. This special function is a probabilistic and time consuming.

In the work, by combining ring signature and designated verifier signature scheme, a ring signature scheme with Multi-designated verifiers are proposed to satisfy the multi-user setting. And the proposed scheme is proven to be secure in a novel assumption: the Chosen-Target-Inverse-CDH problem. Finally, the security of the scheme is given in the random oracle model.

The rest of the paper is organized as follows. in Section 2, we recall the basic knowledges about bilinear pairing and the computational assumptions which underlie our scheme, and security model of ring signature scheme is given in section 3; our ring signature scheme is proposed in section 4 and the security of the scheme is formally proven in section 5. The conclusions of the work are given in section 6.

II. Preliminaries

Here, we review some fundamental backgrounds used throughout this paper, namely bilinear pairing, complexity assumption and the formal models of ring signature scheme with multi-designated verifiers .

A. Bilinear Pairing

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of a large prime order p. P is a generator of $\mathbb{G}_1$. The map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is said

978–1–4244–1674–5/08/$25.00 © 2008 IEEE

to be an admissible bilinear pairing if the following conditions hold:

- Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1$ and for all $a, b \in Z_p$;
- Non-degeneracy: There exists $P \in \mathbb{G}_1$ such that $e(P, P) \neq 1$.
- Computability: There is an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in \mathbb{G}_1$.

We say that $(\mathbb{G}_1, \mathbb{G}_2)$ are bilinear groups if there exists the bilinear pairing as above. See [3] for more details on the construction of such pairings.

Definition 1: (**Prime-order-BDH-parameter-generator**) A prime-order-BDH -parameter-generator is a probabilistic algorithm that takes on input a security parameter k, and outputs a $5-$tuple $(q, P, \mathbb{G}_1, \mathbb{G}_2, e)$ satisfying the following conditions: q is a prime with $2^{k-1} < q < 2^k$, $\mathbb{G}_1$ and $\mathbb{G}_2$ are two groups with the same order q, P be a generator of $\mathbb{G}_1$ and $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is an admissible bilinear map.

The Chosen-Target-Inverse-CDH problem is defined as follows: the solver $\mathcal{S}'$ receives as input a pair (P', aP'), where P' is a generator of $\mathbb{G}$ with prime order q, and $a' \in Z_q$ is a random value. The solver $\mathcal{S}'$ can adaptively access to the following two oracles:

- Target Oracle: this oracle outputs a random element $Z_i \in \mathbb{G}$
- Helper Oracle: this oracle takes as input an element $W_i \in \mathbb{G}$ and outputs the element $\frac{1}{a'} W_i$.

We say that the solver $\mathcal{S}$ can $(q_t, q_h, d)-$ solve the Chosen-Target-Inverse-CDH problem, for $q_t \geq d \geq q_h$, if it makes q_t and q_h queries, respectively, to the target oracle and helper oracles, and after that it outputs d pairs $((V_1, j_1), \cdots, (V_d, j_d))$ such that:

1) all the elements V_i are different;
2) for all $i \in \{1, 2, \cdots, d\}$, the relation $V_i = \frac{1}{a'} Z_{j_i}$ is satisfied, where Z_{j_i} is the element output by the target oracle in the $j_i - th$ query.

In [15], Herranz *et al* show that the Chosen-Target-CDH problem is equivalent to the Chosen-Target-Inverse-CDH problem.

III. Security Model

A ring signature scheme with multi-designated verifiers consists of the following five algorithms: RSMDVS.Setup, RSMDVS.SKeyGen , RSMDVS.VKenGen, RSMDVS.Sign and RSMDVS.Verify . Let n be the number of members in the signer group, m be the number of the designated-verifiers. The scheme is described as follows:

- Setup: It is a probabilistic algorithm which takes as input a security parameter k, and outputs the public parameters.
- SKeyGen: It is a probabilistic algorithm which takes as input the public parameters and a signer group list A_{inf}, and outputs a pair of keys (a_i, P_{A_i}) for $1 \leq i \leq n$, A_{inf} is the information of the members in the signer group.
- VKeyGen: It is a probabilistic algorithm which takes as input the public parameters and a signer group list B_{inf}, and outputs a pair of keys (b_i, P_{B_i}) for $1 \leq i \leq m$, B_{inf} is the information of the members in the designated verifier group.
- Sign: It is an algorithm which takes as input of a message M, the public keys of n members in the singer group, the public keys of m designated verifiers and an the secret key of a member, a_π, where $1 \leq \pi \leq n$; and outputs a signature δ on the message m.
- Verify: It is a deterministic algorithm which takes as inputs a signature δ, a message M , a secret key b_i of a designated verifier and the public keys of n members in the singer group, it outputs ”true” or ”false”, depending on whether δ is a valid signature signed by a certain member of the signer group.

Correctness. A ring signature scheme with multi-designated verifiers should satisfy *Verification Correctness* $-$ signatures signed by the signer are verified to be valid in the negligible probability, and only the designated verifier can verify a signature validity.

A. Security Requirement of the ID-based Ring Signature Scheme with multi-designated verifiers

For an ordinary signature scheme, the strongest security notion was defined by Goldwasser, Micali and Rivest in [9] as existential forgery against adaptive chosen-message attack (EF-CMA). In the RSMDVS setting, an EF-CMA-Adversary $\mathcal{A}$ has access to the n public key of the designated verifiers beside access to the random oracle and to a signing oracle. As $\mathcal{A}$ cannot verify a signature validity by himself. Here, we allow the attacker to corrupt up to $m - 1$ designated verifier (and to do so adaptively) during the attack, $i.e$ he has access to a corrupting oracle to obtain the secret information of the corresponding corrupted verifier. Therefore, he can verify validity of a signature by himself, and we omit the verifying oracle here.

Definition 2: (Security against existential forgery). Let L_B be a list of m designated verifiers, L_A be a list n signers, k and t be integers and ε be a real in $[0, 1]$, let $RSMDVS$ be ring signature scheme with security parameter k. Let $\mathcal{A}$ be an EF-CMA-adversary against multi-designated verifier signature scheme. We consider the following random experiment:

Anonymity. It is impossible for an adversary to guess the identity of the real signer with a probability larger than $1/n$, where n is the size of the ring, even if the adversary has unlimited computing power.

Definition 3:(Anonymity). An ID-based ring signature scheme is unconditional anonymous if for any group of n members with identity $\{ID_1, \cdots, ID_n\}$, any message m and signature δ, any adversary cannot identify the actual signer with probability better than random guess. That is, $\mathcal{A}$ can only output the identity of the actual signer with probability $1/n$.

IV. Our Proposed Ring Signature Scheme

In this section, we give a novel ring signature scheme with multi-designated verifier, which can make a designated group to verify a ring signature valid. The scheme is composed of five algorithms, SkyGen, VKeyGen, RSign and RVerify. Let k be a security parameter, for $i \in [1, \cdots, n]$, let A_i denote the signer i of the ring, B_i be the verifier i of the designated group. The detail scheme is described as follows:

[Setup:]
Let Gen be a prime-order-BDH-parameter-generator and $(q, P, \mathbb{G}, H, e)$ be the output of $Gen(k)$. H is a hash function which satisfies $H : \{0,1\}^* \times \mathbb{G}^{n+2} \rightarrow \mathbb{G}$.

[SkeyGen:]
For $i = 1$ to n, the member i of the ring randomly picks $a_i \in Z_q^*$ as the secret key of the signer A, and computes the corresponding public key $P_{A_i} = a_i P$.

[VKeyGen:]
it randomly picks $b_i \in Z_q^*$ as the secret key of the designated verifier B_i, and computes his public key $P_{B_i} = b_i P$.

[RSign:]
Given a message m, the verifier group B and the signer list L, let the signer be index $\pi \in [1, n]$, then the signer A_π computes as follows:

1) compute $P_B = P_{B_1} + \cdots + P_{B_n}$.
2) randomly choose $r \in Z_q$ and set $Y_{B_i} = rP_{B_i}$ for all $i \in [1, \cdots, n]$.
3) for $j = 1, 2, \cdots, \pi - 1, \pi + 1, \cdots, n$, the signer A_i randomly selects $l_j \in Z_p$ to compute $Q_{A_j} = l_j P$
4) Then, the signer A_π randomly selects $r' \in Z_q$ to $Q_B = r'P$.
5) Finally, it computes

$$M = H(m, L_A, L_B, Y, Q_B) \qquad (1)$$

and

$$Q_{A_\pi} = a_\pi^{-1}(M - r'P_B - \sum_{j=1, j\neq i}^{n} l_j P_{A_j}) \qquad (2)$$

where $L_A = A_1 || \cdots || A_n$ and $L_B = Y_{B_1} || \cdots || Y_{B_n}$

The resultant signature is

$$\sigma = (Q_{A_1}, \cdots, Q_{A_n}, Q_B, Y_{B_1}, \cdots, Y_{B_n})$$

[RVerify:]
Given a signature σ on the message m, each designated verifier B_i retrieves $Y = rP$ as $b_i^{-1} Y_{B_i}$ by his secret key. Firstly, for $j \in [1, \cdots, n] \setminus \{i\}$, it verifies whether $e(P_{B_j}, Y) = e(Y_{B_j}, P)$ holds. If they are valid, then it computes $M = H(m, P_A, P_{B_1}, \cdots, P_{B_n}, Y)$ and checks whether

$$e(M, P) = \prod_{i=1}^{n} e(Q_{A_i}, P_{A_i}) \cdot e(Q_B, P_B) \qquad (3)$$

In the following, we show that our proposed scheme satisfies correctness.

$$\begin{aligned}
& e(Q_B, P_B) \prod_{j=1}^{n} e(Q_{A_j}, P_{A_j}) = e(Q_B, P_B) \prod_{j=1}^{n} e(Q_{A_j}, P_{A_j}) \\
= \; & e(r'P, P_B) e(Q_{A_i}, P_{A_i}) \prod_{j=1, j\neq i}^{n} e(Q_{A_j}, P_{A_j}) \\
= \; & e(M, P) e(-\sum_{j=1, j\neq i}^{n} l_j P_{A_j}, P) \prod_{j=1, j\neq i}^{n} e(Q_{A_j}, P_{A_j}) \\
= \; & e(M, P) \prod_{j=1, j\neq i}^{n} e(P_{A_j}, Q_{A_j})^{-1} \prod_{j=1, j\neq i}^{n} e(Q_{A_j}, P_{A_j}) \\
= \; & e(M, P)
\end{aligned}$$

V. Security Analysis

In the section, we will prove that our proposed ring signature scheme is unconditional anonymous and existentially unforgeable under a chosen message in the random oracle.

Theorem 1: Our proposed scheme is unconditional anonymous.

Proof: Given a ring signature $(\sigma = (Q_{A_1}, \cdots, Q_{A_n}, Q_B, Y_{B_1}, \cdots, Y_{B_n}))$, Q_{A_i}, $i \in [1, n] \backslash \pi$ and Q_B are randomly generated which provide no information on the actual signer. While n random numbers, $r', l_1, \cdots, l_{\pi-1}, l_{\pi+1}, \cdots, l_n$ are included in the $Q_{A_\pi} = a_\pi^{-1}(M - r'P_B - \sum_{j=1, j\neq i}^{n} l_j P_{A_j})$, thus, Q_{A_π} is also randomly distributed. $Y_{B_1}, \cdots, Y_{B_n}$ are some information on the verifiers, and they have not provide any information on the actual signer and a random number r is contain among them. All of them provide no information on the actual signer. It is no better for an adversary to do a wild guess. Thereby, our proposed scheme is unconditional anonymous. □

Theorem 2: If there is an adversary $\mathcal{A}$ which is able to $(\epsilon, q_t, q_s)-$ break our proposed scheme with a non-negligible probability, then the CDH problem can be solved with non-negligible probability in polynomial time.

Proof: Supposed that there is a $(\epsilon, q_h, q_s)-$adversary $\mathcal{A}$ exists. We are going to construct a PPT solver $\mathcal{S}'$ of the Chosen-Target-Inverse-CDH problem that makes use of $\mathcal{A}$ to solve the Chosen-Target-Inverse-CDH problem in non-negligible probability. Firstly, $\mathcal{S}'$ chooses a security parameter k, a list L_A of users and a list L_B of designated verifiers to initialize $\mathcal{A}$. And the solver $\mathcal{S}'$ selects a group $\mathbb{G}_1$ with prime order $q > 2^k$ which admits a bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$.

The solver $\mathcal{S}'$ is given an instance (P, Y) of the Chosen-Target-Inverse-CDH problem in the group $\mathbb{G}_1$, where $Y = aP$ and $a \in_R Z_q$ is an unknown random number. It is also provided with access to the target oracle and the helper oracle.

For every user of the list L_A, the solver $\mathcal{S}'$ chooses a random value $\alpha_i \in Z_q$ and sets his public key to be $P_{A_i} = a_i Y$. To reduce the proof, we randomly choose a designated verifier B_{i_0} and replace his public key by $\omega Y - \sum_{i\neq i_0}^{n-1} P_{B_i}$, where $l_0 \in Z_q$.

If B_{i_0} is among the corrupted verifiers, then the reduction is aborted.

Finally, the solver $\mathcal{S}'$ sends to $\mathcal{A}$ the public parameters $(q, P, \mathbb{G}_1 =< P >, \mathbb{G}_2, e)$, the public keys P_{A_i} of the users in the list L_A and the public keys of P_{B_i} of designated verifiers in the list L_B. And provide it with access to a random oracle for a hash function $H : \{0,1\}^* \to \mathbb{G}_1^*$.

Hash Oracles: When the adversary $\mathcal{A}$ queries $(m_i, L_A, L_B, Y_i, Q_{B_i})$ for hash oracle, the solver $\mathcal{S}'$ maintains a H-list where it stores the following relations $H(m_i, L_A, L_B, Y_i, Q_{B_i}) = Z_i$ which it is computed as follows:

- if a query $(m_i, L_A, L_B, Y_i, Q_{B_i})$ exists in the H-list, then $\mathcal{S}'$ returns Z_i to $\mathcal{A}$.
- Otherwise, $\mathcal{S}'$ makes a query to its target oracle and receives a random answer $Z_i \in \mathbb{G}_1$. Then, it stores the new relation $H(m_i, L_A, L_B, Y_i, Q_{B_i}) = Z_i$ in the H-list and sends Z_i to the forger $\mathcal{A}$.

Ring Signing Oracles: For a given query of a signature on the list L_A, the designated verifiers list L_B and a message m_i ($\mathcal{A}$ makes at most q_s signing queries; m_i is only queried for Ring Signing Oracle once), the solver $\mathcal{S}'$ responds as follows:

- choose at random an index $\pi \in \{1, 2, \cdots, n\}$
- for $i \in \{1, \cdots, n\}$, $i \neq \pi$, the solver randomly chooses $l_{\pi_i} \in Z_q$ to compute $Q_{A_i} = l_{\pi_i} P$
- compute $P_B = \sum_{i=0}^{n-1} P_{B_i} = P_{B_0} + \sum_{i=1}^{n-1} P_{B_i} = \omega Y$
- the solver $\mathcal{S}'$ first checks whether the hash query of M_i exists in the H-list. If it exists, then (Z_i, L_B) is returned. Otherwise, It randomly chooses $r_i, r_i' \in Z_q$ to compute $Y_i = r_i P, Q_{B_i} = r_i' P$ and $L_B = Y_{B_1} || \cdots || Y_{B_n}$ where for $j = 1$ to n, $Y_{B_j} = r_i P_{B_j}$. It makes a query to its target oracle, and receives a random element $Z_i \in \mathbb{G}_1$ as answer, then stores $H(m_i, L_A, L_B, Y_i, Q_{B_i}) = Z_i$ in the H-list.
- it sends Z_i to the helper oracle and obtains the corresponding return $\beta_i = a^{-1} Z_i$.
- Finally, it computes $Q_{A_\pi} = \beta_i - \omega Q_{B_i} - \sum_{j=1, j\neq\pi}^{n} l_{\pi_j} a_j P$ and returns $(Q_{A_1}, \cdots, Q_{A_n}, Q_{B_i}, L_A, L_B)$ as the resultant signature on m_i. Obviously, this is a valid ring signature, the simulation is indistinguishable from a real execution of the protocol. Since

$$\begin{aligned} Q_{A_\pi} &= \beta_i - \omega Q_{B_i} - \sum_{j=1, j\neq\pi}^{n} l_{\pi_j} a_j P \\ &= a^{-1}(a\beta_i - \omega a Q_{B_i} - \sum_{j=1, j\neq\pi}^{n} l_{\pi_j} a_j a P) \\ &= a^{-1}(Z_i - \omega a r_i' P - \sum_{j=1, j\neq\pi}^{n} l_{\pi_j} a_j Y) \\ &= a^{-1}(Z_i - r_i' P_B - \sum_{j=1, j\neq\pi}^{n} l_{\pi_j} P_{A_j}) \end{aligned}$$

where $Z_i = H(m_i, L_A, L_B, Y_i, Q_{B_i})$

Output: Finally, $\mathcal{A}$ returns a message m^* with a forged ring signature $\sigma = (Q_{A_1}^*, \cdots, Q_{A_n}^*, Q_B^*, Y_{B_1}^*, \cdots, Y_{B_n})$ in non-negligible probability ϵ. If m^* is not queried for **Ring Signing Oracles** and m^* has queried **Hash Oracles**. We look up m^* in the H-list and $Z^* = H(m^*, L_A^*, L_B, Y^*, Q_B^*)$ is returned. (Note that Z^* is a returned answer by helper oracle, when the solver $\mathcal{S}'$ queried target oracle with $(m^*, L_A^*, L_B, Y^*, Q_B^*)$). Then we can solve

$$\beta^* \quad = \quad a^{-1} Z^* = Q_{A_\pi}^* - \omega Q_B^* - \sum_{j=1, j\neq\pi}^{n} a_j Q_{A_j}^*$$

the $q_s + 1$th pair is (Z^*, β^*). Thus, for $i = 1, \cdots, q_s + 1$, the solver $\mathcal{S}'$ outputs the pair (β_i, i), where $\beta_i = a^{-1} Z_i$. The probability that $\mathcal{A}$ obtains a valid ring signature for the message m_i without querying the hash function H is $1/q$. Therefore, we have that with probability $1 - \frac{q_s+1}{q}$ the forger $\mathcal{A}$ has queried the random oracle with $(m_i, L_A, L_B, Y_i, Q_{B_i})$ for the $q_s + 1$ forged pairs. According to the statement above, the solver $\mathcal{S}'$ makes q_h queries to its target oracle, makes $q_s < q_h$ queries to its helper oracle, while it outputs $q_s + 1$ valid pair (β_i, i) with probability $\epsilon' > \epsilon - \frac{q_s+1}{q}$. □

VI. Conclusion

As a special signature, ring signature is an anonymous signature which allows a user to anonymously sign on behalf of a group. In real life, we often work in the multi-user setting and hope only the designated users can check our signatures, such as hospital records. In the work, by combining ring signature and designated verifier signature scheme, a ring signature scheme with Multi-designated verifiers are proposed to satisfy the multi-user setting. And the proposed scheme is proven to be secure in a novel assumption: the Chosen-Target-Inverse-CDH problem under the random oracle model.

Acknowledgement

This work is supported by Natural Science Foundation of China (NO:60703044,90604010), the New Star Plan Project of Beijing Science and Technology (NO:2007B001), the PHR, Program for New Century Excellent Talents in University(NCET-06-188), The Beijing Natural Science Foundation Programm and Scientific Research Key Program of Beijing Municipal Commission of Education (NO:KZ2008 10009005) and 973 Program (No:2007CB310700).

References

[1] D.Chaum and H.van Antwerpen. Undeniable Signatures. Crypto'89, LNCS 435, pp 212-216, springer-verlag, Berlin, 1990.

[2] M.Jakobsson, K.sako,and R.Impagliazzo. Designated Verifier Proofs and Their Applications. Eurocrypt'96, LNCS 1070, pp 143-154, Springer-verlag, Berlin, 1996.

[3] F.Laguillaumie, D.Vergnaud, Designated verifier signatures: Anonymity and Efficient Construction from any Bilinear Map, SCN'04, Lecture Notes in Computer science 3352,pp 107-121, 2005

[4] R.Steinfeld, L.Bull, H.Wang and J.Pieprzyk. Universal Designated Verifier Signatures. Proc. of Asiacrypt'03, Springer LNCS Vol.2894, 523-542.

[5] R.Steinfeld, H.Wang and J.Pieprzyk.Efficient Extension of Standard Schnorr/RSA signatures into Universal Designated-verifier Signature. Proc.of PKC 2004, Springer LNCS vol.2947, pp 86-100, 2004

[6] W.Ogata, K.Kurosawa, and S.H. Heng,The security of the FDH variant of Chaums Undeniable Signature Scheme. PKC 2005, LNCS vol.3385, pp 328-345, Springer, 2005.

[7] Xinyi Huang, Willy Susilo, Yi Mu, Futai Zhang: Short (Identity-Based) Strong Designated Verifier Signature Schemes. ISPEC 2006, LNCS 3903, 214-225, 2006

[8] H.Lipmaa, G.Wang and F.Bao. Designated verifier Signature Scheme: Attacks, New Security Notions and A New Construction. ICALP 2005, LNCS 3580, pp 459-471, Springer, Berlin, 2005

[9] S.Goldwasser, S.Micali, R.L.Rivest: A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal of Computing, Vol17(2) 281-308 (1998).

[10] Tatsuaki Okamoto, Efficient Blind and Partially Blind Signatures Without Random Oracles , TCC 2006, LNCS 3876, Springer-verlag, Berlin, 80-99, 2006

[11] S.Saeednia,S.Kramer, and O.Markovitch. An Efficient Strong Designated Verifier Signature Scheme. ICISC 2003, LNCS 2894,pp 40-53, Springer, Berlin, 2003

[12] W.Susilo, F.Zhang, and Y.Mu. Identity-based Strong Designated Verifier Signature Schemes. ACISP 2004, LNCS 3108, pp 313-324, Springer, Berlin, 2004

[13] Fabien Laguillaumie, Benoit Libert, and Jean-Jacques Quisquater, Universal Designated Verifier Signatures without Random Oracles or Assumptions, To appear in Proc. of SCN'06. Springer LNCS (2006)

[14] 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.

[15] M.Abe, M.Ohkubo, and K.Suzuki. 1-out-of-n Signatures from a Variety of Keys. AsizCrypt 2002, LNCS 2501, pp 415-432, Springer-verlag, 2002.

[16] R.L.Rivest, A.Shamir, and Y.Tauman, How to leak a Secret. AsiaCrypt'2001, LNCS 2248,pp 552-565, Springer-Verlag, 2001.