Identity-based Threshold Signature Secure in the Standard Model

Hu Xiong, Zhiguang Qin, and Fagen Li
(Corresponding author: Hu Xiong)

School of Computer Science and Engineering, University of Electronic Science and Technology of China
No. 4, Section 2, North Jianshe Road, Chengdu, 610054, China (Email: xionghu.uestc@gmail.com)
(Received Sept. 18, 2008; revised and accepted Feb. 5, 2009)

Abstract

Recently, design of Identity-based (ID-based) threshold signature schemes which are efficient and provably secure in the standard model has drawn great concerns. In this paper, an ID-based threshold signature scheme based on Paterson and Schuldt's signature scheme is presented. The proposed construction is proved secure in the standard model and its security rests on the hardness of the computational Diffie-Hellman problem. To the best of authors' knowledge, this is the first ID-based threshold signature scheme in the literature to achieve this security level.

Keywords: Identity-based threshold signature, provable security, standard model

1 Introduction

Digital signatures can be produced by a group of players rather than by one party using a threshold signature scheme. In contrast to the regular signature schemes where the signer is a single entity which holds the secret key, in (k, n)-threshold signature schemes the secret key is shared by a group of n players. In order to produce a valid signature on a given message m, individual players produce their partial signatures on that message, and then combine them into a full signature on m. A distributed signature scheme achieves threshold k, if no coalition of $k-1$ (or less) players can produce a new valid signature, even after the system has produced many signatures on different messages. A signature resulting from a threshold signature scheme is the same as if it was produced by a single signer possessing the full secret signature key [13, 14, 16]. The first threshold secret sharing schemes, based on the Lagrange interpolating polynomial and linear project geometry, were proposed by Shamir [22] and Blakley [6], respectively. After that, threshold cryptography and secret sharing have been given considerable attention [8, 11, 24].

Identity Based Encryption (IBE) provides a public key encryption mechanism where a public key is an arbitrary string such as an email address or a telephone number. The corresponding private key can only be generated by a Private Key Generator (PKG) who has knowledge of a master secret. In an IBE system, users authenticate themselves to the PKG and obtain private keys corresponding to their identities. This eliminates the need for certificates as used in a traditional public key infrastructure. Although Shamir [23] proposed the idea of Identity based encryption in 1984, no construction that was both efficient and secure was found until recently, when the work of Boneh and Franklin [7] and Cocks [10] was published. Since then, a large number of papers have been published in this area, including several direct constructions of identity-based signature scheme.

ID-based threshold signature, the combination of ID-based cryptography and threshold signature schemes, has rapidly emerged in recent years and been well-studied as well. Baek and Zheng [2] suggested a new approach for ID-based threshold decryption in which the private key associated with an identity rather than the master key of PKG is shared. Moreover, they [3] first proposed an ID-based threshold signature without distributed PKGs. Chen *et al.* [9] proposed a new ID-based threshold signature scheme by combining the advantages of both Certificate-based public key cryptography and ID-based public key cryptography. All of these schemes are proved to be secure in the random oracle model [4]. However, several papers proved that some popular cryptosystems previously proved secure in the random oracle are actually provably insecure when the random oracle is instantiated by any real-world hashing functions [5]. Therefore, provably secure identity-based threshold signature scheme in the standard model attracts a great interest.

To the best of our knowledge, though Wang *et al.* [26] and Li *et al.* [15] proposed two secure threshold signature schemes without random oracles respectively, ID-based threshold signature secure in the standard model has not been treated in the literature. Our current work is aimed at filling this void. An efficient ID-based threshold signature scheme, which is secure in the standard model (without random oracles), is proposed in our paper. Our

scheme is based on Paterson and Schuldts' scheme [17], which was a extension of Waters's scheme [27]. Meantime, the proposed scheme is proved to be secure under the computational Diffie-Hellman assumption. This assumption seems more natural than many of the hardness assumptions recently introduced to pairing based cryptography.

The remainder of this paper is organized as follows. A brief review of some basic concepts and tools used in our scheme is described in Section 2. The proposed ID-based threshold signature scheme is given in Section 3. The security of our scheme is analyzed in Section 4. Finally, the conclusions are given in Section 5.

2 Preliminaries

2.1 Security Definitions and Notations

An identity-based (k, n)-threshold signature scheme consists of algorithms (Setup, Distributing-Extract, Sign, Verify). These algorithms are specified as follows.

Setup. On input a security parameter, this algorithm generates and publishes the public parameters params of the scheme.

Distributing-Extract. Given an identity u and params, n PKGs jointly generate the private key share d_u^i and verification key share to signer i such that the values $(d_u^1, \cdots, d_u^n)$ form a (k, n)-threshold secret sharing of d_u, where d_u is the private key of u. PKGs will use this algorithm to generate private key shares for all entities participating in the scheme and send the private key shares to their respective owners through a secure channel.

Sign. Given a message m, an identity u, params and Φ different secret shares $\{d_i\}_{i\in\Phi}$, where $\Phi \subset \{1, 2, \cdots, n\}$ is a set and $|\Phi| \geq k$, this algorithm generates the signature σ of u on m.

Verify. Given a signature σ, a message m, an identity u and params, this algorithm outputs accept if σ is a valid signature on m for identity u, and outputs reject otherwise.

Existential Unforgeability. The following EUF-IDTHS-CMIA2 game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ formally defines the existential unforgeability of ID-based threshold signature under adaptive chosen-message-and-identity attack.

EUF-IDTHS-CMIA2 Game:

Setup. The challenger runs the algorithm **Setup** of the signature scheme and obtains the public parameters *params*, then the challenger sends it to the adversary.

Queries. The adversary adaptively makes a number of different queries to the challenger. Each query can be one of the following.

- Distributing-Extract oracle. The adversary $\mathcal{A}$ can ask for all of the private key shares of any identity u. The challenger responds by running **Distributing-Extract(params,u)** and forwards the private key shares $(d_u^1, \cdots, d_u^n)$ to the adversary.
- Sign oracle. $\mathcal{A}$ can ask for the signature of any identity u on any message m, with a threshold value k' where $k' \leq n$. Furthermore, $\mathcal{A}$ corrupts $k' - 1$ players and obtains the secret key shares of the corrupted players, along with the public key and verification key. $\mathcal{C}$ outputs a (k', n) ID-based threshold signature σ of identity u on message m. The Sign oracle may query the Extract oracle during its operation.

Forgery. The adversary $\mathcal{A}$ outputs a message m^*, an identity u^* and a string σ. The adversary succeeds if the following hold true:

1) $Verify(params, u^*, m^*, \sigma^*, n, k') = accept$.
2) (m^*, u^*, n, k') does not appear in the set of previous sign oracles.
3) u^* does not appear in the set of previous Distributing-Extract oracles.

The advantage of an adversary $\mathcal{A}$ is defined as the probability that it wins.

Definition 1. *An adversary $\mathcal{A}$ is said to be an (ϵ, t, q_e, q_s)-forger of an identity-based threshold signature scheme if $\mathcal{A}$ has advantage at least ϵ in the above game, runs in time at most t, and makes at most q_e and q_s distributing-extract and sign oracles queries, respectively. A scheme is said to be (ϵ, t, q_e, q_s)-secure if no (ϵ, t, q_e, q_s)-forger exists.*

Note that the above game can easily be extended to cover strong unforgeability [1] by changing the second requirement in the forgery stage to "the forged signature was not output as a response to a sign query". However, our concrete scheme does not enjoy security in this stronger sense, as an adversary can easily modify an existing signature on a message into a new signature on the same message.

2.2 Bilinear Pairing and Complexity Assumption

We briefly review the facts about groups with efficient computable bilinear maps [7]. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of prime order p. Let g be a generator of $\mathbb{G}_1$, and $\hat{e}$ be a bilinear map such that $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ with the following properties:

Bilinearity. For all $u, v \in \mathbb{G}_1$, and $a, b \in \mathbb{Z}$, $\hat{e}(u^a, v^b) = \hat{e}(u, v)^{ab}$.

Non-degeneracy. $\hat{e}(g, g) \neq 1$.

Computability. It is efficient to compute $\hat{e}(u, v)$ for all $u, v \in \mathbb{G}_1$.

The security of our signature scheme will be reduced to the hardness of the computational Diffie-Hellman (CDH) problem in the group in which the signature is constructed. We brief review the definition of the CDH problem.

Definition 2. *Given a group $\mathbb{G}$ of prime order p with generator g and elements $g^a, g^b \in \mathbb{G}$ where a, b are selected uniformly at random from $\mathbb{Z}_p^*$, the CDH problem in $\mathbb{G}$ is to compute g^{ab}.*

3 Proposed Scheme

3.1 Construction

Motivated by Gennaro et al.'s [12] distributed key generation, we propose an identity-based (k, n)-threshold signature scheme which is secure in the standard model in this section. Our scheme consists of the following four algorithms: Setup, Distributing-Extract, Sign, and Verify.

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of prime order p. Let g and h be generators of $\mathbb{G}_1$ where $\log_g h$ is unknown, and $\hat{e}$ be a bilinear map such that $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. In the following all identities and messages will be assumed to be bit strings of length n_u and n_m, respectively. To construct a more flexible scheme which allows identities and messages of arbitrary lengths, collision-resistant hash functions, $H_u : \{0,1\}^* \rightarrow \{0,1\}^{n_u}$ and $H_m : \{0,1\}^* \rightarrow \{0,1\}^{n_m}$, can be defined and used to create identities and messages of the desired length.

Setup. Choose $g_2 \leftarrow_R \mathbb{G}_1$. Furthermore, pick elements $u', m' \leftarrow_R \mathbb{G}_1$ and vectors $\mathbf{U} = (u_i), \mathbf{M} = (m_i)$ of length n_u and n_m, respectively, whose entries are random elements from $\mathbb{G}_1$. The public parameters are params=$(\mathbb{G}_1, \mathbb{G}_2, \hat{e}, g, h, g_2, u', \mathbf{U}, m', \mathbf{M})$.

Distributing-Extract. Let u be a bit string of length n_u representing an identity and let $u[i]$ be the ith bit of u. Define $\mathcal{U} \subset \{1, \ldots, n_u\}$ to be the set of indices i such that $u[i] = 1$.

1) In order to generate a private key $d_u = (d_{u1}, d_{u2}) = (g_2^{\alpha}(u' \prod_{i \in \mathcal{U}} u_i)^r, g^r)$, each private key generator PKG_i performs interactively as follows:
   a. PKG_i chooses two random polynomials $f_i(z)$ and $g_i(z)$ over Z_p of degree $k-1$: $f_i(z) = a_{i0} + a_{i1}z + \cdots + a_{i,k-1}z^{k-1}$, $g_i(z) = b_{i0} + b_{i1}z + \cdots + b_{i,k-1}z^{k-1}$. Let $z_i = a_{i0} = f_i(0)$. PKG_i broadcasts $C_{it} = g^{a_{it}}h^{b_{it}} \bmod p$ for $t = 0, \cdots, k-1$. PKG_i computes the shares $s_{ij} = f_i(j)$, $s'_{ij} = g_i(j) \bmod p$ for $j = 1, \cdots, n$ and sends s_{ij}, s'_{ij} to PKG_j.
   b. Each PKG_j verifies the shares he received from the other PKGs. For each $i = 1, \cdots, n$, PKG_j checks if $g^{s_{ij}}h^{s'_{ij}} = \prod_{t=0}^{k-1}(C_{it})^{j^t} \bmod p$. If the verification is not passed, then PKG_j broadcasts a complaint to PKG_i.
   c. Each PKG_i who received a complaint from PKG_j broadcasts the values s_{ij}, s'_{ij}. Otherwise, PKG_i is disqualified.
   d. The distributed master secret α is not explicitly computed by any party, but it equals $\alpha = \sum_{i=1}^{n} z_i \bmod p$. Each PKG_i sets his secret share as $\alpha_i = \sum_{i=1}^{n} s_{ji} \bmod p$ and the value $r_i = \sum_{i=1}^{n} s'_{ji} \bmod p$. Then PKG_i computes the secret key share $d_u^i = (d_{u1}^i, d_{u2}^i) = (g_2^{\alpha_i}(u' \prod_{i \in \mathcal{U}} u_i)^{r_i}, g^{r_i})$ and transmits to signer i secretly.
2) PKGs generate the public key $Y(= \hat{e}(g_2, g)^{\alpha})$ and verification key share $B_i(= \hat{e}(g_2, g)^{\alpha_i})$ for $i = 1, \cdots, n$.
   a. Each PKG_i broadcasts $A_{it} = \hat{e}(g_2, g)^{a_{it}} \bmod p$ for $t = 0, \cdots, k-1$.
   b. PKG_j verifies the values broadcast by the other PKGs, PKG_j checks if $\hat{e}(g_2, g)^{s_{ij}} = \prod_{t=0}^{k-1}(A_{it})^{j^t} \bmod p$ for $i = 1, \cdots, n; i \neq j$. If the check fails for an index i, PKG_j complains against PKG_i by broadcasting the values s_{ij}, s'_{ij}.
   c. Each PKG_i can compute and publish public parameter $Y = \prod_{j=1}^{n} A_{j0} \bmod p$ and $B_l = \hat{e}(g_2, g)^{\alpha_l} = \prod_{j=1}^{n}\prod_{t=0}^{k-1}(A_{jt})^{l^t} \bmod p$ $(l = 1, \cdots, n)$.

Sign. Let u be the bit string of length n_u representing a signing identity and let m be a bit string representing a message. Furthermore, let $\mathcal{U}$ be the set of indices i such that $u[i] = 1$, and $\mathcal{M} \subset \{1, \ldots, n_m\}$ be the set of indices j such that $m[j] = 1$, where $m[j]$ is the jth bit of m.

After receiving the secret key share $d_u^i = (d_{u1}^i, d_{u2}^i)$ from PKG_i, signer i checks if the following equations holds:

$$\hat{e}(d_{u1}^i, g) = \hat{e}(d_{u2}^i, u' \prod_{l \in \mathcal{U}} u_l) \cdot B_i.$$

If the check fails, signer i broadcasts a complaint against PKG_i. Otherwise, signer i picks $r_m^i \in_R \mathbb{Z}_p$ to generate a signature share of u on message m:

$$\begin{aligned} \sigma_i &= (d_{u1}^i (m' \prod_{k \in \mathcal{M}} m_k)^{r_m^i}, d_{u2}^i, g^{r_m^i}) \\ &= (g_2^{\alpha_i}(u' \prod_{l \in \mathcal{U}} u_l)^{r_i}(m' \prod_{k \in \mathcal{M}} m_k)^{r_m^i}, g^{r_i}, g^{r_m^i}) \\ &= (V_i, R_{ui}, R_{mi}) \in \mathbb{G}_1^3. \end{aligned}$$

Verify.

1) On input partial signature $\sigma_i = (V_i, R_{ui}, R_{mi})$, verification key B_i, the verifier checks if the following equations holds:

$$\hat{e}(V_i, g) = B_i \cdot \hat{e}(u' \prod_{l \in \mathcal{U}} u_l, R_{ui}) \cdot \hat{e}(m' \prod_{k \in \mathcal{M}} m_k, R_{mi})$$

Output 1 if it is valid. Otherwise, output 0.

2) Let $\lambda_1, \ldots, \lambda_k \in \mathbb{Z}_p$ be the Lagrange coefficients so that $\alpha = f(0) = \sum_{i=1}^{k} \lambda_i \alpha_i$. Assuming that there are $|\Phi|$ valid signature shares $\sigma_i = (V_i, R_{ui}, R_{mi})$, where $|\Phi| \geq k$. Without loss of generality we assume that signer $i = 1, \ldots, k$ were used to generate the shares. The signature of u on message m can be computed as

$$\sigma = (\prod_{i=1}^{k} (V_i)^{\lambda_i}, \prod_{i=1}^{k} (R_{ui})^{\lambda_i}, \prod_{i=1}^{k} (R_{mi})^{\lambda_i}).$$

3) Given a signature $\sigma = (V, R_u, R_m)$ on message m of u, it checks if the following equation holds:

$$\hat{e}(V, g) = Y \cdot \hat{e}(u' \prod_{l \in \mathcal{U}} u_l, R_u) \cdot \hat{e}(m' \prod_{k \in \mathcal{M}} m_k, R_m).$$

Output 1 if it is valid. Otherwise, output 0.

3.2 Efficiency

So far as we know, there are only a few threshold signature schemes [15, 26] secure in the standard model. However, the scheme in [26] is very inefficient since it requires the signers generate signature shares interactively. Therefore, we compare the efficiency of our scheme with the scheme in [15]. The comparison is shown in Table 1. Here we only consider the costly operations and we omit the computation efforts which can be pre-computed by the signer in the **Sign** and **Verify** phase. We denote by P a pairing operation, by S a multiplication in $\mathbb{G}_1$, by E an exponentiation in $\mathbb{G}_1$.

The comparison shows that in the signature share generation algorithm in our scheme requires at most $n_m + 1$ multiplications in $\mathbb{G}_1$ ($(n_m+1)/2+1$ on average), two pairing computations and two exponentiations in $\mathbb{G}_1$ for each signer. Verification requires at most $(n_m + n_u)$ multiplications in $\mathbb{G}_1$ ($(n_m+n_u)/2+1$ on average) and three pairing computations. The signature share generation in [15] requires only two exponentiation computation for each signer and, two pairing computations and n_m multiplications in $\mathbb{G}_1$ in verification. Thus, our scheme is slightly more expensive than Li et al's scheme. However, to the best of author's knowledge, our scheme is the first ID-based threshold signature secure in the standard model, while the other ones are build in the traditional PKI.

4 Proof of Security

Definition 3 ([3]). *A (k, n) ID-based threshold signature scheme is said to be robust if it computes a correct output even in the presence of a malicious attacker that makes the corrupted signers deviate from the normal execution.*

Motivated by Gennaro et al.'s [12] idea for proving the security of the threshold DSS signature scheme, Baek and Zheng [3] defined Simulatability of the ID-based threshold signature and proved the relationship between the security of ID-based threshold signature and that of ID-based signature.

Definition 4 ([3]). *An (k, n) ID-based threshold signature scheme is said to be simulatable if the following conditions hold.*

1) *"Distributed key generation" is simulatable: Given the system parameters and the identity ID, there exists a simulator which can simulate the view of the adversary on an execution of "Private Key Distribution".*

2) *"Sign" is simulatable: Given the system parameters and the identity ID, the message m, the corresponding signature σ, $k-1$ private key shares and the corresponding verification key shares, there is a simulator which can simulate the view of the adversary on an execution of "Signing".*

Theorem 1 (Robustness). *The proposed ID-based threshold signature scheme is robust, i.e., the scheme outputs correctly even in the presence of a malicious adversary that makes the corrupted singers deviate from the normal execution.*

Proof. The robust of "Distributing Extract" is trivial for each signer can validate his private key share using the published verification key share.

In the "Signing" protocol, if the following equation holds, the signer i is sure not to be corrupted by a malicious adversary: $\hat{e}(V_i, g) = B_i \cdot \hat{e}(u' \prod_{l \in \mathcal{U}} u_l, R_{ui}) \cdot \hat{e}(m' \prod_{k \in \mathcal{M}} m_k, R_{mi})$. □

Theorem 2. *If the ID-based threshold signature(IDTHS) scheme is simulatable and the ID-based signature(IDS) scheme which is associated with the IDTHS scheme is EUF-IDS-CMIA2-secure, then the IDTHS scheme is EUF-IDTHS-CMIA2-secure. Concretely, we obtain the following bound:*

$$\boldsymbol{Succ}_{\mathcal{IDTHS}}(t, q_e, q_s) \leq \boldsymbol{Succ}_{\mathcal{IDS}}(t', q'_e, q'_s),$$

where $t' = t + T_{SIM_{DKG}} + T_{SIM_{Sign}}$, $q'_e = q_e$, and $q'_s = 1$. Here, $T_{SIM_{DKG}}$ and $T_{SIM_{Sign}}$ denote the running time of the simulators SIM_{DKG} and SIM_{Sign} respectively.

As mentioned in [17], Paterson and Schuldts' scheme was proven in the standard model and rested on the hardness of the computational Diffie-Hellman problem.

Table 1: Comparison between Li et al.'s scheme and our scheme

Schemes	Signature share generation	Verify
Scheme in [15]	$2E$	$(n_m+1)S+2P$
Our Scheme	$(n_m+1)S+2P+2E$	$(n_m+n_u)S+3P$

Lemma 1. *The proposed ID-based threshold signature scheme is simulatable.*

Proof. Without loss of generality, we assume that the signers corrupted by the adversary are signer_1, signer_2, $\cdots$, signer_{k-1}. First, we prove "Distribution key generation" is simulatable. Given the system parameters params and the identity ID, the adversary computes $Y = \hat{e}(g_2, g)^{\alpha} = \prod_{j=1}^{n} A_{j0} \bmod p$. Note that $\hat{e}(g_2, g)^{\alpha} = \hat{e}(g_2, g)^{\sum_{i=1}^{k} \lambda_i \alpha_i}$, where $\lambda_1, \ldots, \lambda_k$ are the Lagrange coefficients. So the adversary can compute $\hat{e}(g_2, g)^{\alpha_k}$ and the simulated value is correct and identically to the signer_k as the real execution of "Distribution Extract".

Then we prove "Signing" is simulatable. Given the system parameters params, the identity ID, the message m, the corresponding signature $\sigma = (V, R_u, R_m)$, $k-1$ private key share $d_u^i = (d_{u1}^i, d_{u2}^i) = (g_2^{\alpha_i}(u' \prod_{i \in \mathcal{U}} u_i)^{r_i}, g^{r_i})$ and the corresponding verification key shares. Then the adversary can compute the signature share $\sigma_i = (d_{u1}^i (m' \prod_{k \in \mathcal{M}} m_k)^{r_m^i}, d_{u2}^i, g^{r_m^i}) = (V_i, R_{ui}, R_{mi})$ for $1 \leq i \leq k-1$. Note that $V = \prod_{i=1}^{k} (V_i)^{\lambda_i}$, $R_u = \prod_{i=1}^{k} (R_{ui})^{\lambda_i}$ and $R_m = \prod_{i=1}^{k} (R_{mi})^{\lambda_i}$, where $\lambda_1, \ldots, \lambda_k$ are the Lagrange coefficients. So the adversary can compute the signature share σ_i for $i = k, \cdots, n$ and the simulated signature share is correct and identically to the signer_k as the real execution of "Sign". □

Combining Theorem 1, 2, Lemmas 1, and the unforgeability of Paterson and Schuldts'scheme from [17], we obtain the following theorem.

Theorem 3. *The proposed ID-based threshold signature scheme is secure in the sense of unforgeability.*

5 Conclusions

An identity-based threshold signature scheme secure in the standard model(without using random oracle) is proposed in this paper. Our construction is based on the recently proposed signature scheme of Paterson and Schuldt [17]. Additionally, signature share generation and verification is completely non-interactive. To the best of authors' knowledge, this is the first identity-based threshold signature scheme in the literature to achieve this security level.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (60673075 and 60803133). The authors are grateful to the anonymous reviewers for valuable comments.

References

[1] J. H. An, Y. Dodis, and T. Rabin, "On the security of joint signature and encryption," *Eurocrypt 2002*, LNCS 2332, pp. 83-107, Springer, 2002.

[2] J. Baek and Y. Zheng, "Identity-based threshold decryption," *PKC 2004*, LNCS 2947, pp. 262–276, Springer-Verlag, 2004.

[3] J. Baek and Y. Zheng, "Identity-based threshold signature scheme from the bilinear pairings," *Proceeding of the International Conference on Information and Technology: Coding and Computing (ITCC'04)*, pp. 124–128, 2004.

[4] M. Bellare and P. Rogaway, "Random oracles are practical: a paradigm for designing efficient protocols," *First ACM Conference on Computer and Communications Security*, pp. 62–73, 1993.

[5] M. Bellare, A. Boldyreva, and A. Palacio, "An uninstantiable random-oracle-model scheme for a hybrid-encryption problem," *Euroocrypt 2004*, LNCS 3027, pp. 171–188, Springer, 2004.

[6] G. R. Blakley, "Safeguarding cryptographic keys," *Proceedings of AFIPS'79*, pp. 313-317, 1979.

[7] D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing," *Crypto 2001*, LNCS 2139, pp. 213–229, Springer, 2001.

[8] M. Cerccedo, M. Matsumoto, and H. Imai, "Efficient and secure multiparty feneration of digital signatrues based on discrete logarithms," *IEICE Transactions on Fundamentals*, vol. E76-A, pp. 532–545, 1993.

[9] X. Chen, F. Zhang, D. M. Konidala, and K. Kim, "New ID-based threshold signature scheme from bilinear pairings," *Indocrypt 2004*, LNCS 3348, pp. 371–383, Springer-Verlag, 2004.

[10] C. Cocks, "An identity based encryption scheme based on quadratic residues," *Cryptography and Coding*, LNCS 2260, pp. 360–364, Springer-Verlag, 2001.

[11] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Robust threshold DSS signatures," *Advances in Cryptology-Eurocrypt 1996*, LNCS 1070, pp. 354–371, Springer-Verlag, 1996.

[12] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Secure distributed key generation for discrete-log based cryptosystem," *Cryptology-Eurocrypt 1999*, LNCS 1592, pp. 295–310, Springer-Verlag, 1999.
[13] M. H. Ibrahim, "Efficient dealer-less threshold sharing of standard RSA," *International Journal of Network Security*, vol. 8, no. 2, pp. 139-150, 2009.
[14] C. T. Li and Y. P. Chu, "Cryptanalysis of threshold password authentication against guessing attacks in Ad Hoc networks," *International Journal of Network Security*, vol. 8, no. 2, pp. 166-168, 2009.
[15] J. Li, T. H. Yuen, K. Kim, "Practical threshold signatures without random oracles," *ProvSec 2007*, LNCS 4784, pp. 198–207, 2007.
[16] Y. Long, Z. Gong, K. Chen, and S. Liu, "Provably secure identity-based threshold key escrow from pairing," *International Journal of Network Security*, vol. 8, no. 3, pp. 227-234, 2009.
[17] K. G. Paterson and J. C. N. Schuldt, "Efficient identity-based signatures secure in the standard", *ACISP 2006*, LNCS 4058, pp. 207–222, 2006.
[18] S. C. Pohlig and M. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance," *IEEE Transactions on Information Theory*, vol. 24, no. 1, pp. 106-110, 1978.
[19] P. D. Rooij, "On Schnorr's preprocessing for digital signature schemes," *Eurocrypt'93*, LNCS 765, pp. 435–439, Springer-Verlag, 1993.
[20] B. Schneier, *Applied Cryptography: Protocols, Algorithm, and Source Code in C*, 2nd Edition, Wiley, 1996.
[21] C. P. Schnorr, "Efficient identification and signatures for smart cards," *Proceedings on Advances in cryptology*, pp. 239–252, Santa Barbara, USA, 1989.
[22] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
[23] A. Shamir, "Identity-based cryptosystems and signature schemes," *Advances in Cryptology: Proceedings of CRYPTO 84*, LNCS 196, pp. 47–53, Springer, 1984.
[24] D. Stinson and R. Strobl, "Provably secure distributed Schnorr signatures and a (t,n) threshold scheme for implicit certificate", *ACISP 2001*, LNCS 2119, pp. 417–434, Springer-Verlag, 2001.
[25] X. Verians and J. M. Boucqueau, *Next Generation Conditional Access System for Satellite Broadcasting*, Final Report, Contract no. 16696/02/NL/US, Published on 12, Jan. 2004.
[26] H. Wang, Y. Zhang, and D. Feng, "Short threshold signature schemes without random oracles," *Indocrypt 2005*, LNCS 3797, pp. 297–310, Springer, 2005.
[27] B. Waters, "Efficient identity-based encryption without random oracles," *Eurocrypt 2005*, LNCS 3494, pp. 114–127, Springer, 2005.

Hu Xiong is a Ph.D. candidate in the School of Computer Science and Engineering, University of Electronic Science and Technology of China. He received his MS degree in Mathematics from University of Electronic Science and Technology of China, 2004. His research interests include: information security and cryptography.

Zhiguang Qin is a professor in the School of Computer Science and Engineering,University of Electronic Science and Technology of China. He received his PH.D. degree from University of Electronic Science and Technology of China in 1996. His research interests include: information security and computer network.

Fagen Li received his B.S. degree from Luoyang Institute of Technology, Luoyang, P.R. China in 2001 and M.S. degree from Hebei University of Technology, Tianjin, P.R. China in 2004. He is now a Ph.D. candidate in Key Laboratory of Computer Networks and Information Security, Xidian University, Xi'an, P.R. China. His recent research interests include network security, mobile ad hoc network and cryptography.