A New and Efficient Signature on Commitment Values

Fangguo Zhang[1,3], Xiaofeng Chen[2,3], Yi Mu[4], and Willy Susilo[4]
(Corresponding author: Fangguo Zhang)

Department of Electronics and Communication Engineering, Sun Yat-Sen University[1]
Guangzhou 510275, P. R. China (Email: isszhfg@mail.sysu.edu.cn)
Department of Computer Science, Sun Yat-Sen University, Guangzhou 510275, P. R. China[2]
Guangdong Key Laboratory of Information Security Technology Guangzhou 510275, P. R. China[3]
School of IT and Computer Science University of Wollongong, Wollongong, NSW 2522, Australia[4]

(Received July 15, 2006; revised and accepted Nov. 8, 2006)

Abstract

We present a new short signature scheme based on a variant of the Boneh-Boyen's short signatures schemes. Our short signature scheme is secure without requiring the random oracle model. We show how to prove a committed value embedded in our short signature. Using this primitive, we construct an efficient anonymous credential system.

Keywords: Anonymity, anonymous credentials, commitment, signature

1 Introduction

Signature schemes are a central cryptographic primitive. Besides being an important stand-alone application, they also constitute a building block in many cryptographic protocols. One of important applications of signatures is *anonymous credential*.

The notion of anonymous credential was introduce by Chaum [11]. A credential system allows a user to obtain credentials, and to prove that he has a given set of credentials. An anonymous credential system enables a user to work with his credentials without revealing any information not explicitly requested. A user should be able to obtain a credential without revealing his identity, and to prove that he has a set of credentials without revealing any information beyond that fact. To be useful for this application, a signature scheme must have efficient protocols for obtaining a signature on a hidden (committed) value, and for proving in zero-knowledge the knowledge of a signature.

An anonymous credential system should meet some essential properties: It should be secure against attacks from a coalition of users. It should be able to be used for multiple times, i.e., so-called "multi-show". It is also essential that one a credential has been issued to a user, it cannot be transferred to any one else, i.e. "non-transferability". It is desirable that the overheads of communication and computation imposed by a credential system to users and services must not heavily affect their performance.

The studies of anonymous credential have gone through several stages. After its introduction by Chaum, Brands presented a public key based construction of anonymous credential in which a user can provide in zero knowledge that the credentials encoded by its certificate satisfy a given linear Boolean formula [6]. This scheme allows only one show, namely, two transactions from the same user can be found performed by the same user. Camenisch and Lysyanskaya proposed an anonymous credential scheme based on the strong RSA assumption [7]. In this scheme, it is possible to unlinkably prove possession of a credential supporting multi-show property. There are several other schemes that are based on different security assumptions. Verheul recently proposed an efficient solution for multi-show credentials based on the security assumptions of Decisional Diffie-Hellman problem and Computational Diffie-Hellman problem [15]. Camenisch and Lysyanskaya recently also proposed generalized anonymous credential systems and showed how to construct them from known signature and encryption schemes [1].

As claimed by Camenisch and Lysyanskaya [8], in order to construct an anonymous credential system, it is sufficient to exhibit a commitment scheme, a signature scheme, and efficient protocols for (1) proving equality of two committed values; (2) getting a signature on a committed value (without revealing this value to the signer); and (3) proving knowledge of a signature on a committed value.

In this paper, we propose a variant of Boneh-Boyen short signature scheme without random oracle such that it can be used as a building block for cryptographic protocols. We provide a protocol to prove knowledge of a sig-

nature on a committed message and to obtain a signature on a committed message. Our scheme can be naturally converted into an anonymous credential scheme.

The organization of the rest of this paper is as follows. In the next section, we define the definitions and requirements for signature on commitment values. The Section 3 contains some preliminaries required throughout the paper. In Section 4, we present a variant of Boneh-Boyen short signature scheme without random oracle and give its security analysis. In Section 5 we propose a signature on a committed message. In Section 6, we present a basic anonymous credential system based the proposed signature scheme. Section 7 concludes this paper.

2 Definitions and Requirements

Our signature scheme consists of a committer, a signer, and a verifier. The committer commits to a value and the signer then signs the committed value. Any one can verify the correctness of the signature. The committer can prove to the verifier that he knows the committed value embedded in the signature.

Definition 1. *Our signature scheme is a 6-tuple of polynomial-time algorithms (*KeyGen*,* Commit*,* Sign*,* Verify*,* Prove*,* PVerify*), where*

- $\mathsf{KeyGen}(1^\ell)$ *is a probabilistic algorithm that takes as input the security parameter ℓ and outputs a pair of keys* $(\mathsf{SK}, \mathsf{VK})$ *and* param0. SK *is the user's signing key, which is kept secret, and* VK *the user's verification key, which is made public.*
- Commit*, a probabilistic algorithm, takes as input a message m from the associated message space $\mathcal{M}$ and a number a and outputs a commitment c.*
- Sign*, a probabilistic algorithm, takes as input the signer's secret key* SK*,* param0*, and the commitment c and outputs a signature $s \leftarrow \mathsf{Sign}_{\mathsf{SK},\mathsf{VK}}(c)$.*
- Verify *is a deterministic algorithm that takes as input the signed commitment c and the signer's public key* VK *and outputs true or $\perp$.*
- Prove *is a probabilistic algorithm that takes as input s and c and outputs (*PK*,* Proof*) proving the knowledge of the committed m and c without revealing the committed values.*
- PVerify *is a deterministic algorithm that takes as input (*PK*,* Proof*) and outputs true or $\perp$.*

Our anonymous multi-show credential scheme is based the proposed signature scheme and consists of an organization, a group of users, and a service provider. The organization acts as the signer who issues credentials to users for some service provided by the service provider.

Definition 2. *The proposed anonymous multi-show credential scheme is a 5-tuple of polynomial-time algorithms (*KeyGen, CIssue, CVerify, CProve, CPVerify*).*

- $\mathsf{KeyGen}(1^\ell)$.
- CIssue*: The user uses* Commit *and the signer uses* Sign*. In the end of the process, the user obtains (c, s).*
- CVerify*. The user checks the validity of (c, s) using* Verify*.*
- CProve*. Using* Prove*, the user proves to the service provider about his knowledge on (m, a) and s on c and outputs (*PK*,* Proof*).*
- CVerify*. The service provider checks the correctness of (*PK*,* proof*) using* PVerify*.*

We define the security notion for our basic signature scheme only. It is easy to extend it to the anonymous multi-show credential scheme.

Completeness property for the signature on commitment values is defined as follows.

$$\Pr\left[\begin{array}{rl} (\mathsf{SK},\mathsf{VK},\mathsf{param0}) \leftarrow \mathsf{KeyGen}(1^\ell) & \wedge \\ (c,s) \leftarrow \mathsf{Sign}(c,\mathsf{SK}) & \wedge \\ true \leftarrow \mathsf{Verify}(c,s) & \wedge \\ (\mathsf{PK},\mathsf{Proof}) \leftarrow \mathsf{Prove}(c,s) & \wedge \\ true \leftarrow \mathsf{PVerify}(\mathsf{PK},\mathsf{Proof}) & \end{array}\right] = 1.$$

We require our schemes to meet the requirement of existentially unforgeable against the chosen message attacks. We split it into to properties: Security of signature of commitment and security of proving knowledge of committed message in a signature. Assume there exists a TTP adversary $\mathcal{A}$ who launches a chosen message attack against our signature scheme and at most asks n queries to the signing oracle.

$$\Pr\left[\begin{array}{r} true \leftarrow \mathsf{Verify}(c',s') \wedge (c',s') \\ \leftarrow \mathcal{A}(c_i, \mathsf{VK}, \mathsf{param0}, i = 1, \cdots, n) \end{array}\right] = \epsilon.$$

Here, ϵ is negligible.

For security of proving knowledge of committed message in a signature, we also require statistical zero knowledge; that is, it is negligible for an adversary $\mathcal{A}$ to obtain any information on m.

$$\Pr\left[\ \mathcal{A} \text{ knows } m | true \leftarrow \mathsf{Verify}(\mathsf{PK}(m), \mathsf{Proof})\ \right] = \epsilon.$$

3 Preliminaries

3.1 Bilinear Pairings

In recent years, the bilinear pairings have been widely applied to cryptography and enable us to construct some new cryptographic primitives. We briefly review the necessary facts about bilinear pairings using the same notation as [2, 4, 5]:

Let $\mathbb{G}_1, \mathbb{G}_2$ be (multiplicative) cyclic groups of prime order p. Let g_1 be a generator of $\mathbb{G}_1$ and g_2 be a generator of $\mathbb{G}_2$. Let ψ is a computable isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$, with $\psi(g_2) = g_1$.

Definition 3. *A map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ (here $\mathbb{G}_T$ is another multiplicative cyclic group such that $|\mathbb{G}_1| = |\mathbb{G}_2| = |\mathbb{G}_T| = p$) is called a bilinear pairing if this map satisfies the following properties:*

1) **Bilinearity:** *for all $u \in \mathbb{G}_1, v \in \mathbb{G}_2$ and $a, b \in \mathbb{Z}_p$, we have $e(u^a,\ v^b) = e(u,\ v)^{ab}$.*

2) **Non-degeneracy:** $e(g_1, g_2) \neq 1$. *In other words, if g_1 be a generator of $\mathbb{G}_1$ and g_2 be a generator of $\mathbb{G}_2$, then $e(g_1,\ g_2)$ generates $\mathbb{G}_T$.*

3) **Computability:** *There is an efficient algorithm to compute $e(u,\ v)$ for all $u \in \mathbb{G}_1$ and $v \in \mathbb{G}_2$.*

We say that $(\mathbb{G}_1, \mathbb{G}_2)$ are bilinear groups if there exists a group $\mathbb{G}_T$, a computable isomorphism $\psi : \mathbb{G}_2 \to \mathbb{G}_1$, and a bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ as above.

In this paper, we assume that $\mathbb{G}_1 \neq \mathbb{G}_2$. In this case, the co-Decision Diffie-Hellman problem (co-DDH) in $(\mathbb{G}_1, \mathbb{G}_2)$ is easy, but we can still assume that the Decision Diffie-Hellman problem (DDH) in $\mathbb{G}_1$ is hard.

The following Strong Diffie-Hellman assumption is suggested by [2, 13, 16]. [2] also provides a lower bound on the computational complexity in a generic group model.

Definition 4. *(q-SDH problem) The q-Strong Diffie-Hellman problem in $(\mathbb{G}_1, \mathbb{G}_2)$ is defined as follows: given a $(q+2)$-tuple $(g_1, g_2, {g_2}^{\gamma}, \cdots, {g_2}^{\gamma^q})$ as input, outputs a pair $({g_1}^{1/\gamma+x}, x)$ where $x \in \mathbb{Z}_p^*$.*

An algorithm $\mathcal{A}$ has advantage ϵ in solving q-SDH in $(\mathbb{G}_1, \mathbb{G}_2)$ if

$$Pr[\mathcal{A}(g_1, g_2, {g_2}^{\gamma}, \cdots, {g_2}^{\gamma^q}) = ({g_1}^{1/\gamma+x}, x)] \geq \epsilon,$$

where the probability is over the random choice of generator in $g_2 \in \mathbb{G}_2$, of $\gamma \in \mathbb{Z}_p^*$, and of the random bits of $\mathcal{A}$.

We say that the (q, t, ϵ)-SDH assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$ if no t-time algorithm has advantage at least ϵ in solving the q-SDH problem in $(\mathbb{G}_1, \mathbb{G}_2)$.

3.2 Proofs of Knowledge of Discrete Logarithms

We will use the notation introduced by Camenisch and Stadler [10] for various proofs of knowledge of discrete logarithms. For instance,

$$PK\{(\alpha, \beta, \gamma) : y = g^{\alpha}h^{\beta} \wedge z = g'^{\alpha}h'^{\gamma} \wedge (a \leq \alpha \leq b)\}$$

is used for proving the knowledge of integers α, β and γ such that $y = g^{\alpha}h^{\beta}$ and $z = g'^{\alpha}h'^{\gamma}$ holds, where $a \leq \alpha \leq b$. Here y, g, h, z, g' and h' are elements of some groups $\mathbb{G} =< g >=< h >$ and $\mathbb{G}_T =< g' >=< h' >$.

3.3 Pedersen Commitment Scheme

Recall the Pedersen commitment scheme [14]: given a group $\mathbb{G}$ of prime order p with generators g and h, a commitment to $x \in \mathbb{Z}_p^*$ is formed by choosing a random $r \in \mathbb{Z}_p^*$ and setting the commitment $C = g^x h^r$. This commitment scheme is information-theoretically hiding, and is binding under the discrete logarithm assumption.

4 A Variant of BB04 Signature Scheme

We describe the new signature scheme as follows. Let $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ be the bilinear pairing where $|\mathbb{G}_1| = |\mathbb{G}_2| = |\mathbb{G}_T| = p$ for some prime p. We assume that $|p| \geq 160$. As for the message space, if the signature scheme is intended to be used directly for signing messages, then $|m| = 160$ is good enough, because, given a suitable collision resistant hash function, such as SHA-1, one can first hash a message to 160 bits, and then sign the resulting value. So the messages m to be signed can be regarded as an element in $\mathbb{Z}_p$. We also need a very efficient and suitable conversion function from $\mathbb{G}_1$ to $\mathbb{Z}_p^*$: $[\cdot] : \mathbb{G}_1 \to \mathbb{Z}_p^*$. The system parameter is $(\mathbb{G}_1,\ \mathbb{G}_2, \mathbb{G}_T,\ e,\ p,\ g_1,\ h,\ g_2,\ [\cdot])$, here $g_1, h \in \mathbb{G}_1$, $g_2 \in \mathbb{G}_2$ are random generators.

Key Generation. Randomly select $x, y \in_R \mathbb{Z}_p^*$, and compute $u = g_2^x, v = g_2^y$. The public key is u, v. The secret key is x, y.

Signing: Given the secret key $x, y \in_R \mathbb{Z}_p^*$, and a message $m \in \mathbb{Z}_p$, compute the signature

$$\sigma = (g_1^m)^{\frac{1}{x+[g_1^m]+yr}} \in \mathbb{G}_1.$$

Here r is randomly selected from $\mathbb{Z}_p^*$. The signature is (r, σ).

Verification: Verify that $e(\sigma,\ ug_2^{[g_1^m]}v^r) = e(g_1^m,\ g_2)$.

We now give the security theorems and proofs for the above instantiation.

Lemma 1. *If there exists a (t, q_S, ϵ)-forger $\mathcal{F}$ using adaptive chosen message attack for the proposed signature scheme, then there exists a (t, q_S, ϵ)-forger $\mathcal{F}$ for BB04 scheme.*

Proof. Recall that BB04 signature scheme is described as follows. The system parameter is same as the above scheme.

Key Generation. Randomly select $x, y \in_R \mathbb{Z}_p^*$, and compute $u = g_2^x, v = g_2^y$. The public key is u, v. The secret key is x, y.

Signing: Given the secret key $x, y \in_R \mathbb{Z}_p^*$, and a message $m \in \mathbb{Z}_p$, compute the signature

$$\sigma = g_1^{\frac{1}{x+m+yr}} \in \mathbb{G}_1.$$

The signature is (r, σ).

Verification: Verify that $e(\sigma,\ ug_2^m v^r) = e(g_1,\ g_2)$.

Suppose that there exists a (t, q_S, ϵ)-forger $\mathcal{F}$ using adaptive chosen message attack for the proposed signature scheme, i.e., after at most q_S signatures queries and t processing time, $\mathcal{F}$ outputs a valid signature forgery (r, σ) on message m with probability at least ϵ, here $e(\sigma,\ ug_2^{[g_1^m]}v^r) = e(g_1^m,\ g_2)$.

Let $m' = [g_1^m]$, $\sigma' = \sigma^{m^{-1}}$, then we have a forgery on BBS04 scheme. This is because of

$$e(\sigma',\ ug_2^{m'}v^r) = e(\sigma^{m^{-1}},\ ug_2^{[g_1^m]}v^r) = e(g_1,\ g_2).$$

□

Theorem 1 ([2]). *Suppose the (q, t', ϵ')-SDH assumption holds in $\mathbb{G}$. Then BBS04 signature scheme is (t, q_S, ϵ)-secure against existential forgery under an adaptive chosen message attack provided that*

$$q_S < q,\ \epsilon \geq 2(\epsilon' + \frac{q_S}{p}) \approx 2\epsilon',\ t \leq t' - \Theta(q^2 T),$$

where T is the maximum time for an exponentiation in $(\mathbb{G}_1, \mathbb{G}_2)$.

So, we have the following theorem:

Theorem 2. *The proposed signature scheme is secure against existential forgery under an adaptive chosen message attack if the (q, t', ϵ')-SDH assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$.*

5 Obtaining a Signature on a Committed Value

Following Camenisch and Lysyanskaya, in order to construct an anonymous credential system, it is sufficient to exhibit a signature on a committed value. We provide a new signature on a committed value based on the variant of BB04 signature scheme in this section.

The system parameter is ($\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$, e, p, g_1, h, g_2, $[\cdot]$), here g_1, $h \in \mathbb{G}_1$, $g_2 \in \mathbb{G}_2$ are random generators.

KeyGen. Randomly select $x, y \in_R \mathbb{Z}_p^*$, and compute $u = g_2^x, v = g_2^y$. The public key is u, v. The secret key is x, y.

Commit: Compute $c = g_1^m h^a$.

Sign: Given the secret key $x, y \in_R \mathbb{Z}_p^*$, and a commitment $c \in \mathbb{G}_1$, compute the signature as follows: Randomly select $r \in_R \mathbb{Z}_p^*$, compute

$$\sigma = c^{\frac{1}{x+[c]+ry}} \in \mathbb{G}_1.$$

The signature one $c = g_1^m h^a$ is (r, σ).

Verify: Verify that $e(\sigma,\ ug_2^{[c]}v^r) = e(c,\ g_2)$.

Prove: The following protocol is a zero-knowledge proof of knowledge of a signed message for above signature scheme.

Common input. The system parameter is ($\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$, e, p, g_1, h, g_2, $[\cdot]$), and the public key (u, v).

Prover's input. The committed message m and a, and signature (r, σ).

Protocol. The prover does the following:

1) Compute a blinded version of his signature (r, σ): Randomly select $r_1, r_2 \in_R \mathbb{Z}_p^*$, and compute

$$c' = (ug_2^{[c]}v^r)^{r_1} = u^{r_1} g_2^{r_1[c]} v^{rr_1},\ \sigma' = \sigma^{r_2}.$$

Send (c', σ') to the verifier.

2) PVerify. The prover and verifier compute the following values:

$$A = e(\sigma',\ c'),\ B = e(g_1, g_2),\ C = e(h, g_2)$$

and then carry out the following zero-knowledge proof protocols:

$$ZKP\{(\alpha, \beta, \lambda_1, \lambda_2, \lambda_3) | A = B^\alpha C^\beta \wedge c' = u^{\lambda_1} g_2^{\lambda_2} v^{\lambda_3} \wedge \lambda_1 \neq 0\}.$$

Here $\alpha = mr_1r_2,\ \beta = ar_1r_2,\ \lambda_1 = r_1,\ \lambda_2 = r_1[c], \lambda_3 = rr_1$. blind the credential by using two randomly generate numbers r_1, r_2. The completeness of the proposed signature scheme on a committed value is obvious. Due to the using of two randomly generate numbers r_1, r_2, the protocol can provide the anonymity. The protocol above uses zero-knowledge proof, so, it is a zero-knowledge proof of a signature on a value.

6 A Multi-show Anonymous Credential Scheme

Based on the proposed signature scheme, we can now construct the multi-show anonymous credential scheme. We will follow the notations given previously in this paper.

The system parameter is same as above signature scheme.

- KeyGen(1^ℓ): Generate public (u, v) and private signing key (x, y).
- CIssue: The user commits to (m, a) by computing $c = g_1^m h^a$. and the signer computes the signature on c: $(r,\ \sigma = c^{\frac{1}{x+[c]+ry}})$.
- CVerify. The user checks $e(\sigma,\ ug_2^{[c]}v^r) \stackrel{?}{=} e(c,\ g_2)$.
- CProve. Using Prove, the user proves to the service provider about his knowledge on (m, a) and (r, σ) on

c and outputs (PK, Proof). Here, the (Proof) is the zero-knowledge proof:

$$ZKP\{(\alpha,\beta,\lambda_1,\lambda_2,\lambda_3)|A = B^{\alpha}C^{\beta} \wedge c' = u^{\lambda_1}g_2^{\lambda_2}v^{\lambda_3} \wedge \lambda_1 \neq 0\}.$$

- CVerify. The service provider checks the correctness of (PK, Proof) using PVerify.

Our credential scheme is of multi-show, i.e., the user can blind the credential by using two randomly generate numbers r_1, r_2. The credential itself is never sent to the service provider in clear. Clearly, our scheme also supports non-transferability. To show a credential to the service provider, the user has to know his secret (m, a). Of course, we have to assume that his secret should not be given to others. However, it is also not hard for us to modify the scheme such that there exists a revocation manager who can revoke the identity of the user if needed.

7 Conclusion

In this paper, we propose a variant of Boneh-Boyen short signature scheme without random oracle such that it can be used as a building block for cryptographic protocols. We provide a protocol to prove knowledge of a signature on a committed message and to obtain a signature on a committed message such that it can be converted into an efficient multi-show credential scheme. The proposed signature scheme on a committed value in this paper has many good properties, and for the further work, we expect to design a group signature scheme based on this signature scheme.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (No. 60403007, No. 60503006 and No. 60633030), Natural Science Foundation of Guangdong Province, China (No. 04205407), 973 Program (2006CB303104) and ARC Discovery Grant DP055749.

References

[1] E. Bangerter, J. Camenisch, and A. Lysyanskaya, "A cryptographc framework for the controlled release of certified data," in *Twelfth International Workshop on Security Protocols*, LNCS 3957, pp. 20-42, Springer-Verlag, 2006.

[2] D. Boneh, and X. Boyen, "Short signatures without random Oracles," in *Advances in Cryptology (Eurocrypt'04)*, LNCS 3027, pp. 56-73, Springer-Verlag, 2004.

[3] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures using strong diffie hellman," in *Advances in Cryptology (Crypto'04)*, LNCS 3152, pp. 41-55, Springer-Verlag, 2004.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology (Crypto'01)*, LNCS 2139, pp. 213-229, Springer-Verlag, 2001.

[5] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," in *Advances in Cryptology (Asiacrypt'01)*, LNCS 2248, pp. 514-532, Springer-Verlag, 2001.

[6] S. Brands, *Rethinking Public Key Infrastructures and Digital Certificates; Bulding in Privacy*, MIT Press, 2000.

[7] J. Camenisch and A. Lysyanskaya, "Efficient non-transferable anonymous multishow credential system with optional anonymity revocation," in *Advances in Cryptology (Eurocrypt'01)*, LNCS 2045, pp. 93-118, Springer-Verlag, 2001.

[8] J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols,"in *Security in Communication Networks (SCN'02)*, LNCS 2576, pp. 268-289, Springer-Verlag, 2003.

[9] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," in *Advances in Cryptology (Crypto'04)*, LNCS 3152, pp. 56-72, Springer-Verlag, 2004.

[10] J. Camenisch and M. Michels, "Efficient group signature schemes for large group," in *Advances in Cryptology (Crypto'97)*, LNCS 1296, pp. 410-424, Springer-Verlag, 1997.

[11] D. Chaum, "Security without identification: transacation systems to make big brother obsolete," *Communications of ACM*, vol. 28, no. 10, pp. 1030-1044, Oct. 1985.

[12] A. Joux, "A one round protocol for tripartite Diffie-Hellman," in *4th International Symposium on Algorithmic Number Theory (ANTS IV)*, LNCS 1838, pp. 385-394, Springer-Verlag, 2000.

[13] S. Mitsunari, R. Sakai, and M. Kasahara, "A new traitor tracing," *IEICE Transactions on Fundamentals*, vol. E85-A, no. 2, pp. 481-484, 2002.

[14] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Advances in Cryptology (Crypto'91)*, LNCS 576, pp. 129-140. Springer-Verlag, 1992.

[15] E. Verheul, "Self-blindable credential certificates from the Weil pairing," in *Advances in Cryptology (Asiacrypt'01)*, LNCS 2248, pp. 533-551, Springer-Verlag, 2001.

[16] F. Zhang, R. S. Naini, and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," in *Public Key Cryptography (PKC'04)*, LNCS 2947, pp. 277-290, Springer-Verlag, Singapore, 2004.

Fangguo Zhang is a Professor in the Department of Electronics and Communication Engineering at Sun Yansen 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 and its applications.

Xiaofeng Chen is an Associate Professor in the Department of Computer Science 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 E-commerce security.

Yi Mu received his PhD from the Australian National University in 1994. He was a lecturer in the School of Computing and IT at the University of Western Sydney and a senior lecturer in the Department of Computing at Macquarie University. He currently is an associate professor in the Information Technology and Computer Science, University of Wollongong. His current research interests include network security, computer security, and cryptography. Yi Mu has published more than 140 research papers in international conferences and journals. He has served in technical program committees of a number of international conferences and the editorial boards of six international journals. He is a senior member of the IEEE, and a member of the IACR.

Willy Susilo received a Ph.D. in Computer Science from University of Wollongong, Australia. He is currently an Associate Professor at the School of Information Technology and Computer Science of the University of Wollongong. He is the coordinator of Network Security Research Laboratory at the University of Wollongong. His research interests include cryptography, information security, computer security and network security. His main contribution is in the area of digital signature schemes, in particular fail-stop signature schemes and short signature schemes. He has served as a program committee member in a number of international conferences. He has published numerous publications in the area of digital signature schemes and encryption schemes.