New Constructions of Short Signatures in the Standard Model

Leyou Zhang
Department of Mathematical Science, Xidian University, Xi'an, 710071, China
Email: leyouzhang77@yahoo.com.cn

Qing Wu
School of Automation, Xi'an Institute of Posts and Telecommunications, Xi'an, China
Email: xidianwq@yahoo.com.cn

Yupu Hu
Key Laboratory of Computer Networks and Information
Security, Ministry of Education, Xidian University, Xi'an, 710071, China
Email: yphu@mail.xidian.edu.cn

***Abstract*—To meet the needs in low-bandwidth communication, low-storage and less computation environments, a new technique is introduced to construct short signature in the standard model. The new short signature scheme is constructed based on the bilinear pairing and has short public parameters. In addition, the size of the signature achieves 160 bits. Under the *n*-Exponent Computational Diffie-Hellman Problem(*n*-CDH), the new scheme is provable security. Finally, we also give the application of the new scheme by constructing the short identity-based signature and threshold signatures.**

***Index Terms*—Short signature, threshold signature, identity-based signature, *n*-CDH, random oracle, the standard model, provable security.**

I. INTRODUCTION

Short signature schemes are needed in environments with space and bandwidth constraints. There are going to be a lot of devices exchanging messages with each other in these environments, e.g., PDAs, cell phones, RFID chips, sensor networks and vehicle-2-vehicle communications [1, 2]. For these systems to work properly, messages must carry some form of authentication, but the system requirements on the authentication are particularly demanding.

A. Related works

Short signature is an active research area. As mentioned in [3,4], there are two paradigms of shortening signatures at present.

· Shorten the total length of a signature and the corresponding message. In such schemes[5,6], one encodes a part of the messageinto the signature thus shortening the total length of themessage-signature pair. For long messages, one can then achieve aDSA signature overhead of length of 160 bits.

· Shorten the signature directly. This technique is to shorten the signature directly while preserving the same level of security. Boneh, Lynn and Shacham [7] used a totally new approach to design such short digital signatures in 2001. Their scheme is based on the Computational Diffie-Hellman (CDH) assumption on elliptic curves with low embedding degree. A number of desirable schemes were proposed at present.

Currently, provable security is the basic requirement for the public key cryptosystem. The provably secure short signature schemes are based on two security model. One is the random oracles model. The other is standard model. Most of practical efficient schemes are provable secure in the random oracles model. Random oracle model is a formal model at present, where a hash function is considered as a black-box that contains a random function. However, many results have shown that security in the random oracle model does not imply the security in the real world. Security in the standard model usually provides a higher security level than security in the random oracle model. Gennaro, Halevi and Rabin [8] firstly proposed practical secure signature schemes under the strong RSA assumption in the standard model. In 2004, Boneh and Boyen [9] proposed a short signature scheme from bilinear groups which is secure under the Strong Diffie-Hellman assumption without using random oracles. Later, Zhang F. et a [4], Wei and Yuen [10] also proposed some short signature schemes in the standard model. However, it is also true that schemes providing security in the random oracle model are usually more efficient than schemes secure in the standard model. Table 1 gives a summary of signature size of the different schemes.

In Table 1, RO and SM denote the random oracle model and standard model respectively. Size is the signature size.

Part of contents in this paper had appeared in proceeding of ICICA 2010.

Corresponding author: Leyou Zhang.

doi:10.4304/jsw.6.10.1921-1928

TABLE I.
SIGNATURE SIZE OF DIFFERENT SCHEMES

Scheme	[3]	[6]	[7]	[11]	[13]	[14]	[4]	[9]	[10]	[15]
Model	RO	RO	RO	RO	RO	RO	SM	SM	SM	SM
Size	160	160	160	160	160	320	320	320	320	320

B. Related works

We construct a new short signature in the standard model from the bilinear pairing. The size of new signature achieves 160 bits, which is shorter than others at present. The security of our scheme depends on the *n*-CDH assumption. Another contribution is the applications of new scheme. We construct the short identity-based signature and threshold signatures, by the same technique, thus testing the applicability of our scheme.

II. PRELIMINARIES

A. Bilinear Pairing

G and G_1 are cyclic groups of order *N*. A bilinear map *e* is a map $e: G \times G \to G_1$ with the following properties:

(i) Bilinearity: for all $u, v \in G$, $a, b \in Z_N$, we have $e(u^a, v^b) = e(u, v)^{ab}$;

(ii) Non-degeneracy: $\exists\ g \in G$ such that $e(g, g) \neq 1$.

(iii) Computability: there is an efficient algorithm to compute $e(u, v)$ for all $u, v \in G$.

B. Hardness Assumption

Security of our scheme will be reduced to the hardness of the *n*-CDH problem in the group. We briefly recall the definition of the *n*-CDH problem:

Definition 1 (*n*-Exponent Computational Diffie-Hellman Problem) Given a group G of prime order *p* with generator g and elements g^{α}, $g^{\alpha^2}, \cdots, g^{\alpha^n} \in G$, where α is selected uniformly at random from Z_p and n ≥ 1, the *n*-CDH problem in G is to compute $g^{\alpha^{n+1}}$.

Note that it was shown in [11] that *n*-CDH problem is equivalent to CDH problem for n=1.

Definition 2 We say that the (t, ε) *n*-CDH assumption holds in a group G, if no adversary running in time at most *t* can solve the *n*-CDH problem in G with probability at least ε.

C. Security Definition

A signature scheme is made up of three algorithms, KeyGen, Sign, and Verify, for generating keys, signing, and verifying signatures, respectively.

The standard notion of security for a signature scheme is called existential unforgeability under a chosen message attack [12-18], which is defined using the following game between a challenger and an adversary A:

Setup The challenger runs algorithm KeyGen to obtain a public key *PK* and a private key *SK*. The adversary A is given *PK*.

Queries Proceeding adaptively, A requests signatures on at most q_s messages of his choice $M_1, \cdots, M_{q_s} \in \{0, 1\}$, under PK. The challenger responds to each query with a signature $\sigma_i = Sign(M_i, SK)$.

Forgery A outputs a pair (M, σ) and wins the game if

(1) M is not any of ($M_1, \cdots, M_{q_s}$);

(2) *Verify*(PK, M, σ)=*Valid*.

We will use a weaker notion of security which we call existential unforgeability under a weak chosen message attack. Here we require that the adversary submit all signature queries before seeing the public key. This notion is defined using the following game between a challenger and an adversary A:

Query A sends the challenger a list of q_s messages $M_1, \cdots, M_{q_s} \in \{0, 1\}$, where q_i is one of the following:

Response: The challenger runs algorithm KeyGen to generate a public key *PK* and private key *SK*. Next, the challenger generates signatures $\sigma_i = Sign(M_i, SK)$. The challenger then gives A the public key *PK* and signatures σ_i.

Forgery: Algorithm A outputs a pair (M,σ) and wins the game if

(1) M is not any of ($M_1, \cdots, M_{q_s}$);

(2) *Verify*(PK, M, σ)=*Valid*.

Definition 3 A signature scheme is (t, ε) existentially unforgeable under a weak adaptive chosen message attack if no probabilistic polynomial time(running in time at most *t*) adversary has a non-negligible advantage ε in the above game.

III. NEW SHORT SIGNATURE FROM THE BILINEAR PAIRING

In this section, we describe our schemes as follows:

A. Initial Construction

KeyGen Let G be a group of prime order *p* and g be a random generator of G. Pick α, $\alpha_1, \cdots, \alpha_n$,

$\beta_1,\cdots,\beta_n$, from Z_p at random. Set $g_1 = g^\alpha$. Then choose g_2 randomly in G. The public key is

$$PK=(g,\ g_1,\ g_2).$$

The private key is

$$SK=(\alpha,\ \alpha_1,\cdots,\alpha_n,\ \beta_1,\cdots,\beta_n).$$

Note: We omit the public keys corresponding to $\alpha_1,\cdots,\alpha_n$, $\beta_1,\cdots,\beta_n$ since they are not used at the phase of *Verify*.

Sign Message is represented as bit-strings of length n. Let $M=(m_1,\cdots,m_n)$ be a n-bit message to be signed, where $m_i \in \{0,1\}$. Signer first generates the auxiliary information parameters as follows:

Let $h_0 = g$, then for $i=1,\cdots,n$, compute

$$h_i = (h_{i-1})^{\alpha_i^{m_i}\beta_i^{1-m_i}}.$$

Then the signature is computed as

$$\sigma=(\sigma_1,\sigma_2)=((g_2h_n)^\alpha,h_n).$$

Verify Given the signature σ, message M and the public keys, verifier accepts the signature if and only if the following holds.

$$e(\sigma_1,g)=e(g_1,g_2\sigma_2)$$

Correctness: If σ is valid, one can obtain

$$e(\sigma_1,g)=e((g_2h_n)^\alpha,g)=e(g_2h_n,g^\alpha)=e(g_2h_n,g_1).$$

B. New Construction

KeyGen Let G be a group of prime order p and g be a random generator of G. Pick α , $\alpha_1,\cdots,\alpha_n$, $\beta_1,\cdots,\beta_n$, from Z_p at random. Set $g_1 = g^\alpha$. Then choose g_2 randomly in G, compute $t_{0i}=e(g_1,g^{\alpha_i})$ and $t_{1i}=e(g_1,g^{\beta_i})$. The public key is

$$PK=(g,\ g_1,\ g_2,t_{0i},t_{1i},\ v),$$

where $v=e(g_1,g_2)$. The private key is

$$SK=(\alpha,\ \alpha_1,\cdots,\alpha_n,\ \beta_1,\cdots,\beta_n).$$

Sign Message is represented as bit-strings of length n. Let $M=(m_1,\cdots,m_n)$ be a n-bit message to be signed, where $m_i \in \{0,1\}$. Signer first generates the auxiliary information parameters as follows:

Let $h_0 = g$, then for $i=1,\cdots,n$, compute

$$h_i = (h_{i-1})^{\alpha_i^{m_i}\beta_i^{1-m_i}}.$$

Then the signature is computed as

$$\sigma=(g_2h_n)^\alpha.$$

Verify Given the signature σ, message M and the public keys, verifier accepts the signature if and only if the following holds.

$$e(\sigma,g)=v\prod_{i=1}^{n}p_i\ .$$

where

$$p_i=\begin{cases}t_{0i} & if\ \ m_i=1\\ t_{1i} & if\ \ m_i=0\end{cases},$$

Correctness: If σ is valid , one can obtain

$$\begin{aligned}e(\sigma,g)&=e((g_2h_n)^\alpha,g)\\&=e(g_2h_n,g^\alpha)\\&=e(g_2,g^\alpha)e(h_n,g^\alpha)\\&=e(g_2,g_1)e(h_n,g_1)\\&=ve(g_1,g^{\sum_{i=1}^{n}\alpha_i^{m_i}\beta_i^{1-m_i}})\\&=v\prod_{i=1}^{n}e(g_1,g^{\alpha_i^{m_i}\beta_i^{1-m_i}})\\&=v\prod_{i=1}^{n}p_i\ .\end{aligned}$$

C. Efficiency

The size of our initial scheme achieves $2|G_1|$ which is similar with the previous schemes in the standard model. But our new scheme has a signature of 160 bits. It is the shortest signature in the standard model at present. Table 2 gives the comprehensive comparison between our signature scheme and other schemes. We assume that all these short signature schemes use the GDH group which is derived from the curve $E/F_{3^{163}}$ defined by the equation $y^2=x^3-x+1$. This group provides 1551-bit discrete log security.

Note: In Table 2, we denote by e a computation of the pairing.

TABLE II.
Comparison of Efficiency

Scheme	Hardness	Security Model	Signature Size	Verify
[4]	k+1-SRP	Standard	320	2e
[9]	q-SDH	Standard	320	2e
Our initial scheme	n-CDH	Standard	320	2e
Our new scheme	n-CDH	Standard	160	1e

D. Security Proof

We only give a proof of the security of our second scheme since the first one can be proved by the similar method.

Theorem If n-CDH assumption holds, then our scheme is secure.

Proof: Assume that there is an adversary A which breaks the proposed scheme with advantage ε , we then show how to build an adversary B that solves the decisional n-CDH problem with advantage $\frac{\varepsilon}{2^n}$. For a

generator $g \in G$ and $\alpha, c \in Z_p$, set $y_i = g^{\alpha^i} \in G$. Algorithm B is given as input a random tuple (g, y_1, $\cdots$, y_n). B works by interacting with A as follows:

Init A first outputs a message $M^* = (m_1^*, \cdots m_n^*)$ that it wants to attack.

We only give a proof of the security of our second scheme since the first one can be proved by the similar method.

Setup To generate the system parameters, B sets $g_1 = y_1$. Then it selects randomly a $\gamma \in Z_p^*$ and sets

$$g_2 = y^n g^\gamma = g^{\alpha^n + \gamma}.$$

It chooses $a, \alpha_i, \beta_i \in Z_p^*$ for $1 \le i \le n$ and computes

$$g_{0i} = \begin{cases} g^{\alpha_i} & if\ m_i^* = 0 \\ y_1^* & if\ m_i^* = 1 \end{cases},$$

$$g_{0i} = \begin{cases} y_1^{\beta_i} & if\ m_i^* = 0 \\ g^{\beta_i} & if\ m_i^* = 1 \end{cases},$$

where $1 \le i \le n$. It implicitly sets to private key

$$(a\alpha, \alpha_i \alpha^{m_i^*}, \beta_i \alpha^{1-m_i^*}, 1 \le i \le n)$$

and the public key

$$PK = (g, g_1, g_2, t_{0i}, t_{1i}, v)$$

where $t_{0i} = e(g_1, g_{0i})$ and $t_{1i} = e(g_1, g_{0i})$ for $1 \le i \le n$ and $v = e(g_1, g_2)$.

Signature Queries A issues up to q private signature queries. Each query q_i works as follows:

Suppose A asks for the signature corresponding to an message $M_i = (m_{i1}, \cdots, m_{in})$. The only restriction is that $M_i \ne M^*$. It means that there exists at least an j such that $m_{ij} \ne m_i^*$. To respond the query, B first derives the auxiliary information parameters as follows:

$$h_1' = \begin{cases} g^{\alpha_1^{m_{i1}} \beta_1^{1-m_{i1}}} & if\ m_{i1} \ne m_1^* \\ y_1^{\alpha_1^{m_{i1}} \beta_1^{1-m_{i1}}} & if\ m_{i1} \ne m_1^* \end{cases},$$

$$h_2' = \begin{cases} h_1'^{\alpha_2^{m_{i2}} \beta_2^{1-m_{i2}}} & if\ m_{i2} \ne m_2^* \\ y_1^{\alpha_2^{m_{i2}} \beta_2^{1-m_{i2}}} & if\ m_{i2} = m_2^* \wedge m_{i1} \ne m_1^* \\ y_2^{\alpha_2^{m_{i2}} \beta_2^{1-m_{i2}}} & if\ m_{i2} = m_2^* \wedge m_{i1} = m_1^* \end{cases},$$

$$\vdots$$

Finally, $H' = (h_0, h_1', \cdots, h_n')$ is obtained. For simplify, we suppose that k denotes the number of positions such that $m_{ij} \ne m_i^*$. Then one can obtain $h_n' = y_k^{\tau(M_i)}$, where $\tau(M_i) = \prod_{j=1}^{n} \alpha_j^{m_{ij}} \beta_j^{1-m_{ij}}$ and $k < n$.

Finally, B sets $h_i = \dfrac{h_i'}{y_n g^\gamma}$ and the signature as follows:

$$\sigma = (h_n')^{a\alpha}.$$

In fact, one can obtain

$$\sigma = (h_n')^{a\alpha} = \left(\frac{y_n g^\gamma h_n'}{y_n g^\gamma}\right)^{a\alpha} = (g_2 h_n)^{a\alpha}.$$

Thus, B can derive a valid signature for M_i.

Notice that, from the received inputs, A gets no information at all about the M^* chosen by B, thus such a choice will be identical to the challenge message with probability $\dfrac{1}{2^n}$.

Forgery Finally, A outputs a forged signature σ^* for M^*. Using this signature, B can give the solution to the given the *n*-CDH problem. In fact,

$$\sigma^* = (g_2 h_n)^{a\alpha} = g_2^{a\alpha} h_n^{a\alpha} = y_{n+1}^a g_1^{a\gamma} (h_n)^{a\alpha}.$$

If σ^* is valid, then $h_n = y_k^{\tau(M^*)}$ and $(h_n)^{a\alpha} = y_{k+1}^{a\tau(M^*)}$. Hence

$$\left(\sigma^* \Big/ y_{k+1}^{a\tau(M^*)} g_1^{a\gamma}\right)^{a^{-1}} = y_{n+1}.$$

Probability Following the above, if A has an advantage ε against our scheme, B will solve the *n*-CDH problem with advantage $\frac{\varepsilon}{2^n}$.

IV. APPLICATIONS

A. Identity-based Signature

In this section, based on the our previous signatures, we give an identity based signature scheme in the standard model.

Setup Let G be a group of prime order p and g be a random generator of G. Pick α, $\alpha_1, \cdots, \alpha_n$, $\beta_1, \cdots, \beta_n$, from Z_p at random. Set $g_1 = g^\alpha$. Then choose g_2, $u_0, u_1, \cdots, u_t$ randomly in G, compute $t_{0i} = e(g_1, g^{\alpha_i})$ and $t_{1i} = e(g_1, g^{\beta_i})$. The public key is

$$PK = (g, g_1, g_2, t_{0i}, t_{1i}, u_0, u_1, \cdots, u_t\ v),$$

where $v = e(g_1, g_2)$. The master key is

$$Msk = (\alpha, \alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_n).$$

Keygen Let $ID = (v_1, \cdots v_n)$ denote the user's identity, where $v_i \in \{0,1\}$. Then the private keys corresponding to ID are generated in the following manner. PKG first generates the auxiliary information parameters as follows:

Let $h_0 = g$, then for $i = 1, \cdots, n$, compute

$$h_i = (h_{i-1})^{\alpha_i^{v_i} \beta_i^{1-v_i}}.$$

Then the signature is computed as

$$d_{ID} = (g_2 h_n)^{\alpha}.$$

Sign Message is represented as bit-strings of length *n*. Let $M = (m_1, \cdots, m_t)$ be a *t*-bit message to be signed, where $m_i \in \{0,1\}$. Then pick randomly $r \in Z_p^*$ and compute the signature as follows:

$$\sigma = (\sigma_1, \sigma_2) = (d_{ID}(u_0 \prod_{i=1}^{t} u_i^{m_i})^r, g^r).$$

Verify Given the signature σ, message M and the public keys, verifier accepts the signature if and only if the following holds.

$$e(\sigma_1, g) = v \prod_{i=1}^{n} p_i e(u_0 \prod_{i=1}^{t} u_i^{m_i}, \sigma_2).$$

where

$$p_i = \begin{cases} t_{0i} & if\ m_i = 1 \\ t_{1i} & if\ m_i = 0 \end{cases},$$

Correctness: If σ is valid , one can obtain

$$\begin{aligned}
& e(\sigma_1, g) \\
&= e(d_{ID}(u_0 \prod_{i=1}^{t} u_i^{m_i})^r, g) \\
&= e((g_2 h_n)^{\alpha}(u_0 \prod_{i=1}^{t} u_i^{m_i})^r, g) \\
&= e((g_2 h_n)^{\alpha}, g) e((u_0 \prod_{i=1}^{t} u_i^{m_i})^r, g) \\
&= e(g_2, g_1) e(h_n, g_1)\ e((u_0 \prod_{i=1}^{t} u_i^{m_i})^r, g) \\
&= v e(g_1, g^{\sum_{i=1}^{n} \alpha_i^{m_i} \beta_i^{1-m_i}})\ e(u_0 \prod_{i=1}^{t} u_i^{m_i}, g^r) \\
&= v \prod_{i=1}^{n} e(g_1, g^{\alpha_i^{m_i} \beta_i^{1-m_i}})\ e(u_0 \prod_{i=1}^{t} u_i^{m_i}, \sigma_2) \\
&= v \prod_{i=1}^{n} p_i\ e(u_0 \prod_{i=1}^{t} u_i^{m_i}, \sigma_2).
\end{aligned}$$

Efficiency : The well known identity-based signature in the standard model is issued by Paterson[19]. But it's signature size is 480 bits. The size of our scheme achieves 320 bits.

Security Analysis

Theorem If n-CDH assumption holds, then our scheme is secure.

The proof can be obtained from the previous proof.

B. Threshold Signature

In this paper, we also focus on the short threshold signature. To the best of our knowledge, very few works have dealt with this problem recently. A (*t*, *n*) threshold signature is to distribute a secret key and signature generation among *n* parties in order to remove single point of failure. The goal is to allow any subset of *t* or more parties to jointly produce a signature while preserving security of the system even in the presence of an active adversary up to *t*-1 parties. Threshold signature plays an important role not only in cryptographic literature but also in practice. Table 3 gives a summary of threshold signature size of the different schemes.

TABLE III.
Signature size of the different threshold schemes

Scheme	[20]	[21]	[22]	[24]	[25]	[26]
Model	RO	RO	SM	SM	SM	SM
Size	320	960	320	480	320	320

4.2.1 First Construction

Based on the initial construction, we give a new short threshold signature as follows:

KeyGen Let *G* be a group of prime order *p* and g be a random generator of *G*. Pick α , $\alpha_1, \cdots, \alpha_n$, $\beta_1, \cdots, \beta_n$, from Z_p at random. Set $g_1 = g^{\alpha}$. Then choose g_2 randomly in *G*, pick up randomly $a_1, \cdots, a_{t-1}$ and construct a *t*-1 degree polynomial $f(x) = \alpha + \sum_{i=1}^{t-1} a_i x^i$. Let P_i denote the $i-th$ signer where $i = 1, \cdots, n$. For $i = 1, \cdots, n$, compute $v_i = g^{f(i)}$. The public key is

$$PK=(g,\ g_1,\ g_2,\ v_i, v),$$

where $v = e(g_1, g_2)$. And the private key for each signer P_i is $SK=(f(i),\ \alpha_1, \cdots, \alpha_n\ ,\ \beta_1, \cdots, \beta_n)$.

Partial Signing Message is represented as bit-strings of length *n*. Let $M = (m_1, \cdots, m_n)$ be a *n*-bit message to be signed, where $m_i \in \{0,1\}$. Signer first generates the auxiliary information parameters as follows:

Let $h_0 = g$, then for $i = 1, \cdots, n$, compute

$$h_i = (h_{i-1})^{\alpha_i^{m_i} \beta_i^{1-m_i}}.$$

Then the signature is computed as

$$\sigma_i = (\sigma_{i1}, \sigma_{i2}) = ((g_2 h_n)^{f(i)}, h_n).$$

Threshold Signing Anyone can be designated to reconstruct the partial signature. After having received the partial signatures, the designated signer first verifies the validity of partial signatures. He accepts it if and only if the following holds:

$$e(\sigma_{i1}, g) = e(v_i, g_2) e(v_i, \sigma_{i2}).$$

Let Ω denote the set of validate users. Then the signature is reconstructed as

$$\sigma = (\sigma_1, \sigma_2) = (\prod_{i \in \Omega} \sigma_i^{L_i}, \sigma_{i2}),$$

where L_i is Lagrange coefficient.

Verify Given the signature σ, message M and the public keys, verifier accepts the signature if and only if the following holds:

$$e(\sigma_1, g) = ve(g_1, \sigma_2).$$

Correctness: One can verify easily the correctness of partial signature and threshold signature.

4.2.2 Main Construction

Based on the above construction, we give a new short threshold signature as follows:

KeyGen Let G be a group of prime order p and g be a random generator of G. Pick α, $\alpha_1, \cdots, \alpha_n$, $\beta_1, \cdots, \beta_n$, from Z_p at random. Set $g_1 = g^{\alpha}$. Then choose g_2 randomly in G, compute $t_{0i} = e(g_1, g^{\alpha_i})$ and $t_{1i} = e(g_1, g^{\beta_i})$. Pick up randomly $a_1, \cdots, a_{t-1}$ and construct a t-1 degree polynomial $f(x) = \alpha + \sum_{i=1}^{t-1} a_i x^i$. Let P_i denote the $i-th$ signer where $i = 1, \cdots, n$. For $i = 1, \cdots, n$, compute $v_i = g^{f(i)}$. The public key is

$$PK=(g,\ g_1,\ g_2, t_{0i}, t_{1i}, y_{0i}, y_{1i}\ \ v_i, v),$$

where $y_{0i} = e(g^{f(i)}, g^{\alpha_i}), y_{1i} = e(g^{f(i)}, g^{\beta_i})$, $v_i = e(g^{f(i)}, g_2)$, $v = e(g_1, g_2)$, $i = 1, \cdots, n$. And the private key for each signer P_i is

$$SK=(\ f(i),\ \alpha_1, \cdots, \alpha_n,\ \beta_1, \cdots, \beta_n).$$

Partial Signing Message is represented as bit-strings of length n. Let $M = (m_1, \cdots, m_n)$ be a n-bit message to be signed, where $m_i \in \{0,1\}$. Signer first generates the auxiliary information parameters as follows:

Let $h_0 = g$, then for $i = 1, \cdots, n$, compute

$$h_i = (h_{i-1})^{\alpha_i^{m_i} \beta_i^{1-m_i}}.$$

Then the signature is computed as

$$\sigma_i = (g_2 h_n)^{f(i)}.$$

Threshold Signing Anyone can be designated to reconstruct the partial signature. After having received the partial signatures, the designated signer first verifies the validity of partial signatures. He accepts it if and only if the following holds:

$$e(\sigma_{i1}, g) = v \prod_{i=1}^{n} k_i.$$

where

$$k_i = \begin{cases} y_{0i} & if\ \ m_i = 1 \\ y_{1i} & if\ \ m_i = 0 \end{cases},$$

Let Ω denote the set of validate users. Then the signature is reconstructed as

$$\sigma = \prod_{i \in \Omega} \sigma_i^{L_i},$$

where L_i is Lagrange coefficient.

Verify Given the signature σ, message M and the public keys, verifier accepts the signature if and only if the following holds:

$$e(\sigma, g) = v \prod_{i=1}^{n} p_i.$$

where

$$p_i = \begin{cases} t_{0i} & if\ \ m_i = 1 \\ t_{1i} & if\ \ m_i = 0 \end{cases}.$$

Correctness: One can verify easily the correctness of partial signature and threshold signature.

Efficiency In our first scheme, both the partial signature size and the threshold signature size achieve 320 bits. But in our new scheme, these sizes achieve 160 bits, which is the shortest signature in the standard model at present. In addition, the pairing (y_{0i}, y_{1i}) and (t_{0i}, t_{1i}) are precomputed. Hence, there is only one pairing computation in the verifying stage. Table 4 gives the comprehensive comparison between our signature scheme and other schemes. We assume that all these short signature schemes use the GDH group which is derived from the curve $E/F_{3^{163}}$ defined by the equation $y^2 = x^3 - x + 1$. This group provides 1551-bit discrete log security.

Note: In Table 4, we denote by e a computation of the pairing.

TABLE IV.
Comparison of Efficiency

Scheme	Hardness	Security Model	Signature Size	Verify
[24]	CDH	Standard	480	2*e*
[9]	CDH	Standard	320	2*e*
Our first scheme	*n*-CDH	Standard	320	2*e*
Our second scheme	*n*-CDH	Standard	160	1*e*

4.2.3 Security Analysis

A threshold signature scheme is secure if it has the properties of unforgeability and robustness. The proposed threshold signature has the property of robustness. In fact, the threshold signature is reconstructed from at least t partial signatures. The designated player first verifies all the partial signatures and then chooses the valid ones to reconstruct a threshold signature. Even if having corrupted up to t-1 signers, the adversary still cannot produce a valid threshold signature since there is no way to get the t-th valid partial signature.

In order to prove the property of unforgeability of the scheme, we use the method given by R.Gennaro et al. [23], which indicates that a threshold signature is unforgeable if the underlying signature is secure and the

threshold signature is simulatable. A threshold signature scheme is simulatable if the following properties hold:

(1) The private key generation and distribution protocol is simulatable, that is, there is a simulator to simulate the view of the adversary on the execution.

(2) The threshold signature generation protocol is simulatable. That is, there exists a simulator to simulate the view of the adversary on the execution of threshold signature generation.

The private key generation and distribution protocol in our scheme is only a variant of our first scheme. So we only prove that the threshold signature generation protocol is simulatable. We assume that the adversary has corrupted up to t-1 signers $P_{i_1},\cdots,P_{i_{t-1}}$. The simulator is given the system parameters, the corrupted user's private key, the message *M* and the corresponding signature σ. The simulator first generates the partial signature σ_i for each corrupted signer where $1 \le i \le t-1$. It can compute the partial signature σ_t for uncorrupted signer P_{i_t}. In fact, let $\sigma = \prod_{i\in\Omega}\sigma_i^{L_i}$, where $\Omega = \{i_1,\cdots,i_{t-1},i_t\}$. Then the simulator can compute

$$\sigma_t = \sigma \Big/ \prod_{i\in\Omega-\{i_t\}}\sigma_i^{L_i}.$$

Hence we can obtain the following Lemma.

Lemma The proposed threshold signature is simulatable.

Hence we can obtain the following theorem.

Theorem If *n*-CDH assumption holds, then our scheme is secure.

V. CONCLUSION

In this paper, we propose a short signature scheme which is more efficient than other short signature schemes proposed so far. Based on the *n*-CDH problem, we provide a rigorous proof of security for our scheme in the standard model. Finally, we give the application of the proposed scheme by constructing the short identity-based signature and threshold signature.

ACKNOWLEDGMENT

This work is supported in part by the Nature Science Foundation of China under grant 60970119, 60803149 and the National Basic Research Program of China(973) under grant 2007CB311201.

REFERENCES

[1] M. Bellare, G. Neven. "Multi-signatures in the plain public-key model and a general forking lemma". In proceedings of the 13th ACM Conference on Computer and Communication Security, pp. 390-398, 2006.

[2] K. Barr, K. Asanovic. "Energy aware lossless data compression". In proceedings of the ACM Conference on Mobile Systems, Applications, and Services , 2003.

[3] R. Tso, T.Okamoto. "Efficient Short Signatures from Pairing". In: 2009 Sixth International Conference on Information Technology: New Generations. pp. 417-422, IEEE Press, New York ,2009.

[4] F. Zhang, X. Chen, W.Susilo, and Y. Mu. "A new short signature scheme without random oracles from bilinear pairings". Cryptology ePrint Archive, Report 2005/386, 2005. Available at http://eprint.iacr.org/2005/386.pdf

[5] R. Tso, C. Gu, T. Okamoto and E. Okamoto. "Efficient ID-based digital signatures with message recovery". In Proceedings of the 6th international conference on cryptology and network security (CANS 2007), Lecture Notes in Computer Science 4586, pp.47-59, 2007.

[6] F. Zhang, W.Susilo, and Y. Mu. "Identity-based partial message recovery signatures (or How to shorten IDbased signatures)". FC'05, Lecture Notes in Computer Science 3570, pp.45-56, 2005.

[7] D. Boneh, B. Lynn and H. Shacham. "Short signatures from the Weil pairing". Advances in cryptology – CRYPTO'01, Lecture Notes in Computer Science 2248 , 514-532, 2001.

[8] R. Gennaro , S. Halevi and T. Rabin, Secure hash-and-sign signature without the random oracle, Advances in Cryptology-Eurocrypt 1999, LNCS 1592, pp.123-139, Springer-Verlag , 1999.

[9] D. Boneh and X. Boyen. "Short signatures without random oracles." Advances in Cryptology-Eurocrypt 2004, LNCS 3027, pp.56-73, Springer-Verlag, 2004.

[10] V. K. Wei and T. Hon Yuen. "More Short Signatures without Random Oracles." Cryptology ePrint Archive: Report 2005/463.

[11] F. Zhang , R. Safavi-Naini and W. Susilo. "An efficient signature scheme form bilinear pairing and its application." PKC'04, Lecture Notes in Computer Science 2947 , 277-290, 2004.

[12] S. Goldwasser, S. Micali, and R. Rivest. "A digital signature scheme secure against adaptive chosen message attacks". *SIAM J. Comput.*, 17(2):281-308 ,1988.

[13] H. Du, Q. Wen. "Efficient and provably-secure certificateless short signature scheme from bilinear pairings." *Computer Standards and Interfaces*, 31: 390-394, 2009.

[14] Z. Shao. "A provably secure short signature scheme based on discrete logarithms". *Information Sciences*, 177:5432-5440, 2007.

[15] L. Kang, X. Tang and X. Lu. "A Short Signature Scheme in the Standard Model". Cryptology ePrint Archive, Report 2007/398, 2007. Available at http://eprint.i acr.org/2007/398.pdf.

[16] F. Zhang, X. Chen and Y. Mu. "A new and efficient signature on commitment values". *International Journal of Network Security*, 7(1), pp. 100-105, 2008.

[17] M. Zhang, B. Yang and Y. Zhong. "Cryptanalysis and Fixed of Short Signature Scheme without Random Oracle from Bilinear Parings". *International Journal of Network Security*, 12(2): 159-165, 2011. (Will appear)

[18] F. Guo, Y. Mu and Z. Chen. "Efficient batch verification of short signatures for a single-signer setting without random oracles". Advances in Information and Computer Security, LNCS 5312,pp. 49-63, Springer-Verlag, 2008.

[19] K. G. Paterson, J. C. N. Schuldt. "Efficient identity-based signatures secure in the standard". ACISP 2006, LNCS 4058, pp. 207-222,Springer-Verlag, 2006.

[20] X. Ch, J. M. Liu and X. M. Wang. "An Identity-Based Signature and It s Threshold Version". Proceedings of the 19th International Conference on Advanced Information Networking and Applications(AINA'05). Washington : IEEE Computer Society, pp. 973-977, 2005.

[21] X. F. Chen, F. G. Zhang. "New ID-based Threshold Signature Scheme from Bilinear Pairings". INDOCRYPT

2004, LNCS 3348. Berlin: Springer-Verlag, pp. 371-383, 2004.
[22] H. Wang, Y. Q. Zhang and D. G. Feng. "Short Threshold Signature Schemes without Random Oracles." Advances in Cryptology-Docrypt 2005, Lectures Notes in Computer Science 3797. Berlin: Springer-Verlag, pp. 297-310, 2005.
[23] R. Gennaro, S. Jarecki. "Robust Threshold DSS Signatures." Advances in Cryptology-ROCRYPT 1996, Lectures Notes in Computer Science 1070. Berlin: Springer2Verlag,pp. 354-371, 1996.
[24] H. Xiong, Z. Qin, and F. Li. "Identity-based Threshold Signature Secure in the Standard Model". *International Journal of Network Security*, Vol.10, No.1, PP.75-80(2010).
[25] Z. Wang, H. Qian and Z. Li. "Adaptively Secure Threshold Signature Scheme in the Standard Model". *Informatic*, 2009, Vol. 20, No. 4, pp. 591-612, 2009.
[26] L.Y. Zhang, Y. P. Hu and Z. Liu. "Provable secure ID-based threshold signature scheme without random oracles". *Journal of Xidian University*, Vol. 35, No. 1, pp. 81-86, 2008.

Leyou Zhang: male. He received his M.E. and Ph.D. degrees in Applied Mathematics form Xidian University, Xi'an, China in 2002 and 2009, respectively. Now he is an Associate Professor in the department of Mathematical science of Xidian University. His current research interests include network security, computer security, and cryptography. He has published more than thirty papers in international and domestic journals and conferences.

Qing Wu: female. She received her Ph.D. from the Xidian University in 2009. Now she is an Associate Professor in the school of automation of Xi'an institute of posts and telecommunication. Her current research interests include information security and applied mathematics. She has published more than twenty papers in international and domestic journals and conferences.

Yupu Hu: male. He received his Ph.D. from the Xidian University in 1999. Now he is a Professor in the School of Telecommunications Engineering of Xidian University. His current research interests include information security and cryptography. He has published more than a hundred papers in international and domestic journals and conferences. He is a Member of China Institute of Communications and a Director of Chinese Association for Cryptologic Research.