Anais da Academia Brasileira de Ciências
ISSN: 0001-3765
aabc@abc.org.br
Academia Brasileira de Ciências
Brasil

DONG, GUOFAGN; GAO, FEI; SHI, WENBO; GONG, PENG
An efficient certificateless blind signature scheme without bilinear pairing
Anais da Academia Brasileira de Ciências, vol. 86, núm. 2, junio, 2014, pp. 1003-1011
Academia Brasileira de Ciências
Rio de Janeiro, Brasil

Anais da Academia Brasileira de Ciências (2014) 86(2): 1003-1011
(Annals of the Brazilian Academy of Sciences)
Printed version ISSN 0001-3765 / Online version ISSN 1678-2690
http://dx.doi.org/10.1590/0001-3765201420130199
www.scielo.br/aabc

An efficient certificateless blind signature scheme without bilinear pairing

GUOFAGN DONG[1,4], FEI GAO[1], WENBO SHI[2] and PENG GONG[3]

[1]Yunnan Nationalities University, School of Electrical and Information Technology,
Yi Er Yi Avenue, No.134, 650031, Kunming,Yunnan, China
[2]Northeastern University at Qinhuangdao,School of Computer and Communication Engineering,
Taishan Road, No. 143, Economic and Technological Development Zone, 066004, Qinhuangdao, Hebei, China
[3]Beijing Institute of Technology, School of Mechatronical Engineering South Zhongguancun Street,
No.5 Haidian District, 100081, Beijing, China
[4]Kunming University of Science and Technology, National Engineering Laboratory for Vacuum Metallurgy,
Yi Er Yi Avenue, No. 68, 650031, Kunming, Yunnan, China

Manuscript received on May 27, 2013; accepted for publication on December 10, 2013

ABSTRACT

Recently, the certificateless public key cryptography (CLPKC) has been studied widely since it could solve both of the certificate management problem in traditional public key cryptography (TPKC) and the key escrow problem in the identity-based public key cryptography (ID-based PKC). To satisfy requirements of different applications, many certificateless blind signature (CLBS) schemes using bilinear pairing for the CLPKC setting have been proposed. However, the bilinear pairing operation is very complicated. Therefore, the performance of those CLBS schemes is not very satisfactory. To solve the problem, we propose an efficient CLBS scheme without bilinear pairing. Performance analysis shows that the proposed scheme could reduce costs of computation and storage. Security analysis shows the proposed scheme is provably secure against both of two types of adversaries.

Key words: blind signature, certificateless cryptography, bilinear pairing, random oracle model.

INTRODUCTION

The blind signature (BS) scheme is a variation of digital signature scheme, which was first proposed by Chaum (1983). In the BS scheme, a user could get a signature for any message but the signer does not know the content of the message. Due to such properties, BS schemes are widely used in electronic voting, electronic payment and electronic cash.

After Chaum's work, many BS schemes in the traditional public key cryptography (TPKC) were proposed for different applications. However, the TPKC faces with the certificate management problem since a certificate generated by a trusted third party is needed to bind the user's identity and his public key. To solve the problem, Shamir (1984) introduced the concept of the identity-based public key cryptography (ID-based PKC). In the ID-based PKC, no certificate is required since the user's identity is his public key. However, the ID-based PKC faces with the key escrow problem since the user's private key is generated by the key generation centre (KGC) and the KGC knows all users' private keys. To solve the certificate management problem in the TPKC and the key escrow problem in ID-based PKC, Al-Riyami and Paterson (2003) proposed

Correspondence to: Peng Gong
E-mail: penggong@bit.edu.cn

the concept of the certificateless public key cryptosystem (CLPKC). In the CLPKC, a user's private key consists of two parties, i.e. a partial secret key generated by the KGC and a secret value generated by the user.

Since groundbreaking work of Al-Riyami and Paterson (2003), many certificateless encryption (CLE) schemes (Sun and Zhang 2010) (Yang and Tan 2011), certificateless signature (CLS) schemes (Tian and Huang 2012) (Tsai et al. 2012) (Gong and Li 2012) (He et al. 2012c, 2013a, b) and certificateless key agreement schemes (HE et al. 2011c, 2012a, d) have been proposed for applications in CLPKC setting. Several certificatless blind signature (CLBS) schemes (Zhang and Zhang 2008) (Wang and Lu 2008) (Yang et al. 2009) (Sun and Wen 2009) (Zhang and Gao 2010) (Zhang et al. 2011) also were proposed. Zhang and Zhang (2008) proposed the fist CLBS scheme using bilinear pairing. Then several other CLBS schemes (Wang and Lu 2008) (Yang et al. 2009) (Sun and Wen 2009) (Zhang and Gao 2010) (Zhang et al. 2011) using bilinear pairing were proposed to improve performance or security of Zhang et al.'s scheme. However, the bilinear pairing operation is very complicated. Theoretical analysis (Chen et al. 2007) (Hankerson et al. 2004) and experimental results (Cao and Kou 2010) (He et al. 2011a, 2012b) demonstrate that the computation cost of a bilinear pairing operation is similar to that of a dozen or so elliptic curve scalar multiplication operations. Therefore, the performance of those CLBS schemes is not very satisfactory and CLBS scheme without bilinear pairing is required for practical applications.

In this paper, we propose an efficient CLBS scheme without bilinear pairing operation and show it is secure against both of two kinds of various attacks. Section 2 gives some background about CLBS schemes. Section 3 proposes a new CLBS scheme without bilinear paring. Security analysis and performance analysis are proposed in Section 4 and Section 5 separately. Some conclusions are given in Section 6.

PRELIMINARIES

Notations

For convenience, some notations used in the paper are described as follows.

- p, n: two large prime numbers;
- F_p: a finite field;
- $E(F_p)$: an elliptic curve defined by the equation $y^2 = x^3 + ax + b$ over F_p, where a, $b \in F_p$ and $\Delta = 4a^3 + 27b^2 \neq 0$ (Koblitz 1987);
- G: the group with order n consisting of points on $E(F_p)$ and the point at infinity O;
- P: a generator of the group G;
- DLP: the discrete logarithm problem (DLP), whose task is to compute x for given $Q = xP$;

CLBS Scheme

There are six polynomial time algorithms (Zhang et al. 2011) in a CLBS scheme, i.e. *Setup*, *PartialPrivateKeyExtract*, *SetSecretValue*, *SetPublicKey*, *Sign* and *Verify*.

Setup: Taking a security parameter k as input, this algorithm is executed by the KGC to generate the system parameters *params* and the master key *mk*.

PartialPrivateKeyExtract: Taking the system parameters *params*, the master key *mk* and a users identity ID as inputs, this algorithm is executed by the KGC to generate the users partial private key ID_D.

SetSecretValue: Taking the system parameters *params* as input, this algorithm is executed by a user to generate his secret value x_{ID}.

SetPublicKey: Taking the system parameters *params* and a users secret value x_{ID} as inputs, this algorithm is executed by the user to generate his public key PK_{ID}.

Sign: Taking the system parameters *params*, the partial private key D_{ID}, the secret value x_{ID} and a message m as inputs, this algorithm is executed by the user to generate a signature. There are three sub-algorithms in the algorithm, i.e. *Blind*, *BSign* and *Unblind*.

(1) *Blind*. Taking message m and a random string r as inputs, the sub-algorithm is executed by the user to generate a blinded message m'.

(2) *BSign*. Taking a blind message m', the signers private signing key sk_{ID_A} and the system parameters *params* as inputs, the sub-algorithm is executed by the signer to generate a blind signature σ'.

(3) *Unblind*. Taking a blind signature σ', the previously generated random string r and the system parameters *params* as inputs, the sub-algorithm is executed by the user to generate an unblinded signature σ.

Verify: Taking the system parameters *params*, a signer's identity *ID* , a signer's public key PK_{ID}, a message m and a signature σ as inputs, this algorithm is executed by the verifier to verify the legality of σ. If σ is legal, 1 will be outputted; otherwise, 0 will be outputted.

Security Model for CLBS Scheme

There are two kinds of adversaries in the CLBS scheme, i.e. the Type I adversary A_1 and the Type II adversary A_2. A_1 could replace user's public keys with some value he chooses, but he cannot get the master key. A_2 represents a malicious KGC, who cannot replace users' public keys but he could use the master key to generate users' partial private keys. The type adversaries in CLBS could be divided into normal adversary, strong adversary, and super adversary according to their attacks power (Huang et al. 2007). In the security analysis of the proposed CLBS scheme, we just need to consider two strongest types of adversaries, i.e. the super Type I adversary and the super Type II adversary. The abilities of an adversary $A \in \{A_1, A_2\}$ are formally modeled by queries issued by adversaries.

ExtractPartialPrivateKey(*ID*): The adversary A could get the partial private key D_{ID} through the query.

ExtractSecretValue(*ID*): The adversary A could get the secret value x_{ID} through the query.

RequestPublicKey(*ID*): The adversary A could get the public key PK_{ID} through the query. *ReplacePublicKey*(*ID*, PK'_{ID}): The adversary A could replace the public key PK_{ID} with a new public key PK'_{ID} through the query.

SuperSign(*ID*, *m*): The adversary A could get a signature σ through the query such that $1 \leftarrow$ *Verify* (*params*, *ID*, PK'_{ID}, *m*, σ), where PK'_{ID} is the current public key and it may be replaced by A.

We consider the following games against the super Type I and the super Type II adversaries.

Game 1: The first game is performed between a challenger C and a super Type I adversary A_1 for a CLBS scheme as follows.

Initialization. C runs *Setup* algorithm and generates a master secret key *mk*, public system parameters *params*. C keeps *mk* secret and then gives *params* to A_1.

Queries. A_1 can adaptively issue the *Extract-PartialPrivateKey*, *ExtractSecretValue*, *Request-PublicKey*, *ReplacePublicKey*, and *SuperSign* queries to C.

Output. Eventually, A_1 outputs (ID_t, m_t, σ_t). A_1 wins the game if

(1) *ExtractPartialPrivateKey*(*IDt*) and *SuperSign* (ID_t, m_t) queries have never been queried.

(2) $1 \leftarrow$ *Verify*(*params*, ID_t, PK'_{ID_t}, *m*, σ), where PK'_{ID_t} which may be replaced by A_1 is the current public key of ID_t

Game 2: The second game is performed between a challenger C and a super Type II adversary A_2 for a CLBS scheme as follows:

Initialization. C runs *Setup* algorithm and generates a master secret key *mk*, public system parameters *params*. C gives *mk* and *params* to A_2.

Queries. A_2 can adaptively issue the *Extract-PartialPrivateKey*, *ExtractSecretValue*, *Request-PublicKey*, and *SuperSign* queries to C.

Output. Eventually, A_2 outputs (ID_t, m_t, σ_t). A_1 wins the game if

(1) *ExtractSecretValue*(*IDt*) and *SuperSign* (ID_t, *mt*) queries have never been queried.

(2) $1 \leftarrow Verify(params, ID_t, PK'_{ID_t}, m, \sigma)$, where PK_{ID_t} is the original public key of ID_t

Definition 1 (Blindness) (Zhang et al. 2011). Suppose two honest users U_0 and U_1 engage in the blind signature issuing protocol with a probabilistic polynomial-time adversary A on two messages m_b and m_{1-b}, and output two signatures σ and σ' respectively, where $b \in \{0; 1\}$ is a random bit chosen uniformly. At last, (m_0, m_1, σ_b, σ_{1-b}) are sent to A and then A outputs $b' \in \{0, 1\}$. We call a signature scheme is blind if the inequation $|Pr[b = b'] - 1/2| < n^{-c}$ holds for all such adversaries A, any constant c, and sufficiently large n.

Definition 2. We say that a certicateless blind signature scheme is secure against the super Type I adversary if for any polynomially bounded super Type I adversary A_1, $Succ_{A_1}$ is negligible, where $Succ_{A_1}$ denote the success probability that A wins in **Game 1**.

Definition 3. We say that a certicateless blind signature scheme is secure against the super Type II adversary if for any polynomially bounded super Type II adversary A_2, $Succ_{A_2}$ is negligible, where $Succ_{A_2}$ denote the success probability that A_1 wins in the **Game 2**.

We say a certificateless blind signature scheme is secure if it is blind and secure against two types of adversaries.

THE PROPOSED CLBS SCHEME

Based on He et al. work (He et al. 2011a, b), we propose a new CLBS scheme without bilinear pairing. The proposed scheme consists of six algorithms, i.e. *Setup*, *PartialPrivateKeyExtract*, *SetSecretValue*, *SetPublicKey*, *Sign* and *Verify*. The details of these algorithms are described as follows:

Setup: Given a security parameters k, KGC does the following steps to generate the system parameters and the mast key.

(1) KGC chooses a k-bit prime p, generates an elliptic curve $E(Fp)$ over finite feld F_p. KGC chooses a group G) with order n over $E(F_p)$ and chooses a generator P) of the group G).

(2) KGC chooses a random $s \in Z_n^*$ as the master mk and computes public key $P_{pub} = sP$.

(3) KGC chooses three secure hash functions $H_1 : \{0, 1\}^* \times G \rightarrow Z_n^*$, $H_2 : \{0, 1\}^* \times G \times \{0, 1\}^* \times G \times G \times G \rightarrow Z_n^*$ and $H_3 : \{0, 1\}^* \times G \times G \times G \rightarrow Z_n^*$.

(4) KGC publishes the system parameter $params = \{p, n, E(F_p), G, P, P_{pub}, H_1, H_2, H_3\}$ and keeps the master key s secretly.

PartialPrivateKeyExtract: Given the system parameter *params*, the master key *mk*, and a user's identity *ID*, KGC generates a random number $r_{ID} \in Z_n^*$, computes $R_{ID} = r_{ID}P$, $h_{ID} = H_1(ID, R_{ID})$ and $s_{ID} = r_{ID} + h_{ID}s \bmod n$. Then KGC returns the partial private key $D_{ID} = (s_{ID}, R_{ID})$ to the user.

SetSecretValue: Given the system parameter *params*, the user with identity ID generates a random number $x_{ID} \in Z_n^*$, computes $P_{ID} = x_{ID}P$ and sets x_{ID} as his secret value.

SetPublicKey: Given the system parameter *params* and the user's secret value x_{ID}, the user computes his public key $P_{ID} = x_{ID}P$.

Sign: Given a message m, the following three sub-algorithms are executed to generate a legal signature. First of all, the signer generates a random number $\overline{k} \in Z_n^*$, computes $\overline{R} = \overline{k}P$ and sends $\overline{R}$ and R_{ID} to the user.

(1) *Blind*: Upon receiving the message $\overline{R}$ and R_{ID}, the user generates three random numbers $\alpha, \beta, \gamma \in Z_n^*$, computes $h = H_2(m, R, ID, R_{ID}, PK_{ID}, P_{pub})$, $h_{ID} = H_1(ID, R_{ID})$, $\hat{h} = H_3(ID, R_{\mathrm{ID}}, PK_{ID}, P_{pub})$, $R = \alpha P + \beta P + \gamma(\hat{h}PK_{ID} + R_{ID} + h_{ID}P_{pub})$ and $\overline{h} = \alpha^{-1}(h + \gamma) \bmod n$. At last, the user sends $\overline{h}$ to the signer.

(2) *BSign*: Upon receiving the message $\overline{h}$, the signer computes $\hat{h} = H_3(ID, R_{ID}, PK_{ID}, P_{pub})$ and $\overline{z} = \overline{h}(\hat{h}x_{ID} + s_{ID}) + \overline{k} \bmod n$. At last, the signer sends $\overline{z}$ to the user.

(3) *Unblind*: Upon receiving the message $\bar{z}$, the user computes $z = \alpha\bar{z} + \beta \bmod n$ and outputs the signature $\sigma = (R_{ID}, R, z)$.

Verify: To verify the legality of the signature $\sigma = (R_{ID}, R, z)$ for message m and the signer with identity ID, the verifier computes $h = H_2(m, R, ID, R_{ID}, PK_{ID}, P_{pub})$, $h_{ID} = H_1(ID, R_{ID})$ and $\hat{h} = H_3(ID, R_{ID}, PK_{ID}, P_{pub})$. The verifier checks whether zP and $h(\hat{h}PK_{ID} + R_{ID} + h_{ID}P_{pub}) + R$ are equal. If they are equal, 1 is returned; otherwise, 0 is returned.

SECURITY ANALYSIS

In this section, we will analyze the security of the proposed CLBS scheme. We will show the proposed scheme is provably secure in the random oracle model (Bellare and Rogaway 1993). The following theorems are proposed for the security.

Theorem 1. The proposed CLBS scheme is blind.

Proof. Let (R_{ID}, R, z) be one of the two signatures given to the adversary A. Let $(R_{ID}, \overline{R}, \overline{h}, \bar{z})$ be the message transmitted between the user and the signer. We just need to show that there are three random factors (α, β, γ) that could map $(R_{ID}, \overline{R}, \overline{h}, \bar{z})$ to (R_{ID}, R, z). From the description of the proposed CLBS scheme, we could get that

$$R = \alpha\overline{R} + \beta P + \gamma(\hat{h}PK_{ID} + R_{ID} + h_{ID}P_{pub}) \quad (1)$$

$$\overline{h} = \alpha^{-1}(h + \gamma) \bmod n \quad (2)$$

$$z = \alpha\bar{z} + \beta \bmod n \quad (3)$$

Through equations (2) and (3), we could get that $\beta = z - \alpha\bar{z} \bmod n$ and $\gamma = \alpha\overline{h} - h \bmod n$. With the two above equations and equation (1), we could get that only a unique element $\alpha \in Z_n^*$ exists. Then we could get β and γ also exist uniquely since $\beta = z - \alpha\bar{z} \bmod n$ and $\gamma = \alpha\overline{h} - h \bmod n$.

Then, we could conclude that three random factors (α, β, γ) always exist between (R_{ID}, R, z) and $(R_{ID}, \overline{R}, \overline{h}, \bar{z})$. Therefore, A outputs a correct value b' with probability exactly 1/2 and the proposed CLBS scheme is blind.

Theorem 2. The proposed CLBS scheme is secure against the super Type I adversary in random oracle model if the DLP is hard.

Proof. Suppose there is a super Type I adversary A_1 has non-negligible ε advantage in attacking the proposed CLBS scheme. We will show that an algorithm C could solve the DLP running A_1 as a subroutine.

Given a DLP instance $Q = \alpha P$ for randomly chosen $\alpha \in Z_n^*$, C picks an identity ID^* at random as the challenged ID, sets $P_{pub} = Q$, chooses three secure functions and gives system parameters to A_1. C answers A_1's queries as follows.

- H_1 query: A_1 maintains a list L_{H_1} of tuples $< ID, R_{ID}, h_{ID} >$. Upon receiving a query on a message ID, R_{ID}, C returns h_{ID} to A_1 if L_{H_1} contains a tuple $< ID, R_{ID}, h_{ID} >$, otherwise, C picks a random number $h_{ID} \in Z^*_n$, adds $< ID, R_{ID}, h_{ID} >$ to L_{H_1} and returns h_{ID} to A_1.
- H_2 query: A_1 maintains a list L_{H_2} of tuples $< m, R, ID, R_{ID}, PK_{ID}, P_{pub}, h >$. Upon receiving a query on a message $< m, R, ID, R_{ID}, PK_{ID}, P_{pub} >$, C returns h to A_1 if L_{H_2} contains a tuple $< m, R, ID, R_{ID}, PK_{ID}, P_{pub}, h >$; otherwise, C picks a random number $h \in Z^*_n$, adds $< m, R, ID, R_{ID}, PK_{ID}, P_{pub}, h >$ to L_{H_2} and returns h to A_1.
- H_3 query: A_1 maintains a list L_{H_3} of tuples $< ID, R_{ID}, PK_{ID}, P_{pub}, h >$. Upon receiving a query on a message $< ID, R_{ID}, PK_{ID}, P_{pub} >$, C returns h to A_1 if L_{H_3} contains a tuple $< ID, R_{ID}, PK_{ID}, P_{pub}, h >$, otherwise, C picks a random number $h \in Z^*_n$, adds $< ID, R_{ID}, PK_{ID}, P_{pub}, h >$ to L_{H_3} and returns h to A_1.
- *ExtractPartialPrivateKey*(ID) query. Upon receiving a query with the user's identity ID, C answers the query as follows.

  1) If $ID \neq ID^*$, C generates two random numbers $a_{ID}, b_{ID} \in Z^*_n$, sets $R_{ID} \leftarrow a_{ID}P -$

$b_{ID}P_{pub}$, $h_{\text{ID}} = H_1(ID, R_{ID})$ b_{ID} and $s_{ID} \leftarrow a_{ID}$. C adds $< ID, R_{ID}, h_{ID} >$ and $< ID, s_{ID}, R_{ID}$ to $L_{H_1} >$ and L_{K_1} separately. C returns $< s_{ID}, R_{ID} >$ to A_1.

2) Otherwise, C generates two random numbers $a_{ID}, b_{ID} \in Z_n^*$, sets $R_{ID} \leftarrow a_{ID}P$, $h_{ID} = H_1(ID, R_{ID}) \leftarrow b_{ID}$ and $s_{ID} \leftarrow \perp$. C adds $< ID, R_{ID}, h_{ID} >$ and $< ID, \text{s}_{ID}, R_{ID}$ to $L_{H_1} >$ and L_{K_1} separately. C returns $< \text{s}_{ID}, R_{ID}$ to A_1.

- *RequestPublicKey*(ID) query. Upon receiving a query with the user's identity ID , C returns PK_{ID} to A_1.
- *ExtractSecretValue*(ID) query. Upon receiving a query with the user's identity ID, C picks a random number $x_{ID} \in Z_n^*$, computes $PK_{ID} = x_{ID}P$, adds $< ID, x_{ID}, PK_{ID} >$ to L_{K_2} and returns x_{ID} to A_1.
- *ReplacePublicKey*(ID, $PK'_{ID} = x'_{ID}P$) query. Upon receiving a query with the message (ID; $PK'_{ID} = x'_{ID}P$), C sets $PK_{ID} = PK'_{ID}$, and $x_{ID} = x'_{ID}$ if the list L_{K_2} contains $< ID, x_{ID}, PK_{ID} >$, otherwise, C makes a *ExtractSecretValue* query with ID, sets $PK_{ID} = PK'_{ID}$, and $x_{ID} = x'_{ID}$.
- *SuperSign*(ID, m) query. Upon receiving a query with the message (ID, m), C looks up L_{K_1} and L_{K_2} for the tuples$< ID, s_{ID}, R_{ID} >$ and $< ID, x_{ID}, PK_{ID} >$ and performs as follows:

  1) If $x_{ID} \neq \perp$, then C performs according to the description of the scheme, and returns the generated (R_{ID}, R, z) to A_1.

  2) Otherwise, C generates two random a; $b \in Z_n^*$, sets $z \leftarrow a$, $H_2(m, R, ID, R_{ID}, PK_{ID}, P_{pub}) \leftarrow b$, $R \leftarrow aP - b(\hat{h}PK_{ID} + R_{ID} + h_{ID}P_{pub})$, where $\hat{h} = H_3(ID, R_{ID}, PK_{ID}, P_{pub})$. C returns $\sigma = (R_{ID}, R, s)$ to A_1 and adds $< m, R, PK_{ID}, R_{ID}, P_{pub}, b >$ to L_{H_2}.

Eventually, A_1 outputs a valid signature (ID, mt, σ_t), where $\sigma_t = (\text{R}_{ID_t}, \text{R}, \text{z})$. If $ID_t \neq ID^*$, C stops the simulation; otherwise, C finds $< ID_t, s_{IDt}, R_{IDt} >$ and $< ID_t, \text{x}_{ID_t}, PK_{ID_t} >$ in L_{K_1} and L_{K_2} respectively. From the forgery lemma (David and Jacque 2000), we know that A_1 could output another legal signature $\sigma'_t = (R_{ID_t}, R, z')$ if the same random number replayed but with different choice of the random oracle H_2.

The following equation holds because the signature is valid

$$zP = h(\hat{h}PK_{IDt} + R_{IDt} + h_{IDt}P_{pub}) + R \qquad (4)$$

and

$$z'P = h(\hat{h}PK_{IDt} + R_{IDt} + h_{IDt}P_{pub}) + R \qquad (5)$$

Let l, x_{ID_t}, r_{ID_t} and α denote discrete logarithms of R; PK_{ID_t}, R_{ID_t} and P_{pub} respectively, i.e. $R = lP$, $PK_{ID_t} = x_{ID_t}P$, $R_{ID_t} = r_{ID_t}P$ and $P_{pub} = P$. Then we could get the following two equations.

$$z = h(\hat{h}x_{ID_t} + r_{ID_t} + h_{ID_t}) + l \qquad (6)$$

and

$$z' = h'(\hat{h}x_{ID_t} + r_{ID_t} + h_{ID_t}\alpha) + l \qquad (7)$$

Because only l and α are unknown to C in the above two equations, he could solve those equations and outputs α as the solution of the DLP. Since ID^* is randomly chosen, then we have $Pr[ID^* = ID_t] = 1/q_{H_1}$, where q_{H_1} is the number of H_1 query A_1 has made. C could solve the DLP with a non-negligible probability ε/q_{H_1}. This contradicts the hardness of the DLP. Therefore, the proposed scheme is secure against the super Type I adversary.

Theorem 3. The proposed CLBS scheme is secure against the super Type II adversary in random oracle model if the DLP is hard.

Proof. Suppose there is a super Type II adversary A_2 has non-negligible advantage ε in attacking the proposed CLBS scheme. We will show that there is an algorithm C could solve the DLP running A_2 as a subroutine.

Given a DLP instance $Q = \alpha P$ for randomly chosen $\alpha \in Z_n^*$, C picks an identity ID^* at random as

the challenged ID, chooses a random number $s \in Z_n^*$, sets $P_{pub} = sP$, and chooses three secure functions. C give the master key s and system parameters to A_2. C answer H_1 query, H_2 query, H_3 query, *ExtractPartialPrivateKey* query, *ReplacePublicKey* query and *SuperSign*(ID, m) query like he does in the above theorem. C simulates other oracle queries of A_2 as follows:

- *ExtractPartialPrivateKey*(ID) query. Upon receiving a query with the user's identity ID, C generates a random number $r_{ID} \in Z_n^*$, computes $R_{ID} = r_{ID}P$, $h_{ID} = H_1(ID, R_{ID})$ and $s_{ID} = r_{ID} + h_{ID}s \bmod n$. C adds $< ID, R_{ID}, h_{ID} >$ and $< ID, s_{ID}, R_{ID} >$ to L_{H_1} and L_{H_2} separately. Then, C returns $< s_{ID}, R_{ID} >$ to A_2.
- *ExtractSecretValue*(ID) query. Upon receiving a query with the user's identity ID, C does as follows. If $ID \neq ID^*$, C picks a random number $x_{ID} \in Z_n^*$ and computes $PK_{ID} = x_{ID}P$, returns x_{ID} to A_2 and adds $< ID, x_{ID}, PK_{ID} >$ to L_{K_2} ; otherwise, C sets $PK_{ID} = Q$, adds $< ID, \perp, PK_{ID} >$ to L_{K_2}.

Eventually, A_2 outputs a valid signature (ID, m_t, σ_t), where $\sigma_t = (R_{ID_t}, R, z)$. If $ID_t \neq ID^*$, C stops the simulation; otherwise, C finds $< ID_t, s_{ID_t}, R_{ID_t} >$ and ID_t, x_{ID_t}, PK_{ID_t} in L_{K_1} and L_{K_2} respectively. The public key PK_{ID_t} is the original pub key is ID_t. From the forgery lemma (David and Jacque 2000), we know that A^2 could output another legal signature $\sigma'_t = (RI_{D_t}, R, z')$ if the same random number replayed but with different choice of the random oracle H_2. The following equation holds because the signature is valid.

$$zP = h(\hat{h}PK_{ID_t} + R_{ID_t} + h_{ID_t}P_{pub}) + R \qquad (8)$$

and

$$z'P = h'(\hat{h}PK_{ID_t} + R_{ID_t} + h_{ID_t}P_{pub}) + R \qquad (9)$$

Let l, α, r_{ID_t} and s denote discrete logarithms of R, PK_{ID_t}, R_{ID_t} and P_{pub} respectively, i.e. $R = lP$, $PK_{ID_t} = P$, $R_{ID_t} = r_{ID_t}P$ and $P_{pub} = sP$. Then we

$$z = h(\hat{h}\alpha + r_{ID_t} + h_{ID_t}s) + l \qquad (10)$$

and

$$z' = h'(\hat{h}\alpha + r_{ID_t} + h_{ID_t}s) + l \qquad (11)$$

Because only l and α are unknown to C in the above two equations, he could solve those equations and outputs as the solution of the DLP. Since ID^* is randomly chosen, then we have $Pr[ID^* = ID_t] = 1/q_{H_1}$, where q_{H_1} is the number of H_1 query A_2 has made. C could solve the DLP with a non-negligible probability $\varepsilon = q_{H_1}$. This contradicts the hardness of the DLP. Therefore, the proposed scheme is secure against the super Type II adversary.

PERFORMANCE ANALYSES

In this section, we will compare the efficiency of the proposed CLBS scheme with the three latest CLBS schemes, i.e. Sun et al.'s CLBS scheme (Sun and Wen 2009), Zhang et al.'s scheme (Zhang and Gao 2009) and Zhang et al.'s CLBS scheme (Zhang et al. 2011).

To achieve the security level of 1024 bits RSA, bilinear pairing-based CLBS scheme and ECC-based CLBS scheme, we have to use the Tate pairing defined over a supersingular elliptic curve on a finite field F_q and a secure elliptic curve on a finite field F_p separately, where the length of q and p are 512 bits and 160 bits respectively. We also assume the output of the hash function is 160 bits. Some notations are defined as follows.

- e: a bilinear pairing operation;
- E: a modular exponentiation operation;
- M: an ECC-based scale multiplication operation;
- *Mpair*: a bilinear pairing-based scale multiplication operation;

It is well known that the computational cost of a hash function operation could be ignored when it is compared with that of a bilinear pairing operation, a modular exponentiation operation, a ECC-based

TABLE I
Performance comparisons of different schemes.

	Sun et al.'s scheme	Zhang and Gao's scheme	Zhang et al.'s scheme	Our scheme
Sign	$3E + 1M_{pair}$	$3E + 2M_{pair}$	$2e + 2E + 1M_{pair}$	$6M$
Verify	$1e + 1E + 1M_{pair}$	$1e + 1E + 1M_{pair}$	$3e + 1E$	$4M$
Size	256B	148B	148B	100B

scale multiplication operation or a bilinear pairing-based scale multiplication operation. Therefore, we just need to counter the bilinear pairing operation, the modular exponentiation operation, the ECC-based scale multiplication operation and the bilinear pairing-based scale multiplication operation in performance comparisons. The comparisons are listed in Table I.

Theoretical analyses (Chen et al. 2007) and experimental results (Cao and Kou 2010) (He et al. 2011a, 2012b) demonstrate that the computation costs of a bilinear pairing operation, a modular exponentiation operation and a bilinear pairing-based scale multiplication operation are about 19, 3 and 3 times of that of a ECC-based scale multiplication operation. Therefore, we could get that the computational cost of the *Sign* algorithm in the proposed scheme is 60%, 54.55% and 10.71% of that in Sun et al.'s CLBS scheme (Sun and Wen 2009), Zhang et al.'s CLBS scheme (Zhang and Gao 2009) and Zhang et al.'s CLBS scheme (Zhang et al. 2011) separately. The computational cost of the *Verify* algorithm in the proposed scheme is 16%, 16%, 6.35% of that in Sun et al.'s CLBS scheme (Sun and Wen 2009), Zhang et al.'s CLBS scheme (Zhang and Gao 2009) and Zhang et al.'s CLBS scheme (Zhang et al. 2011) separately. Besides, the signature size in the proposed scheme is 39.06%, 39.06% and 67.57% of that in Sun et al.'s CLBS scheme (Sun and Wen 2009), Zhang and Gao's CLBS scheme (Zhang and Gao 2009) and Zhang et al.'s CLBS scheme (Zhang et al. 2011) separately. Therefore, the proposed CLBS scheme has better performance than those previous CLBS schemes.

CONCLUSIONS

Recently, the certicicateless public key cryptography without bilinear pairing operation attracted wide attention since such schemes have better performance than traditional ones. In this paper, we propose the first CLBS scheme without bilinear pairing operation. Performance analyses demonstrates that the proposed scheme has much better performance than previous CLBS schemes. We also show that the proposed scheme is provably secure against both of two types of adversaries in the random oracle. Therefore, the proposed scheme is more suitable for practical applications.

ACKNOWLEDGMENTS

The authors thank Dr. Alexander Kellner and the anonymous reviewers for their valuable comments. This research was supported by the Application Foundation Research Project of Yunnan Science and Technology Department (No. 2011FZ168), the Key Scientific Research Projects of Yunnan Education Department (No. ZD201109) and the National Natural Science Foundation of China (Nos. 61202447 and 61201180).

RESUMO

Recentemente, a criptografia de chave pública sem certificado (CLPKC) tem sido amplamente estudada, uma vez que poderia resolver o problema de gerenciamento de certificados na criptografia de chave pública tradicional (TPKC) e o problema chave de escrow da criptografia de chave pública baseada em identidade (ID-based PKC). Para atender aos requisitos de diferentes aplicações, têm sido propostos muitos sistemas de assinatura

cega sem certificado (CLBs), sistemas que utilizam o emparelhamento bilinear para a configuração de CLPKC. No entanto, a operação de emparelhamento bilinear é muito complicada. Portanto, o desempenho desses regimes CLBs não é muito satisfatório. Para resolver o problema, propomos um esquema de CLBS eficiente sem emparelhamento bilinear. Uma análise de desempenho mostra que o esquema proposto poderia reduzir os custos de computação e armazenamento. Uma análise de segurança mostra que o esquema proposto é comprovadamente seguro contra dois tipos de adversários.

Palavras-chave: assinatura cega, criptologia sem certificado, emparelhamento bilinear, modelo de oráculo aleatório.

REFERENCES

AL-RIYAMI S AND PATERSON K. 2003. Certificateless public key cryptography. Proceedings of ASIACRYPT03, 452 p.

BELLARE M AND ROGAWAY P. 1993. Random oracles are practical: a paradigm for designing efficient protocols. ACM CCCS'93, 62 p.

CAO X AND KOU W. 2010. A pairing-free identity-based authenticated key agreement scheme with minimal message exchanges. Inform Sciences 180: 2895-2903.

CHAUM D. 1983. Blind signatures for untraceable payments. Proc CRYPTO 82,199 p.

CHEN L, CHENG Z AND SMART N. 2007. Identity-based key agreement protocols from pairings. Int J Inf Secur 6: 213-241.

DAVID P AND JACQUE S. 2000. Security arguments for digital signatures and blind signatures. J Cryptol 13: 361-396.

GONG P AND LI P. 2012. Li, Further improvement of a certificateless signature scheme without pairing. Int J Commun Syst. DOI: 10.1002/dac.2457.

HANKERSON D, MENEZES A AND VANSTONE S. 2004. Guide to elliptic curve cryptography. New York: Springer-Verlag, 220 p.

HE D, CHEN J AND HU J. 2011a. An ID-based proxy signature schemes without bilinear pairings. Ann Telecommun 66: 657-662.

HE D, CHEN J AND HU J. 2012a. A pairing-free certificateless authenticated key agreement protocol. Int J Commun Syst 25: 221-230.

HE D, CHEN J AND HU J. 2012b. n ID-based client authentication with key agreement protocol for mobile client-server environment on ECC with provable security, Inform Fusion 13: 223-230.

HE D, CHEN J AND ZHANG R. 2012c. An efficient and provably-secure certificateless signature scheme without bilinear pairings. Int J Commun Syst 25: 1432-1442.

HE D, CHEN Y AND CHEN J. 2013a. A provably secure certificateless proxy signature scheme without pairings. Math Comput Model Dyn 57: 2510-2518.

HE D, CHEN Y, CHEN J AND ZHANG R. 2011b. An efficient identity-based blind signature scheme without bilinear pairings. Comput Electr Eng 37: 444-450.

HE D, CHEN Y, CHEN J AND ZHANG R. 2011c. A new two-round certificateless authenticated key agreement protocol without bilinear pairings. Math Comp Model Dyn 54: 3143-3152.

HE D, PADHYE S AND CHEN J. 2012d. An efficient certificateless two-party authenticated key agreement protocol. Comput Math Appl 64: 1432-1442.

HE D, HUANG B AND CHEN J. 2013b. A new certificateless short signature scheme, IET Information Security 7: 113-117.

HUANG X, MU Y, SUSILO W, WONG D AND WU W. 2007. Certificateless signature revisited. 12th Australasian Conference Information Security and Privacy, 308 p.

KOBLITZ N. 1987. Elliptic curve cryptosystem. Math Comput 48: 203-209.

SHAMIR A. 1984. Identity-based cryptosystems and signature schemes. Proc CRYPTO 84, 47 p.

SUN S AND WEN Q. 2009. Novel efficient certificateless blind signature schemes. International Symposium on Computer Network and Multimedia Technology, 1 p.

SUN Y AND ZHANG F. 2010. Secure certificateless encryption with short ciphertext. Chinese J Electron 19: 313-318.

TIAN M AND HUANG L. 2012. Cryptanalysis of a certificateless signature scheme without pairings. DOI: 10.1002/dac.2310.

TSAI J, LO N AND WU T. 2012. Weaknesses and improvements of an efficient certificateless signature scheme without using bilinear pairings. DOI: 10.1002/dac.2388.

WANG C AND LU R. 2008. A certificateless restrictive partially blind signature scheme. 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 279 p.

YANG G AND TAN C. 2011. Certificateless public key encryption: A new generic construction and two pairing-free schemes. Theor Comput Sci 412: 662-674.

YANG X, LIANG Z AND WEI P. 2009. A provably secure certificateless blind signature scheme. 5th International Conference on Information Assurance and Security, 643 p.

ZHANG AND GAO S. 2009. Efficient provable certificateless blind signature scheme. International Conference on Networking, Sensing and Control, 292 p.

ZHANG L AND ZHANG F. 2008. Certificateless signature and blind signature. J Electron 25: 629-635.

ZHANG L, ZHANG F, QIN B AND LIU S. 2011. Provably-secure electronic cash based on certificateless partially-blind signatures. Electron Commer R A 10: 545-552.