An Efficient Fair Blind Signature Scheme with Message Recovery Using Pairing-based Cryptosystems with Provable Security

Woei-Jiunn Tsaur
Department of Information Management, Da-Yeh University, Taiwan, R.O.C.
E-mail: wjtsaur@yahoo.com.tw

Chii-Jyh Guo
Department of Computer Science & Information Engineering National Chi Nan University, Taiwan, R.O.C.
E-mail: hubys@sinamail.com

Abstract*- The blind signature could be used in electronic payment systems to achieve the properties of unlinkability and anonymity. Unfortunately, this characteristic may be used to pervert the ability of the scheme. Accordingly, Lee and Kim proposed a fair blind signature scheme with message recovery in 1999. However, the fairness of blind signature can not be actually achieved in Lee and Kim's scheme. In this paper, the proposed cryptosystems are first constructed by using the pairing-based cryptosystems instead of modular exponentiation, and further integrating the identity-based self-certified public key cryptosystems. Furthermore, we employ the integrated cryptosystems to design a fair blind signature scheme with message recovery to improve the drawback on Lee and Kim's scheme, and give security proofs on the proposed blind signature scheme.*

1. Introduction

Blind signature scheme, which was first proposed by Chaum [1] in 1983, allows users to achieve anonymous property in electronic voting systems and electronic cash payment systems. With the characteristic of blind signature scheme, a sender can obtain a signature on a message from a signer, but the signer knows nothing about the content of the message, such that the signer cannot link the signature and sender. Unfortunately, this characteristic may be used to pervert the ability of the scheme. Therefore, in 1999 Lee and Kim [8] proposed the fair blind signature scheme with message recovery to withstand the misapplication of financial crime in electronic cash payment systems. However, in 2000 Hsien *et al*. [6] proposed an attack on Lee and Kim's scheme. They proved that the sender can generate an untraceable signature, which cannot be recovered by the system authority (the trusted entity). In 2002, Chung [2] improved the checking way of the revocation key in Lee and Kim's scheme such that the sender cannot create a pretended revocation key to satisfy the fair requirement. Regrettably, Chung's proposed scheme, which was based on modular exponentiation, is inefficient.

In recent years, Zhang *et al*. [16, 17] proposed several kinds of ID-based blind signature schemes using the bilinear pairings. Although the ID-based cryptosystems have the advantage of simple procedure in managing the public key list, a secure channel is required for the key generation center to deliver private keys to corresponding users. Also, the key generation center is a single point of failure in the systems. If the private key of the key generation center is compromised, the security of the entire scheme will be removed. Moreover, a dishonest key generation center may impersonate each user in the systems, because each user's private key is generated by it. Thus there exist many drawbacks in identity-based public key cryptosystems.

In 1991, the self-certified public key cryptosystem, which can implicitly verify public keys without accompanying additional certificates, were proposed by Girault [4]. Self-certified public key cryptosystems can allow a user generates the secret key by himself/herself (i.e. the secret key needn't be transmitted through a secure channel). Thus the system authority cannot obtain the user's secret key from communications with the user [18]. Moreover, the user and the system authority cooperatively generate the user's public key, and the user can verify the public key by himself/herself when the system authority delivers the public key to him/her. Consequently, the system authority cannot impersonate any user by generating false guarantees, and all frauds of the system authority are detectable.

In this paper, the proposed cryptosystems are first constructed by using the pairing-based cryptosystems instead of modular exponentiation, and further integrating the identity-based self-certified public key cryptosystems. Furthermore, we employ the integrated cryptosystems to design a fair blind signature scheme with message recovery to improve the drawback on Lee and Kim's scheme, and give security proofs on the proposed blind signature scheme.

2. A Fair Blind Signature Scheme with Message Recovery

In this section, we propose a public key cryptosystem by integrating the pairing-based cryptosystems with the identity-based self-certified public key cryptosystems. In addition, we further employ the integrated cryptosystems to design a fair blind signature scheme with message recovery to

efficiently achieve the essential properties of blind signature. The proposed scheme is described as follows.

2.1 Initialization

The entities in the system are a certification authority (*CA*) and users (U_i). Assume that the system authority *CA* is responsible for key generation and user registration. We define notations used in the proposed scheme as follows:

$E(F_{3^m})$: a supersingular elliptic curve E:$y^2=x^3-x+1 \pmod{3^m}$, where the characteristic is 3, and the security multiplier is 6.

G_1 : an additive group of the elliptic curve E whose order is a large prime q. We also write $G_1^* \equiv G_1 - \{O\}$, and O is the point at infinity.

B : a base point of G_1 whose order is q.

G_2 : a multiplicative group of order q on the elliptic curve E.

e : a bilinear pairing map where $e: G_1 \times G_1 \to G_2$.

H_1: a one-way hash function, where $H_1:\{0,1\}^* \to G_1^*$.

H_2: a one-way hash function, where $H_2:\{0,1\}^* \to \mathbf{Z}_q^*$.

H_3: a one-way hash function $H_3:G_2 \to \{0,1\}^*$, where $n \in N$ denotes the size of message.

H_4: a one-way hash function, where $H_2:\{0,1\}^n \to \mathbf{Z}_q^*$.

2.2 The Proposed Public Key Cryptosystems

The operational procedure of the proposed public key cryptosystems is divided into two phases: system setup and key generation.

[System Setup]

CA creates a system public key and some public parameters in this phase, and then *SA* releases these parameters.

CA randomly chooses a number $S_{CA} \in \mathbf{Z}_q^*$ and keeps it secret. Then *CA* computes the system public key $P_{CA} = S_{CA} \cdot B$. Accordingly, the public parameters in the system are $<E,q,G_1,G_2,e,B,P_{CA}, H_1, H_2, H_3, H_4>$, and the private key of *CA* is S_{CA}.

[Key Generation]

Suppose that a user U_i wants to generate keys with *CA*, he/she performs the following steps to register to *CA*, and obtains the corresponding public key. He/She also computes his/her private key in this phase.

Setp1. U_i chooses a random number $k_i \in \mathbf{Z}_q^*$. Then he/she computes $K_i = k_i \cdot B$, and transmits his/her own K_i and identity $ID_i \in \{0,1\}^*$ to the *CA*.

Step2. After receiving ID_i and K_i, *CA* calculates $Q_i = H_1(ID_i) \in G_1^*$, and randomly chooses an integer $x_i \in \mathbf{Z}_q^*$ to compute $X_i = x_i \cdot B$. Then *CA* generates U_i's Public key $P_i=K_i+X_i$ and the witness of the public key $W_i=S_{CA}(P_i+X_i)+x_i(P_{CA}+Q_i)$. Finally, *CA* sends $\{P_i, W_i\}$ to U_i.

Step3. Upon receiving $\{P_i, W_i\}$, U_i calculates his/her own private key $S_i=W_i+k_iQ_i$, and he/she can verify the public key by performing the following formula:

$$e(S_i, B) = e(P_i, P_{CA})e(Q_i, P_i)$$

If the result is correct, then U_i's private key is S_i; otherwise, it means that the public key P_i is altered in the transmission.

2.3 The Proposed Scheme

In this section, we will present a fair self-certified blind signature scheme with message recovery. Our proposed scheme is constructed based on bilinear pairings instead of modular exponentiation for the consideration of efficiency. We define notations used in the proposed scheme as follows:

[Notations]

S_{CA}: *CA*'s secret key, where $S_{CA} \in \mathbf{Z}_q^*$.

P_{CA}: *CA* 's public key, where $P_{CA} = S_{CA} \cdot B$.

h(): a one-way hash function that accepts variable-length input and produces a fixed-length output value, and its length is 160bits.

x(P): the x-coordinate value of point P.

M: message.

$\|$: a symbol denoting concatenation.

$\in_R$: a symbol denoting the uniform random selection.

$\oplus$: bitwise *exclusive-or* operator

[Registration]

In this phase, user U_i registers to derive the revocation keys α and β from *CA*.

Step1. Requesting for registration:

User U_i computes $\Lambda = \lambda \cdot B$, where $\lambda \in \mathbf{Z}_q^*$ is a random number. U_i submits Λ and his/her identity information ID_{U_i} to *CA* under a secret channel.

Step2. Registering:

After receiving Λ and ID_{U_i}, *CA* generates the revocation keys $\alpha, \beta \in \mathbf{Z}_q^*$, where α and β are prime. Then, *CA* randomly chooses $\gamma \in \mathbf{Z}_q^*$ and computes $F = \gamma \cdot B$. He/She uses a one-way hash function h() to compute $g = h(x(\Lambda)\alpha \| x(\Lambda)\beta \| x(F))$ and generates $d = S_{CA} \cdot g + \gamma$. *CA* returns $(x(\Lambda)\alpha, x(\Lambda)\beta, d, g)$ to U_i. Moreover, *CA* computes $H=H_1(g)$ and

$D = \alpha\beta \cdot B$. At last, *CA* saves $(\alpha, \beta, ID_{U_i}, H, D)$ in *CA*'s database.

Step3. Verifying registration:

After receiving $(x(\Lambda)\alpha, x(\Lambda)\beta, d, g)$ sent from *CA*, user computes $F' = d \cdot B - g \cdot P_{CA}$ and $g' = h(x(\Lambda)\alpha \| x(\Lambda)\beta \| x(F'))$, and verifies $g = g'$. If g' is equal to g, we can confirm that the message $(x(\Lambda)\alpha, x(\Lambda)\beta, d, g)$ sent from *SA* is correct.

[Blind Signature Issuing Protocol]

In this phase, user U_i wants to get a blind signature from the signer (*sg*), and verifies the message recovery blind signature.

Step1. Initial oblivious transformation:

First U_i computes $H=H_1(g)$, $\phi = \alpha\beta \cdot B$ and $\phi' = H - \alpha\beta \cdot B$. Then U_i submits ϕ and ϕ' to the signer.

Step2. Generating fair blind factors:

The signer computes $H = \phi + \phi'$ by using the message (ϕ, ϕ') from user, and checks whether the value *H* has been stored in *CA*'s database. If *H* is *CA*'s database, the signer obtains the values *D* from *CA*'s database and verify ϕ = *D* furthermore. Right after that, the signer Randomly chooses $r \in \mathbf{Z}_q^*$, and computes $U = r \cdot P_{sg}$ and $\delta = r \cdot \phi$, where P_{sg} is the signer's public key. Finally, he/she sends the blind factors (U, δ) to U_i.

Step3. Blinding the message:

After receiving (U, δ), U_i verifies the following formula:

$$e(\alpha\beta \cdot U, B) = e(P_{sg}, \delta)$$

If it is valid, U_i computes $U' = \alpha U + \alpha\beta P_{sg}$ and $U'' = H_3(e(U', P_{CA} - Q_{sg})) \oplus M$. Then, U_i generates $h = \alpha^{-1} H_4(U'') + \beta$. Finally, U_i submits *h* to the signer.

Step4. Generating a blind signature:

The signer sends back *V*, where $V = (r + h) S_{sg}$. And, U_i computes $V' = \alpha V$, and outputs $\{M, U'', V'\}$. Then (U'', V') is the blind signature of message *M*.

[Verifying the Fair Blind Signature with Message recovery]

Accept the signature when the following equation holds:

$$M = H_3\left(e(V', B)\, e(P_{sg}, P_{CA} - Q_{sg})^{-H_4(U'')}\right) \oplus U'' \cdot$$

If the check is correct, then (U'', V') is the blind signature of message *M*.

3. Security Proofs

3.1 Blindness Property

To prove the blindness, we show that given a valid signature (M, U'', V') and any view $(\phi, \phi', U, \delta, h, V)$, there always exists a unique pair of blind factors $\alpha, \beta \in \mathbf{Z}_q^*$. Since the blind factors $\alpha, \beta \in \mathbf{Z}_q^*$ are chosen randomly, the blindness of the signature scheme are naturally satisfied.

Given a valid signature (M, U'', V') and any view $(\phi, \phi', U, \delta, h, V)$, then the following equations must hold for $\alpha, \beta \in \mathbf{Z}_q^*$:

$$U' = \alpha U + \alpha\beta P_{sg} \quad (1)$$

$$U'' = H_3\left(e\left(U', P_{CA} - Q_{sg}\right)\right) \oplus M \quad (2)$$

$$h = \alpha^{-1} H_4\left(U''\right) + \beta \quad (3)$$

$$V' = \alpha V \quad (4)$$

It is obvious that $\alpha \in \mathbf{Z}_q^*$ exists uniquely from Eq.(4) denoted by $\log_V V'$. So we can get $\beta = h - \left(\log_V V'\right)^{-1} H_4\left(U''\right)$ from Eq.(3), and it is unique in $\mathbf{Z}_q^*$. Furthermore, we show that such α and β satisfy Eq.(1). Apparently, due to the non-degenerate of the bilinear pairing, we have

$$U' = \alpha U + \alpha\beta P_{sg} \Leftrightarrow e\left(U', P_{CA}\right) = e\left(\alpha U + \alpha\beta P_{sg}, P_{CA}\right)$$

Just we need to show that such α and β satisfy

$$e\left(U', P_{CA} - Q_{sg}\right) = e\left(\alpha U + \alpha\beta P_{sg}, P_{CA} - Q_{sg}\right). \quad (5)$$

We have

$$e\left(\alpha U + \alpha\beta P_{sg}, P_{CA} - Q_{sg}\right)$$

$$= e\begin{pmatrix} \log_V V' \cdot U + \log_V V' \cdot \left(h - \left(\log_V V'\right)^{-1} H_4\left(U''\right) P_{sg}\right) \\ , P_{CA} - Q_{sg} \end{pmatrix}$$

$$= e\left(\log_V V' \cdot (r + h) P_{sg}, P_{CA} - Q_{sg}\right) e\left(V', B\right)^{-1} e\left(U', P_{CA} - Q_{sg}\right)$$

$$= e\left(\left(\log_V V'\right) \cdot V, B\right) e\left(V', B\right)^{-1} e\left(U', P_{CA} - Q_{sg}\right)$$

$$= e\left(U', P_{CA} - Q_{sg}\right)$$

Since α and β satisfy Eq.(5), we can show that such α and β also satisfy Eq.(2).Thus there always exist the blind factors to lead to the same relation defined in the blind signature issuing protocol.

3.2 Non-forgeability

Let $\mathcal{A}$ be the attacker who controls the sender. $\mathcal{A}$ can forge valid blind signatures once gets the signer's secret key. We consider four lemmas as follows.

Lemma 1 The advantage of $\mathcal{A}$ in revealing the signer's secret key S_{sg} from $e(P_{sg}, P_{CA} - Q_{sg}) = e(S_{sg}, B)$ by interacting the signer's *ID* is negligible.

Proof:

The proof of this case is by contradiction. We assume that $\mathcal{A}$ successful produces a valid

message-signature pair $(m,\sigma(m))$ with a non-negligible probability ε. Then the attacker $\mathcal{A}$ constructs a simulator $\mathcal{S}$ to solve the Computational Diffie-Hellman (CDH) problem. In other words, $\mathcal{S}$ successful solve the CDH-problem with a non-negligible probability ε.

Let q_H be the maximum number of queries asked from $\mathcal{A}$ to $\mathcal{S}$, it is limited by a polynomial in *k*. The attacker $\mathcal{A}$ gets public parameters *PARAMS*(G_1, G_2, *q*, *e*, *B*, P_{CA}, Q_{sg}) and wants to find $S_{sg} \in G_1$ from $e(P_{sg}, P_{CA} - Q_{sg}) = e(S_{sg}, B)$. We describe the process of simulator $\mathcal{S}$ as follows:

1. The simulator $\mathcal{S}$ randomly chooses $I \in \{1,\cdots,q_H\}$.
2. For $\mathcal{A}$'s *i*-th query to $\mathcal{S}$, if $i = I$, the attacker $\mathcal{A}$ randomly chooses $k_{sg} \in \mathbf{Z}_q^*$, and sends $\{K_{sg} = k_{sg} \cdot B, ID_{sg}\}$ to the simulator $\mathcal{S}$. The simulator $\mathcal{S}$ outputs P_{sg}.
3. If $i \neq I$, $\mathcal{A}$ randomly chooses a number $r \in \mathbf{Z}_q^*$ and outputs *r* to the simulator $\mathcal{S}$. The simulator $\mathcal{S}$ outputs $U = r \cdot P_{sg}$.
4. The simulator $\mathcal{S}$ returns $\{P_{sg}, U\}$ to $\mathcal{A}$, then $\mathcal{A}$ outputs a valid message-signature pair $(m,\sigma(m))$.

Now $\mathcal{A}$ wants to use P_{sg} (from $\mathcal{S}$) to get S_{sg} from $e(P_{sg}, P_{CA} - Q_{sg}) = e(S_{sg}, B)$.

Let $Q_{sg} = H_1(ID_{sg}) = s \cdot B$, where $s \in \mathbf{Z}_q^*$, then

$$e\left(P_{sg}, P_{CA} - Q_{sg}\right) = e\left(B, B\right)^{(k_{sg}+x_{sg})(S_{CA}-s)} \qquad (6)$$

Let

$$\begin{cases} t = k_{sg} + x_{sg} \\ u = S_{CA} - s \end{cases}, \text{where } t,u \in \mathbf{Z}_q^*.$$

Therefore

$$e\left(B, B\right)^{(k_{sg}+x_{sg})(S_{CA}-s)} = e\left(B, B\right)^{tu} = e\left(S_{sg}, B\right).$$

From Eq.(6) We can know that the advantage of $\mathcal{A}$ in getting S_{sg} from $e(P_{sg}, P_{CA} - Q_{sg}) = e(S_{sg}, B)$ is

$$\mathrm{Adv}_{\mathcal{A},G_1} = \Pr\left[\begin{array}{l} \mathcal{A}\begin{pmatrix} B, tB, \\ uB, tuP \end{pmatrix} = 1 \\ : t,u \in_R \mathbf{Z}_q^* \end{array}\right] = \varepsilon.$$

By the CDH assumption, for every probabilistic, polynomial-time, 0/1-valued algorithm $\mathcal{A}$, $\mathrm{Adv}_{\mathcal{A},G_1}^{\mathrm{CDH}}$ is negligible. This is a contradiction, because the advantage of $\mathcal{A}$ in solving CDH problem in G_1 is negligible. In other words, the success probability of the forgery in this attack is negligible.

Theorem 1 An attacker can not reveal the signer's secret key S_{sg} from $e(P_{sg}, P_{CA} - Q_{sg}) = e(S_{sg}, B)$ by interacting the signer's *ID*.

Proof:

By Lemma 1, we have completed the proof.

Lemma 2: The advantage of $\mathcal{A}$ in revealing the signer's secret key S_{sg} from $M = H_3\left(e(V', B)e\left(P_{sg}, P_{CA} - Q_{sg}\right)^{-H_4(U')}\right) \oplus U''$ by interacting the signer's *ID* is negligible.

Proof:

Assuming that $\mathcal{A}$ successful produces a valid message-signature pair (*m*, σ (*m*)) with a non-negligible probability ε. Then the attacker $\mathcal{A}$ constructs a simulator $\mathcal{S}$ to solve the Computational Diffie-Hellman (CDH) problem. In other words, $\mathcal{S}$ successful solve the CDH-problem with a non-negligible probability ε.

Let q_H be the maximum number of queries asked from $\mathcal{A}$ to $\mathcal{S}$, it is limited by a polynomial in *k*. The attacker $\mathcal{A}$ gets public parameters *PARAMS*(G_1, G_2, *q*, *e*, *B*, P_{CA}, Q_{sg}) and wants to find $S_{sg} \in G_1$ from $M = H_3\left(e(V', B)e\left(P_{sg}, P_{CA} - Q_{sg}\right)^{-H_4(U')}\right) \oplus U''$. The process of simulator $\mathcal{S}$ is the same with the simulator in Lemma 1. And now, $\mathcal{A}$ wants to use P_{sg} to get S_{sg} from $M = H_3\left(e(V', B)e\left(P_{sg}, P_{CA} - Q_{sg}\right)^{-H_4(U')}\right) \oplus U''$.

Since

$$H_3\left(e(V', B)e\left(P_{sg}, P_{CA} - Q_{sg}\right)^{-H_4(U')}\right) \oplus U''$$
$$= H_3\left(e\left(U', P_{CA} - Q_{sg}\right)\right) \oplus M \oplus H_3\left(e\left(U', P_{CA} - Q_{sg}\right)\right)$$

$\mathcal{A}$ reveals S_{sg} from $e\left(U', P_{CA} - Q_{sg}\right)$. and $U' = \alpha U + \alpha\beta P_{sg} = P_{sg}\left(\alpha r + \alpha\beta\right)$, we can get

$$e\left(U', P_{CA} - Q_{sg}\right) = e\left(P_{sg}, P_{CA} - Q_{sg}\right)^{(\alpha r + \alpha\beta)} \qquad (7)$$

According to Lemma 1, the advantage of $\mathcal{A}$ in revealing the signer's secret key S_{sg} from Eq.(7) by interacting the signer's *ID* is negligible. In other words, the success probability of the forgery in this attack is negligible.

Theorem 2: An attacker can not reveal the signer's secret key S_{sg} from $M = H_3\left(e(V', B)e\left(P_{sg}, P_{CA} - Q_{sg}\right)^{-H_4(U')}\right) \oplus U''$ by interacting the signer's *ID*.

Proof:

By Lemma 2, we have completed the proof.

Lemma 3: The advantage of $\mathcal{A}$ in revealing the signer's secret key S_{sg} by using the generic parallel attack is negligible.

In 2001, Schnorr [12] proposed a new attack, called generic parallel attack, on Schnorr's blind signature scheme. We prove that our scheme is secure against the generic parallel attack under the assumption of the ROS problem in the following.

First, we describe how $\mathcal{A}$ uses the generic parallel attack to forge *l*+1 valid blind signatures in ours scheme. Let q_H be the maximum number of queries H_3 from $\mathcal{A}$.

Step1. The signer sends commitments $U_1 = r_1 P_{sg}, U_2 = r_2 P_{sg}, \cdots, U_3 = r_3 P_{sg}$.

Step2. $\mathcal{A}$ randomly selects $a_{k,1}, a_{k,2}, \cdots, a_{k,l} \in \mathbf{Z}_q$ and messages $m_1, m_2, \cdots, m_t$. Then $\mathcal{A}$ computes $f_k = e\left(\sum_{i=1}^{l} a_{k,l} U_i, P_{CA} - Q_{sg}\right)$ and $H_3(f_k) \oplus U_k^{"}$ for $k = 1, 2, \cdots, t$; $t < q_H$.

Step3. $\mathcal{A}$ solves Eq.(1) in the unknown $h_1, h_2, \cdots, h_l$ over $\mathbf{Z}_q$:

$$H_4\left(U_k^{"}\right) = \sum_{j=1}^{l} a_{k,j} h_j \quad \text{for } k = 1, 2, \cdots, t \qquad (8)$$

Step4. $\mathcal{A}$ sends those solutions $h_1, h_2 \ldots, h_l$ to the signer.

Step5. The signer computes $V_i = h_i S_{sg} + r_i S_{sg}$ for $i = 1, 2, \cdots, l$ and returns V_i to $\mathcal{A}$.

Step6. $\mathcal{A}$ can get valid signatures $\left(m_k, U_k^{"}, V_k^{'}\right)$ by setting $H_4\left(U_k^{"}\right) = \sum_{j=1}^{l} a_{k,j} h_j$ and $V_k^{'} = \sum_{j=1}^{l} a_{k,j} V_j$.

Step7. $\mathcal{A}$ outputs $l+1$ signatures $\left(m_k, U_k^{"}, V_k^{'}\right)$ for $k = 1, 2, \cdots, l+1$.

In the above step, it's easy to see that the forged signature is valid. According to Eq.(8), we have:

$$\begin{aligned} & e\left(V_k^{'}, B\right) e\left(P_{sg}, P_{CA} - Q_{sg}\right)^{-H_4(U_k^{"})} \\ &= e\left(\sum_{j=1}^{l} a_{k,j} V_j, B\right) e\left(P_{sg}, P_{CA} - Q_{sg}\right)^{-H_4(U_k^{"})} \\ &= e\left(S_{sg}, B\right)^{\sum_{j=1}^{l} a_{k,j} h_j} e\left(\sum_{j=1}^{l} a_{k,j} r_j S_{sg}, B\right) e\left(P_{sg}, P_{CA} - Q_{sg}\right)^{-H_4(U_k^{"})} \\ &= e\left(\sum_{j=1}^{l} a_{k,j} U_j, P_{CA} - Q_{sg}\right) = f_k \end{aligned}$$

and $H_3(f_k) \oplus U_k^{"} = M_k$

The essence of the above attack is to solve the ROS-problem, which is shown as follows:

ROS-problem: Giving an oracle access to a random function $F : \mathbf{Z}_q^l \to \mathbf{Z}_q$, find co-efficient $a_{k,i} \in \mathbf{Z}_q$ and a solvable system of $l+1$ distinct equations in the unknowns $h_1, h_2, \cdots, h_l$ over $\mathbf{Z}_q$:

$a_{k,1} h_1 + \cdots + a_{k,l} h_l = F(a_{k,1}, \cdots, a_{k,l})$ for $k = 1, 2, \cdots, t$.

Depending on the difficulty of ROS-problem, we prove that our blind signature scheme is secure against the generic parallel attack.

Theorem 3: An attacker tries to reveal the signer's secret key S_{sg} by using the generic parallel attack.

Proof:

By Lemma 3, we have completed the proof.

4. Performance Evaluation

In this section, we discuss both computational complexity and communicational cost of the proposed fair blind signature scheme with message recovery (FBSMR).

4.1 Computational complexity

The following notations are used for measuring the performance of the proposed systems.

$T_{MM}/T_{EXP}/T_{MA}$: the time for computing a modular multiplication/exponentiation/addition

T_{INV}: the time for computing modular inversion

T_{EM}: the time for computing the multiplication of a number and an elliptic curve point

T_{EA}: the time for computing the addition of two points on an elliptic curve

T_H: the time for computing the one-way has function h

According to the paper proposed by Koblitz *et al.* [7], the above time complexities have the following relationship:

$T_{EM} \approx 29 T_{MM}$; $T_{EA} \approx 0.12 T_{MM}$; $T_{EXP} \approx 240 T_{MM}$; T_{MA} and T_H are negligible as compared to the above complexities measures.

In Table 1, we can see that our proposed scheme is more efficient than Lee-Kim's [8] in computational complexity. Although our scheme is one T_{EM} more than Tsaur-Chou's scheme in the steps of verifying the fair blind signature with message recovery, the computational complexity in the step of generating fair blind factors is half of Tsaur-Chou's [14] scheme.

4.2 Communicational Cost

In the following, we will analyze the communicational cost of the proposed schemes. To evaluate the communicational cost, the following notations are defined:

$|G_1|$: the size of the elements in the group G_1.

$|ID|$: the size of user's identity.

$|x(P)|$: the size of $x(P)$, where $P \in G_1$.

$|q|$: the size of a prime q.

$|p'|$、$|q|$：denoting the bit-length of p' and q, respectively. In Lee-Kim's scheme [8], p' is 512 bits and q is 160 bits.

$|p|$、$|n|$：denoting the bit-length of p and n, respectively. In ECC, p and n all are 160 bits.

$|h|$：the bit-length of output value of one-way hash function h.

According to Table 2, it is obvious that we have improved the performance of communicational cost as compared with previous schemes [8, 14] successfully.

5. Conclusions

In this paper, we propose a public key cryptosystem by integrating the paring-based

cryptosystems with the ID-based self-certified public key cryptosystems, and further employ the integrated cryptosystems to design a fair blind signature scheme with message recovery. Based on the proposed security proofs and performance evaluation, we affirm that we not only improve the efficiency of Lee and Kim's scheme, but also achieve the essential properties of blind signature with provable security.

6. References

[1] D. Chaum, "Blind Signature for Untraceable Payments," *Proceedings of Advances in Cryptology – CRYPOT '82*, pp. 199-203, 1983.

[2] M. Y. Chung, "Message Recovery Fair Blind Signature Schemes," *Ms.D. Thesis, Department of Computer Science, National Chung Hsing University*, Taiwan, 2002.

[3] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, pp. 644-654, 1976.

[4] M. Girault, "Self-Certified Public Keys," *Proceedings of EUROCRYPT '91*, LNCS, Vol. 547, Springer-Verlag, pp. 491-497, 1991.

[5] F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," *Proceedings of SAC 2002*, LNCS, Vol. 2595, Springer-Verlag, pp. 310-324, 2002.

[6] J. E. Hsien, P. W. Ko and C. Y. Chen, "Comments on Lee and Kim's Message Recovery Fair Blind Signature Scheme," *Proceedings of the Tenth National Conference on Information Security*, Chinese Cryptology and Information Security Association (CCISA), Taiwan, pp. 123-125, 2000.

[7] N. Koblitz, A. Menezes, S. Vanstone, "The State of Elliptic Curve Cryptography," *Designs, Codes and Cryptography*, Vol. 19, pp. 173-193, 2000.

[8] H. W. Lee and T. Y. Kim, "Fair Blind Signature with Message Recovery Based on Oblivious Transfer Protocol," *Public Key Cryptography, Second International Workshop on Practice and Theory in Public Key Cryptography (PKC '99)*, pp. 97-111, 1999.

[9] A. J. Menezes, T. Okamoto, and S. Vanstone, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field," *IEEE Transactions on Information Theory*, Vol. 39, pp. 1639-1646, 1993.

[10] R. Rivest and A. Shamir, "PayWord and MicroMint: Two Simple Micropayment Schemes," *Proceedings of RSA'96 Conference*, 1996.

[11] C. P. Schnorr, "Efficient Identification and Signatures for Smart Cards," *Proceedings of Advances in Cryptology – CRYPTO '89*, pp. 339-351, 1990.

[12] C. P. Schnorr, "Security of Blind Discrete Log Signatures against Interactive Attacks," *Proceedings of ICICS 2001*, LNCS, Vol. 2229, Springer-Verlag, pp. 1-12, 2001.

[13] A. Shamir, "Identity-based Cryptosystems and Signature schemes," *Advances in Cryptology – CRYPTO '84*, pp. 47-53, 1985.

[14] W. J. Tsaur and C. H. Chou, "An Efficient and Secure Fair Blind Signature Scheme with Message Recovery," *Proceedings of the Thirteenth National Conference on Information Security*, Chinese Cryptology and Information Security Association (CCISA), Taiwan, pp. 54-62, 2003.

[15] E. Verheul, Self-blindable Credential Certificates from the Weil Pairing, *Proceedings of Advances in Cryptology – ASIACRYPT 2001*, LNCS, Vol. 2248, Springer-Verlag, pp. 533-551, 2001.

[16] F. G. Zhang and K. Kim, "Efficient ID-Based Blind Signature and Proxy Signature from Bilinear Pairings," *Proceedings of ACISP'03*, LNCS, Vol. 2727, Springer-Verlag, pp. 312-323, 2003.

[17] F. G. Zhang and K. Kim, "ID-Based Blind Signature and Ring Signature from Pairings," *Proceedings of Advances in Cryptology – ASIACRYPT 2002*, LNCS, Vol. 2501, Springer-Verlag, pp. 533-547, 2002.

[18] T. S. Wu and C. L. Hsu, "Convertible Authenticated Encryption Scheme," *Journal of Systems and Software*, Vol. 62, No. 3, pp. 205-209, 2002.

Table 1. The comparison of computational complexity.

Phase	Lee-Kim's scheme [8]	Tsaur-Chou's scheme [14]	The proposed FBSMR
Registration	962 T_{MM} + T_{INV}	147.12 T_{MM}	145.12 T_{MM}
Signature	2837 T_{MM} + 5T_{INV}	471.36 T_{MM}	435.72 T_{MM}

Table 2. The comparison of communicational cost

Phase	Lee-Kim's scheme [8]	Tsaur-Chou's scheme [14]	The proposed FBSMR
Registration	3|p'|+2|q|+|h|	|p|+4|n|+|h|	2|p|+3|n|+|h|
Signature	6|p'|+2|q|	6|p|+2|n|	5|p|+|h|