International Journal of Innovative
Computing, Information and Control
Volume **8**, Number **2**, February **2012**

 ISSN 1349-4198
pp. 1117–1133

A NEW MESSAGE-RECOVERY-COMBINED FAIR BLIND SIGNATURE SCHEME WITH PROVABLE SECURITY USING SELF-CERTIFIED PAIRING-BASED CRYPTOSYSTEM

Woei-Jiunn Tsaur[1] and Chih-Hung Wang[2]

[1]Department of Information Management
Da-Yeh University
No. 168, University Rd., Dacun, Changhua 51591, Taiwan
wjtsaur@yahoo.com.tw

[2]Department of Computer Science and Information Engineering
National Chiayi University
No. 300, Syuefu Rd., Chiayi City 60004, Taiwan
wangch@mail.ncyu.edu.tw

Received October 2010; revised February 2011

Abstract. *The fair blind signature scheme indeed plays significant roles in a wide variety of e-commerce and network applications; for example, it can withstand the misapplication of financial crime in electronic cash payment systems. In this paper, we propose a new fair blind signature scheme with message recovery using the self-certified pairing-based public key cryptosystem. Preserving the merits inherent in the pairing-based cryptosystem, it can possess fewer bits to achieve the higher security level. In addition, our new scheme has the advantage that the authentication of the public key can be accomplished with the verification of the fair blind signature in a logically single step due to the use of the self-certified public key cryptosystem. Furthermore, the fairness of blind signature with message recovery can be actually achieved in our proposed scheme. Based on the proposed security proofs and performance evaluation, we affirm that we not only improve the efficiency of the previously proposed schemes, but also achieve the essential properties of blind signature with provable security.*
Keywords: Fair blind signature, Provable security, Pairing-based public key cryptosystem, Self-certified public key cryptosystem, Electronic payment system

1. **Introduction.** The blind signature scheme, first proposed by Chaum [1] in 1983, is a nice technique that allows achieving the properties of unlinkability and anonymity to protect users' privacy in secure electronic voting and electronic payment systems [2-4]. With the characteristic of the 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. This kind of property used in the untraceable cash can provide a useful protection of users' payment privacy; e.g., when an account holder takes e-coins from the bank, the bank knows nothing about what he bought and when he used these e-coins. Contrarily, the credit card payment cannot have this feature, because the card issuer will get a complete purchase notification when the card holder pays by credit. Another application is the e-voting scheme. Since the vote is blindly signed by the trustee, the frauds are preventable and the voter's selection can be hidden from the vote counting center. Unfortunately, this kind of characteristic may be used to pervert the ability of the scheme, such as black-mailing or money laundering. That is, the blind signature can successfully prevent from linking the withdrawal and the actual

purchase of the customer; however, a criminal of huge amounts of money transformation through the electronic payment may occur. In the original blind signature scheme, there is no way that can remove the anonymity and find the offender. In 1995, Stadler et al. [5] introduced the concept of fair blind signature that adds a new property to avoid the above flaws; therefore, the message-signature pair and the corresponding protocol view of the signer can possibly be linked by some special conditions. Fair blind signatures indeed play significant roles in real case security situations, because they have been applied to many e-commerce and network applications, e.g., [6,7]. Fan and Lei [6] employed the fair blind signatures to deal with the abuse of unlinkability in e-cash schemes. Based on the fair blind signature scheme, Wang and Sun [7] proposed a novel security model in P2P networks that the anonymity and authentication of the honest user can be guaranteed and the misbehavior of the malicious user can be appropriately traced.

In 1999, Lee and Kim [8] further enhanced the fair blind signature scheme with message recovery to withstand the misapplication of financial crime in electronic cash payment systems. The advantage of the message recovery is that the original message of the signature has been concealed into the signature and thus the message can be recovered according to the verification (or called message recovery) process. This kind of signature is different from the designated verifier signature scheme [9] or signcryption [10] since the message can be recovered by everyone without the receiver's private key, so that the size of transmission can be minimized and especially applicable to bandwidth-limited environments. However, Hsien et al. [11] proposed an attack on Lee and Kim's scheme. They showed that the sender can generate an untraceable signature, which cannot be recovered by the system authority (the trusted entity). In 2002, Chung [12] improved the checking way of the revocation key in Lee and Kim's scheme so that the sender cannot create a pretended revocation key to satisfy the fair requirement. Regrettably, Chung's proposed scheme, based on the modular exponentiation, is inefficient. Thus, in order to gain much efficiency in saving both the communicational cost and the computational effort, Tsaur and Chou [13] proposed a Fair Blind Signature Scheme with Message Recovery based on the elliptic curve cryptosystem (ECC). However, Tsaur and Chou's scheme does not give security proofs on the blindness and non-forgeability properties of the proposed blind signature scheme.

The provably secure fair blind signature scheme was first proposed by Abe and Ohkubo [14] in 2001. They gave an efficient scheme proven under Decisional Diffie-Hellman (DDH) and Discrete Logarithm (DL) assumptions. However, Hufschmitt and Traore [15] presented a flaw existing in the proof of unforgeability of Abe and Ohkubo's scheme, and proposed a new scheme based on bilinear maps. Since most of the papers used random oracles as their proof primitives, Fuchsbuaer and Vergnaud [16] applied a stronger security model to [15] and then proposed the first fair blind signature scheme with the standard model to remove the hash function heuristic. In addition, some variants have been developed such as fair partially blind signatures in [17]. Unfortunately, though these papers have proposed some new approaches to the security models or valuable applications, they were all designed based on the ordinary public-key cryptography [18] which had additional overheads on certificates management. Furthermore, none of them has the nice property of message recovery.

On the other hand, Chen et al. [19] and Zhang et al. [20-23] proposed several kinds of ID-based blind signature schemes using the bilinear pairings. Although the ID-based cryptosystem [24] has 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 the ID-based public key cryptosystem. In 1991, Girault [25] proposed the self-certified public key cryptosystem, which can implicitly verify public keys without accompanying additional certificates. The self-certified public key cryptosystem can allow a user to generate his/her private key by himself/herself (i.e., the private key need not be transmitted through a secure channel). Thus, the system authority cannot obtain the user's private key from communications with the user [26]. 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 pairing-based cryptosystem [27] and the self-certified public key cryptosystem are integrated to reach the purpose of constructing a new fair blind signature scheme with message recovery. Also, it is shown that the proposed scheme can actually achieve the fairness of blind signature with message recovery. In addition, based on the proposed security proofs and performance evaluation, we affirm that the proposed scheme not only improves the efficiency of the previously proposed schemes, but also accomplishes the essential properties of blind signature with provable security.

The summary of contributions of the proposed scheme is listed below.

1. We propose the first secure and efficient fair blind signature scheme with message recovery and self-certified public keys.
   (a) The property of message recovery offers a minimized size of transmission that can be suitable for bandwidth-limited environments.
   (b) The self-certified public key cryptosystems have the advantages of eliminating complicate key management procedure, and further prevent from the system authority's frauds on impersonation.
2. We give the formal proof on the security of the proposed fair blind signature scheme.
3. We provide a fast, convenient, privacy preserving and flaw-free signature system in the environments of low bandwidth communication, such as cell-phones or PDAs payment systems, or the commercial affairs in vehicular networks.

The remainder of this paper is organized as follows. Section 2 briefly reviews the properties of the bilinear pairings. In Section 3, the self-certified pairing-based public key cryptosystem is proposed, and then a new fair blind signature scheme with message recovery is further developed. The security of the proposed fair blind signature scheme is then proven in Section 4. In Section 5, the proposed fair blind signature scheme with message recovery (FBSMR) is first compared with the recently proposed related schemes in terms of security properties, and then both computational complexity and communicational cost of the proposed FBSMR are analyzed by comparing with the previously proposed FBSMR. Finally, some concluding remarks are presented in Section 6.

2. **Review of Bilinear Pairings.** Let G_1 be a cyclic additive group generated by P with a prime order q, and G_2 be a cyclic multiplicative group of the same order q. We assume that solving the discrete logarithm problem (DLP) in both G_1 and G_2 are computationally infeasible. Let $e : G_1 \times G_1 \to G_2$ be a pairing which satisfies the following requirements:

1. **Bilinearity:**

$$e(P+R,Q) = e(P,Q) \cdot e(R,Q), e(P,R+Q) = e(P,R) \cdot e(P,Q), \text{ and}$$
$$e(aP,bQ) = e(P,Q)^{ab} \text{ for all } P,Q \in G_1,\ a,b \in \mathbf{Z}_q^*.$$

2. **Non-degenerate:**
   There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$.
   There exists $P \in G_1$ and $Q \in O$ such that $e(P, Q) = 1$ (O is a point at infinity).
3. **Computability:**
   There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

In the setting of prime order groups, the non-degenerate is equivalent to $e(P, Q) \neq 1$ for all $P, Q \in G_1$. Therefore, if P is a generator in G_1, then $e(P, P)$ is a generator in G_2. Such the bilinear maps are called the bilinear pairings.

Furthermore, we further describe the Diffie-Hellman problems [28] in bilinear pairings below. A function is said to be *negligible* if it is less than $1/m^l$ for all fixed $l > 0$ and sufficiently large integer m.

1. Decisional Diffie-Hellman (DDH) problem in G_1:
   ***Instance*:** (P, aP, bP, cP) for some $a, b, c \in \mathbf{Z}_q^*$.
   ***Solution*:** Output *yes* if $c = ab \pmod q$; otherwise, output *no*.
   The advantage of a probabilistic, polynomial-time, 0/1-valued algorithm A in solving DDH problem in G_1 is defined as:
   $$\mathrm{Adv}_{A,G_1}^{\mathrm{DDH}} = \left|\Pr\left[A(P, aP, bP, cP) = 1\right] - \Pr\left[A(P, aP, bP, abP) = 1\right] : a, b, c \in_R \mathbf{Z}_q^*\right|$$
   By verifying $e(aP, bP) = e(P, cP)$, DDH problem in G_1 can be solve in polynomial time.
   ***DDH assumption*:** For a probabilistic, polynomial-time, 0/1-valued algorithm A, $\mathrm{Adv}_{A,G_1}^{\mathrm{DDH}}$ is negligible.
2. Computational Diffie-Hellman (CDH) problem in G_1:
   ***Instance*:** (P, aP, bP) for some $a, b \in \mathbf{Z}_q^*$.
   ***Solution*:** Output abP.
   The advantage of a probabilistic, polynomial-time, 0/1-valued algorithm A in solving CDH problem in G_1 is defined as:
   $$\mathrm{Adv}_{A,G_1}^{\mathrm{CDH}} = \Pr\left[A(P, aP, bP, abP) = 1 : a, b \in_R \mathbf{Z}_q^*\right]$$
   ***CDH assumption*:** For a probabilistic, polynomial-time, 0/1-valued algorithm A, $\mathrm{Adv}_{A,G_1}^{\mathrm{CDH}}$ is negligible.
3. Bilinear Diffie-Hellman (BDH) problem in (G_1, G_2, e):
   ***Instance*:** (P, aP, bP, cP) for some $a, b, c \in \mathbf{Z}_q^*$.
   ***Solution*:** Output $e(P, P)^{abc}$
   The advantage of a probabilistic, polynomial-time, 0/1-valued algorithm A in solving BDH problem in (G_1, G_2, e) is defined as:
   $$\mathrm{Adv}_{A}^{\mathrm{BDH}} = \Pr\left[A\left(P, aP, bP, cP, e(P, P)^{abc}\right) = 1 : a, b, c \in_R \mathbf{Z}_q^*\right]$$
   ***BDH assumption*:** For a probabilistic, polynomial-time, 0/1-valued algorithm A, $\mathrm{Adv}_{A}^{\mathrm{BDH}}$ is negligible.
4. Bilinear Decisional Diffie-Hellman (BDDH) problem in (G_1, G_2, e):
   ***Instance*:** (P, aP, bP, cP, r) for some $a, b, c, r \in \mathbf{Z}_q^*$.
   ***Solution*:** Output *yes* if $r = e(P, P)^{abc} \pmod q$; otherwise, output *no*.
   This is decision version of BDH problem in (G_1, G_2, e). The advantage of a probabilistic, polynomial-time, 0/1-valued algorithm A in solving BDDH problem in (G_1, G_2, e) is defined as:
   $$\mathrm{Adv}_{A}^{\mathrm{BDDH}} = \left|\left|\begin{array}{l}\Pr\left[A(P, aP, bP, cP, r) = 1\right] \\ -\Pr\left[A\left(P, aP, bP, cP, e(P, P)^{abc}\right) = 1\right]\end{array}\right| : a, b, c, r \in_R \mathbf{Z}_q^*\right|$$

***DBDH assumption*:** For a probabilistic, polynomial-time, 0/1-valued algorithm A, $\mathrm{Adv}_A^{\mathrm{BDDH}}$ is negligible.

3. **Proposed Fair Blind Signature Scheme with Message Recovery.** In this section, we first propose a public key cryptosystem by integrating the pairing-based cryptosystem with the self-certified public key cryptosystem. In addition, we further employ the integrated cryptosystem to design a new fair blind signature scheme with message recovery. Finally, we show that the fairness of our proposed blind signature scheme is achieved actually.

3.1. **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 $E : \mathrm{y}^2 = \mathrm{x}^3 - \mathrm{x} + 1(\mathrm{mod}3^m)$, 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 denoted by $H_1 : \{0,1\}^* \to G_1^*$, which means that the input is a string $\{0,1\}^*$ and the output is a point 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 $H_4 : \{0,1\}^n \to \mathbf{Z}_q^*$.

3.2. **The integrated public key cryptosystem.** The operational procedure of the proposed integrated public key cryptosystem is divided into two phases: system setup and key generation.

[System setup phase]

CA creates and publishes its public key and some public parameters in this phase. First, CA randomly chooses a number $s_{CA} \in \mathbf{Z}_q^*$ and keeps it secret. Then CA computes its public key $P_{CA} = s_{CA} \cdot B$. Accordingly, the CA's public key and public parameters in the system are $\langle P_{CA}, E, q, G_1, G_2, e, B, H_1, H_2, H_3, H_4\rangle$, and the CA's private key is s_{CA}.

[Key generation phase]

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

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

Step 2. 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 $W_i = s_{CA} \cdot (P_i + X_i) + x_i \cdot (P_{CA} + Q_i)$. Finally, CA sends $\{P_i\ , W_i\}$ to U_i.

Step 3. Upon receiving $\{P_i, W_i\}$, U_i calculates his/her own private key $S_i = W_i + k_i \cdot Q_i$, and he/she can verify the public key by performing the following equation:

$$e\,(S_i, B) = e\,(P_i, P_{CA} - Q_i) \tag{1}$$

If Equation (1) holds, then U_i's private key is S_i; otherwise, it means that the public key P_i has been altered in the transmission.

In the following, we show that the private key S_i (derived by U_i) and the public key P_i (issued by CA) satisfy Equation (1).

Theorem 3.1. *User U_i can utilize Equation (1) to verify his/her public key P_i by himself/herself.*

Proof:

$$\begin{aligned}
& e(S_i, B) \\
&= e(W_i + k_i \cdot Q_i, B) \\
&= e(s_{CA} \cdot (P_i + X_i) + x_i \cdot (P_{CA} + Q_i) + k_i \cdot Q_i, B) \\
&= e(s_{CA} \cdot P_i + s_{CA} \cdot X_i + x_i \cdot P_{CA} + x_i \cdot Q_i + k_i \cdot Q_i, B) \\
&= e(P_i, P_{CA}) \cdot e(X_i, P_{CA}) \cdot e(P_{CA}, X_i) \cdot e(Q_i, X_i) \cdot e(Q_i, K_i) \\
&= e(P_i, P_{CA}) \cdot e(X_i, P_{CA}) \cdot e(P_{CA}, X_i) \cdot e(Q_i, P_i) \\
&= e(P_i, P_{CA}) \cdot e(Q_i, P_i) \\
&= e(P_i, P_{CA}) \cdot e(P_i, Q_i)^{-1} \\
&= e(P_i, P_{CA} - Q_i),
\end{aligned}$$

which implies Equation (1).

3.3. **The new fair blind signature scheme.** In this section, we will present a new fair blind signature scheme with message recovery. Our proposed scheme is constructed based on bilinear pairings instead of modular exponentiation for the consideration of efficiency. In the following, we first define notations used in the proposed scheme, and then propose the new fair blind signature scheme, including the registration phase, blind signature issuing phase and phase of verifying the fair blind signature with message recovery.

[Notations]

s_{CA}: CA's private 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 160 bits.
$x(P)$: the x-coordinate value of point P.
M: message, where $M = \{0,1\}^*$ denotes that the message space is $\{0,1\}^*$.
$||$: a symbol denoting concatenation.
$\in_R$: a symbol denoting the uniform random selection.
$\oplus$: bitwise *exclusive-or* operator.

[Registration phase]

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

Step 1. Requesting for registration:
User U_i computes $\Lambda = \lambda \cdot B$, where $\lambda \in \mathbf{Z}_q^*$ is a random number. Then U_i submits Λ and his/her identity information ID_{U_i} to CA through a secret channel.

Step 2. Registering:
After receiving Λ and ID_{U_i}, CA generates the revocation keys $\alpha, \beta \in \mathbf{Z}_q^*$, where α and β are primes. Then it randomly chooses $\gamma \in \mathbf{Z}_q^*$ and computes $F = \gamma \cdot B$. Afterwards, CA uses a one-way hash function $h()$ to compute $g = h(x(\Lambda)\alpha || x(\Lambda)\beta || x(F))$, and then generates $d = s_{CA} \cdot g + \gamma$ and returns $(x(\Lambda)\alpha, x(\Lambda)\beta, d, g)$ to U_i. Moreover, it computes $H = H_1(g)$ and $D = \alpha\beta \cdot B$, and then saves $(\alpha, \beta, ID_{U_i}, H, D)$ in its database.

Step 3. Verifying registration:
After receiving $(x(\Lambda)\alpha,\ x(\Lambda)\beta,\ d,\ g)$ sent from CA, U_i computes $F' = d \cdot B -$

$g \cdot P_{CA}$ and $g' = h\left(x\left(\Lambda\right)\alpha||x\left(\Lambda\right)\beta||x\left(F'\right)\right)$, and verifies whether $g' = g$. If the checking passes, U_i can confirm that the message $\left(x\left(\Lambda\right)\alpha,\ x\left(\Lambda\right)\beta,\ d,\ g\right)$ sent from CA is correct.

In the following, we demonstrate why the registration verification procedure described in Step 3 works correctly.

Theorem 3.2. *U_i can confirm that the message $\left(x\left(\Lambda\right)\alpha,\ x\left(\Lambda\right)\beta,\ d,\ g\right)$ sent from CA is correct by verifying whether $g' = g$ if $F' = F$.*

Proof:

$$\begin{aligned}(1)\ F' &= d \cdot B - g \cdot P_{CA} = \left(s_{CA}g + \gamma\right) \cdot B - g \cdot P_{CA} \\ &= g \cdot P_{CA} + \gamma \cdot B - g \cdot P_{CA} = \gamma \cdot B = F \\ (2)\ g' &= h\left(x\left(\Lambda\right)\alpha||x\left(\Lambda\right)\beta||x\left(F'\right)\right) = h\left(x\left(\Lambda\right)\alpha||x\left(\Lambda\right)\beta||x\left(F\right)\right) = g\end{aligned}$$

[**Blind signature issuing phase**]

In this phase, user U_i wants to get a blind signature from the signer (U_{sg}).

Step 1. 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 U_{sg}.

Step 2. Generating fair blind factors:
U_{sg} computes $H = \phi + \phi'$ by employing ϕ and ϕ' sent from U_i, and checks whether the value H has been stored in CA's database. If H is in CA's database, U_{sg} obtains the value D from CA's database and verifies whether $\phi = D$ holds. If the result is positive, U_{sg} randomly chooses $r \in \mathbf{Z}_q^*$, and computes $U = r \cdot P_{sg}$ and $\delta = r \cdot \phi$, where P_{sg} is U_{sg}'s public key. Finally, U_{sg} sends the blind factors (U, δ) to U_i.

Step 3. Blinding the message:
After receiving (U, δ), U_i verifies the following equation:

$$e\left(\alpha\beta \cdot U, B\right) = e\left(P_{sg}, \delta\right) \tag{2}$$

If it holds, U_i computes $U' = \alpha \cdot U + \alpha\beta \cdot P_{sg}$ and $U'' = H_3\left(e\left(U', P_{CA} - Q_{sg}\right)\right) \oplus M$, where $Q_{sg} = H_1\left(ID_{sg}\right) \in G_1^*$. Then U_i generates $h = \alpha^{-1}H_4\left(U''\right) + \beta$ and submits h to U_{sg}.

Step 4. Generating a blind signature:
U_{sg} sends $V = (r + h) \cdot S_{sg}$ back to U_i, where S_{sg} is U_{sg}'s private key. And, U_i computes $V' = \alpha \cdot V$ and outputs $\{M, U'', V'\}$, where (U'', V') is the blind signature of the message M.

[**Phase of verifying the fair blind signature with message recovery**]

U_i verifies whether the following equation holds:

$$M = H_3\left(e\left(V', B\right) \cdot e\left(P_{sg}, P_{CA} - Q_{sg}\right)^{-H_4(U'')}\right) \oplus U'' \tag{3}$$

If the result is positive, then (U'', V') is the blind signature of the message M.

In the following, we show that U_i can utilize Equation (2) to verify whether the blind factors (U, δ) are from U_{sg}. Also, we demonstrate why U_i can utilize Equation (3) to verify the blind signature (U'', V') with message recovery.

Theorem 3.3. *User U_i can utilize Equation (2) to verify whether the blind factors (U, δ) are from the signer U_{sg}.*

Proof:

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

which implies Equation (2).

Theorem 3.4. *User U_i can utilize Equation (3) to verify the blind signature (U'', V') with message recovery.*

Proof: Since

$$e(S_{sg}, B) = e(P_{sg}, P_{cA} - Q_{sg}), \quad \text{(derived from Equation (1))} \tag{4}$$
$$V' = \alpha \cdot V$$
$$= \alpha(r + h) \cdot S_{sg}$$
$$= \alpha(r + \alpha^{-1} H_4(U'') + \beta) \cdot S_{sg}$$
$$= (\alpha r + H_4(U'') + \alpha\beta) \cdot S_{sg}, \text{ and}$$
$$U' = \alpha \cdot U + \alpha\beta \cdot P_{sg} = \alpha r \cdot P_{sg} + \alpha\beta \cdot P_{sg},$$

multiplying both sides of Equation (4) by $(\alpha r + H_4(U'') + \alpha\beta)$ can yield that $e((\alpha r + H_4(U'') + \alpha\beta) \cdot S_{sg}, B) = e((\alpha r + H_4(U'') + \alpha\beta) \cdot P_{sg}, P_{cA} - Q_{sg})$, and therefore

$$e(V', B) = e(U' + H_4(U'') \cdot P_{sg}, P_{cA} - Q_{sg}). \tag{5}$$

Then

$$H_3\left(e(V', B) \cdot e(P_{sg}, P_{CA} - Q_{sg})^{-H_4(U'')}\right) \oplus U''$$
$$= H_3\left(e(U' + H_4(U'') \cdot P_{sg}, P_{CA} - Q_{sg}) \cdot e(P_{sg}, P_{CA} - Q_{sg})^{-H_4(U'')}\right) \oplus U''$$
(derived from Equation (5))
$$= H_3\left(e(U' + H_4(U'') \cdot P_{sg}, P_{CA} - Q_{sg}) \cdot e\left(-H_4(U'') \cdot P_{sg}, P_{CA} - Q_{sg}\right)\right)$$
$$\oplus H_3(e(U', P_{CA} - Q_{sg})) \oplus M$$
$$= H_3(e(U', P_{CA} - Q_{sg})) \oplus M \oplus H_3(e(U', P_{CA} - Q_{sg}))$$
$$= M,$$

which implies Equation (3).

3.4. **Fairness of the proposed blind signature scheme.** In this section, we will show the fairness of our proposed scheme in two parts. First, *CA* can associate the signer's signature (h, V) with the sender's signature (U'', V') and the message M by using the revocation function r_I (denoted by $(h, V) \to r_I \to (M, U'', V')$). Second, *CA* can associate the sender's signature (U'', V') and the message M with the signer's signature (h, V) by using the revocation function r_{II} (denoted by $(M, U'', V') \to r_{II} \to (h, V)$). The detailed steps for achieving the fairness are described in the following.

$$[(h, V) \to r_I \to (M, U'', V')]$$

Step 1. *CA* uses h (from the signer's signature) and the revocation keys α and β to verify U'' (from the sender's signature) by testing the following equation:

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

CA accepts U'' if the result is positive.

Step 2. *CA* uses V (from the signer's signature) and the revocation key α to verify V' (from the sender's signature) by verifying the following equation:

$$V' = \alpha \cdot V$$

If the result is positive, *CA* accepts V'.

Step 3. After verifying U'' and V' in Step 1 and Step 2 respectively, CA verifies M by Equation (3). CA accepts M if Equation (3) holds.

$$[(M, U'', V') \to r_{II} \to (h, V)]$$

CA can publicly verify the signer's signature V using the signer's private key S_{sg} and his/her random number r. Also, the revocation function r_{II} can be provided by the additional preprocessing between CA and the signer.

Step 1. CA asks for the signer's random number r. Since

$$\begin{aligned} &U = r \cdot P_{sg}, \\ &U' = \alpha \cdot U + \alpha\beta \cdot P_{sg}, \text{ and} \\ &U'' = H_3\left(e\left(U', P_{CA} - Q_{sg}\right)\right) \oplus M, \end{aligned}$$

we can get

$$\begin{aligned} h &= \alpha^{-1} H_4\left(U''\right) + \beta = \alpha^{-1} H_4\left(H_3\left(e\left(U', P_{CA} - Q_{sg}\right)\right) \oplus M\right) + \beta \\ &= \alpha^{-1} H_4\left(H_3\left(e\left(\alpha \cdot U + \alpha\beta \cdot P_{sg}, P_{CA} - Q_{sg}\right)\right) \oplus M\right) + \beta \\ &= \alpha^{-1} H_4\left(H_3\left(e\left(\alpha r \cdot P_{sg} + \alpha\beta \cdot P_{sg}, P_{CA} - Q_{sg}\right)\right) \oplus M\right) + \beta \end{aligned} \tag{6}$$

CA accepts h if Equation (6) holds.

Step 2. By Equation (6), CA accepts V if the following equation holds:

$$V = \left(r + \alpha^{-1} H_4\left(H_3\left(e\left(\alpha r \cdot P_{sg} + \alpha\beta \cdot P_{sg}, P_{CA} - Q_{sg}\right)\right) \oplus M\right) + \beta\right) \cdot S_{sg}$$

4. Security Proofs.

In the following, we will give security proofs on the properties of blindness and non-forgeability existing in the proposed blind signature scheme.

4.1. The property of blindness.

In order 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 is 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 $\alpha, \beta \in \mathbf{Z}_q^*$:

$$U' = \alpha \cdot U + \alpha\beta \cdot P_{sg} \tag{7}$$

$$U'' = H_3\left(e\left(U', P_{CA} - Q_{sg}\right)\right) \oplus M, \tag{8}$$

$$h = \alpha^{-1} H_4\left(U''\right) + \beta \tag{9}$$

$$V' = \alpha \cdot V \tag{10}$$

It is obvious that $\alpha \in \mathbf{Z}_q^*$ exists uniquely from Equation (10), and therefore we denote α by $\log_V V'$. So we can further get $\beta = h - \left(\log_V V'\right)^{-1} H_4\left(U''\right)$, unique in $\mathbf{Z}_q^*$, from Equation (9). Furthermore, we show that such α and β satisfy Equation (7). Apparently, due to the non-degenerate of the bilinear pairing, we have

$$U' = \alpha \cdot U + \alpha\beta \cdot P_{sg} \Leftrightarrow e\left(U', P_{CA}\right) = e\left(\alpha \cdot U + \alpha\beta \cdot P_{sg}, P_{CA}\right) \tag{11}$$

We just need to show that such α and β satisfy

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

We have

$$
\begin{aligned}
& e\left(\alpha \cdot U+\alpha \beta \cdot P_{sg}, P_{CA}-Q_{sg}\right) \\
=& e\left(\left(\log_V V'\right) \cdot U+\left(\log_V V'\right)\left(h-\left(\log_V V'\right)^{-1} H_4\left(U''\right)\right) \cdot P_{sg}, P_{CA}-Q_{sg}\right) \\
=& e\left(\left(\log_V V'\right) r \cdot P_{sg}+\left(\log_V V'\right) h \cdot P_{sg}, P_{CA}-Q_{sg}\right) \cdot e\left(H_4\left(U''\right) \cdot P_{sg}, P_{CA}-Q_{sg}\right)^{-1} \\
=& e\left(\left(\log_V V'\right) r \cdot P_{sg}+\left(\log_V V'\right) h \cdot P_{sg}, P_{CA}-Q_{sg}\right) \cdot e\left(U'+H_4\left(U''\right) \cdot P_{sg}, P_{CA}-Q_{sg}\right)^{-1} \\
& \cdot e\left(U', P_{CA}-Q_{sg}\right) \\
=& e\left(\left(\log_V V'\right) r \cdot P_{sg}+\left(\log_V V'\right) h \cdot P_{sg}, P_{CA}-Q_{sg}\right) \cdot e\left(V', B\right)^{-1} \cdot e\left(U', P_{CA}-Q_{sg}\right) \\
& \text{(derived from Equation (5))} \\
=& e\left(\left(\log_V V'\right)(r+h) \cdot P_{sg}, P_{CA}-Q_{sg}\right) \cdot e\left(V', B\right)^{-1} \cdot e\left(U', P_{CA}-Q_{sg}\right) \\
=& e\left(\left(\log_V V'\right)(r+h) \cdot S_{sg}, B\right) \cdot e\left(V', B\right)^{-1} \cdot e\left(U', P_{CA}-Q_{sg}\right) \\
& \text{(derived from Equation (1))} \\
=& e\left(\left(\log_V V'\right) \cdot V, B\right) \cdot e\left(V', B\right)^{-1} \cdot e\left(U', P_{CA}-Q_{sg}\right) \\
=& e\left(V', B\right) \cdot e\left(V', B\right)^{-1} \cdot e\left(U', P_{CA}-Q_{sg}\right) \\
=& e\left(U', P_{CA}-Q_{sg}\right)
\end{aligned}
$$

Since α and β satisfy Equation (11), we have shown that such α and β also satisfy Equation (8). Thus, there always exist the blind factors to lead to the same relation as defined in the blind signature issuing phase.

4.2. **The property of non-forgeability.** Let A be the attacker who controls the sender. A can forge valid blind signatures once he/she gets the signer's private key. We consider four lemmas as follows.

Lemma 4.1. *The advantage of A in revealing U_{sg}'s private key S_{sg} from*

$$e(P_{sg}, P_{CA}-Q_{sg}) = e(S_{sg}, B) \tag{12}$$

by interacting with U_{sg}'s ID is negligible. (Notice that in Theorem 3.1, a registered user U_i can utilize the equation $e\left(P_i, P_{CA}-Q_i\right)=e\left(S_i, B\right)$, i.e., Equation (1), to verify his/her public key.)

Proof: The proof of this case is by contradiction. We assume that A successfully produces a valid message-signature pair $(m, \sigma(m))$ with a non-negligible probability ε. Then the attacker A constructs a simulator S to solve the Computational Diffie-Hellman (CDH) problem. In other words, S successfully solve the CDH-problem with a non-negligible probability ε.

Let q_H be the maximum number of queries asked from A to S. The attacker A gets public parameters $PARAMS\left(G_1, G_2, q, e, B, P_{CA}, Q_{sg}\right)$ and wants to find $S_{sg} \in G_1$ from Equation (12). We describe the operation process of the simulator S as follows:

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

Now A wants to use P_{sg} (from S) to get S_{sg} from Equation (12). From Section 3.2, we can get

$$\begin{cases} K_{sg} = k_{sg} \cdot B \\ X_{sg} = x_{sg} \cdot B \\ P_{CA} = s_{CA} \cdot B \\ P_{sg} = K_{sg} + X_{sg} \end{cases},$$

where k_{sg}, x_{sg} and $s_{CA} \in \mathbf{Z}_q^*$.

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

$$\begin{aligned} & e(P_{sg}, P_{CA} - Q_{sg}) \\ = \ & e(K_{sg} + X_{sg}, P_{CA} - Q_{sg}) \\ = \ & e(k_{sg} \cdot B + x_{sg} \cdot B, s_{CA} \cdot B - s \cdot B) \\ = \ & e(B, B)^{(k_{sg}+x_{sg})(s_{CA}-s)} \end{aligned} \tag{13}$$

Let

$$\begin{cases} t = k_{sg} + x_{sg} \\ u = s_{CA} - s \end{cases},$$

where t and $u \in \mathbf{Z}_q^*$.

Therefore, $e(B, B)^{(k_{sg}+x_{sg})(s_{CA}-s)} = e(B, B)^{tu} = e(S_{sg}, B)$. From Equation (13), we can know that the advantage of A in getting S_{sg} from Equation (12) is

$$\mathrm{Adv}_{A,G_1} = \Pr\left[A(B, t \cdot B, u \cdot B, tu \cdot B) = 1 : t, u \in_R \mathbf{Z}_q^*\right] = \varepsilon.$$

By the CDH assumption, for a probabilistic, polynomial-time and 0/1-valued algorithm A, $\mathrm{Adv}_{A,G_1}^{\mathrm{CDH}}$ is negligible. This is a contradiction, because the advantage of 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 4.1. *An attacker cannot reveal U_{sg}'s private key S_{sg} from Equation (12) by interacting with U_{sg}'s ID.*

Proof: By Lemma 4.1, we have completed the proof.

Lemma 4.2. *The advantage of A in revealing U_{sg}'s private key S_{sg} from Equation (3) by interacting with U_{sg}'s ID is negligible.*

Proof: Assume that A successfully produces a valid message-signature pair $(m, \sigma(m))$ with a non-negligible probability ε. Then the attacker A constructs a simulator S to solve the Computational Diffie-Hellman (CDH) problem. In other words, S successfully solve the CDH-problem with a non-negligible probability ε.

Let q_H be the maximum number of queries asked from A to S. The attacker 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 Equation (3). The operation process of the simulator S is the same as the one of the simulator in Lemma 4.1. And now, A wants to use P_{sg} to get S_{sg} from Equation (3). From the proof of Theorem 3.4, we can obtain

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

so A may reveal S_{sg} from $e(U', P_{CA} - Q_{sg})$. Since

$$U' = \alpha \cdot U + \alpha\beta \cdot P_{sg} = \alpha r \cdot P_{sg} + \alpha\beta \cdot P_{sg} = (\alpha r + \alpha\beta) \cdot P_{sg},$$

A can get

$$e\left(U', P_{CA} - Q_{sg}\right) = e\left((\alpha r + \alpha\beta) \cdot P_{sg}, P_{CA} - Q_{sg}\right) = e\left(P_{sg}, P_{CA} - Q_{sg}\right)^{(\alpha r + \alpha\beta)} \quad (14)$$

According to Lemma 4.1, the advantage of A in revealing U_{sg}'s private key S_{sg} from Equation (14) by interacting with U_{sg}'s *ID* is negligible. In other words, the success probability of the forgery in this attack is negligible.

Theorem 4.2. *An attacker cannot reveal U_{sg}'s private key S_{sg} from Equation (3) by interacting U_{sg}'s ID.*

Proof: By Lemma 4.2, we have completed the proof.

Lemma 4.3. *The advantage of A in revealing U_{sg}'s private key S_{sg} by using the arbitrary signer's ID is negligible.*

Proof: We assume that *Extract* is a random oracle, and allow the attacker A to query it.

1. The attacker A queries *Extract* to get P_{ID} and S_{ID}.
$$(P_{ID}, S_{ID}) \leftarrow Extract\left(PARAMS, K_{ID}, ID\right).$$
2. The attacker A queries *Extract* q_E times with $(PARAMS, K_i, ID_i \neq ID)$ for $i = 1, \cdots, q_E$. Then *Extract* returns the q_E corresponding secrete keys S_{ID_i} to A.
3. The attacker A generates q_E signatures with the help of (P_{ID_i}, S_{ID_i}), and outputs a valid message-signature pair $(m, \sigma(m))$.

Since H_1, H_2, H_3, H_4 are random oracles, sender and signer generate random numbers with uniform distributions in both *Extract* and the blind signature issuing phases. This means that the attacker A learns nothing from query results. In other words, under the CDH assumption and the argument that all hash functions are random oracles, the success probability of the forgery in this case is negligible.

Theorem 4.3. *An attacker cannot reveal U_{sg}'s private key S_{sg} by using the arbitrary signer's ID.*

Proof: By Lemma 4.3, we have completed the proof.

Lemma 4.4. *The advantage of A in revealing U_{sg}'s private key S_{sg} by utilizing the generic parallel attack is negligible.*

Proof: In 2001, Schnorr [29] proposed a new attack, called generic parallel attack, on Schnorr's blind signature scheme [30]. 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 A uses the generic parallel attack to forge $l + 1$ valid blind signatures in our proposed scheme. Let q_H be the maximum number of queries H_3 from A.

Step 1. The signer U_{sg} sends commitments $U_1 = r_1 \cdot P_{sg}$, $U_2 = r_2 \cdot P_{sg}$, $\cdots$, $U_l = r_l \cdot P_{sg}$.

Step 2. 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 A computes $f_k = e\left(\sum_{i=1}^{l} a_{k,i} \cdot U_i, P_{CA} - Q_{sg}\right)$ and $H_3\left(f_k\right) \oplus U_k{}''$ for $k = 1, 2, \cdots, t$; $t < q_H$.

Step 3. A solves the following equation for obtaining the unknown $h_1, h_2, \cdots, h_l$ over $\mathbf{Z}_q$:
$H_4\left(U_k{}''\right) = \sum_{j=1}^{l} a_{k,j} h_j$ for $k = 1, 2, \cdots, t$.

Step 4. A sends these solutions $h_1, h_2, \ldots, h_l$ to the signer U_{sg}.

Step 5. U_{sg} computes $V_i = h_i \cdot S_{sg} + r_i \cdot S_{sg}$ for $i = 1, 2, \cdots, l$ and returns V_i to A.

Step 6. A can get the valid signatures (m_k, U_k'', V_k') by setting $H_4\left(U_k''\right) = \sum_{j=1}^{l} a_{k,j}h_j$ and

$$V_k' = \sum_{j=1}^{l} a_{k,j} \cdot V_j.$$

Step 7. A outputs $l+1$ signatures (m_k, U_k'', V_k') for $k = 1, 2, \cdots, l+1$.

From the above steps, it is easy to see that the forged signatures are valid. Because the following equation

$$\begin{aligned}
& e\left(V_k', B\right) \cdot e\left(P_{sg}, P_{CA} - Q_{sg}\right)^{-H_4(U_k'')} \\
&= e\left(\sum_{j=1}^{l} a_{k,j} \cdot V_j, B\right) \cdot e\left(P_{sg}, P_{CA} - Q_{sg}\right)^{-H_4(U_k'')} \\
&= e\left(\sum_{j=1}^{l} a_{k,j}\left(h_j \cdot S_{sg} + r_j \cdot S_{sg}\right), B\right) \cdot e\left(P_{sg}, P_{CA} - Q_{sg}\right)^{-H_4(U_k'')} \\
&= e\left(S_{sg}, B\right)^{\sum_{j=1}^{l} a_{k,j}h_j} \cdot e\left(\sum_{j=1}^{l} a_{k,j}r_j \cdot S_{sg}, B\right) \cdot e\left(P_{sg}, P_{CA} - Q_{sg}\right)^{-H_4(U_k'')} \\
&= e\left(S_{sg}, B\right)^{H_4(U_k'')} \cdot e\left(\sum_{j=1}^{l} a_{k,j}r_j \cdot S_{sg}, B\right) \cdot e\left(P_{sg}, P_{CA} - Q_{sg}\right)^{-H_4(U_k'')} \\
&= e\left(\sum_{j=1}^{l} a_{k,j}r_j \cdot S_{sg}, B\right) \\
&= e\left(\sum_{j=1}^{l} a_{k,j}r_j \cdot P_{sg}, P_{CA} - Q_{sg}\right) \text{(derived from Equation (12))} \\
&= e\left(\sum_{j=1}^{l} a_{k,j} \cdot U_j, P_{CA} - Q_{sg}\right) = f_k
\end{aligned}$$

holds, $H_3\left(f_k\right) \oplus U_k'' = m_k$ can be derived according to Equation (3).

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 coefficient $a_{k,i} \in \mathbf{Z}_q$ and a solvable system of $l+1$ distinct equations in the unknown $h_1, h_2, \cdots, h_l$ over $\mathbf{Z}_q$:

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

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

Theorem 4.4. *It is intractable for an attacker to try to reveal U_{sg}'s private key S_{sg} by utilizing the generic parallel attack.*

Proof: By Lemma 4.4, we have completed the proof.

5. **Discussion and Performance Evaluation.** In this section, the proposed fair blind signature scheme with message recovery (FBSMR) is first compared with the recently

proposed related schemes in terms of security properties. We then analyze both computational complexity and communicational cost of the proposed FBSMR by comparing with the previously proposed FBSMR.

5.1. **Property comparisons.** The proposed scheme has nice properties, including complete security proofs, pairing technology, message recovery and high efficiency. Table 1 shows the property comparisons among the proposed scheme and others. In these schemes, we can find Lee-Kim [8], Stadler-Piveteau-Camenisch [5] and Tsaur-Chou [13] have no security proofs on their proposed schemes. Abe-Ohkubo [14] used a complicate interactive proof system, called verifiable encryption of discrete logarithms, in the signature generation phase to prove that the secret of identity can be recovered by the trustee later. Due to applying the ordinary public key cryptosystem and lacking for the property of message recovery, Abe and Ohkubo's scheme [14] is not suitable for resource-limited environments. Although both Hufschmitt-Traore [15] and Fuchsbauer-Vergnaud [16] adopted the pairing cryptography to construct their efficient and security-provable schemes, our proposed scheme is superior to theirs in providing the advantages of self-certified public keys together with message recovery, which makes the proposed scheme more practical and flexible. The recent result of new notion called partial blind signature is proposed by Ruckert and Schroder [17]. However, they still presented a normal structure and did not consider the special application on minimizing the size of transmission messages and key management issues. In summary, due to employing the message recovery and self-certified public key cryptosystem, our proposed scheme can be suitable for the environments of low bandwidth communication, such as cell-phones or PDAs payment systems, or the commercial affairs in vehicular networks.

Table 1. The property comparisons among the proposed scheme and others

Schemes	Security Assumption	Security Proofs	Message Recovery	Used Techniques	Self-certified Public Key
Abe-Ohkubo [14]	DDH, DLP	Yes	No	Schnorr-type proof of knowledge	No
Fuchsbauer-Vergnaud [16]	DLIN, DHSDH, HDL	Yes	No	NIZK, Bilinear pairings	No
Hufschmitt-Traore [15]	Decisional composite residuosity, External DDH	Yes	No	Bilinear pairings, Double ElGamal encryption	No
Lee-Kim [8]	DLP	No (Insecure)	Yes	Meta-ElGamal signature scheme	No
Ruckert-Schroder [17]	Common reference string model	Yes	No	Fischlin's blind signature scheme, Partial blind signature scheme	No
Stadler-Piveteau-Camenisch [5]	Factorization	No	No	Cut-and-choose, Oblivious transfer	No
Tsaur-Chou [13]	ECDLP	No	Yes	Elliptic curve cryptosystem	No
Proposed Scheme	CDH, ECDLP	Yes	Yes	Bilinear pairings	Yes

Note: DLIN, DHSDH, HDL, NIZK and ECDLP represent Decision Linear, Double Hidden Strong Diffie-Hellman, Hard Discrete Logarithm, Non-Interactive Zero-Knowledge, and Elliptic Curve Discrete Logarithm Problem, respectively.

5.2. **Computational complexity.** The following notations are used for measuring the computational complexity.

$T_{MM}/T_{EXP}/T_{MA}$: the time for computing a modular multiplication/exponentiation/addition in a finite field.
T_{INV}: the time for computing modular inversion in a finite field.
T_{EM}: the time for performing an ECC multiplication in the group G_1.
T_{EA}: the time for performing an ECC addition in the group G_1.
T_e: the time for performing a bilinear pairing e.
T_h: the time for computing the one-way has function h.

According to the paper proposed by Koblitz et al. [31], the above time complexities have the following relationship: $T_e \approx T_{EM} \approx 29T_{MM}$; $T_{EA} \approx 0.12T_{MM}$; $T_{EXP} \approx 240T_{MM}$; T_{MA} and T_h are negligible as compared to the above complexities measures.

In Table 2, we can see that the proposed FBSMR is more efficient than Lee-Kim's [8] or Tsaur-Chou's scheme [13] in computational complexity.

Table 2. The comparison of computational complexity

Phase	Lee-Kim's scheme [8]	Tsaur-Chou's scheme [13]	The proposed FBSMR
Registration	$962T_{MM} + T_{INV}$	$147.12T_{MM}$	$145.12T_{MM}$
Blind signature issuing and verification	$2837T_{MM} + 5T_{INV}$	$471.36T_{MM}$	$435.72T_{MM}$

5.3. **Communicational cost.** In the following, we will analyze the communicational cost of the proposed FBSMR. 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 3, it is obvious that the proposed FBSMR has improved the performance of communicational cost as compared with the previously proposed schemes [8,13].

Table 3. The comparison of communicational cost

Phase	Lee-Kim's scheme [8]	Tsaur-Chou's scheme [13]	The proposed FBSMR
Registration	$3\|p'\|+2\|q\| + \|h\|$	$\|p\|+4\|n\| + \|h\|$	$2\|p\|+3\|n\| + \|h\|$
Blind signature issuing and verification	$6\|p'\|+2\|q\|$	$6\|p\|+2\|n\|$	$5\|p\| + \|h\|$

6. **Conclusions.** In this paper, we develop a new fair blind signature scheme with message recovery based on the self-certified pairing-based public key cryptosystem. Preserving the merits inherent in the pairing-based cryptosystem, it can possess fewer bits to achieve the higher security level. Moreover, our new scheme has the advantage that the authentication of the public key can be accomplished with the verification of the fair blind signature in a logically single step due to the use of the self-certified public key cryptosystem. Integrating the two key features, namely the message recovery and self-certified public key cryptosystem, makes the proposed scheme more easily be conducted in resource-limited environments, such as wireless communication and ad hoc networks, since they require less computations and a simplified key management strategy. Furthermore, the fairness of blind signature with message recovery can be actually achieved in our proposed scheme. In summary, the proposed FBSMR can not only improve the efficiency of the previously proposed schemes, but also achieve the blindness and non-forgeability properties of blind signature based on the proposed security proofs.

Acknowledgment. This work is partially supported by the National Science Council of Taiwan under contract numbers NSC 100-2219-E-212-001, NSC 99-2219-E-212-001, NSC 99-2622-E-212-010-CC3 and NSC 99-2628-E-415-002. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] D. Chaum, Blind signature for untraceable payments, *Advances in Cryptology – Proc. of CRYPTO, LNCS*, pp.199-203, 1982.

[2] C. I. Fan, C. I. Wang and W. Z. Sun, Fast randomization schemes for Chaum blind signatures, *International Journal of Innovative Computing, Information and Control*, vol.5, no.11(A), pp.3887-3900, 2009.

[3] L. Han, X. Hu and Y. Sun, A competition model on network externalities between payment card networks, *ICIC Express Letters*, vol.3, no.4(B), pp.1293-1298, 2009.

[4] G. Liu and Y. Zhou, Transportation cost payment problem in a two-echelon decentralized supply chain, *ICIC Express Letters*, vol.4, no.2, pp.427-434, 2010.

[5] M. Stadler, J.-M. Piveteau and J. Camenisch, Fair blind signatures, *Advances in Cryptology – Proc. of EUROCRYPT, LNCS*, vol.921, pp.209-219, 1995.

[6] C. I. Fan and C. L. Lei, A user efficient fair blind signature scheme for untraceable electronic cash, *Journal of Information Science and Engineering*, vol.18, no.1, pp.47-58, 2002.

[7] X. Wang and X. Sun, Fair blind signature based authentication for super peer P2P network, *Information Technology Journal*, vol.8, no.6, pp.887-894, 2009.

[8] H. W. Lee and T. Y. Kim, Message recovery fair blind signature, *Proc. of the 2nd International Workshop on Practice and Theory in Public Key Cryptography*, pp.97-111, 1999.

[9] M. Jakobsson, K. Sako and R. Impagliazzo, Designated verifier proofs and their applications, *Advances in Cryptology – Proc. of Eurocrypt, LNCS*, vol.1070, pp.199-205, 1996.

[10] Y. Zheng, Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption), *Advances in Cryptology – Proc. of CRYPTO, LNCS*, vol.1294, pp.165-179, 1997.

[11] J. E. Hsien, P. W. Ko and C. Y. Chen, Comments on Lee and Kim's message recovery fair blind signature scheme, *Proc. of the 10th National Conf. on Information Security*, Chinese Cryptology and Information Security Association (CCISA), Taiwan, pp.123-125, 2000.

[12] M. Y. Chung, *Message Recovery Fair Blind Signature Schemes*, Master Thesis, National Chung Hsing University, Taiwan, 2002.

[13] W. J. Tsaur and C. H. Chou, An efficient and secure fair blind signature scheme with message recovery, *Proc. of the 13th National Conf. on Information Security*, Chinese Cryptology and Information Security Association (CCISA), Taiwan, pp.54-62, 2003.

[14] M. Abe and M. Ohkubo, Provably secure fair blind signatures with tight revocation, *Advances in Cryptology – Proc. of ASIACRYPT, LNCS*, vol.2248, pp.583-601, 2001.

[15] E. Hufschmitt and J. Traore, Fair blind signature revised, *Pairing-based Cryptography – Pairing 2007, LNCS*, vol.4575, pp.268-292, 2007.
[16] G. Fuchsbauer and D. Vergnaud, Fair blind signatures without random oracles, *Progress in Cryptology – Proc. of AFRICACRYPT, LNCS*, vol.6055, pp.16-33, 2010.
[17] M. Ruckert and D. Schroder, Fair partially blind signatures, *Progress in Cryptology – Proc. of AFRICACRYPT, LNCS*, vol.6055, pp.34-51, 2010.
[18] Y. F. Chung and H. F. Chen, Cross platform layer for public key infrastructure interoperability, *International Journal of Innovative Computing, Information and Control*, vol.5, no.6, pp.1699-1710, 2009.
[19] X. F. Chen, F. G. Zhang and K. Kim, ID-based multi-proxy signature and blind multisignature from bilinear pairings, *Proc. of KIISC Conf. 2003*, Korea, pp.11-19, 2003.
[20] F. G. Zhang and K. Kim, Efficient ID-based blind signature and proxy signature from bilinear pairings, *Proc. of ACISP, LNCS*, vol.2727, pp.312-323, 2003.
[21] F. G. Zhang and K. Kim, ID-based blind signature and ring signature from pairings, *Advances in Cryptology – Proc. of ASIACRYPT, LNCS*, vol.2501, pp.533-547, 2002.
[22] F. G. Zhang, S. N. Reihaneh and W. Susilo, An efficient signature scheme from bilinear pairings and its applications, *Proc. of PKC, LNCS*, vol.2947, pp.277-290, 2004.
[23] F. G. Zhang, S. N. Reihaneh and W. Susilo, Efficient verifiably encrypted signature and partially blind signature from bilinear pairings, *Proc. of INDOCRYPT 2003, LNCS*, vol.2904, pp.191-204, 2003.
[24] A. Shamir, Identity-based cryptosystems and signature schemes, *Advances in Cryptology – Proc. of CRYPTO, LNCS*, vol.196, pp.47-53, 1984.
[25] M. Girault, Self-certified public keys, *Advances in Cryptology – Proc. of EUROCRYPT, LNCS*, vol.547, pp.491-497, 1991.
[26] T. S. Wu and C. L. Hsu, Convertible authenticated encryption scheme, *Journal of Systems and Software*, vol.62, no.3, pp.205-209, 2002.
[27] E. Verheul, Self-blindable credential certificates from the Weil pairing, *Advances in Cryptology – Proc. of ASIACRYPT, LNCS*, vol.2248, pp.533-551, 2001.
[28] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, vol.IT-22, no.6, pp.644-654, 1976.
[29] C. P. Schnorr, Security of blind discrete log signatures against interactive attacks, *Proc. of ICICS, LNCS*, vol.2229, pp.1-12, 2001.
[30] C. P. Schnorr, Efficient identification and signatures for smart cards, *Advances in Cryptology – Proc. of CRYPTO, LNCS*, vol.435, pp.239-252, 1990.
[31] N. Koblitz, A. Menezes and S. Vanstone, The state of elliptic curve cryptography, *Designs, Codes and Cryptography*, vol.19, no.2, pp.173-193, 2000.