Secure Rewarding Schemes *

Chun-I Fan
Department of Electrical Engineering
National Taiwan University
Taipei, Taiwan, R.O.C.
fan@crypto.ee.ntu.edu.tw

Chin-Laung Lei
Department of Electrical Engineering
National Taiwan University
Taipei, Taiwan, R.O.C.
lei@thunder.ee.ntu.edu.tw

Abstract

In this paper, we propose a secure rewarding scheme. In the scheme, a reward provider publishes a problem, and provides a reward for a person who can supply him a satisfactory solution of the problem. The first qualified claimant with satisfactory solution of the problem is selected to obtain the reward. The selected claimant can obtain the reward from the reward provider without revealing his identity. Nobody except the selected claimant can get the reward, and the provider cannot decline the selected claimant his entitled reward. In addition, we also propose another secure rewarding scheme with two-way untraceability to protect the privacy of the reward provider as well.

1. Introduction

Due to the fast progress of network technologies, many advanced communication services have been proposed in the literature. Among these services, electronic payment is a popular one since the technique makes it possible for a payer to pay electronic cash to the payee by transmitting the cash through an electronic channel. Furthermore, numerous economic activities can be operated and performed through the communication networks quickly and correctly. However, in some situations, the privacy of the participants who take part in these activities must be protected against dishonest parties. Especially, the privacy consideration is more important if these activities are sensitive, such as the police pays a reward to an anonymous witness who provides a crucial evidence for a crime.

In real world, a person usually has many problems to solve. Some of the problems can be solved by himself, while some difficult problems may need the help of others. For privacy considerations, a helper usually requests to keep his identity secret when what he faces is a sensitive problem. Is it possible for the helper to supply the solution of the problem to the helpee and claim the reward provided by the helpee without exposing his identity to anybody?

Formally, a problem and a deadline are published by a reward provider. If one can supply the provider a solution of the problem before the deadline, then the provider gives a reward to him. Assume that a reward claimant knows how to solve the problem, and he can satisfy the requirements published by the provider. How can the claimant submit the provider the solution of the problem and obtain the reward from the provider without revealing his identity?

In this paper, we introduce a secure rewarding scheme. In our scheme, the first qualified claimant is selected to obtain the reward offered by the reward provider. Based on the techniques of communication networks and cryptography, our proposed scheme makes it possible for the selected claimant to submit his solution of the problem to the provider and get the reward from the provider privately, without exposing his identity. In our scheme, no one can obtain the reward except the selected claimant, and the reward provider cannot decline the selected claimant his entitled reward. In addition, another secure rewarding technique with two-way untraceability is proposed in this paper. In the proposed two-way untraceable rewarding scheme, the privacy of both the reward claimants and the reward providers is protected against each other.

The rest of the paper is organized as follows. In section 2, we review the cryptographic techniques used in our schemes. The proposed rewarding scheme is described in section 3, and the security of the scheme is examined in this section. In section 4, we present a secure rewarding scheme with two-way untraceabil-

*This research is supported in part by the National Science Council of the Republic of China under grant NSC-86-2221-E-002-014.

1060-3425/97 $10.00 © 1997 IEEE

ity, and discuss the security of the scheme. Finally, a concluding remark is given in section 5.

2. Preliminary

In this section, we provide a summary of several basic cryptographic primitives which are prerequisite in order to build the proposed rewarding schemes in the following sections. These primitives include the techniques of public-key encryptions, untraceable e-mails, digital signature schemes, blind signature techniques, and electronic cash systems.

2.1. Public-key encryptions

Public-key encryptions are used in our proposed rewarding scheme since the key distribution overhead of a secret-key encryption system is not acceptable. Secure public-key encryptions can protect the privacy of messages transmitted in open communication environments. Typically, a public-key encryption scheme consists of two kinds of participants, encrypters and a decrypter. Initially, the decrypter chooses an encryption function $E_{decrypter}$ and the decryption function $D_{decrypter}$ corresponding to $E_{decrypter}$. The encryption function is public, and the decryption function is kept secret by the decrypter. It is computationally infeasible to derive $D_{decrypter}$ from $E_{decrypter}$. An encrypter encrypts a plaintext message m by applying the encryption function, and then submits the ciphertext message $E_{decrypter}(m)$ to the decrypter. The decrypter can decrypt the ciphertext to obtain m by performing $D_{decrypter}(E_{decrypter}(m)) = m$. In addition, the public encryption function of a decrypter can be authenticated by using the registered license obtained from an authority.

2.2. Untraceable e-mails

The techniques of sender untraceable e-mails can protect the privacy of a sender against the receiver when the sender submits messages to the receiver. Based on public-key encryptions and the untraceable techniques proposed in [3], we show a secure sender untraceable e-mail scheme in this sub-section. The scheme consists of four roles, senders, receivers, center X, and center Y. The senders send messages to the centers, and then the centers forward the messages to the receivers. The details of the scheme are described below.

E_X, E_Y, and E_R are the public-key encryption functions of center X, center Y, and a message receiver, respectively. Let $E(a_1, a_2, ..., a_n)$ denote the ciphertext of $(a_1, a_2, ..., a_n)$ under the encryption function E. To send a plaintext m to the receiver, the sender computes,

$$c_X = E_X(E_Y(E_R(m), Addr, r_Y), r_X)$$

where $Addr$ is the address of the receiver, and r_X, r_Y are two strings randomly chosen by the sender. The sender submits c_X to center X. After receiving the message c_X, center X computes,

$$D_X(c_X) = (E_Y(E_R(m), Addr, r_Y), r_X)$$

where D_X is the decryption function corresponding to E_X. By discarding r_X, center X obtains,

$$c_Y = E_Y(E_R(m), Addr, r_Y).$$

Center X sends c_Y to center Y. After receiving the message c_Y, center Y computes,

$$D_Y(c_Y) = (E_R(m), Addr, r_Y)$$

where D_Y is the decryption function corresponding to E_Y. By discarding r_Y and $Addr$, center Y can get $E_R(m)$. According to the $Addr$, center Y sends $E_R(m)$ to the receiver. After receiving the ciphertext $E_R(m)$, the receiver can compute $D_R(E_R(m)) = m$ where D_R is the decryption function corresponding to E_R.

In the sender untraceable e-mail scheme, center X cannot derive the receiver's address since the address is encrypted by the encryption function of center Y. In addition, Center Y receives the message form center X, so the identity of the sender is unknown to center Y. Similarly, the sender's identity is protected against the receiver since the receiver receives the message form center Y. Therefore, the e-mail system is sender untraceable from the receiver's point of view. In this e-mail system, it is necessary to assume that center X does not collude with center Y. For a system with n centers, only one honest center is required to protect the privacy of the sender.

2.3. Digital signatures

Digital signatures are important primitives of modern cryptography since the techniques make it possible to sign digital electronic messages. Typically, a digital signature scheme consists of two participants, verifiers and a signer. Initially, the signer chooses a signature function S_{signer} and the verification function V_{signer} corresponding to S_{signer}. The signature function is kept secret by the signer, and the verification function is public. It is computationally infeasible to derive S_{signer} from V_{signer}. The signer signs a plaintext

message m with some proper redundancy by computing $S_{signer}(m)$, and then submits the signed message to verifiers. To verify the signature $S_{signer}(m)$, the verifiers examine if $V_{signer}(S_{signer}(m)) = m$ contains proper redundancy.

2.4. Blind signatures

Blind signature is another kind of advanced signature techniques. It has been widely used in many popular network services proposed in the literature, such as untraceable voting systems [1, 14, 10, 22] and payment systems [5, 15]. A general blind signature scheme consists of two kinds of participants, a signer and requesters. A requester requests signatures from the signer, and the signer issues blind signatures to the requester. There are two sets of messages known to the signer, one contains the signatures actually performed by him; the other contains the signatures submitted by the requesters for verification later. The key point is that the actual correspondence between these two sets of signatures is unknown to the signer. This property is usually referred to as the unlinkability property. Owing to the unlinkability feature, blind signature techniques can be used to protect the privacy of the claimants in our proposed rewarding scheme. We have proposed some efficient blind signature schemes in [7, 8, 9]. These schemes are based on the theories of quadratic residues [13, 24]. Under a modulus n, x is a quadratic residue (QR) in Z_n^* if and only if there exists an integer y in Z_n^* such that $y^2 \equiv_n x$ where Z_n^* is the set of all positive integers less than and relatively prime to n. Given x, it is infeasible to compute the square root y of x in Z_n^* if n contains large prime factors and the factorization of n is unknown [20]. The blind signature scheme presented in [9] consists of four phases: (1) initialization, (2) requesting, (3) signing, and (4) extraction. The signer publishes the necessary information in the initialization phase. To obtain the signature of a message, a requester submits an encrypted version of the message to the signer in the requesting phase. In the signing phase, the signer computes the blind signature of the message, and then sends the result back to the requester. Finally, the requester extracts the signature from the result he receives in the extraction phase. The details of the blind signature scheme are presented as follows.

(1) Initialization. The signer randomly selects $n = p_1 p_2$ where p_1, p_2 are distinct large primes and $p_1 \equiv p_2 \equiv 3 \pmod 4$. The signer publishes n.

(2) Requesting. To request the signature of a plaintext m in Z_n^*, a requester randomly chooses r and $(u^2 + v^2)$ in Z_n^*, and then submits $(r^4 m(u^2 + v^2) \bmod n)$ to the signer. If m has no redundancy, a suitable one-way hashing function should be applied to m in order to avoid the multiplicative attacks. After receiving $(r^4 m(u^2 + v^2) \bmod n)$, the signer randomly selects x and y such that $r^4 m(u^2 + v^2)(x^2 + y^2)$ is a QR in Z_n^*, and then sends x and y to the requester. The requester submits the signer $(b^2(uy - vx) \bmod n)$ where b is an integer randomly chosen by him in Z_n^*.

(3) Signing. After receiving $(b^2(uy - vx) \bmod n)$, the signer computes,

$$
\begin{aligned}
& r^4 m(u^2 + v^2)(x^2 + y^2)(b^2(uy - vx))^{-2} \\
& \equiv_n r^4 b^{-4} m(u^2 + v^2)(x^2 + y^2)(uy - vx)^{-2} \\
& \equiv_n r^4 b^{-4} m((ux + vy)^2 + (uy - vx)^2)(uy - vx)^{-2} \\
& \equiv_n r^4 b^{-4} m((ux + vy)^2 (uy - vx)^{-2} + 1).
\end{aligned}
$$

Since the signer knows the primes p_1 and p_2, the signer can derive an integer t in Z_n^* [16, 20] such that,

$$t^4 \equiv_n r^4 b^{-4} m((ux + vy)^2 (uy - vx)^{-2} + 1).$$

Then, the signer sends t to the requester.

(4) Extraction. After receiving t, the requester computes $s = (r^{-1} bt \bmod n)$ and $c = ((ux + vy)(uy - vx)^{-1} \bmod n)$. The signature of m is (s, m, c). To verify the signature (s, m, c), one can examine if $s^4 \equiv_n m(c^2 + 1)$.

2.5. Electronic cash

In an electronic cash system, the bank issues electronic cash (e-cash), and a customer can withdraw e-cash from his account, or deposit e-cash into his account in the bank. By means of the techniques of blind signatures, an electronic cash system can be constructed. Based on the blind signature scheme described in section 2.4, we show an electronic cash system below.

(1) Initialization. The bank randomly selects $n = p_1 p_2$ where p_1, p_2 are distinct large primes and $p_1 \equiv p_2 \equiv 3 \pmod 4$. The bank publishes n.

(2) Withdrawing. Let w be the denomination of an e-cash issued by the bank. To withdraw w dollars, a customer chooses m, r, and $(u^2 + v^2)$ in Z_n^*, and then submits $(r^4 m(u^2 + v^2) \bmod n)$ to the bank. After receiving $(r^4 m(u^2 + v^2) \bmod n)$, the bank randomly selects x and y such that

$r^4m(u^2+v^2)(x^2+y^2)$ is a QR in Z_n^*, and then sends x and y to the customer. The customer submits the bank $(b^2(uy-vx) \bmod n)$ where b is an integer randomly chosen by the customer in Z_n^*. After receiving $(b^2(uy-vx) \bmod n)$, the bank computes,

$$r^4m(u^2+v^2)(x^2+y^2)(b^2(uy-vx))^{-2}$$
$$\equiv_n r^4b^{-4}m((ux+vy)^2+(uy-vx)^2)(uy-vx)^{-2}$$
$$\equiv_n r^4b^{-4}m((ux+vy)^2(uy-vx)^{-2}+1).$$

The bank derives an integer t in Z_n^* such that,

$$t^4 \equiv_n r^4b^{-4}m((ux+vy)^2(uy-vx)^{-2}+1).$$

Then, the bank sends t to the customer. After receiving t, the customer computes $s = (r^{-1}bt \bmod n)$ and $c = ((ux+vy)(uy-vx)^{-1} \bmod n)$. The electronic cash is (s,m,c).

(3) Paying. To pay a payee the cash, the customer gives him (s,m,c). The payee verifies the correctness of the cash by examining if $s^4 \equiv_n m(c^2+1)$, and he immediately calls the bank to verify if the cash is fresh. An e-cash is fresh if and only if the cash has been deposited in the bank, i.e., the cash has been used. If yes, the payee accepts this payment, and the bank stores the cash in a database. In addition, the amount of money deposited of the payee in this bank increases w dollars.

3. Secure rewarding

In this section, we present our proposed secure rewarding scheme. The scheme consists of four roles, a reward provider, a verifier, reward claimants, and the bank. A reward provider publishes a problem and a deadline, and offers a reward (e-cash) to a reward claimant who can supply him a satisfactory solution of the problem before the deadline. A reward claimant is a person who supplies the provider a solution of the problem before the deadline. Since the privacy of the claimant has to be protected in the scheme and the provider cannot obtain the solution without paying the reward, another participant independent of the provider must take part in the rewarding scheme to verify the solution. Such participants are referred as the verifiers. A verifier has enough power to verify if a solution provided by a claimant is correct, and he does not reveal the solution to the provider before the provider pays the reward. There may be more than one qualified claimants in a rewarding system. For simplicity, the first qualified claimant will be selected to obtain the reward in our proposed scheme. However, in a practical implementation, the selected claimant can be chosen among the qualified claimants by an appropriate fair selection policy. The bank issues fixed-denomination e-cash which is of the form (s,m,c) produced by the electronic cash scheme in section 2.5. The details of our proposed rewarding scheme are described as follows.

(1) Publishing problem. A reward provider publishes a problem, a deadline, and the amount w of a reward. The provider will give w dollars to the selected claimant who is the first claimant to supply the provider a satisfactory solution of the problem before the deadline. For simplicity, w is equal to the denomination of an e-cash issued by the bank. However, the reward can also be composed of more than one e-cash.

(2) Claiming reward. A claimant knows a solution λ of the problem before the deadline. He chooses m, r and (u^2+v^2) in Z_n^* where n is the parameter of the electronic cash scheme described in section 2.5. Compute $d = (r^4m(u^2+v^2) \bmod n)$ and $\delta = F(\lambda)$ where F is a public one-way hashing function. An integer h is chosen at random by the claimant, and he randomly selects a signature function S_h. Through a secure sender untraceable e-mail, the claimant sends $E_{verifier}(h,\lambda,d,V_h)$ and (h,δ,d,V_h) to the provider where $E_{verifier}$ is the public encryption function of the verifier and V_h is the verification function corresponding to S_h.

After receiving the messages $E_{verifier}(h,\lambda,d,V_h)$ and (h,δ,d,V_h), the provider submits the verifier the message $S_{provider}(E_{verifier}(h,\lambda,d,V_h))$ where $S_{provider}$ is the signature function of the provider.

(3) Verifying solutions. After receiving the message $S_{provider}(E_{verifier}(h,\lambda,d,V_h))$, the verifier can decrypt the message to obtain (h,λ,d,V_h). There may be more than one claimants before the deadline. The verifier verifies that which of the solutions submitted by the claimants are satisfactory, and then selects the first one from them with satisfactory solutions as the selected claimant. Without loss of generality, let the claimant who submits $E_{verifier}(h,\lambda,d,V_h)$ and (h,δ,d,V_h) to the provider be the selected claimant. The verifier signs the message h by computing $S_{verifier}(h)$, and then sends the provider $S_{verifier}(h)$ where $S_{verifier}$ is the signature function of the verifier.

(4) Preparing reward. After receiving the message $S_{verifier}(h)$, the provider verifies if $S_{verifier}(h)$ is

signed by the verifier. If yes, he learns that the problem is solved, and the solution is kept secret by verifier. Thus, the provider submits d to the bank to withdraws an e-cash.

Let $S(a_1, a_2, ..., a_n)$ denote the signature of the message $(a_1, a_2, ..., a_n)$ under the signature function S. The bank randomly selects x and y such that $d(x^2 + y^2)$ is a QR in Z_n^*, and then sends $S_{bank}(d, x, y)$ to the provider where S_{bank} is the signature function of the bank. The provider publishes $S_{bank}(d, x, y)$.

The selected claimant submits $S_h(h, b^2(uy - vx) \bmod n)$ to both the provider and the verifier through secure sender untraceable e-mails where b is an integer randomly chosen by the claimant in Z_n^*. Then, the provider sends $(b^2(uy - vx) \bmod n)$ to the bank.

After receiving $(b^2(uy - vx) \bmod n)$, the bank computes,

$$d(x^2 + y^2)(b^2(uy - vx))^{-2}$$
$$\equiv_n r^4 m(u^2 + v^2)(x^2 + y^2)(b^2(uy - vx))^{-2}$$
$$\equiv_n r^4 b^{-4} m((ux + vy)^2(uy - vx)^{-2} + 1).$$

Since the bank knows the primes p_1 and p_2, the bank can derive an integer t in Z_n^* [16, 20] such that,

$$t^4 \equiv_n r^4 b^{-4} m((ux + vy)^2(uy - vx)^{-2} + 1).$$

The bank sends t to the provider, and then the provider publishes t.

(5) Obtaining solutions. The verifier examines if $t^4 \equiv_n d(x^2 + y^2)(b^2(uy - vx))^{-2}$. If true, the verifier sends the solution λ to the provider on a secret channel. The provider can verify λ by checking if $F(\lambda) = \delta$. In addition, the verifier sends the provider the other solutions λ's, which are submitted by all the other claimants, on secret channels, and, similarly, the provider can examine each of these λ's through the function F and its corresponding δ.

(6) Obtaining reward. The selected claimant computes $s = (r^{-1}bt \bmod n)$ and $c = ((ux+vy)(uy-vx)^{-1} \bmod n)$. Thus, he obtains the reward, the e-cash (s, m, c). To verify the cash (s, m, c), he can examine if $s^4 \equiv_n m(c^2 + 1)$.

The security of the proposed rewarding scheme is discussed as follows. We will show that the rewarding scheme is private, fair, eligible, complete, and robust.

Definition 1 *A rewarding scheme is private if and only if the identity of the selected claimant is not revealed.*

Theorem 1 *The scheme of section 3 is private.*

Proof.

The identity of the selected claimant does not appear in any transmitted message of the proposed scheme. Hence, the identity of the selected claimant cannot be revealed from any transmitted message. Considering the sending-message operations, the selected claimant performs all sending-message operations on sender untraceable channels, so the identity of the selected claimant cannot be revealed from the operations. Considering the receiving-message operations, the selected claimant does not perform any receiving-message operation, so the identity of the selected claimant cannot be revealed from any receiving operation.

Therefore, the identity of the selected claimant is not revealed in the scheme. The rewarding scheme of section 3 is private.

□

Definition 2 *A rewarding scheme is fair if and only if the provider cannot decline the selected claimant his entitled reward.*

Theorem 2 *The scheme of section 3 is fair.*

Proof.

In the step 2 of the proposed scheme, the selected claimant sends the provider the messages $E_{verifier}(h, \lambda, d, V_h)$ and (h, δ, d, V_h). The provider cannot get the solution λ since $E_{verifier}$ is the encryption function of the verifier and $\delta = F(\lambda)$, where F is a one-way hashing function.

The only way for the provider to obtain λ is to publish $S_{bank}(d, x, y)$ and t. After verifying that $t^4 \equiv_n d(x^2 + y^2)(b^2(uy - vx))^{-2}$, the verifier sends the solution λ to the provider. Finally, the selected claimant can obtain the reward, the e-cash (s, m, c), by computing $s = (r^{-1}bt \bmod n)$ and $c = ((ux + vy)(uy - vx)^{-1} \bmod n)$.

Therefore, the provider cannot get the solution λ without paying the reward. Since the provider cannot decline the selected claimant his entitled reward, the rewarding scheme of section 3 is fair.

□

Definition 3 *A rewarding scheme is eligible if and only if one cannot obtain the reward without being the selected claimant.*

Theorem 3 *The scheme of section 3 is eligible.*

Proof.

Let Alice be not the selected claimant. If Alice wants to get the reward, he has four possible ways:

(1) Steal the solution λ transmitted on the communication channels, and then impersonate the selected claimant to obtain the reward.

(2) Catch the reward from the published messages $S_{bank}(d, x, y)$ and t.

(3) Forge $S_{verifier}(h')$ to impersonate the verifier where h' is chosen by Alice.

(4) Forge electronic cash.

Considering the first way, λ is transmitted on secret channels in the scheme, so λ cannot be stolen from the channels. By the first way, Alice cannot get the reward. As r, u, and v are kept secret by the selected claimant, Alice cannot obtain the reward (s, m, c) from the published messages $S_{bank}(d, x, y)$ and t. Thus, the second way fails. It is computationally infeasible to forge $S_{verifier}(h')$ or any illegal electronic cash in the proposed scheme of section 3 since deriving square roots of an integer in Z_n^* is difficult [20]. The third and the fourth ways fail. Hence, one cannot obtain the reward without being the selected claimant. The rewarding scheme of section 3 is eligible.

□

Definition 4 *A rewarding scheme is complete if and only if the selected claimant can obtain the reward.*

Theorem 4 *The scheme of section 3 is complete.*

Proof.

Let $E_{verifier}(h, \lambda, d, V_h)$ and (h, δ, d, V_h) be the messages submitted by the selected claimant to the provider in the step 2 of the scheme. The sufficient conditions of that the selected claimant can obtain the reward are below:

(1) In the step 2 of the scheme, no intruder can steal λ from the secret channel to impersonate the selected claimant.

(2) In the step 3 of the scheme, no one can forge the signature $S_{verifier}(h)$ to impersonate the verifier.

(3) The provider cannot decline the selected claimant his entitled reward, i.e., the provider has to publish $S_{bank}(d, x, y)$ and t to obtain the solution λ.

(4) Only the selected claimant can compute $s = (r^{-1}bt \bmod n)$ and $c = ((ux + vy)(uy - vx)^{-1} \bmod n)$.

Considering condition 1, since the secret channel is secure, no intruder can steal λ from the channel. Condition 1 holds. Considering condition 2, since the signature $S_{verifier}(h)$ cannot be forged, no one can impersonate the verifier. Therefore, condition 2 meets. By theorem 2, the scheme is fair, so the provider cannot decline the selected claimant his entitled reward. Thus, condition 3 holds. Since r, u, and v are only known to the selected claimant, only he can compute $s = (r^{-1}bt \bmod n)$ and $c = ((ux+vy)(uy-vx)^{-1} \bmod n)$ to obtain the reward (s, m, c). Hence, condition 4 holds.

Since condition 1, condition 2, condition 3, and condition 4 hold, the selected claimant can obtain the reward. The rewarding scheme of section 3 is complete.

□

Definition 5 *A rewarding scheme is robust if and only if the verifier cannot select a claimant other than the first qualified claimant as the selected claimant without being detected.*

Theorem 5 *The scheme of section 3 is robust.*

Proof.

Since the provider receives a sequence of δ's from all the claimants in step 2 and the verifier has to send all the corresponding solutions λ's to the provider in step 5, the provider can examine if $F(\lambda) = \delta$ for every pair (λ, δ). Let the provider have the power to verify that which of the solutions λ's are satisfactory, and then the provider can derive that who is the first qualified claimant. If the verifier selects a claimant other than the first qualified claimant as the selected claimant in step 3, then it will be detected by the provider in step 5. So, the rewarding scheme of section 3 is robust.

4. Two-way untraceable rewarding

In the rewarding scheme of section 3, the identities of the claimants are kept secret, but the privacy of the reward providers is exposed. However, in some circumstance, the identities of the providers may also need to be protected. A rewarding scheme is said to be two-way untraceable if and only if both the identities of the claimants and the providers are not revealed. In this section, a secure rewarding scheme with two-way untraceability is proposed, which can protect the identities of the providers as well as the claimants. Since

the privacy of both the claimants and the provider has to be protected in the scheme, instead of a verifier, a trusted center is required to achieve the two-way untraceability property. The trusted center is honest, and it has enough power to verify if a solution provided by a claimant is correct, such as the government, the judge, or credit bureaus. The proposed scheme is described below.

(1) Publishing problem. Through a secure sender untraceable e-mail, the provider sends a problem, a deadline, the amount w of a reward, and a public-key encryption function $E_{provider}$ randomly chosen by him to the trusted center. Then, the trusted center publishes the problem, the deadline, and w.

(2) Claiming reward. A claimant knows a solution λ of the problem before the deadline. He chooses m, r and (u^2+v^2) in Z_n^* where n is the parameter of the electronic cash scheme shown in section 2.5. Compute $d = (r^4 m(u^2+v^2) \bmod n)$. By a secure sender untraceable e-mail, the claimant sends (h, λ, d) to the trusted center where h is an integer randomly selected by the claimant.

(3) Verifying solutions. There may be more than one claimants who send the trusted center their solutions before the deadline. The trusted center verifies that which of these solutions are satisfactory, and then selects the first one from the claimants with satisfactory solutions as the selected claimant. Without loss of generality, let the claimant who submits (h, λ, d) to the trusted center be the selected claimant. The trusted center publishes $E_{provider}(S_{center}(z))$ where S_{center} is the signature function of the trusted center and z is a message indicating that the problem is solved.

(4) Preparing reward. The provider decrypts the message $E_{provider}(S_{center}(z))$, and verifies if $S_{center}(z)$ is signed by the trusted center. If true, he learns that the problem is solved and the solution is kept secret by the trusted center. Thus, the provider withdraws an e-cash β, which is produced by performing the protocol shown in section 2.5, from the bank. Send β to the trusted center by a secure sender untraceable e-mail.

After receiving β, the trusted center submits β and d to the bank on a secret channel. The bank verifies if β is correct and fresh. If yes, the bank randomly selects x and y such that $d(x^2+y^2)$ is a QR in Z_n^*, and then sends x and y to the trusted center. The trusted center publishes d, x, and y.

The selected claimant sends $(h, b^2(uy - vx) \bmod n)$ to the trusted center by a secure sender untraceable e-mail where b is an integer randomly chosen by the claimant in Z_n^*. The trusted center forwards the message $(b^2(uy - vx) \bmod n)$ to bank.

After receiving $(b^2(uy - vx) \bmod n)$, the bank computes,

$$d(x^2+y^2)(b^2(uy-vx))^{-2}$$
$$\equiv_n r^4 m(u^2+v^2)(x^2+y^2)(b^2(uy-vx))^{-2}$$
$$\equiv_n r^4 b^{-4} m((ux+vy)^2(uy-vx)^{-2}+1).$$

The bank derives an integer t in Z_n^* such that,

$$t^4 \equiv_n r^4 b^{-4} m((ux+vy)^2(uy-vx)^{-2}+1).$$

The bank sends t to the trusted center, and then the trusted center publishes t.

(5) Obtaining solution. The trusted center gives the provider the solution λ of the problem by publishing $E_{provider}(S_{center}(\lambda))$ and $E_{provider}(\lambda)$. Thus, the provider can obtain the solution λ since he knows how to decrypt the ciphertext messages $E_{provider}(S_{center}(\lambda))$ and $E_{provider}(\lambda)$.

(6) Obtaining reward. The selected claimant computes $s = (r^{-1} bt \bmod n)$ and $c = ((ux+vy)(uy-vx)^{-1} \bmod n)$. Hence, he can obtain the reward, the e-cash (s, m, c). To verify the cash (s, m, c), he can examine if $s^4 \equiv_n m(c^2+1)$.

The security of the proposed rewarding scheme is examined below. We will show that the rewarding scheme is two-way untraceable, fair, eligible, and complete.

Theorem 6 *The scheme of section 4 is two-way untraceable.*

Proof.

By theorem 1, the rewarding scheme of section 4 is private, i.e., the identities of the claimants are not revealed.

On the other hand, the identity of a provider does not appear in any transmitted message of the scheme. Hence, the identity of the provider cannot be revealed from any transmitted message. In step 4 of the scheme, the provider withdraws the e-cash β from the bank. By the unlinkability property of the blind signature scheme shown in section 2.4, the privacy of the

provider is protected against the bank.. Considering the sending-message operations, all of the messages transmitted by the provider are through the sender untraceable e-mails, so the identity of the provider cannot be revealed from any sending-message operation. Considering the receiving-message operations, the provider does not perform any receiving-message operation, so it is impossible to reveal the identity of the provider from any receiving-message operation.

From the above, the identity of the provider is not revealed in the rewarding scheme. Hence, the rewarding scheme of section 4 is two-way untraceable.

□

Theorem 7 *The scheme of section 4 is fair.*

Proof.

In the step 2 of the proposed scheme, the selected claimant sends the trusted center the message (h, λ, d) on a secret channel, so the provider cannot catch the solution λ from that transmission.

The only way for the provider to obtain λ is to send the e-cash β to the trusted center. After verifying that β is correct and fresh, the trusted center publishes x, y, and t, and sends the solution λ to the provider. Hence, the selected claimant can obtain the reward, the e-cash (s, m, c), by computing $s = (r^{-1}bt \bmod n)$ and $c = ((ux + vy)(uy - vx)^{-1} \bmod n)$.

The provider cannot obtain the solution λ without paying the reward. Hence, the provider cannot decline the selected claimant his entitled reward. The rewarding scheme of section 4 is fair.

□

Theorem 8 *The scheme of section 4 is eligible.*

Proof.

Let Alice be not the selected claimant. If Alice wants to get the reward, he has four possible ways:

(1) Steal the solution λ transmitted on the communication channels, and then impersonate the selected claimant to obtain the reward.

(2) Steal the e-cash β transmitted on the communication channels

(3) Catch the reward from the published messages x, y, and t.

(4) Forge electronic cash.

Considering the first way and the second way, λ and β are transmitted on secret channels in the scheme, so they cannot be stolen from the communication channels. Since r, u, and v are kept secret by the selected claimant, Alice cannot obtain the reward (s, m, c) from the published messages x, y, and t. In addition, it is computationally infeasible to forge any illegal e-cash in the proposed scheme since deriving square roots of an integer in Z_n^* is difficult [20]. Hence, one cannot obtain the reward without being the selected claimant. The rewarding scheme of section 4 is eligible.

□

Theorem 9 *The scheme of section 4 is complete.*

Proof.

Let (h, λ, d) be the message sent by the selected claimant to the trusted center in the step 2 of the scheme. The sufficient conditions of that the selected claimant can obtain the reward are below:

(1) In the step 2 of the scheme, no intruder can steal λ from the secret channel, on which (h, λ, d) is transmitted, to impersonate the selected claimant.

(2) In the step 3 of the scheme, no one can forge the signature $S_{center}(z)$ to impersonate the trusted center.

(3) The provider cannot decline the selected claimant his entitled reward, i.e., the provider has to send the trusted center the e-cash β to obtain the solution λ.

(4) No intruder can steal the e-cash β transmitted on the secret channels.

(5) Only the selected claimant can compute $s = (r^{-1}bt \bmod n)$ and $c = ((ux + vy)(uy - vx)^{-1} \bmod n)$.

Considering condition 1 and condition 4, since the secret channels are secure, no intruder can steal λ or β from the channels. Condition 1 and condition 4 holds. Considering condition 2, since the signature $S_{center}(z)$ cannot be forged, no one can impersonate the trusted center. Therefore, condition 2 meets. By theorem 7, the scheme is fair, so the provider cannot decline the selected claimant his entitled reward. Thus, condition 3 holds. Since r, u and v are only known to the selected claimant, only he can compute $s = (r^{-1}bt \bmod n)$ and $c = ((ux + vy)(uy - vx)^{-1} \bmod n)$ to obtain the reward (s, m, c). Hence, condition 5 holds.

Since condition 1, condition 2, condition 3, condition 4, and condition 5 hold, the selected claimant can obtain the reward. The rewarding scheme of section 4 is complete.

□

5. Conclusion

In this paper, we have proposed a claimant untraceable rewarding scheme. The scheme realizes that the selected claimant can successfully submit his solution to the reward provider, and obtain the reward without revealing his own identity. Besides, we have shown that our proposed scheme is private, fair, eligible, complete, and robust. Furthermore, a two-way untraceable rewarding scheme is proposed. The scheme can protect the identities of the reward providers as well as the reward claimants.

Acknowledgment

We would like to thank the unknown referees of this paper for their valuable comments.

References

[1] C.A. Boyd, "A new multiple key ciphers and an improved voting scheme," *Advances in Cryptology-EUROCRYPT'89*, LNCS 434, Springer-Verlag, 1990, pp. 617-625.

[2] J.C. Benaloh and D. Tuinstra, "Receipt-free secret-ballot elections," *Proc. 26th ACM Symp. on the Theory of Computing*, 1994, pp. 544-553.

[3] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, 1981, pp. 84-88.

[4] D. Chaum, "The dining cryptographers problem: unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, 1988, pp. 65-75.

[5] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash," *Advances in Cryptology-CRYPTO'88*, LNCS 403, Springer-Verlag, 1990, pp. 319-327.

[6] J.D. Cohen and M.J. Fisher, "A robust and verifiable cryptographically secure election scheme," *Proc. 26th IEEE Symp. on Foundations of Computer Science*, 1985, pp. 372-382.

[7] C.I. Fan and C.L. Lei, "Efficient blind signature scheme based on quadratic residues," *Electronics Letters*, vol. 32, no. 9, 1996, pp. 811-813.

[8] C.I. Fan and C.L. Lei, "Low-computation blind signature schemes based on quadratic residues," *Electronics Letters*, vol. 32, no. 17, 1996, pp. 1569-1570.

[9] C.I. Fan and C.L. Lei, "A multi-recastable ticket scheme for electronic elections," to appear in *Advances in Cryptology-AISACRYPT'96*, Springer-Verlag, 1996.

[10] A. Fujioka, T. Okamoto, and K.Ohta, "A practical secret voting scheme for large scale elections," *Advances in Cryptology-AUSCRYPT'92*, LNCS 718, Springer-Verlag, 1992, pp. 244-251.

[11] K.R. Iversen, "A cryptographic scheme for computerized general elections," *Advances in Cryptology-CRYPTO'91*, LNCS 576, Springer-Verlag, 1991, pp. 405-419.

[12] W.S. Juang, C.L. Lei, and C.I. Fan, "A collision free secret ballot protocol for computerized general elections," *International Computer Symposium*, Taiwan, R.O.C., 1994. (A revised version will appear in *Computers & Security.*)

[13] W.J. LeVeque, *Fundamentals of Number Theory*, Addison-Wesley, Reading, Mass., 1977.

[14] H. Nurmi, A. Salomaa, and L. Santean, "Secret ballot elections in computer networks," *Computers & Security*, vol. 10, 1991, pp. 553-560.

[15] T. Okamoto and K. Ohta, "Universal electronic cash," *Advances in Cryptology-CRYPTO'91*, Springer-Verlag, 1992, pp. 324-337.

[16] R.C. Peralta, "A simple and fast probabilistic algorithm for computing square roots modulo a prime number," *IEEE Trans. Inform. Theory*, vol. 32, no. 6, 1986, pp. 846-847.

[17] S. Pohlig and M.E. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance," *IEEE Trans. on Inform. Theory*, vol. 24, 1978, pp. 106-110.

[18] C. Park, K. Itoh, and K. Kurosawa, "All/nothing election scheme and anonymous channel," *Advances in Cryptology-EUROCRYPT'93*, LNCS 765, Springer-Verlag, 1993, pp. 248-259.

[19] J.M. Pollard and C.P. Schnorr, "An efficient solution of the congruence $x^2 + ky^2 = m \pmod{n}$," *IEEE Trans. Inform. Theory*, vol. 33, no. 5, 1987, pp. 702-709.

[20] M.O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," *Technical Report*, MIT/LCS/TR212, MIT Lab., Computer Science, Cambridge, Mass. Jan. 1979.

[21] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, 1978, pp. 120-126.

[22] K. Sako and J. Kilian, "Secure voting using partially compatible homomorphisms," *Advances in Cryptology-CRYPTO'94*, LNCS 839, Springer-Verlag, 1994, pp. 411-424.

[23] P.H. Slessenger, "Socially secure cryptographic election scheme," *Electronics Letters*, vol. 27, no. 11, 1991, pp. 955-957.

[24] I.M. Vinogradov, *An Introduction to the Theory of Numbers*, Pergamon Press, Elmsford, N.Y., 1955.