Provably Secure Partially Blind Signature Scheme Based on Quadratic Residue

Yi Zhao[1], Qiliang Yang[2], and Bo Yang[1]
(Corresponding author: Yi Zhao)

[1]School of Computer Science, Shaanxi Normal University
Xi'an 710062, China
[2]College of Informatics, Shu-Te University
Kaohsiung City 82445, Taiwan
(Email: yizhaore@gmail.com)

(Received Dec. 11, 2013; revised and accepted Nov. 6, 2014)

Abstract

Partially blind signature schemes are the most important ingredient for anonymity in off-line e-cash system. In this paper, a new approach to setup formal security arguments in random oracle model for factorization based partially blind signature schemes is presented. Then a provably secure and efficient scheme based on quadratic residue is proposed. The approach also allows one to give formal proofs in the random oracle model for all the factorization based fully blind signature schemes. Our scheme takes an outstanding performance in computational costs compared to the existing schemes.

Keywords: Partially blind signature, Provable security, Quadratic residue, Random oracle model

1 Introduction

1.1 Background

In an e-cash system, customers are always not willing to reveal their privacies like transaction records to others while trading on line. To offer protection for privacy by the blindness property, Chaum first introduced the technique called "blind signature" in 1983 [4]. Though blind signature was sufficient to solve the problem of privacy protection, two other new matters appeared next. The first is that the bank has to keep an unlimited database which stores all the transaction records in history to check the occurrence of double-spending issues. Apparently the cost of storage space and searching goes higher at fast speed as the period of blind signature scheme used is getting longer. The second is that the signer can not assure that the message to sign includes the right information without seeing it. The signature may be used for illegal purposes.

The above two shortcomings can be eliminated by partially blind signatures which is introduced by Abe and Fujisaki in 1996 [1]. By injecting some agreed common information such as the expiration date and the face value to the signature which can't be replaced by users, the scheme gets the property of partial blindness. So the bank can delete all the expired records to keep a constant size of the database. And also the bank will confirm that the message to sign contains the information it really concerns. Without loss of privacy of other information, the user just needs to renew the e-cash when the old one is close to expire.

The first partially blind signature scheme based on RSA was proposed by Abe and Fujisaki along with the concept which is vulnerable to one-more-forgery attack. It was realized that a signature scheme should be enhanced by adding random factors to get the randomization property which was suggested by Ferguson [7]. Until now, numerous security enhanced partial blind signature schemes have been proposed. Abe and Okamoto proposed a provably secure partially blind signature based on Schnorr signature scheme [2] and then Okamoto also presented a scheme under standard model based on bilinear groups [14]. The computational costs of both schemes above are so high to be in application. Wu et al. gave an improved Abe scheme and a inverse Schnorr based scheme with higher efficiency [19]. There are also some discrete logarithm based schemes which is not of Schnorr type like [9, 11, 12]. Tianjie Cao et al. proposed a partial blind signature scheme based on RSA [3], which turned out to be insecure [8, 13]. Some other RSA based schemes were proposed by Tahat et al. [16] and Fang et al. [6]. Fan et al. proposed a scheme based on quadratic residue and emphasized on reducing the cost in verification [5]. It is notable that these factorization related schemes [3, 5, 6, 16] didn't give a formal proof. We can see that some successful attacks on blind signatures like [8, 13, 17] are due to the unproved constructions. A formal proof which rigorously claims the security under certain condition is necessary. Besides these standard assumption based schemes, other interesting schemes like [18] which is based on Braid groups were also presented.

1.2 Our Contribution

As Pointcheval said [15], general methods of proofs used to establish security arguments for signature schemes no longer work in the blind context since we lose control over the value that the signer receives. The value doesn't only come from the random oracle but also the attacker(blinding factor). As a consequence, the signer can't be simulated without the secret key as usual. Thus, the ability of the attacker to make a forgery is hard to be related to a difficult problem. To overcome this problem, the existing DDH-based schemes like [1, 2, 15] use the concept of witness indistinguishable proofs which requires that many secret keys are associated to the same public key and the knowledge of two distinct secret keys provides the solution of a difficult problem. So the simulation can be constructed with the key pair generated by simulator, but the forgery output by the attacker may be associated to one secret key indistinguishable to the one simulator uses. The fact that one forgery can be implemented by two distinct secret keys provides the solution to a difficult problem. This approach is useful for the DDH-based schemes but the factorization based schemes don't satisfy the requirement of nontrivial witness indistinguishability since the public key modulus is one-to-one corresponded to the secret key factorization. The second scheme proposed in [19] didn't use witness indistinguishable proofs by employing key evolution to construct multiple public key environment to simulate the signer. We try to apply this thought to give proofs for the factorization based schemes.

Our approach uses a simple fact which we prove later that if computing factorization of one of a polynomial bounded number of moduli randomly generated is feasible with non-negligible probability, then computing factorization of one modulus randomly generated is also feasible with non-negligible probability. We setup security definition of unforgeability on the former problem. This is a kind of computational indistinguishability obtained by randomness. Our security definition is more close to the real applications of the schemes where several public keys are used on line in the same time.

In this paper, we design a partial blind signature scheme based on quadratic residue with low computational cost. We first introduce the basic theory and definitions, then we describe our scheme and give a formal proof under random oracle model. Also, we make a comparison of the computational cost between our scheme with existing ones. Our scheme is quite applicable in e-cash system especially for resource-limited user device like smart card.

2 Preliminaries

2.1 Legendre Symbol and Jacobi Symbol

Let p be a prime, Q_p denote the set of quadratic residues modulo n, $\overline{Q_p}$ the set of quadratic non-residues. For any $a \in Z_p^*$, the Legendre symbol of a is denoted by

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & p|a. \\ 1, & a \in Q_p. \\ -1, & a \in \overline{Q_p}. \end{cases}$$

Let $Z_n^* = \{k \in Z_n, \gcd(k,n) = 1\}$ denote the multiplicative group with $n = pq$, where p and q are two large primes of the same size. the Jacobi symbol of $a \in Z_n^*$ is denoted by

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$$

The Jacobi symbol can be efficiently computed without the factorization of n.

2.2 Blum Integers

An integer $n = pq$ is called Blum integer if $p \equiv 3 \bmod 4$ and $q \equiv 3 \bmod 4$. When n is a Blum integer, the function $f(x) = x^2 \bmod n$ is a permutation over Q_n. If n is a Blum integer, $\left(\frac{-1}{n}\right) = 1$. That means the Jacobi symbols of any x and $-x$ are the same, which makes it hard to distinguish x and $-x$ by computing Jacobi symbols.

2.3 Quadratic Residues Modulo a Composite

An element $x \in Z_n^*$ is a quadratic residue if there exists a $y \in Z_n^*$ with $y^2 \equiv x \bmod n$, otherwise is called quadratic non-residue. Let Q_n denote the set of quadratic residues modulo n, $\overline{Q_n}$ the set of quadratic non-residues and $\overline{Q_n}^+$ the set of quadratic non-residues whose Jacobi symbol is $+1$. There are four square roots for each quadratic residue and only one of them is also a quadratic residue when the modulus is a Blum integer.

2.4 Related Complexity Assumptions and Results

Claim 1. *(decisional quadratic residue assumption). Without the factorization of n, deciding quadratic residuosity of any $x \in \overline{Q_n}^+$ is computationally infeasible to succeed with probability more than 1/2 for all probabilistic polynomial time algorithms [10].*

Definition 1. *(computational quadratic residue problem, denoted CQR). Without the factorization of n, compute square roots of x mod n where x is randomly chosen in Q_n and $\gcd(x,n) = 1$.*

Claim 2. *If factoring is computationally infeasible, then solving CQR is also computationally infeasible [10].*

Definition 2. *(multiple computational quadratic residue assumption, denoted MCQR). For a set S of moduli $n_1, \cdots, n_N$ randomly generated, where N is polynomial bounded, the factorization of n_i for any i is unknown, and $(x, n_i) = 1$, compute square roots of x modulo n_i for any one i.*

Claim 3. *If solving CQR is computationally infeasible, then solving MCQR is also computationally infeasible, and vice versa.*

Proof. It is trivial that if one can solve CQR, then one can solve MCQR by picking any n_i as modulo. Let's focus on the other direction.

If there exists a machine M that can solve MCQR with probability ϵ in polynomial time t in a uniform way (which means the probability of the modulo of the solution is uniformly distributed over S), then we can construct M' which uses M as a subroutine to solve CQR. Let n^* and x be the parameters in CQR. M' randomly generates $n_1, \cdots, n_{N-1}$ and obtains a set of N moduli by adding n^*. Then M' invokes M by giving it the set and x as inputs. The output of M is a tuple $(x^{1/2}, x, n_i)$. Since M works in a uniform way, the probability that M outputs $(x^{1/2}, x, n^*)$ is at least ϵ/N. In this case, $x^{1/2}$ is the solution of the CQR problem we want to solve. □

2.5 Using Chinese Remainder Theorem to Compute Square Roots [10]

Theorem 1. *(Chinese remainder theorem). Let $n = pq$ where p and q are relatively prime. Then $Z_n \cong Z_p \times Z_q$ and $Z_n^* \cong Z_p^* \times Z_q^*$. Moreover, let f be the function mapping elements $x \in \{0, 1, \cdots, N-1\}$ to pairs (x_p, x_q) with $x_p \in \{0, 1, \cdots, p-1\}$ and $x_q \in \{0, 1, \cdots, q-1\}$ defined by*

$$f(x) \overset{def}{=\!=} ([x \bmod p], [x \bmod q])$$

Then f is an isomorphism from Z_n to $Z_p \times Z_q$ as well as an isomorphism from Z_n^* to $Z_p^* \times Z_q^*$.

To compute a square root of x modulo a Blum integer $n = pq$ of known factorization, we use Chinese remainder theorem to find the presentation of x in $Z_p^* \times Z_q^*$, then compute the square roots in the same presentation and convert the result back to the presentation in Z_n^*. Namely, do as follows.

1) Compute $x_p = x \bmod p$ and $x_q = x \bmod q$.

2) Compute a square root $y_p = x_p^{(p+1)/4}$ of x_p and a square root $y_q = x_q^{(p+1)/4}$ of x_q, by the fact that one square root of any z modulo a prime $p' = 3 \bmod 4$ is $z^{(p'+1)/4}$.

3) Using Chinese Remainder Theorem to convert from the presentation $(y_p, y_q) \in Z_p^* \times Z_q^*$ to $y \in Z_n^*$. Output y.

3 Definitions

In a partially blind signature scheme, the signer and the user are assumed to agree on a piece of common information outside the signature issuing procedure, denoted as c. And a randomizing factor should be negotiated during the procedure for the randomization property. We formalize this notion by introducing function $R()$ which is defined outside the scheme. Function $R()$ is a polynomial-time deterministic algorithm that takes two arbitrary strings x and y that belong to the signer and the user respectively, and outputs u as the randomization factor. To compute $R()$, the signer and the user will exchange x and y with each other. Some parts of the following definitions refer to [2].

Definition 3. *(Partially blind signature scheme). A partially blind signature scheme is a four tuple $(\mathcal{G}, S, U, V)$.*

- *$\mathcal{G}$ is a probabilistic polynomial-time algorithm that takes security parameter n and outputs a public and secret key pair (pk, sk).*

- *S and U are two parties who follow the interactive signature issuing protocol. U takes message m , pk, the description of $R()$, and the common information c as initial inputs. S takes sk, the description of $R()$ and c as initial inputs. Then S and U engage in the signature issuing protocol and stop in polynomial-time. When they stop, S outputs either completed or not completed. If it is completed, U outputs a signature (m, s, u, c) or $\perp$ in private.*

- *V is a probabilistic polynomial-time algorithm that takes (pk, m, s, u, c) and outputs either accept or reject.*

Definition 4. *(Completeness). If the signer and the user follow the signature issuing protocol, then with probability at least $1 - \epsilon$ for negligible ϵ, S outputs completed and the user outputs (pk, m, s, u, c) that satisfies $V(pk, m, s, u, c) = accept$.*

To define the partial blindness property, let us introduce the following game.

Game A. Let U_0 and U_1 are two honest users who follow the signature issuing protocol with the same common information c.

1) The signer S does the key generation and publishes pk.

2) U_0 and U_1 engage the protocol with S respectively and get the message-signature tuple $(m_0, \pm s_0, u_0, c)$ and $(m_1, \pm s_1, u_1, c)$.

3) A random bit $b \in \{0, 1\}$ is selected and U_b sends $(m_b, \pm s_b, u_b, c)$ to S.

4) S outputs $b' \in \{0, 1\}$.

We say that S wins if $b' = b$. We define the advantage as $adv = |Pr[b' = b] - 1/2|$.

Definition 5. *(Partial Blindness). A signature scheme is partially blind if for any probabilistic polynomial-time algorithm S, S wins in Game A with negligible advantage. The probability is taken over the coin flips of S, U_0 and U_1.*

The unforgeability property is defined through the following game.

Game B. Let U^* be the user who tries to forge a signature after issuing the protocol with the signer S.

1) The signer S generates a number of pairs of keys $(n_i, (p_i, q_i))$ and publishes the public keys $n_i (i \in [1, N])$.

2) U^* randomly and independently chooses public keys and engages in the signature issuing protocol in a concurrent way. Let l be the total number of executions of the protocol and $c_{i,j}$ be the common information used corresponding to the j-th execution of the public key N_i.

3) U^* outputs $l+1$ public key-message-signature tuples $(n_i, m_{i,j}, \pm s_{i,j}, u_{i,j}, c_{i,j})$.

Definition 6. *(Unforgeability). A partially blind signature scheme is unforgeable if for any probabilistic polynomial-time algorithm U^* that plays Game B, the probability that all the $l+1$ signatures which U^* outputs after l interactions with S are valid is negligible. The probability is taken over the coin flips of S and U^*.*

4 The Proposed Partially Blinded Signature Scheme

Z_n^* is defined as that of Definition 2.3. Let c be the common information with constant length r containing the message like an expiration date and the e-cash value which is negotiated by the user and the signer. We assume that the messages to be signed can be expressed by the elements in Z_n^*. H is a public hash function: $H : \{0,1\}^r \times \mathbb{N} \rightarrow Q_{\mathbb{N}}$ and H_0 is a public hash function: $H_0 : \{0,1\}^* \times \mathbb{N} \rightarrow Q_{\mathbb{N}}$. (The input of the parameter $\mathbb{N}$ is n to ensure that the hash value is in the valid range when multiple public keys are in use at the same time. We directly use $H(r)$ instead of $H(r, n)$ for short if there is no confusion.)

Key Generation. The signer randomly selects two large primes p and q, computes $n = pq$ and publishes n as the public key. Here the secret key is (p, q).

Blinding. A user submits the common information c to the signer. After checking the validity of the common information, the signer randomly selects a randomizing factor $x \in Q_n$ and sends x^4 to the user as the commitment(signer can choose a random $x^{1/2} \in Z_n^*$ to generate x and compute x^4, and save $x^{1/2}$ to decommit later).

The user randomly selects his randomizing factor $y \in Q_n$ and blinding factor $k \in Q_n$. With the received commitment x^4 and the message m, the user computes the blinded message

$$\hat{m} = k^2 y^2 H_0(m \parallel x^4 y^4 \parallel c)$$

and sends it to the signer.

Signing. After receiving $\hat{m}$, The signer injects his randomizing factor and the common information into the blinded message, computes

$$\hat{m}' = x^2 \hat{m} H^{1/2}(c).$$

Let h_0 and h_1 denote the output by $H_0(m \parallel x^4 y^4 \parallel c)$ and $H(c)$ respectively. Then the signer calculates the square roots of $\hat{m}'$ by Chinese remainder theorem. We pick the square root which is also a quadratic residue of $\hat{m}'$ as the blinded signature. So the blinded signature $\hat{s}$ is $kxyh_0^{1/2}h_1^{1/4}$. Then the signer sends $\hat{s}$ and $(x, x^{1/2})$ to the user.

Unblinding. The user confirms that x is a quadratic residue, then computes $s = k^{-1}\hat{s}$ to remove the blinding factor, and computes $u = xy$ as the randomizing factor in the output. The tuple $(\pm s, u, c)$ is the signer's signature on the message m. (We denote $(s, -s)$ as $\pm s$ for short and treat $(s, -s)$ and $(-s, s)$ as the same signature).

Verifying. $V(pk, m, \pm s, u, c) = accept$ if

$$s^4 = u^4 H_0(m \parallel u^4 \parallel c)^2 H(c).$$

5 Security Analysis

5.1 Completeness

The completeness of our scheme can be easily conformed as follows.

$$\begin{aligned} s^4 &= (xyh_0^{1/2}h_1^{1/4})^4 \\ &= (xy)^4 h_0^2 h_1 \\ &= u^4 H_0(m \parallel x^4 y^4 \parallel c)^2 H(c). \end{aligned}$$

We can see that with probability 1, the signature output by issuing protocol legally satisfies the equation. That is perfect completeness.

5.2 Partial Blindness

Theorem 2. *Our proposed scheme is partially blind.*

Proof. Let S be a player of Game A. Let x_i, $\hat{m}_i$, $\hat{s}_i$ be the data recorded in the view of S during the execution of the protocol for $i = 0, 1$.

S receives $(m_b, \pm s_b, u_b, c)$ and tries to match it to the views. It is sufficient to show that for either view, there always exists a tuple of corresponding random factors

(y_i, k_i) to match the verification equation. We see that $y_i = x_i^{-1} u_b$, $k_i^2 = y_i^{-2} H_0(m_b \parallel u_b^2 \parallel c)^{-1}$, S can obtain k_i by the Chinese remainder theorem. Thus (y_i, k_i), $(x_i, \hat{m}_i, \hat{s}_i)$, and (m_b, s_b, u_b, c) have exactly the same relation as the scheme defined. And such (y_i, k_i) always exists regardless of what the value of $(m_b, \pm s_b, u_b, c)$. That implies that the signature $(m_b, \pm s_b, u_b, c)$ is independent from the blinded signature. So, even an infinitely powerful S wins Game A with probability exactly 1/2. Then the blindness property follows. □

5.3 Unforgeability

Theorem 3. *Our proposed scheme is unforgeable if $l < N\log p(n)$ for sufficiently large n. In other words, let q be the maximum number of queries to H in the simulation, if there exists a forger who can make a forgery in l executions with probability ϵ, then we can solve CQR with probability $\epsilon/(qp(n))$.*

Proof. Let U^* be the forger who plays Game B and produces a valid public key-message-signature tuple $(n_i, m^*, \pm s^*, u^*, c^*)$ that never appeared in the l executions of the protocol with probability ϵ which is not negligible. By using U^*, we construct a machine M to solve the problem of finding square roots in a passive environment. Notice that every n_i is generated randomly so that they are all identically distributed. As a result, the probability that every n_i appears in the output forgery is the same.

Notice that H_0 is only queried by users and blind to the signer. So we can't treat it as a random oracle when we use M to simulate S. The value of H_0 is just treated like a random factor which multiples another random factor k in the message $\hat{m}$ in the signer's view. Let q be the maximum number of queries asked from U^* to H. All the parameters are limited by a polynomial in a security parameter k_s. Let (n^*, x) be the instance that we want to find a square root of x in $Z_{n^*}^*$ without the factorization of n^*. M simulates Game B as follows.

1) Generate N pairs of large primes (p_i, q_i) and randomly select $I \in \{1, \cdots, N\}$. Let
$$n_i = \begin{cases} p_i q_i, & i \neq I. \\ n^*, & i = I. \end{cases}$$

2) Run U^* with those keys and simulate H and S as follows.

   For the query $c_{i,j}$ to H, return z such that

   - If $i = I$, choose $j \in_R Q_{n_i}$, return $z = j^4 x$ and record $(c_{i,j}, j)$.
   - If $i \neq I$, choose $j \in_R Q_{n_i}$, return $z = j^4$.

   For the requests to S,

   - If U^* requests signatures under modulo n_i that $i = I$, the simulation fails and aborts.
   - If U^* requests signatures under modulo n_i that $i \neq I$, return $\hat{s}$ by using Chinese remainder theorem because the factorizations of these n_i where $i \neq I$ are known (they are generated by M). So that M simulates S completely under this condition.

3) If U^* eventually forges a signature (n_i, m^*, $\pm$ s^*, u^*, c^*), output them.

Then we evaluate the probability that the simulation doesn't abort.

Claim 4. *If $l < N\log p(n)$, the probability that the simulation doesn't abort is at least $1/p(n)$.*

Proof. We assume that U^* chooses n_i in a uniformly random way. Such that the probability that the simulation doesn't abort is

$$\begin{aligned} (1-1/N)^l &= (1-1/N)^{N*l/N} \\ &> (1/e)^{l/N} \\ &> (1/e)^{\log p(n)} \\ &> 1/p(n). \end{aligned}$$

□

The probability that U^* makes a forgery successfully without asking H is negligible because of the unpredictability of the hash function. Thus, the success probability of M that doesn't abort to get a forgery on n_I is at least ϵ/q which is not negligible. According to Claim 4, we know that the probability that M make a forgery is $\epsilon/(qp(n))$.

Now we use M to solve the problem (n^*, x). When M obtains a forgery $(n_I, m^*, \pm s^*, u^*, c^*)$, it checks the records $(c_{i,j}, j)$ to find out the $c_{i,j} = c^*$. Then it establishes an equation

$$(s^*)^2 = (u^*)^2 H_0(m^* \parallel (u^*)^4 \parallel c^*) H(c^*)^{1/2}$$

where all the values except $H(c^*)^{1/2}$ are known. We denote the value of $H(c^*)^{1/2}$ by y which can be computed from the equation. M answered the query $c_{i,j}$ by $H(c_{i,j}) = j^4 x$ in the simulation. So

$$y = H(c^*)^{1/2} = j^2 x^{1/2}, x^{1/2} = yj^{-2}$$

Thus M finds a square root of x without the factorization of n_I. That contradicts the fact that the problem can't be computed efficiently.

□

6 Performance

We make a computational performance comparison between our scheme and several former schemes in Table 1 as follow. Using Chinese remainder theorem to compute roots costs about 1/4 of the time that one exponentiation

Table 1: Computation costs

Scheme	Exponentiation	Inverse	Hashing	Multiplication
Fan [5]	3/4	1	4	34
Wu [19]	7	1	5	5
Cao [3]	8	1	4	7
Fang [6]	5	2	4	27
Zhao	2/4	1	4	20

modulo costs [10]. For the reason that we focus on reducing the costs for user in verification, we don't consider the costs of pairing based schemes. Our scheme takes 9 multiplications and 1 hashing in the blinding step, 2 multiplications and 2 square root computations in the signing step, 1 inverse and 2 multiplications in the unblinding step, and 7 multiplications and 2 hashing in verification. We could see that the quadratic residue based schemes have the least number of modular exponentiations and further more, no modular exponentiations in verification which is applicable in the resource limited environment.

7 Conclusions

We have presented an efficient partially blind signature scheme based on the assumption that finding square roots modulo a composite is intractable. We then gave a formal proof of security including blindness and unforgeability in the random oracle model. Also our approach is easily transformed to give formal proofs for other factorization based schemes.

Notice that unlike some other schemes based on quadratic residue [20], the signature space of our scheme is limited in the quadratic residues of the group. It's easy to expand the signature space by adding a "label" in the signature like other schemes, but the blindness property will be weakened by those "label"s. So we still constructed the scheme based on permutations rather than 4-to-1 mappings.

Acknowledgments

This work is supported by the National Nature Science Foundation of China under grants 61272436 and 61363080, the Chunhui Project of Ministry of Education under Grant Z2012094 and the Item of Information Security Innovation Team of Central Finance.

References

[1] M. Abe and E. Fujisaki, "How to date blind signatures," in *Asiacrypt'96*, vol. 1, no. LNCS 1163, pp. 244–251, 1996.

[2] M. Abe and T. Okamoto, "Provably secure partially blind signatures," in *Crypto'00*, vol. 1, no. LNCS 1880, pp. 271–286, 2000.

[3] T. J. Cao, L. D. Dai, and R. Xue, "A randomized rsa-based partially blind signature scheme for electronic cash," *Computer & Security*, vol. 24, no. 1, pp. 44–49, 2005.

[4] D. Chaum, "Blind signatures for untraceable payments," *Advances in cryptology (CRYPTO'82)*, vol. 1, no. 1, pp. 199–203, 1983.

[5] C. I. Fan and C. L. Lei, "Low-computation partially blind signatures for electronic cash," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E81-A, no. 5, pp. 818–824, 1998.

[6] D. Fang, Na Wang, and C. Liu, "An enhanced rsa-based partially blind signature," *International Conference on Computer and Communication Technologies in Agriculture Engineering*, vol. 1, no. 1, pp. 565–567, 2010.

[7] N. Ferguson, "Single term off-line coins," *Advances in Cryptology (EUROCRYPT'93)*, no. LNCS 765, pp. 318–328, 1994.

[8] M. S. Hwang, C. C. Lee, and Y. C. Lai, "Traceability on low-computation partially blind signatures for electronic cash," *IEICE Fundamentals on Electronics, Communications and Computer Sciences*, vol. E85-A, no. 5, pp. 1181–1182, 2002.

[9] M. S. Hwang, C. C. Lee, and Y. C. Lai, "An untraceable blind signature scheme," *IEICE Transactions on Foundations*, vol. E86-A, no. 7, pp. 1902–1906, 2003.

[10] J. Katz and Y. Lindell, *Introduction to Modern Cryptography.* US: Chapman and Hall/CRC, 2007.

[11] C. C. Lee, M. S. Hwang, and W. P. Yang, "Untractable blind signature schemes based on discrete logarithm problem," *Fundamenta Informaticae*, vol. 55, no. 3-4, pp. 307–320, 2003.

[12] C. C. Lee, M. S. Hwang, and W. P. Yang, "A new blind signature based on the discrete logarithm problem for untraceability," *Applied Mathematics and Computation*, vol. 164, no. 3, pp. 837–841, 2005.

[13] G. Martinet, G. Poupard, P. Sola, "Cryptanalysis of a partially blind signature scheme or how to make $ 100 bills with $ 1 and $ 2 ones," *Proceedings of Financial Cryptography and Data Security*, LNCS vol. 4107, no. 1, pp. 171–176, 2006.

[14] T. Okamoto, "Efficient blind and partially blind signatures without random oracles," in *Theory of Cryptography (TCC'2006)*, vol. LNCS 3876, pp. 80–99, 2006.

[15] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, no. 3, pp. 361–396, 2000.

[16] N. M. F. Tahat, S. M. A. Shatnawi, and E. S. Ismail, "A new partially blind signature based on factoring and discrete logarithms," *Journal of Mathematics and Statistics*, vol. 4, no. 2, pp. 124–129, 2008.

[17] M. Tian, Y. Zhu, and Z. Chen, "Two simple attacks on a blind signature scheme," *International Journal of Network Security*, vol. 16, no. 6, pp. 498–500, 2014.

[18] G. K. Verma, "Probable security proof of a blind signature scheme over braid groups," *International Journal of Network Security*, vol. 12, no. 2, pp. 118-120, 2011.

[19] Q. Wu, W. Susilo, Yi Mu, and F. Zhang, "Efficient partially blind signatures with provable security," in *Computational Science and Its Applications (ICCSA'07),* LNCS vol. 4707, pp. 1096–1105, 2007.

[20] Y. Yu, Yi Mu, W. Susilo, Y. Sun, and Y. Ji, "Provably secure proxy signature scheme from factorization," *Mathematical and Computer Modelling*, vol. 55, no. 1, pp. 1160–1168, 2012.

Yi Zhao graduated from Zhejiang University in 2008. He is a master student of Shaanxi Normal University. His main research interests include cryptography and information security.

Qiliang Yang is currently a student at College of Informatics, Shu-Te University. Email:s11115263@stu.edu.tw

Bo Yang received the B.S. degree from Peking University in 1986, and the M.S. and Ph.D. degrees from Xidian University in 1993 and 1999, respectively. From July 1986 to July 2005, he had been at Xidian University. From 2002, he had been a professor of National Key Lab. of ISN in Xidian University. He has served as a program chair for the fourth China Conference on Information and Communications Security in 2005, the vice-chair for ChinaCrypt 2009, and the general co-chair for the Joint Workshop on Information Security since 2010. He is currently a professor and supervisor of Ph.D. candidates at the School of Computer Science, Shaanxi Normal University, a Bai-Ren project special-term professor of Shaanxi Province, and a member of the Council of Chinese Association for Cryptologic Research. His research interests include information theory and cryptography.