International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:3, No:9, 2009

A Secure Blind Signature Scheme for Computation Limited Users

Chun-I Fan and Ming-Te Chen

Abstract**—**This manuscript presents a fast blind signature scheme with extremely low computation for users. Only several modular additions and multiplications are required for a user to obtain and verify a signature in the proposed scheme. Comparing with the existing ones in the literature, the scheme greatly reduces the computations for users.

Keywords**—**Blind signatures, Untraceable electronic cash, Security & privacy, Electronic commerce

I. Introduction

The concept of blind signatures was first introduced by Chaum [2] to prevent digital signatures from being forged and to protect the privacy of users. Based on the RSA cryptosystem, Chaum proposed the first blind signature scheme to achieve the unlinkability property [2]. By means of the techniques of blind signatures, an anonymous electronic cash system was proposed by Chaum in [3]. Based on the RSA cryptosystem, Ferguson [11] introduced another blind signature scheme tailored for his untraceable electronic cash system. In [1], the authors proposed a blind signature scheme based on discrete logarithm (DL) problems, and it is derived from a variation of the DSA [15]. The authors of [1] also presented a blind signature scheme based on the Nyberg-Rueppel signature scheme [16]. Based on Okamoto's protocol of [17] and Schnorr's protocol of [24], a blind signature scheme was proposed in [20]. The authors of [20] presented another blind signature scheme based on Okamoto's protocol of [17] and the Guillou-Quisquater protocol of [13]. In 1997, based on the theories of quadratic residues, two blind signature schemes are proposed in [21]. In all of the above schemes, it is necessary for a user to perform a large amount of computations to obtain and verify a signature. Besides, in 1996, Fan and Lei proposed a blind signature scheme based on quadratic residues [7], and they also presented an enhanced version of the scheme to reduce the computation for requesters or users [8]. Comparing with the schemes of [1], [2], [11], [20], [21], the scheme of [8] greatly reduces the computations for users by more than 99%. Although Shao [26] claimed that Fan-Lei blind signature scheme is not really blind, Fan and Lei had shown that his claim is not true [10].

This manuscript presents a fast blind signature scheme with fairly low computations for users. Comparing with the blind signature schemes of [1], [2], [11], [20], [21], the proposed scheme largely reduces the computations for users by more than 99%. Compared to the user efficient blind signature scheme of [8], the proposed scheme reduces the computations for users by about 37%.

II. The Proposed Scheme

In general, two kinds of roles, a signer and a group of users, participate in a blind signature protocol. A user blinds a message by performing an encryption-like process (or a blinding process) on the message, and then submits the blinded message to the signer to request the signer's signature on the blinded message. The signer signs the blinded message by using its signing function, and then sends the signing result back to the user. Finally, the user unblinds the signing result to obtain the signer's signature on the message by performing a decryption-like operation (or an unblinding operation) on the signing result he receives. The signer's signature on the message can be verified by checking whether the corresponding public verification formula with the signature-message pair as parameters is true or not. In a secure blind signature scheme, it is computationally infeasible for the signer to derive the link between a signature and the instance of the signing protocol which produces the blinded form of that signature. This is usually referred to as the *unlinkability* or *blindness* property.

In this section we propose a blind signature scheme based on quadratic residues [22], [27]. 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 $y^2 \equiv x \pmod{n}$ where Z_n^* is the set of all positive integers less than and relatively prime to n. Given x and n, it is intractable to compute the square root y of x in Z_n^* if n contains large prime factors and the factorization of n is unknown [22], [27].

There are two kinds of participants, a signer and a group of users, in the proposed blind signature scheme. A user requests signatures from the signer, and the signer computes and issues blind signatures to the users. The proposed blind signature scheme consists of four phases: (1) initializing, (2) blinding, (3) signing, and (4) unblinding. The signer publishes the necessary information in the initializing phase. To obtain a signature from the signer, a user performs a blinding process to transform a message into a blinded message, and then submits the blinded message to the signer in the blinding phase. In the signing phase, the signer computes the signature on the blinded message, and then sends the signing result back to the user. Finally, the user performs an unblinding operation to convert the signing result he receives into the exact signature on the

This work was supported in part by the National Science Council of the ROC (Taiwan) under grant NSC96-2221-E-110-071-MY3, NSC96-2219-E-110-002 and NSC96-2219-E-006-009(TWISC@NCKU).

Department of Computer Science and Engineering, National Sun Yat-sen University, 70, Lien-Hai Road, Kaohsiung 804, Taiwan
TEL: +886-7-5252000 ext. 4346 FAX: +886-7-5254301 Email: cifan@cse.nsysu.edu.tw

message in the unblinding phase. The details of the proposed scheme are described as follows.

(1) **Initializing.** The signer randomly selects two distinct large primes p_1 and p_2 such that $p_1 \equiv p_2 \equiv 3$ (mod 4). The signer computes n = $p_1 p_2$ and then publishes n. Since $p_1 \equiv p_2 \equiv 3$ (mod 4), given a QR in Z_n^*, there are four different square roots (or 2nd roots) of the QR in Z_n^*, and one of these roots is a QR in Z_n^*, too [27]. Hence, in addition to the 2nd roots of a QR in Z_n^*, we can derive the 4th roots, 8th roots, and (2^i)th roots of the QR in Z_n^* where i is an integer greater than 1. In addition, such a special form of primes p_1 and p_2 does not affect the difficulty of factoring n [28].

(2) **Blinding.** To request a signature from the signer, a user randomly chooses two integers u and v such that α = $((u+v)(u-v) \bmod n)$ is in Z_n^* and then submits the integer α to the signer.

After receiving α, the signer randomly selects x such that $(\alpha(x^2-1) \bmod n)$ is a QR in Z_n^*, and then sends the integer x to the user.

After receiving x, the user randomly selects an integer b in Z_n^*, and then computes $\delta = (b^2 \bmod n)$ and $\beta = (\delta(u+vx) \bmod n)$. The user sends the integer β to the signer.

(3) **Signing.** After receiving β, the signer computes λ = $(\beta^{-1} \bmod n)$ and derives an integer t in Z_n^* such that[1]

$$t^4 \equiv \alpha(x^2-1)\lambda^2 \pmod n$$

by the algorithms of [18], [22]. Hence t is one of the 4th roots of $(\alpha(x^2-1)\lambda^2 \bmod n)$ in Z_n^*. The signer sends the tuple (t, λ) to the user.

(4) **Unblinding.** After receiving (t, λ), the user computes

$$\begin{cases} c = \delta\lambda(ux+v) \mod n \\ s = bt \bmod n. \end{cases}$$

The tuple (c, s) is a signature of the signer in the scheme. To verify the signature tuple (c, s), one can examine if

$$(c+s^2)(c-s^2) \equiv 1 \pmod n.$$

The proposed protocol is shown in Figure 1.

III. Discussions

A. The Underlying Signature Foundation

The security of Rabin's signature scheme [22] had been proven to be computationally equivalent to the factoring problem. Hence, if factoring n is computationally intractable where n is the product of two large random distinct primes with roughly the same size, then Rabin's scheme is provably secure against a passive adversary. However, Rabin's scheme succumbs to the chosen-message attacks [5], [14].

The proposed scheme is based on Rabin's signatures with injecting randomizing factors x's into the messages before the signer performs the signing operations on them. The scheme of section 2 is robust against a passive adversary due to using the Rabin's method, and the proposed randomizing mechanism enhances the randomization of Rabin's signatures such that it is computationally infeasible for an adversary to predict the contents of the messages the signer exactly signs for the chosen-message attacks such as [5], [12].

In the proposed blind signature scheme, the signer perturbs the message received from each user before he signs it by using a random integer x. This is usually referred to as the *randomization* property [11]. A randomized blind signature scheme can withstand the chosen-message attacks [25]. The proposed scheme and the blind signature schemes of [1], [8], [11], [20], [21] possess the randomization property, while the Chaum's blind signature scheme of [2] does not satisfy this property. In 1999, Coron, Naccache, and Stern presented a signature forgery strategy of the RSA digital signature scheme [5], and the attack is valid on some special cases of Chaum's blind signature scheme [9].

In the signing phase of the proposed blind signature protocol, it is intractable for a user to obtain an integer t' from the signer such that $t'^4 \equiv \alpha \pmod n$ where α is chosen by the user in the blinding phase. In the blinding phase of the scheme, a user chooses and submits the integer α to the signer, and then the user receives the integer x from the signer. If the user tries to select an integer β' such that $\alpha(x^2-1)\beta'^{-2} \equiv \alpha \pmod n$, and in the signing phase, obtains t' from the signer such that $t'^4 \equiv \alpha \pmod n$, then he has to compute β' such that $\beta'^2 \equiv (x^2-1) \pmod n$. Since the integer x is randomly chosen by the signer and the factorization of n is unknown to the user, it is intractable for the user to obtain t' from the signer such that $t'^4 \equiv \alpha \pmod n$ in the signing phase of the proposed scheme [22].

B. Correctness

Theorem 1 ensures that the signature tuple (c, s) produced by the proposed blind signature scheme satisfies that $(c+s^2)(c-s^2) \equiv 1 \pmod n$.

Theorem 1: If (c, s) is produced by the proposed blind signature scheme, then

$$(c+s^2)(c-s^2) \equiv 1 \pmod n.$$

Proof. By the Chinese remainder theorem [27], an integer w in Z_n^* can be represented by $< w_1, w_2 >$ where $w_1 = (w \bmod p_1)$ and $w_2 = (w \bmod p_2)$. For convenience, $< w_1, w_2 >$ is denoted by $< w >$ sometimes. For each $< k >$ = $< k_1, k_2 >$ and $< w >$ = $< w_1, w_2 >$ in Z_n^*, $< kw \bmod n >$ = $< k_1 w_1 \bmod p_1, k_2 w_2 \bmod p_2 >$, and $< k^{-1} \bmod n >$ = $< k_1^{-1} \bmod p_1, k_2^{-1} \bmod p_2 >$. In addition, for each $< k_1, k_2 >$ and $< w_1, w_2 >$ in Z_n^*, $< k_1, k_2 > = < w_1, w_2 >$ if and only if $k_1 \equiv w_1 \pmod{p_1}$ and $k_2 \equiv w_2 \pmod{p_2}$.

Let $\left[\frac{g}{h}\right]$ denote the Legendre symbol g over h where h is a prime [27]. Since both $(\alpha(x^2-1) \bmod n)$ and $(\lambda^2 \bmod n)$ are QR's in Z_n^*,

$$\left[\frac{\alpha(x^2-1)\lambda^2}{p_1}\right] = \left[\frac{\alpha(x^2-1)}{p_1}\right]\left[\frac{\lambda^2}{p_1}\right] = 1 \cdot 1 = 1$$

[1] If $((u+vx) \bmod n)$ is not in Z_n^*, the signer cannot compute $(\beta^{-1} \bmod n)$. However, the probability of that $((u+vx) \bmod n)$ is not in Z_n^* is nearly $\frac{1}{2^{|p_1|}}$ or $\frac{1}{2^{|p_2|}}$ where $|p_1|$, $|p_2|$ denote the bit lengths of p_1, p_2, and 512 $\le |p_1|, |p_2|$ in a practical implementation [14], [27].

and

$$\left[\frac{\alpha(x^2-1)\lambda^2}{p_2}\right] = \left[\frac{\alpha(x^2-1)}{p_2}\right]\left[\frac{\lambda^2}{p_2}\right] = 1\cdot 1 = 1.$$

Therefore, we have that

$$\begin{aligned}
&\alpha(x^2-1)\lambda^2\\
&\equiv \alpha(x^2-1)\beta^{-2}\\
&\equiv (u+v)(u-v)(x^2-1)(b^2(u+vx))^{-2}\\
&\equiv b^{-4}(u^2-v^2)(x^2-1)(u+vx)^{-2}\\
&\equiv b^{-4}((ux+v)^2-(u+vx)^2)(u+vx)^{-2}\\
&\equiv b^{-4}((ux+v)^2(u+vx)^{-2}-1)\\
&\equiv b^{-4}(((ux+v)(u+vx)^{-1})^2-1)\\
&\equiv b^{-4}((b^2b^{-2}(u+vx)^{-1}(ux+v))^2-1)\\
&\equiv b^{-4}((\delta\lambda(ux+v))^2-1)\\
&\equiv b^{-4}(c^2-1) \pmod{n}
\end{aligned}$$

is a QR in Z_n^*. Because $\left[\frac{b^{-4}}{p_1}\right] = \left[\frac{b^{-4}}{p_2}\right] = 1$, the integer $(c^2-1 \bmod n)$ also is a QR in Z_n^*. If $< d_1, d_2 >$ is one of the 4th roots of the integer $(c^2-1 \bmod n)$ in Z_n^*, then the four 4th roots of the integer in Z_n^* are $< \pm d_1 \bmod p_1, \pm d_2 \bmod p_2 >$. Thus, the four 4th roots of $(b^{-4}(c^2-1) \bmod n)$ in Z_n^* are $< \pm b_1^{-1}d_1 \bmod p_1, \pm b_2^{-1}d_2 \bmod p_2 >$. As $t^4 \equiv b^{-4}(c^2-1) \pmod{n}$, t belongs to $\{< \pm b_1^{-1}d_1 \bmod p_1, \pm b_2^{-1}d_2 \bmod p_2 >\}$. Since $s = (bt \bmod n)$, s is an element in $\{< \pm b_1 b_1^{-1}d_1 \bmod p_1, \pm b_2 b_2^{-1}d_2 \bmod p_2 >\} = \{< \pm d_1 \bmod p_1, \pm d_2 \bmod p_2 >\}$. It follows that s is a 4th root of the integer $(c^2-1 \bmod n)$ in Z_n^*. Hence, $s^4 \equiv (c^2-1) \pmod{n}$. Thus, we have that $(c+s^2)(c-s^2) \equiv 1 \pmod{n}$. □

C. Unlinkability

In a blind signature scheme, the unlinkability property makes it impossible for the signer to derive the link between a given signature and the instance of the signing protocol which produces the blinded form of that signature. In this subsection the unlinkability property of the proposed blind signature scheme is examined.

For each instance, numbered i, of the protocol in section 2, the signer can record the messages (α_i, β_i, x_i) transmitted between the user and the signer during the instance i of the protocol. The triple (α_i, β_i, x_i) is usually referred to as the *view* of the signer to the instance i of the protocol. Thus, we have the following theorem.

Theorem 2: Given a signature tuple (c, s) produced by the proposed protocol, the signer can derive b_i', u_i', and v_i' for each (α_i, β_i, x_i) in polynomial time such that

$$\begin{cases} c \equiv (u_i'x_i + v_i')(u_i' + v_i'x_i)^{-1} \pmod{n}, \\ \alpha_i \equiv (u_i' + v_i')(u_i' - v_i') \pmod{n}, \text{ and} \\ \beta_i \equiv (b_i')^2(u_i' + v_i'x_i) \pmod{n}. \end{cases}$$

Proof. If $c \equiv (u_i'x_i + v_i')(u_i' + v_i'x_i)^{-1} \pmod{n}$, then $u_i' \equiv v_i'(1-cx_i)(c-x_i)^{-1} \pmod{n}$. If $\alpha_i \equiv (u_i'+v_i')(u_i'-v_i') \pmod{n}$, we have the following derivations,

$$\begin{aligned}
&\alpha_i \equiv ((u_i')^2 - (v_i')^2) \pmod{n}\\
&\alpha_i \equiv ((v_i')^2(1-cx_i)^2(c-x_i)^{-2} - (v_i')^2) \pmod{n}\\
&\alpha_i \equiv (v_i')^2((1-cx_i)^2 - (c-x_i)^2)(c-x_i)^{-2} \pmod{n}\\
&\alpha_i \equiv (v_i')^2(c^2-1)(x_i^2-1)(c-x_i)^{-2} \pmod{n}\\
&(v_i')^2 \equiv \alpha_i(c^2-1)^{-1}(x_i^2-1)^{-1}(c-x_i)^2 \pmod{n}\\
&(v_i')^2 \equiv \alpha_i s^{-4}(x_i^2-1)^{-1}(c-x_i)^2 \pmod{n}
\end{aligned}$$

Since $(s^{-4} \bmod n)$, $((c-x_i)^2 \bmod n)$, and $(\alpha_i(x_i^2-1)^{-1} \bmod n)$ are QR's in Z_n^*, the signer can derive 4 different values of $v_i^{'}$ in Z_n^* such that $(v_i')^2 \equiv \alpha_i s^{-4}(x_i^2-1)^{-1}(c-x_i)^2 \pmod{n}$ is satisfied.

If $\beta_i \equiv (b_i')^2(u_i' + v_i^{'}x_i) \pmod{n}$, we have that

$(b_i')^2 \equiv \beta_i((1-cx_i)(c-x_i)^{-1} + x_i)^{-1}(v_i')^{-1} \pmod{n}$

There exists a value of v_i' among its 4 different ones in Z_n^* such that $\beta_i((1-cx_i)(c-x_i)^{-1} + x_i)^{-1}(v_i')^{-1} \pmod{n}$ is a QR in Z_n^*. Thus, the signer can derive 4 different values of $b_i^{'}$ in Z_n^* such that $(b_i')^2 \equiv \beta_i((1-cx_i)(c-x_i)^{-1} + x_i)^{-1}(v_i')^{-1} \pmod{n}$ is satisfied.

Thus, the signer can derive b_i', r_i', and u_i' for each (α_i, β_i, x_i) in polynomial time. □

Hence, given a tuple (c, s) produced by the protocol of section 2, the signer can always derive the three blinding factors b_i', u_i', and v_i' for each view (α_i, β_i, x_i). It turns out that all of the signature tuples (c, s)'s are indistinguishable from the signer's point of view. This is the unlinkability or blindness property.

D. Performance

Typically, under a modulus n, the computation time for a modular exponentiation operation is about $O(|n|)$ times that of a modular multiplication where $|n|$ denotes the bit length of n [27]. The modulus n is usually taken about 1024 bits or more in a practical implementation [14], [27]. In [4], [6], some fast modular exponentiation algorithms are proposed. In [6], it requires $0.3381|n|$ modular multiplications and large amount of storage, e.g. 83370 stored values for a 512-bit modulus, to perform a modular exponentiation computation. An enhanced version of [6] is introduced in [4]. However, it still requires $0.3246|n|$ modular multiplications and large amount of storage, e.g. 36027 stored values for a 512-bit modulus, to perform a modular exponentiation computation [4]. Besides, an inverse computation in Z_n^* takes about the same time as that of a modular exponentiation computation in Z_n^*, and a hashing computation does not take longer time than that of a modular multiplication computation [27].

In the proposed blind signature scheme, no modular exponentiation and inverse computations are performed by users. Moreover, only several modular additions and multiplications are required for a user to obtain and verify a signature in the proposed protocol. In the existing blind signature schemes of [1], [2], [11], [20], [21], several modular exponentiation computations and inverse computations are needed for a user to obtain and verify a signature, while these time-consuming computations are not required in the proposed scheme. Compared to the schemes of [1], [2], [11], [20], [21], if we take a modular exponentiation computation to be $0.3246|n|$ modular multiplications under a 1024-bit modulus n [4], the proposed scheme reduces the amount of computations for users by more than 99%. Compared to the user efficient blind signature scheme of [8], the proposed scheme reduces the computations for users by about 37%. The comparisons of the numbers of computations performed by a user between the proposed scheme and the schemes of [1], [2], [8], [11], [20], [21] are summarized in Table 1. In addition, comparing with the blind signature scheme of [2] with a short public key $e = 3$, the proposed method still largely reduces the amount of computations for users by 95% under a 1024-bit modulus since an inverse computation is still needed for a user in that scheme.

In the proposed scheme, the signer performs a 4th root computation and an inverse computation in Z_n^*. Comparing with the scheme of [2], the proposed protocol does not decrease the computation load for the signer. However, in most of the applications based on blind signatures, the signer usually possesses much more computation capabilities than a user such as the bank of an untraceable electronic cash system or the tally center of an anonymous electronic voting protocol, while the computation capabilities of the users are limited in some situations such as mobile clients and smart-card users. Hence, to guarantee the quality of these ever-growing popular communication services based on blind signatures, it is more urgent to reduce the computation load for the users than that for the signer.

IV. Applications

Based on the proposed blind signature scheme, we can construct an untraceable electronic cash protocol. The electronic cash protocol contains three parties (a bank, payers, and payees) and four stages (initializing, withdrawing, unblinding, and paying) where the bank and the payers of the electronic cash protocol are regarded as the signer and the users of the blind signature scheme in section 2, respectively. The protocol is described below.

(1) **Initializing.** The bank randomly selects two distinct large primes p_1 and p_2 such that $p_1 \equiv p_2 \equiv 3$ (mod 4). It computes n = p_1p_2 and then publishes n. Each of the payers and payees performs an account establishment protocol with the bank to open an account in the bank. Let each e-cash issued by the bank worth w dollars.

(2) **Withdrawing.** To withdraw an e-cash from the bank, a payer randomly chooses two integers u and v such that α = $((u + v)(u - v)$ mod $n)$ is in Z_n^* and then submits α to the bank.

After verifying the identity of the payer through a secure identification protocol [14], the bank randomly selects x such that $(\alpha(x^2 - 1)$ mod $n)$ is a QR in Z_n^*, and then sends the integer x to the payer.

After receiving x, the payer randomly selects an integer b in Z_n^*, and then computes $\delta = (b^2$ mod $n)$ and $\beta = (\delta(u + vx)$ mod $n)$. The payer sends the integer β to the bank.

After receiving β, the bank computes λ = $(\beta^{-1}$ mod $n)$ and derives an integer t in Z_n^* such that $t^4 \equiv \alpha(x^2-1)\lambda^2$ (mod n). The bank sends the tuple (t, λ) to the payer, and deducts w dollars from the payer's account in the bank.

(3) **Unblinding.** After receiving (t, λ), the payer computes $c = (\delta\lambda(ux+v)$ mod $n)$ and $s = (bt$ mod $n)$. The tuple (c, s) is an e-cash in the scheme.

(4) **Paying.** If the payer decides to pay a payee the e-cash, then he sends (c, s) to the payee. After verifying that $(c+s^2)(c-s^2) \equiv 1$ (mod n), the payee sends (c, s) to the bank to check whether the e-cash is double-spent or not. If (c, s) is not found in the bank's database which records all spent e-cash, then the bank informs the payee to accept this payment. Finally, the bank stores the e-cash in its database for future double-spending checking and increases the amount of the payee's account by w dollars.

By theorem 2, given the e-cash (c, s), it is intractable for the bank to derive the instance of the withdrawing protocol which produces the blinded version of the e-cash. This is the unlinkability or untraceability property of untraceable electronic cash [2], [3].

V. Conclusions

An efficient blind signature scheme with fairly low computations for users has been proposed. Since no modular exponentiation and inverse computations are performed by users, the scheme is suitable for the situations where the computation capabilities of users are limited. Compared to the existing blind signature schemes, the computations are greatly reduced for users in the proposed blind signature scheme.

References

[1] J. Camenisch, J. Piveteau, and M. Stadler, ”Blind signatures based on the discrete logarithm problem,” *Advances in Cryptology-EUROCRYPT'94*, LNCS 950, Springer-Verlag, 1995, pp. 428-432.

[2] D. Chaum, ”Blind signatures for untraceable payments,” *Advances in Cryptology-CRYPTO'82*, Plenum, 1983, pp. 199-203.

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

[4] C. Chen, C. Chang, and W. Yang, ”Hybrid method for modular exponentiation with precomputation,” *IEE Electronics Letters*, vol. 32, no. 6, 1996, pp. 540-541.

[5] J. Coron, D. Naccache, and J. Stern, ”On the security of RSA padding,” *Advances in Cryptology-CRYPTO'99*, LNCS 1666, Springer-Verlag, 1999, pp. 1-18.

[6] V. Dimitrov and T. Cooklev, ”Two algorithms for modular exponentiation using nonstandard arithmetics,” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E78-A, no. 1, 1995, pp. 82-87.

[7] C. Fan and C. Lei, ”A multi-recastable ticket scheme for electronic elections,” *Advances in Cryptology-ASIACRYPT'96*, LNCS 1163, Springer-Verlag, 1996, pp. 116-124.

[8] C. Fan and C. Lei, ”User efficient blind signatures,” *IEE Electronics Letters*, vol. 34, no. 6, 1998, pp. 544-546.

[9] C. Fan, W. Chen, and Y. Yeh, ”Randomization enhanced Chaum's blind signature scheme,” *Advances in Research and Application of Network Security, Computer Communications*, vol. 23, no. 17, 2000, pp. 1677-1680.

[10] C. Fan and C. Lei, ”Cryptanalysis on Improved User Efficient Blind Signatures,” *IEE Electronics Letters*, vol. 37, no. 10, 2001, pp. 630-631.

[11] N. Ferguson, ”Single term off-line coins,” *Advances in Cryptology-EUROCRYPT'93*, LNCS 765, Springer-Verlag, 1994, pp. 318-328.

[12] S. Goldwasser, S. Micali, and R. Rivest, ”A digital signature scheme secure against adaptive chosen-message attacks,” *Technical Report*, MIT Lab., Computer Science, Cambridge, Mass. March, 1995.

[13] L. Guillou and J. Quisquater, ”A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory,” *Advances in Cryptology-EUROCRYPT'88*, LNCS 330, Springer-Verlag, 1988, pp. 123-128,.

[14] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of applied cryptography*, CRC Press LLC, 1997.

[15] NIST FIPS PUB XX, Digital Signature Standard (DSS), National Institute of Standards and Technology, U.S. Department of Commerce, DRAFT, 1993.

[16] K. Nyberg and R. Rueppel, ”A new signature scheme based on the DSA giving message recovery schemes,” *The first ACM Conference on Computer and Communications Security*, Fairfax, Virginia, 1994.

[17] T. Okamoto, ”Provably secure and practical identification schemes and corresponding signature schemes,” *Advances in Cryptology-CRYPTO’92*, LNCS 740, Springer-Verlag, 1992, pp. 31-53.

[18] R. Peralta, ”A simple and fast probabilistic algorithm for computing square roots modulo a prime number,” *IEEE Transactions on Information Theory*, vol. 32, no. 6, 1986, pp. 846-847.

[19] S. Pohlig and M. Hellman, ”An improved algorithm for computing logarithms over GF(p) and its cryptographic significance,” *IEEE Transactions on Information Theory*, vol. 24, 1978, pp. 106-110.

[20] D. Pointcheval and J. Stern, ”Provably secure blind signature schemes,” *Advances in Cryptology-ASIACRYPT’96*, LNCS 1163, Springer-Verlag, 1996, pp. 252-265.

[21] D. Pointcheval and J. Stern, ”New blind signatures equivalent to factorization,” *Proceedings of the 4th ACM Conference on Computer and Communication Security*, 1997, pp. 92-99.

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

[23] R. 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.

[24] C. Schnorr, ”Efficient identification and signatures for smart cards,” *Advances in Cryptology-CRYPTO’89*, Springer-Verlag, LNCS 435, 1990, pp. 235-251.

[25] A. Shamir and C. Schnorr, ”Cryptanalysis of certain variants of Rabin’s signature scheme,” *Information Processing Letters*, vol. 19, 1984, pp. 113-115.

[26] Z. Shao, ”Improved user efficient blind signatures,” *IEE Electronics Letters*, vol. 36, no. 16, 2000, pp. 1372-1374.

[27] G. Simmons, *Contemporary Cryptology: The Science of Information Integrity*, IEEE Press, N.Y., 1992.

[28] H. Williams, ”A modification of the RSA public-key encryption procedure,” *IEEE Transactions on Information Theory*, vol. 26, no. 6, 1980, pp. 726-729.

Chun-I Fan was born in Tainan, Taiwan on October 15, 1967. He received his M.S. degree in computer science and information engineering from National Chiao Tung University, Taiwan, in 1993, and the Ph.D. degree in electrical engineering at National Taiwan University in 1998. From 1999 to 2003, he was an associate researcher of Telecommunication Laboratories, Chunghwa Telecom Co., Ltd, Taiwan. In 2003, he joined the faculty of the department of computer science and engineering, National Sun Yat-sen University, Kaohsiung, Taiwan. He also is the editor-in-chief of Information Security Newsletter, Chinese Cryptology and Information Security Association. His current research interests include information security, cryptographic protocols, wireless security, and electronic commerce.

Ming-Te Chen was born in Tainan, Taiwan on August 2, 1980. He received his M.S. degree in computer science and engineering from National Sun Yat-sen University (NSYSU), in 2005. He is currently a Ph.D. candidate in the Department of Computer Science and Engineering of NSYSU. His current research interests include watermark security, cryptographic protocols, broadcast encryption and electronic commerce.

TABLE I

COMPUTATIONS REQUIRED FOR A USER TO OBTAIN AND VERIFY A SIGNATURE

	The scheme	[1]*	[2]	[8]	[11]	[20]*	[21]*
Numbers of Exponentiations	0	4	2	0	4	6	3
Numbers of Inverses	0	2	1	0	1	0	0
Numbers of Hashings	0	0	2	2	2	2	2
Numbers of Multiplications	10	6	2	14	3	5	$2k^{**}$
Reduced by:	–	99%	99%	37%	99%	99%	99%

*The fastest scheme mentioned in the paper is selected for comparison in this table.

$^{**}k$ is a large enough integer.

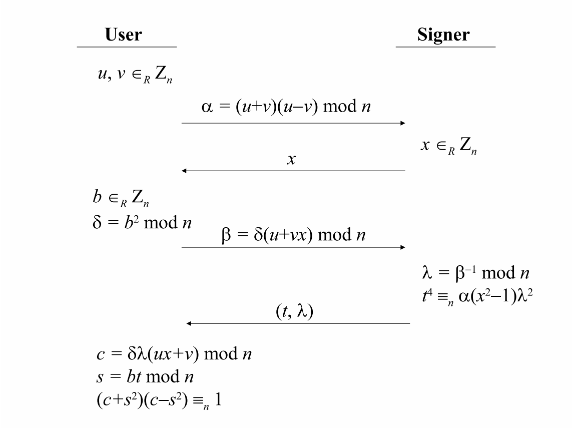
User
Signer
$u, v \in_R Z_n$
$\alpha = (u+v)(u-v) \bmod n$
$x \in_R Z_n$
x
$b \in_R Z_n$
$\delta = b^2 \bmod n$
$\beta = \delta(u+vx) \bmod n$
$\lambda = \beta^{-1} \bmod n$
$t^4 \equiv_n \alpha(x^2-1)\lambda^2$
(t, λ)
$c = \delta\lambda(ux+v) \bmod n$
$s = bt \bmod n$
$(c+s^2)(c-s^2) \equiv_n 1$

Fig. 1. The proposed blind signature scheme