New Blind Signature Protocols Based on a New Hard Problem

Minh Hieu[1], Hai Nam[1], Moldovyan Nikolay[2], and Giang Tien[3]
[1]Faculty of Electronics and Telecommunications, Academy of Cryptography Techniques, Viet Nam
[2]Laboratory of Computer Security Problems, Saint Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, Russia
[3]Department of Information Technology, Ministry of National Defense, Viet Nam

Abstract: *Blind signature and blind multisignature schemes are useful in protocols that guarantee the anonymity of the participants. In practice, in some cases the electronic messages are to be signed by several signers and an electronic message is first blinded then passed to each of the signers, who then sign it using some special signature scheme such as collective signature protocol. In this paper, we propose a new blind signature scheme and two type new blind collective signature protocols. Our protocols are based on the difficulty of finding the k^{th} roots modulo a large prime p in the case when k is a prime such that k^2/p-1. Our proposed protocols produce the signature (E', S'), where E' is a 160-bit value and S' is a 1024-bit value. It seems that such primitives are attractive for applications in the electronic money systems in which the electronic banknotes are issued by one or several banks*.

Keywords: *Collective digital signature, blind signature, blind collective signature, multisignature scheme*.

Received March 17, 2013; accepted October 21, 2016

1. Introduction

The concept of blind signature scheme was introduced by Chaum [6]. Based on the RSA cryptosystem, Chaum proposed the first blind signature scheme to achieve the unlinkability property [6]. A blind signature scheme is allowed to realize secure electronic payment systems protecting customer's privacy [4, 7]. Such signatures require that a signer is able to sign a document without knowing its content. Blind signature protocols are very useful for applications, in which anonymity is a big issue. Examples include online voting systems and electronic cash schemes.

The first multisignature scheme was introduced by Itakura and Nakamura in [10], and has been followed by many other research works [1, 2, 3, 8, 9, 13, 19]. In practice, a particular type of the multisignature schemes provides a possibility to sign a document by some sets of signers with a single Digital Signature (DS). DS haves a fixed size which is independently with the number of signers sharing the DS. Such protocols are called Collective Digital Signature protocols (CDS) [15]. The CDS protocols are a particular type of the multisignature schemes.

Usually calculating k^{th} roots modulo prime p is sufficiently a simple problem, except of a large prime k such that $k^2 | p - 1$ [15]. Recently in [15] proposed the algorithms called the CDS. The new CDS has fixed size and can be generated by arbitrary group of users. The collective public key corresponds to each possible group of users, which is calculated using the public key of each user included in the group. The CDS is verified using the collective public key and computations modulo prime $p = Nk^2 + 1$, where k is a large prime and N is an even integer.

In this paper, we first propose a new cryptographic scheme called a blind DS protocol (blind DS). We then design using blind DS protocol proposed to design on its, the blind CDS protocol (called blind CDS1) and the blind CDS protocol with distinguished signing authorities (called blind CDS2). These cryptoschemes combine the already existing notions of the CDS and the blind DS. Our proposed protocols are constructed based on the difficulty of finding roots modulo a prime. This protocols can be suitable to apply in the electronic money systems and in the electronic voting systems.

The rest of the paper is organized as following: in section 2, we briefly review the difficult computational problem of finding roots modulo a prime in special case. In section 3, we construct a new blind DS scheme based on the difficulty of finding roots modulo a prime. In sections 4 and 5, we propose two novel blind CDS schemes that represent a new type of cryptographic protocols. Our proposed protocols are blind CDS protocols different from the known blind multisignature schemes. Section 6 describes the analysis of our constructions. The last section concludes our research work in this paper.

2. Related Works

In this section, we brief review the difficulty of finding roots modulo a prime in a special case [15].

Difficulty of finding roots modulo a composite number is used in some of the known DS schemes: RSA and Rabin's DS algorithm [11, 14, 21]. The main difference between the RSA and Rabin's DS consists in the following.

In RSA we have gcd(e, $\varphi(n)$)=1, (gcd(e, p-1)=1 and gcd(e, q-1)=1, but in Rabin's DSS gcd(2, p-1) $\neq$ 1 and gcd(2, q-1)$\neq$1. Actually, the fact that 2|p-1 and 2|q - 1 requires to use some special algorithm to calculate the square roots. For some random prime p and large prime divisor k|p-1 with probability very close to 1 the complexity of finding k roots $\sqrt[k]{a} \bmod p$, where a is one of the k^{th} power residues modulo p, is sufficiently low. Indeed, if prime k is sufficiently large, then with high probability k does not divide $\frac{p-1}{k}$ and it is easy to find some value Δ such that k divides $\frac{p-1}{k} + \Delta$, i.e., $\frac{p-1}{k} + \Delta = hk$, where h is an integer (note that k does not divide Δ).

Then we have:

$$a^{\frac{p-1}{k}} \equiv 1 \bmod p \Rightarrow a^{\frac{p-1}{k}+\Delta} \equiv a^{\Delta} \bmod p \Rightarrow a^{hk} \equiv a^{\Delta' d} \bmod p,$$

where d = gcd (Δ, p-1). Let $\Delta'' = \Delta'^{-1}$ mod p-1. Then we have:

$$\left(\left(a^{1/d}\right)^{h\Delta''}\right)^{k} \equiv a \bmod p \Rightarrow a^{1/k} \equiv \left(a^{1/d}\right)^{h\Delta''} \qquad (1)$$

With high probability the value d is sufficiently small and the d^{th} root can be easily found, for example, using the method described in [15].

If k^2|p-1then the method described above does not work, i.e., in the case of the prime $p=Nk^s+1$, where N is an even number and $s\geq 2$, computing the k^{th} roots is difficult [15].

3. New Blind DS Scheme

New hard computational problem described in section 2 is used in the blind signature scheme described below.

In the paper [15] there is proposed a DS scheme based on difficulty of finding the kth roots modulo large prime p such that k^2|p-1, where k and p are primes. Using the general design of the DS scheme [15] in this section there is designed the blind DS scheme, which produces a 1184-bit blind signature. Our blind DS scheme consists of three phases and two parties (the user A and the signer B).

New blind DS scheme works as follows:

3.1. Key Generation

Our scheme uses the prime modulus having the structure $p=Nk^2+1$, where k is a large prime (|k|$\geq$160) and N is even integer such that |p|$\geq$1024 bits.

- The signer B selects a random value x as a private key.
- The public key y is computed using the formula $y=x^k \bmod p$.

3.2. Blind DS Generation

There are four rounds in the blind DS scheme. The signer signs an unknown message M blindly.

- Signer B Round 1. Selects a random value $t < p$ - 1 and computes $R=t^k \bmod p$. Then he sends R to the user A.
- User A Round 2. Generates a random value ε, such that $\varepsilon < Nk$ and k does not divide ε, and a random value $\sigma < p$ and computes $R' = Ry^{\varepsilon}\sigma^{k} \bmod p$. Then user A computes $E' = h(M||R')$, where $h(\cdot)$ is a specified hash function, for example SHA-1 [14], and $E = E' + \varepsilon \bmod N'$, where $N'=Nk$. Then he sends E to the signer B.
- Signer B Round 3. Using his individual value t and his secret key x computes $S = x^{E}t \bmod p$. Then he sends S to the user A.
- User A Round 4. Computes the second parameter of the blind DS $S' = S\sigma \bmod p$.

The pair (R', S') is a blind DS to the message M and the signature length is $|S'|+|R'| \approx 2|p| \approx 2048$ bit.

3.3. Blind DS Verification

- *Step 1*. Using the blind DS (R', S') compute values $E'=h(M||R')$, $S^* = y^{E'}R' \bmod p$ and $S_k = S'^{k} \bmod p$.
- *Step 2*. Compare values S^* and S_k.

If $S^*=S_k$, then the signature is valid. Otherwise, the signature is false.

It is possible to reduce the signature length using the value $E'=h(M||R')$ as signature element instead of the R' element. A variant of the modified blind DS is presented by the following verification procedure:

- *Step 1*. Using the blind DS (E', S') compute value R^*:$R^*=S'^{k}y^{-E'} \bmod p$.
- *Step 2*. Compute $E^*= h(M||R^*)$ and ccompare values E^* and E'.

If $E^*=E'$ then the signature is valid. Otherwise, the signature is false.

The pair (E', S') is a blind DS to the message M and the length of signature is $|S'|+|E'|\approx 1186$ bit.

4. New Blind CDS1 Protocol

The blind DS scheme proposed in section 3 can be used to design on its base the blind CDS protocol.

In this section, we propose blind CDS protocol (called blind CDS1) for broadcasting structure. The protocol consists of three phases: the key generation phase, the blind CDS1 generation phase and blind CDS1 verification phase.

Suppose that the signing group {B$_1$, B$_2$, …, B$_n$} wants to generate the blind CDS1 for the message M proposed for blind signing by some user A.

4.1. Key Generation

In this protocol, individual public key is computed as the k^{th} power of the private key x: $y{=}x^k \bmod p$.

- $x_1, x_2, \ldots, x_n$: Group members' secret keys such that $1 < x_i < p$, x_i (i = 1, 2, ..., n) is selected randomly and known only for the member B$_i$.
- $y_1, y_2, \ldots, y_n$: Group members' public keys such that $y_i{=}x_i^k \bmod p$ is computed and published by the group members B$_i$.
- The collective public key Y is computed as a convolution of the set of individual public keys y_i of all signers: $Y = \prod_{i=1}^{n} y_i^{\,y_i} \bmod p$.

4.2. Blind CDS1 Generation

There are four rounds in the blind CDS1 protocol in which each signer signs an unknown message M blindly.

- Signers Round 1. Each signer generates a random value $t_i < p$ and computes $r_i{=}t_i^k \bmod p$, then sends r_i to all signers. It is computed the common randomization parameter as the product $R = \prod_{i=1}^{n} r_i \bmod p$ and the value R is send to the user A.
- User A Round 2. Generates a random value ε, such that $\varepsilon < Nk$ and k does not divide ε, and a random value $\sigma < p$ and computes $R' = RY^{\varepsilon}\sigma^k \bmod p$. Then user A computes $E' = h(M||R')$ that is the first parameter of the blind CDS1 and $E = E' + \varepsilon \bmod N'$, where $N'{=}Nk$. Then he sends E to all signers.
- Signers Round 3. Each signer using his individual value t_i and his secret key x_i computes $s_i = x_i^{Ey_i} t_i \bmod p$. It is computed the common randomization parameter as the product $S = \prod_{i=1}^{n} s_i \bmod p$ and the value S is send to the user A.
- User A Round 4. Computes the second parameter of the blind CDS1 $S' = S\sigma \bmod p$.

  The pair (E', S') is a blind CDS1 of the message M.

4.3. Blind CDS1 Verification

The blind CDS1 verification procedure uses the collective public key Y.

- *Step 1*. Using the blind CDS1 (E', S') compute value R^*: $R^* = S'^k Y^{-E'} \bmod p$.
- *Step 2*. Compute $E^* = h(M||R^*)$ and compare values E^* and E'.

If $E^*{=}E'$ then the signature is valid. Otherwise, the signature is false.

5. New Blind CDS2 Protocol

In this section, we propose blind CDS protocol (called blind CDS2) with distinguished signing authorities for broadcasting structure.

Suppose that the signing group {B$_1$, B$_2$, …, B$_n$} wants to generate the blind CDS for the message $M = m_1||m_2|| \ldots ||m_n$. The member B$_i$ is only responsible for the partial content m_i, for i = 1, 2, …, n.

5.1. Key Generation

- $x_1, x_2, \ldots, x_n$: group members' secret keys such that $1 < x_i < p$, x_i is selected randomly and known only by the member B$_i$.
- $y_1, y_2, \ldots, y_n$: group members' public keys such that $y_i{=}x_i^k \bmod p$ is computed and published by the group member B$_i$.
- The collective public key Y is computed as a convolution of the set of individual public keys y_i of all signers: $Y = \prod_{i=1}^{n} y_i^{\,y_i} \bmod p$.

5.2. Blind CDS2 Generation

There are five rounds in the blind CDS2 protocol. The each of the signer signs an unknown message m_i blindly, respectively.

- User A Round 1. Computes $h(m_i)$, then sends $h(m_i)$ to each of the signers, respectively.
- Signers Round 2. Each signer generates a random value $t_i < p$ and computes $r_i = t_i^{h(m_i)k} \bmod p$, then sends r_i to all signers. It is computed the common randomization parameter as the product $R = \prod_{i=1}^{n} r_i \bmod p$ and the value R is send to the user A.
- User A Round 3. Generates a random value ε, such that $\varepsilon < Nk$ and k does not divide ε, and a random value $\sigma < p$ and computes $R' = RY^{\varepsilon}\sigma^k \bmod p$. Then user A computes $E' = h(M||R')$ that is the first parameter of the blind CDS2 and $E = E' + \varepsilon \bmod N'$, where $N' = Nk$. Then he sends E to all signers.
- Signers Round 4. Each signer using his individual value t_i and his secret key x_i computes $s_i = x_i^{Ey_i} t_i^{h(m_i)} \bmod p$. It is computed the common

randomization parameter as the product $S = \prod_{i=1}^{n} s_i \bmod p$ and the value S is send to the user A.

- User A Round 5. Computes the second parameter of the blind CDS2 $S' = S\sigma \bmod p$.

The pair (E', S') is a blind CDS2 of the message $M = m_1||m_2|| \dots ||m_n$.

5.3. Blind CDS2 Verification

The blind CDS2 verification procedure uses the collective public key Y.

- *Step 1*. Using the blind CDS2 (E', S') compute value R^*: $R^* = S'^k Y^{-E'} \bmod p$.
- *Step 2*. Compute $E^* = h(M||R^*)$ and compare values E^* and E'.

If $E^* = E'$ then the signature is valid. Otherwise, the signature is false.

The partial contents of the message $m_1||m_2|| \dots ||m_n$ can be verified without revealing the whole document. If the verifier is only allowed to read the partial content m_i, then he will receive $h(m_1)||h(m_2)||\dots||h(m_{i-1})||m_i||h(m_{i+1})||\dots||h(m_n)$ to verify the blind CDS2 (E', S').

6. Analysis of Our Protocols

In this section, we give our results in terms of security analysis and efficiency performance of our proposed blind signature protocols.

6.1. Correctness

- *Theorem 1*. (blind DS): The signature (R', S') is a valid DS corresponding to the message M.
- *Proof*. Indeed, we get:

$$\begin{aligned} S^* &= Y^{E'} R' \bmod p = Y^{E-\varepsilon} R' \bmod p = \\ & Y^{E} R Y^{-\varepsilon} \sigma^{-k} \sigma^{k} \bmod p = Y^{E} R \sigma^{k} \bmod p = \\ &= (x^{E} t)^{k} \sigma^{k} \bmod p = (S\sigma)^{k} \bmod p = S'^{k} \bmod p = S_k \\ & \Rightarrow S^* = S_k \end{aligned} \tag{2}$$

Thus, the protocol works correctly and the described procedure results in the DS (R', S') that is known for user B and unknown for signer A.

- *Theorem 2*. (blind CDS1): The signature (E', S') is a valid CDS1 corresponding to the message M.
- *Proof*. Indeed, using the collective public key $Y = \prod_{i=1}^{n} y_i^{\,y_i} \bmod p$ we get:

$$\begin{aligned} R^* &= S'^{k} Y^{-E'} \bmod p = S^{k} \sigma^{k} Y^{-(E-\varepsilon)} \bmod p \\ &= (S^{k} Y^{-E}) \sigma^{k} Y^{\varepsilon} \bmod p = R Y^{\varepsilon} \sigma^{k} \bmod p = R'. \\ & \Rightarrow E^* = h(M||R^*||Y) = E' \end{aligned} \tag{3}$$

Thus, the protocol works correctly and the described procedure results in the CDS1 (E', S') that is known for user A and unknown for each of the signers.

- *Theorem 3*. (blind CDS2): The signature (E', S') is a valid CDS2 corresponding to the message $M = m_1||m_2|| \dots ||m_n$.
- *Proof*. Indeed, using the collective public key $Y = \prod_{i=1}^{n} y_i^{\,y_i} \bmod p$ we get:

$$\begin{aligned} R^* &= S'^{k} Y^{-E'} \bmod p = S^{k} \sigma^{k} Y^{-(E-\varepsilon)} \bmod p \\ &= (S^{k} Y^{-E}) \sigma^{k} Y^{\varepsilon} \bmod p = R Y^{\varepsilon} \sigma^{k} \bmod p = R'. \\ & \Rightarrow E^* = h(M||R^*||Y) = E' \end{aligned} \tag{4}$$

Thus, the protocol works correctly and the described procedure results in the CDS2 (E', S') that is known for user A and unknown for each of the signers.

6.2. Unlinkability

- *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.
- *Theorem 4*. (blind DS): The protocol provides unlinkability property in the case when the message M and signature (R', S') will be presented to the signer.
- *Proof*. Let (R_1, E_1, S_1) and (R_2, E_2, S_2), two different signatures, produced blindly and stored by some signer B.

In accordance with the equation of the signature verification procedure, we get following relations:

$$S^{k} = y^{E'} R' \bmod p \tag{5}$$

And:

$$S_1^{\,k} = y^{E_1} R_1 \bmod p \tag{6}$$

Dividing Equation 5 by Equation 6 we have:

$$\frac{R'}{R_1} = \left(\frac{S'}{S_1}\right)^{k} y^{E_1 - E'} \bmod p \;\Rightarrow\; R' = R_1 \sigma_1^{\,k} y^{\varepsilon_1} \bmod p.$$

Where $\varepsilon_1 = E_1 - E' \bmod N'$ and $\sigma_1 = S'/S_1$.

The last relation shows that the signature (R', S') could be produced after producing R_1 (in this case the supposed user A_1 had used the values ε_1 and σ_1). The same signature can be also produced by the user A_2 with some signer B from the triple (R_2, E_2, S_2), if the values $\varepsilon_2 = E_2 - E' \bmod N'$ and $\sigma_2 = S'/S_2$ were selected as random choice at round 2 of the protocol. Since the values σ and ε are selected at random, the signature could be produced from each of two considered triples as well as from each of the triple in the database, i.e., the unlinkability property (or blindness property) is provided by the protocol.

- *Theorem 5*. (blind CDS1 and blind CDS2): The protocol provides unlinkability property in the case when the message M and signature (E', S') will be presented to all or to one of the signers.

- *Proof*. We suppose that many different users present electronic messages to some given set of signers for blind signing. Suppose the signers have saved in a database all triples (E, S, R) appeared in the blind CDS procedures. Let (E_1, R_1, S_1) and (E_2, R_2, S_2) are two of such triples. Accordingly to the blind CDS protocol construction, the elements of the first triple satisfy the expression:

$$R_1 = S_1^{k} Y^{-E_1} \bmod p \tag{7}$$

The signature (E', S') satisfy the expression:

$$R' = S'^{k} Y^{-E'} \bmod p \tag{8}$$

Dividing Equation 8 by Equation 7 we have:

$$R'/R_1 = Y^{E_1 - E'} (S'/S_1) \bmod p,$$

Therefore $R' = R_1 Y^{\varepsilon_1} \sigma_1^{k} \bmod p$, where $\varepsilon_1 = E_1 - E' \bmod N'$ and $\sigma_1 = S'/S_1$.

Analogously, the signature (E', S') could be produced from the triple (E_2, R_2, S_2), if the values $\varepsilon_1 = E_1 - E' \bmod N'$ and $\sigma_1 = S'/S_1$ are selected at round 2 of the protocol. Since the values σ and ε are selected at random, the signature could be produced from each of two considered triples as well as from each of the triple in the database, i.e., the unlinkability property (or blindness property) is provided by the protocol.

6.3. Randomization

- *Randomization*: in a secure randomized blind signature scheme a user can not remove signer's randomizing factor.
- *Theorem 6*. (blind DS): the protocol provides randomization property.
- *Proof*. In the proposed protocol, attackers are infeasible to generate a valid signature (R', S') on behalf of the original signer. The signer selects a random value $t<p$-1 and computes $R=t^k \bmod p$ and sends R to the user A. To get a random value t from R is computationally infeasible, since finding k^{th} roots modulo p for sufficiently large prime k (such that k^2 divides p-1) is a computationally difficult problem. Therefore, in the proposed protocol, attackers cannot remove the random t from the corresponding signature (R', S') to the message M.
- *Theorem 7*. (blind CDS1 and blind CDS2): The protocols provide randomization property.

The proof is similar to the proof in the blind DS.

6.4. Unforgeability

- *Unforgeability*: it means that only the signer(s) can generate the valid signatures.
- *Attack 1*. (Outsider attack): intruder tries to derive the signature (E', S'), where $E' = h(M||R')$ and $S'^{k} = R' Y^{h(M||R')} \bmod p$, for a given message M by letting one of the values R' and S' fixed and finding the other one. For example, intruder selects R' and tries to figure out the value of S' satisfying $R' = S^{k} Y^{-E'} \bmod p$ and vise versa. The intruder first chooses at random the value R' and then computes the values E' and $S' = (R' Y^{E'})^{1/k} \bmod p$ only if difficult computational problem of finding roots modulo a prime in special case is breakable. The intruder first chooses at random value S' and then computes R' from the equation $S'^{k} = R' Y^{h(M||R')} \bmod p$ only if the hash function $h(\cdot)$ is insecure (i.e., $h(\cdot)$ is breakable).
- *Attack 2*. (User attack): user can know individual signatures but this doesn't endamage the security of the protocols. If he can't compute the blind CDS correctly from the individual signatures the verification equation of the blind CDS is not satisfied and thus this kind of attack can be detected by the verifier.
- *Attack 3*. (Signer(s) attack): suppose that n-1 signers that share some multisignatue (R, S) with the nth signer are attackers trying to calculate the secret key of the nth signer. The attackers know the values r_n and s_n generated by the n^{th} signer. This values satisfy the equation $r_n = s_n^{k} y_n^{-Ey_n} \bmod p$, where the value E is out of the attackers control. It is supposed that a secure hash function is used in the protocol, therefore the attackers are not able to select the value R producing some specially chosen value E. This means that, computing the secret key requires solving the finding roots modulo a prime in special case problem. If attackers determine the value of t_n (or x_n).
- *Attack 4*. (Signer(s) attack): suppose that n - 1 signers attempts to create a multisignatue (R, S) corresponding to n signers owning the public key $Y = Y' y_n^{y_n} \bmod p$, where $Y' = \prod_{i=1}^{n-1} y_i^{y_i} \bmod p$, i.e., n - 1 users unite their efforts to generate a pair of numbers (R, S) such that $R = S^k Y^{-E} \bmod p = S^k (Y' y_n^{y_n})^{-E} \bmod p.$ Suppose that they are able to do this. Thus, under our assumption the group forger (i.e., the considered n-1 users) is able to calculate a multisignatue (R^*, S^*) corresponding to public key $Y = Y' y_n'^{y_n'} \bmod p$, where y'_n is some hypothetic public key having the value $y_n'^{y_n'} = y_n^{y_n} (Y')^{-1} \bmod p.$ It is an extremely difficult problem to find y'_n [9].

6.5. Performance

The security of Moldovyan's signature scheme had been proven to be computationally equivalent to the finding roots modulo a prime in special case problem [15]. In this paper, we construct protocols in the case of minimum security level that can be estimated at present as 2^{80} modulo exponentiation operations [14]. Taking into account that methods the $O(2^{80})$ difficulty of finding the k^{th} roots mod p is provided, if the primes k and p have the length $|k| \geq 160$ bits and $|p| \geq 1024$ bits. Sufficiently large size of the modulus p defines sufficiently large size of the signature in our protocols based on the mentioned difficult problem. In the best case the signature size is equal to 1184 bits.

For convenience, the following notation is used to facilitate the performance evaluation.

T_E denotes one modular exponentiation operation modular p.

T_M denotes one modular multiplication operation modular p.

T_H denotes the computation cost of the hash function h.

T_I denotes time for performing a modular inverse computation

Note that the time for computing modular addition and subtraction are ignored, since it is much smaller than T_E, T_M and T_H.

The comparisons of the numbers of computations performed by a user between the proposed blind DS and the schemes of [5, 16, 18, 20, 22] are summarized in Table 1.

Table 1. Computations required for a user to obtain and verify a signature.

	Blind DS	[5]	[20]	[16]	[22]	[18]
Numbers of Exponentiations	$4T_E$	$4T_E$	$6T_E$	$3T_E$	$11T_E$	$6T_E$
Numbers of Inverses	0	$2T_I$	0	$3T_I$	$4T_I$	$1T_I$
Numbers of Hashings	$1T_H$	0	$2T_H$	$1T_H$	$4T_H$	$2T_H$
Numbers of Multiplications	$4T_M$	$6T_M$	$5T_M$	$8T_M$	$13T_M$	$6T_M$

The comparisons of the numbers of computations performed by a user between the proposed blind CDS1, blind CDS2 and the schemes of [17] are summarized in Table 2.

Table 2. Computations required for a user to obtain and verify a signature.

	Blind CDS1	Blind CDS2	[17]
Numbers of Exponentiations	$4T_E$	$4T_E$	$4T_E$
Numbers of Inverses	0	0	0
Numbers of Hashings	$2T_H$	$(n+2)T_H$	$2T_H$
Numbers of Multiplications	$4T_M$	$4T_M$	$4T_M$

In most of the applications based on blind signatures, the signer(s) usually possesses much more computation capabilities than a user, while the computation capabilities of the users are limited in some situations such as mobile clients. 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(s).

In our blind CDS protocols the user performs the same computation operations as in the prototype blind DS scheme, i.e., in the scheme put into its base.

7. Conclusions

In this paper, a new blind DS and two novel blind CDS protocols has been designed using the computational difficulty of finding roots modulo a prime in special case. The protocol uses the procedure of blind generation of the DS by a signer or set of the signers. Independent of the number of the signers it is produced a single signature having the fixed size, namely 1184 bits in the case of 80-bit security

The proposed protocols provide parallel process for generating the blind collective signature. It seems that such primitives are attractive for applications in the electronic money systems in which the electronic banknotes are issued by one or several banks.

References

[1] Berezin A., Moldovyan N., and Victor S., “Cryptoschemes Based on Difficulty of Simultaneous Solving Two Different Difficult Problems,” *Computer Science Journal of Moldova*, vol. 21, no. 2, pp. 280-290, 2013.

[2] Boldyreva A., *International Workshop on Theory and Practice in Public Key Cryptography*, Springer Berlin Heidelberg, 2003.

[3] Boyd C., *Cryptography and Coding*, Oxford University Press, 1989.

[4] Brands S., *Advances in Cryptology-CRYPTO’93, Lecture Notes in Computer Sciences*, Springer-Verlag, 1993.

[5] Camenisch J., Piveteau J., and Stadler M., *Advances in Cryptology-EUROCRYPT ’94*, Springer-Verlag, 1995.

[6] Chaum D., *Advances in Cryptology-CRYPTO’82*, Springer Berlin Heidelberg, 1983.

[7] Chaum D., *SMART CARD 2000*, Elsevier Science, 1989.

[8] Hwang M. and Lee C., “Research Issues and Challenges for Multiple Digital Signatures,” *International Journal of Network Security*, vol. 1, no. 1, pp. 1-7, 2005.

[9] Hwang S., Hwang M., and Tzeng S., “A New Digital Multisignature Scheme With Distinguished Signing Authorities,” *Journal of Information Science and Engineering*, vol. 19, no. 5, pp. 881-887, 2003.

[10] Itakura K. and Nakamura K., “A Public-Key Cryptosystem Suitable for Digital Multisignatures,” *NEC Research and Dev*elopment, vol. 71, no. 1-8, 1983.

[11] Koblitz N., *A Course in Number Theory and Cryptography*, Springer-Verlag, 2003.

[12] Lin C., Wu T., and Hwang J., *Advances in Network and Distributed Systems Security*, Springer US, 2001.

[13] Lu S., Ostrovsky R., Sahai A., Shacham H., and Waters B., *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 2006.

[14] Menezes A., Oorschot P., and Vanstone S., *Handbook of Applied Cryptography*, CRC Press, 1996.

[15] Moldovyan N., "Digital Signature Scheme Based on a New Hard Problem," *Computer Science Journal of Moldova*, vol. 16, no. 2, pp. 163-182, 2008.

[16] Moldovyan N., "Blind Signature Protocols from Digital Signature Standards," *The International Journal of Network Security*, vol. 13, no. 1, pp. 22-30, 2011.

[17] Moldovyan N. and Moldovyan A., "Blind Collective Signature Protocol Based on Discrete Logarithm Problem," *International Journal of Network Security*, vol. 12, no. 1, pp.44-51, 2011.

[18] Minh N., Binh D., Giang N., and Moldovyan N., "Blind Signature Protocol Based on Difficulty of Simultaneous Solving Two Difficult Problems," *Journal of Applied Mathematical Sciences*, vol. 6, no. 139, pp. 6903-6910, 2012.

[19] Ohta K. and Okamoto T., *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 1991.

[20] Pointcheval D. and Stern J., *Advances in Cryptology*, Springer Berlin Heidelberg, 1996.

[21] Selvakumaraswamy S. and Govindaswamy U., "Efficient Transmission of PKI Certificates using ECC and its Variants," *the International Arab Journal of Information Technology*, vol. 13, no. 1, pp. 38-43, 2016.

[22] Tahat N., Ismail E., and Ahmad R., "A New Blind Signature Scheme Based on Factoring and Discrete Logarithms," *International Journal of Cryptology Research*, vol. 1, no. 1, pp. 1-9, 2009.

Minh Hieu is a Lecturer with the Academy of Cryptography Techniques (Ha Noi, Viet Nam). His research interests include cryptography, communication and network security. He has authored or co-authored more than 65 scientific articles, books chapters, reports and patents, in the areas of his research. He received his Ph.D. from the Saint Petersburg Electrical Engineering University (2006).

Hai Nam was born in 1961. He is a Lecturer with the Academy of Cryptography Techniques (Ha Noi, Viet Nam). His research interests include cryptography, communication and network security. He has authored or co-authored more than 25 scientific articles, books chapters, reports and patents, in the areas of his research. He received his Ph.D. from the Hanoi University of Science and Technology (1996).

Moldovyan Andreevich was born in 1953. He is a honored inventor of Russian Federation (2002), a laboratory head at St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, and a Professor with the St. Petersburg State Electrotechnical University. His research interests include information security and cryptology. He has authored or co-authored more than 70 inventions and 230 scientific articles, books, and reports. He received his Ph.D. from the Academy of Sciences of Moldova (1981).

Giang Tien was born in 1977 in Viet Nam. He received his MSc degree in computer science from Le Quy Don Technical University, Viet Nam, in 2011. His current research interests include information security, cryptographic protocols, wireless security, and electronic commerce.