Journal of Engineering and Applied Sciences 2 (1): 230-235, 2007

A New Forward-Secure Blind Signature Scheme

[1]Hui-Feng Huang and [2]Chin-Chen Chang
[1]Department of Information Management,
National Taichung Institute of Technology, Taichung 404, Taiwan, R.O.C.
[2]Department of Information Engineering and Computer Science,
Feng Chia University, Taichung 40724, Taiwan, R.O.C.

Abstract: In October, 2003, Duc. *et al*. proposed the new concept of a forward-secure blind signature scheme which preserves the validity of past signatures and which prevents a forger from forging past signatures even if the current secret key has been compromised. Today, to guarantee the quality of the growing and popular communication services on the Internet, it is necessary to reduce the computation load and communication costs for both parties of the signer and the requesters. This study proposes a new efficient method to implement the forward-secure blind signature. Because of its simple algorithm and fewer parameter requirements, our scheme is more efficient than Duc. *et al*.'s scheme. Moreover, only five modular multiplications are required for our key update procedure. The fast key update algorithm is very useful in some electronic applications.

Key words: Blind signature, forward-secure blind signature, electronic cash system

INTRODUCTION

The purpose of the digital signature is to establish the identity of the document's signer. If the secret key of a signer is compromised, then all of the past signatures become worthless since it is possible for a signer to deny ever signing a message by claiming that the private key has been compromised. Ordinary digital signatures have this limitation. Several practical forward-secure signature schemes which are considered to be either extensions of specific digital signature schemes or generic constructions from available digital signature schemes have recently been proposed[1-4]. The goal of these forward-secure signature schemes is to preserve the validity of past signatures and to prevent a forger from forging signatures from past time periods even if a current secret key has been compromised. This is achieved by dividing the total time into T periods and by using a different secret key in each time period. That is, the number of the time periods is part of the signature. Therefore, during signature verification, a signature with incorrect time periods should not be verified.

An interesting extension of a digital signature is the blind signature. The blind signature technique was first introduced by Chaum[5] to protect the right of an individual's privacy. It is a special form of a digital signature. Creating a blind signature for a message involves two parties, which we call the signer and a group of signature requesters. A requester requests the signer to sign on a blinded data. This means that the signer does not know the content of the message. The requester then unblinds the signed message from the signed blinded data. The signer's signature on the message can be verified by checking if the corresponding public verification formula with the signature-message pair as the parameter is true.

In a secure blind signature scheme, the signer is unable to link (trace) this signed message to the previous signing process instance. This property is usually referred to as the unlinkability property. Due to the unlinkability (blindness) property, blind signature techniques have been widely used in the anonymous electronic cash and anonymous voting systems.

We now consider the key problem of exposure in the use of blind signatures which is a very serious problem. For example, in the electronic cash system, a bank is the signer and the customers are the requesters (users). When an attacker steals the secret key of a bank, the attacker of course can generate as much valid electronic cash as he wants. Nobody can trust the signature that is generated with the stolen key. Then, people who have withdrawn their electronic cash but have not spent it, or who were paid electronic cash but have not deposited it, will lose their money. Therefore, the problem is severe

Corresponding Author: Hui-Feng Huang, Department of Information Management, National Taichung Institute of Technology, Taichung 404, Taiwan, R.O.C.

since money is directly involved. To minimize the potential damages, in October, 2003, Duc. et. al[6] first proposed the forward-secure blind signature scheme which based on the Okamoto-Guillou-Quisquater (OGQ) blind signature scheme[7,8]. Their scheme uses the same concept of the forward-secure signature. It is also achieved by using a different secret key for each time period and preferably keeps the "master" public key unchanged over its lifetime. The number of the time periods is part of the signature. Therefore, during signature verification, a signature with incorrect time periods should not be verified. In any case, for the sake of forward secrecy, it should be infeasible to compromise a secret key that was used in the past if the current secret key has already been revealed.

Basically, Duc. *et al.*[6] forward-secure blind signature scheme is the same as an ordinary blind signature scheme. The only difference is that there are time periods and a key update algorithm in the forward-secure blind signature. Because the key update algorithm is public and the "master" public key is unchanged over its lifetime, the verifier does not need to maintain the certificates of the secret key in each time period. However, Duc. *et al.*'s scheme is not efficient for both the signer and the requester.

Today, to guarantee the quality of the growing and popular communication services on the Internet, it is necessary to reduce the computation load and communication costs for both parties of the signer and the requesters. Using the concept of Chaum's blind signature[5], we proposed a new forward-secure blind signature scheme which is more efficient than Duc. *et al.*'s scheme. The goal of the forward-secure blind signature scheme is also to preserve the validity of past signatures even if the current secret key has been compromised. Because of its simple algorithm and fewer parameter requirements, our scheme has less round complexity than Duc. *et al.*'s scheme does. In addition, only five modular multiplications need to be performed in our key update procedure. That is very fast. The fast key update algorithm is important since it can reduce potential damages in some applications.

THE PROPOSED FORWARD-SECURE BLIND SIGNATURE SCHEME

In our forward-secure blind signature scheme, we divide the total time into T periods with a fixed "master" public key and we use a different secret key in each time period so as to attain forward-security. The time is not necessarily a real time. The maximum number of (expired) time periods T should not be considered as a limitation of the system. For example, if each time period represents a day, then T = 3600 denotes roughly ten years. Our scheme consists of four stages: key generation, key update algorithm, signature generation and signature verification. Since the key update algorithm is public and the master public key is fixed, nothing can be certified for a per-period secret (public) key.

Based on RSA[9], the system first chooses two large secure primes p_1 and q_1. Here another two primes p and q have to be formed, such that $p = 2p_1+1$ and $q = 2q_1+1$. N is a public RSA modulus for the system, where N. Thus, $N = p\times q$ is Euler's phi-function. Next, the system selects the private key $d \in Z^*_{\phi(N)}$. Its corresponding public key is e such that $e\times d = 1 \mod \phi(N)$. Then, the parameters N and e are published and the parameters d, p, q and $\phi(N)$ are kept secret by the system. We depict these four stages as follows.

Key generation

- Choose a master public key V, where V is a large prime.
- Select two random integers r and K such that $K > r\times t$, where r is an even integer and K is an odd integer.
- Let $a_1 = d$and the initial secret key $s1 = a_1(K+r)V = d(K+r)V \mod \phi(N)$.
- Finally, let the public key be $pk = \{N,V,K,e,r\}$. The signer uses the secret key s_1 and the requester uses the current public key $t_1 = e$ and the public key (N,V,K,t_1,r) for the signature in the initial time period.

Key update: In the j-th time period, the signer computes $a_j = a_{j-1}\times d$ (i.e. $a_j = d^j$), the secret key $s_j = a_j (K+r\times j)V = d^j (K+r\times j)V \mod\phi(N)$ and the public key $t_j = t_{j-1}\times e = e^j$ for $j = 2,3,..,T$. We note that the value $(K+r+j)$ is odd integer for $j = 1,2,3,...,T$, because r is an even integer and K is an odd integer.

Then, the signer uses the secret key s_j and the requester uses the public key (N,V,J,tj,r) for the current time period $j \leq T$.

Signature generation: According to Chaum's blind signature scheme[5], there are two kinds of participants, a signer and a group of requesters (users). Users request signatures from the signer and the signer issues blind signatures to the users. The protocol for issuing blind signatures is given as follows for each time period i.

Blinding: For each time period i, a user chooses a message m and randomly selects an integer $R \in Z^*_N$. Then, the user computes and submits $\alpha = R^{ti}\, h(i,m) \mod N$ to the signer, where t_i is signer's public key in the i-th time period.

Signing: After receiving α, the signer computes $c = \alpha^{si} \mod N$ and sends the integer c to the user, where s_i is signer's secret key in the i-th time period.

Unblinding: After receiving c, the user performs the unblinding process to obtain $z = R^{-(K+ri)V} \mod N$. The integer z is the signer's signature on m for the time period i.

Here, h ( ) denotes a publicly known one-way hash function. Moreover, $h(i,m)<\min(p,q)$ where i and m denote the input strings and min(p, q) denotes the minimal one of p and q. We can also properly select K and r such that $(K+ri)<\min(p_1,q_1)$.

Signature verification: This process makes sure that z is the signer's valid signature for message m in the time period i. The signature z can be verified by checking if $z^{ti} = h(i,m)^{(K+rj)V} (\mod N)$, where $t_j = e^j$.

We give the following theorem to examine the correctness of the proposed method.

Theorem 1: When the proposed scheme is used, if z is the signature on message m in the time period i, then $z^{ti} = h(i,m)^{(K+rj)V} \mod N$ holds.

Proof: In the proposal, $s_i = d^i (k+ri)V \mod \phi(N)$, $t_i = e^i \mod \phi(N)$ and $z = R^{-(K+2i)V} c \mod N$. On the other hand, $c = \alpha^{si} \mod N$, where $\alpha = R^{ti}\, h(i,m) \mod N$. Thus, we have

$$c = \alpha^{s_i} = R^{t_i \times s_i} h(i,m)^{s_i} = R^{d^i \times e^i (K+ri)V} h(i,m)^{s_i}$$

$$= R^{(K+ri)V} h(i,m)^{s_i} \mod N, \text{where } e \times d = 1 \mod \phi(N)$$

Therefore,

$$z^{t_i} = R^{-(K+ri)Vt_i} c^{t_i} \quad (\mod N)$$

$$= R^{-(K+ri)Vt_i} R^{(K+ri)Vt_i} h(i,m)^{s_i \times t_i} \quad (\mod N)$$

$$= h(i,m)^{s_i \times t_i} \quad (\mod N)$$

$$= h(i,m)^{d^i \times e^i \times (K+ri)V} \quad (\mod N)$$

$$= h(i,m)^{(K+ri)V} \quad (\mod N), \text{where} e \times d = 1 \mod \phi(N)$$

Hence, the theorem is proved.

SECURITY ANALYSIS

In this stydy, we discuss the security of our forward-secure blind signature scheme. Based on the RSA, the security of our scheme lies with the difficulty of factorization problems. N is a public RSA modulus for our system, where $N = p \times q$, $p = 2p_1+1$ and $q = 2q_1+1$. If an intruder can easily factor the integers p and q from $N = p \times q$, then he can derive the secret parameter d from the public key e because $d \times e = 1 \mod \phi(N) = 1$. In this situation, the attacker can compute the secret key $s_j = d^j(K+r \times j)V \mod \phi(N)$ for the time period j = 1,2,...,T. Thus, the proposed method would be insecure. For our scheme to be more secure, N should be large enough to make factorization difficult. Therefore, we suggest that $|N| \approx 1024$ and $|p|=|q|$. Without knowing the parameter $\phi(N)$, no one can masquerade the signer to create all the secret keys for different time periods and then forge a signature for any given message. An intruder may try to attack the proposed schemes by using different strategies. We will show that all attacks on our schemes will fail.

- Given a pair of valid blind signatures z_1 and z_2 for messages m_1 and m_2 produced by the proposed protocol in the time period i, respectively, we have $z_1^{t_i} = h(i,m_1)^{(K+ri)V} \mod(N)$ and $z_2^{t_i} = h(i,m_2)^{(K+ri)V} \mod(N)$, where $t^i = e^i$. Therefore, $(z_1 z_2)^{t_i} = (h(i,m_1)h(i,m_2))^{(K+ri)V} \mod(N)$. If an intruder computes $z_3 = z_1 \times z_2 \mod N$ and tries to derive the valid signature for a message, then he has to find out m_3 such that $h(i,m_3) = h(i,m_1) \times h(i,m_2)$. In this situation, the intruder obtains the signature z_3 for m_3. That is, $(z_3)^{t_i} = h(i,m_3)^{(K+ri)V} \mod(N)$. However, m_3 is protected in the one-way hash function h( ), so the probability of obtaining m_3 such that $h(i,m_3) = h(i,m_1) \times h(i,m_2)$, is equivalent to performing an exhaustive search on m_3.
- Suppose a private key $s_i = d^i (K+ri)V$ has been exposed. In this case, one can compute $s_i \times e^{i-1} = d^i (K+ri)V \times e^{i-1} d(K+ri)V \mod \phi(N)$, but it does not help an attacker to compute $((K+ri)V)^{-1}$ because $\phi(N)$, is unknown. Because the value $((K+ri)V)^{-1} \mod \phi(N)$ is unknown, the attacker cannot derive the secret key d from $s_i \times e^{i-1} = d (K+ri)V$. On the other hand, if the attacker computes $(s_i)^f V^{-(f-1)} = d^{f \times i} (K+ri)^f V \mod \phi(N)$ and tries to obtain the secret key for the (f×i)th period, then he has to find the values V^{-1} and f such that $(s_i)^f V^{-(f-1)} = df^{\times i}(K+ri)^f V = d^{f \times i} (K+r \times f \times i) \mod \phi(N)$. That is, $(K+r \times i)^f = (K+r \times f \times i) \mod \phi(N)$. However, $\phi(N)$ is unknown so that computing $V^{-1} \mod \phi(N)$ and f is infeasible. Thus, the attacker cannot derive the other secret keys sj for the time period $j \neq i$. Therefore, the past sessions are safe and the future sessions are safe. In other words, forward security is provided.

- Assume that the private keys s_j and $s_j (T > j > i)$ have been exposed and suppose that they have $s_i | s_j$. Then, an intruder can directly compute $\frac{s_j}{s_i} = \frac{d^j (K+rj)V}{d^i (K+ri)V} = d^{j-i} \times \frac{(K+rj)}{(K+ri)} \bmod \phi(N)$ and try to obtain the secret parameter d^{j-i}. In our method, since $K > r \times t$, the value $[(K+rj)/(K+ri)]$ is not an integer for any given $i < T$ and $j < T$. In this case, it is impossible to have the property $[(K+rj)/(K+ri)] | s_j/s_i$ for any given $i < T$ and $j < T$. Thus, the intruder has to derive $[(K+rj)/(K+ri)]^{-1} \bmod \phi(N)$ so as to obtain the value $d^{j-i} \bmod \phi(N)$. However, $\phi(N)$ is unknown so that the intruder cannot compute $[(K+rj)/(K+ri)]^{-1} \bmod \phi(N)$. Without knowing $[(K+rj)/(K+ri)]^{-1} \bmod \phi(N)$, the intruder cannot obtain the secret parameter d^{j-1}. On the other hand, we suppose that $j = u \times i$, where u is an integer. Then one obtains $(si)^u V^{-v} = d^{u \times i} (K+ri)^u = d^j (K+ri)^u \bmod \phi(N)$ and $s^j V^{-1} = d^j (K+rj) \bmod \phi(N)$. If $(K+ri)$ and $(K+rj)$ are relatively prime to each other, then $(K+ri)^u$ and $(K+rj)$ are also relatively prime to each other. Therefore, when the Euclidean algorithm is applied,
  $a(si)^u V^{-u} + bs_j V^{-1}$
  $= a(K+ri)^u d^j + b(K+rj)d^j = d^j \bmod \phi(N)$ for some integers a and b. (1)
  In this study, the intruder can derive d^j and then obtain the secret key d by computing $d = d^j \times e^{j-1}$, where $e \times d \bmod \phi(N)$. Then the attacker can generate all the secret keys $s^j = d^j (K + r \times j) V \bmod \phi(N)$ for $j = 1,2...,T$. However, $\phi(N)$ is unknown so that the intruder cannot compute $V^{-1} \bmod \phi(N)$. Without knowing V^{-1}, the intruder cannot derive dj from Eq. (1). Therefore, even if the private keys s_i and s_j have been exposed, the attacker also cannot obtain the past and future session keys.

Unlinkability: For every instance in the time period i, numbered j, of the protocol described in Section 2, the signer can record the transmitted information (α_j, c_j) between the signer and the user during the instance j of the protocol. The pair (α_j, c_j) is usually referred to as the view of the signer of the instance j of the protocol in the period i. To achieve the unlinkability property, for any given signature (z, m), no one expects that the requester will be able to link this signature to its previous instance of the signing process. In the following theorem, we show that our forward-secure blind signature preserves this property.

Theorem 2: For each time period i, given a pair (z, m) produced by the scheme of Section 2, the signer can derive R'_j for every (α_j, c_j) such that

$$\alpha_j = (R'_j)^{t_i} h(i,m) \bmod (N)$$

Proof: If there is an integer R'_j such that $z = (R'_j)^{-(K+ri)V} c_j \bmod N$, then one can obtain $(R'_j)^{(K+ri)V} z^{-1} c_j \bmod N$. According to the proposed method, we have $c_j = \alpha_j^{s_i} \bmod N$ for every (α_j, c_j). Hence, we can compute

$$(R'_j)^{(K+ri)V \times t_i} h(i,m)^{(K+ri)V} = (z^{-1} c_j)^{t_i} h(i,m)^{(K+ri)V} \bmod N$$
$$h(i,m)^{-(K+ri)V} \alpha_j^{t_i \times s_i} h(i,m)^{(K+ri)V} \bmod N$$
$$= \alpha_j^{(K+ri)V} \quad \bmod N \tag{2}$$

where $s_i = d_i (K+ri)V \bmod \phi(N)$ and $\bmod \phi(N)$.
From Eq. (2), we can obtain $\alpha_j^{(K+ri)V} = (R'_j)^{(K+ri)V \times t_i} h(i,m)^{(K+ri)V} \bmod N$ since $(K+ri)$ is an odd integer and less than $\min(p_1, q_1)$ and V is a prime integer. Hence, $(K+ri)V$ is relatively prime to $\phi(N) = 4p_1, q_1$. So the signer can find an integer, say w, such that $(K+ri)V \times w = 1 \bmod \phi(N)$. In this study, the signer can compute

$$\alpha_j^{(K+ri)V \times w} = (R'_j)^{(K+ri)V \times t_i \times w} h(i,m)^{(K+ri)V \times w} \bmod N \tag{3}$$

From Eq. 3, the signer obtains $\alpha_j = (R'j)^{ti} h(i,m) \bmod N$.

According to the above derivations, the signer can derive R'_j for every recorded α_j, c_j in each time period i.

Hence, given a pair (z, m) produced by the protocol described in the Section 2, the signer can always derive the blinding factor R'_j for every view in each time period i. This means that all of the signature-message triples are indistinguishable from the signer's point of view. Therefore, it is computationally infeasible for the signer to derive the link between an instance j of the protocol and the signature produced by that scheme.

PERFORMANCE AND COMPARISONS

This new concept of the forward-secure blind signature was first proposed by Duc *et al.*[6] in Oct. 2003. Their forward-secure blind signature extends the Okamoto-Guillou-Quisquater[7,8] blind signature scheme. With regards to efficiency, in order to clarify the comparison of our scheme with Duc *et al.*'s scheme, here, we briefly describe Duc *et al.*, s scheme below.

Key generation: First, the signer chooses two large secure primes p_1 and q_1. Here another two primes p and q have to be formed, such that $p = 2p_1+1$ and $q = 2q_1+1$ here $N = p \times q$ a public RSA modulus for the system. Thus, we have $\phi(N) = (p-1)(q-1)$. Next, the signer performs the following steps:

- Choose a random prime λ such that $(\lambda,\phi(N)) = 1$.
- Choose $r_0 = Z^*_\lambda$, $a\epsilon Z^*_N$ and $e\epsilon Z^*_N$.
- Compute the fixed master public key $V = a^{-r_0} s_0^{-\lambda} \bmod N$ and $f_1 = a^e \bmod N$, $v_1 = V^2 a^e = V^2 f_1 \bmod N$ and $l1 = 2\lambda_0 e/\lambda$ (we denote the division operation by a a÷, which gives the result as the quotient of the division).
- The signer computes the secret keys $r_1 = (2r_0\text{-}e) \bmod \lambda$ and $s_1 = a^1 s^2_0 \bmod N$ for the initial time.
- Finally, the public key is $pk = \{N,a,V,\lambda\}$. The signer uses these keys r_1,s_1 and v_1 and the requester uses the current public key (N,a,V,λ,f_1) for the signature in the initial time period.

Key update: In the (i+1)-th period, the signer computes $f_{i+1} = f^2_i\,\alpha_e \bmod N$, $v_{i+1} = v^2_i\,a^e = V^{2^{i+1}}\, f_{i+1} \bmod N$ and $li+1 = 2\lambda_i\text{-}e/\lambda$ and then derives the secret keys $r_{i+1} = (2r_i\text{-}e) \bmod \lambda$ and $s_{i+1} = a^{l_{i+1}} s_i^2 \bmod N$. Next, the signer uses these keys r_{i+1}, s_{i+1} and v_{i+1} and the user uses the public key (N,a,V,λ,f_{i+1}) for the signature in the (i+1)-th time period. The signature issuing protocol:

For each time period i, a user chooses a message m and then performs the following steps:

- The signer first chooses two random numbers $t\epsilon Z^*_\lambda$ and $u\epsilon Z^*_N$.
- The signer computes $x = a^t u^\lambda \bmod N$ and sends x to the requester (or user).
- After receiving x, the user selects three blinding factors α, $\gamma\epsilon Z^*_\lambda$ and $\beta\epsilon Z^*_N$.
- The user computes $x' = xa^\alpha\beta^\gamma v^\gamma_i \bmod N$, $c' = H(i|f_i|m|x')$ and $c = c' \bmod \lambda$. Then the user delivers c to the signer.
- After receiving c, the signer computes $y = (t+cr_i) \bmod \lambda$ and $z = a^w u s^c_i \bmod N$. Then the signer sends y and z to the user.
- Finally, the user computes $y' = y+\alpha \bmod \lambda$, $w' = y+\alpha/\lambda$, $w'' = c'\text{-}c/\lambda$ and $z' = a^{w'} v_i^{-w''} z\beta \bmod N$. Hence, (f_i,c',y',z') is a blind signature for m in the time period i.

Signature verification: To make sure (f_i,c',y',z') is a signature for m in the time period i, the verifier first computes $v_i = v^{2i} f_1 \bmod N$ and $x'' = a^{y'}(z')\lambda v^{c'}_i \bmod N$. Next, if the equation $c' = H(i|f_i|m|x'')$ holds, then (f_i,c',y',z') is a valid signature for m for the time period i.

For convenience, the following notations are used for the analysis of the computational complexity. T_e means the time for one exponentiation computation; T_i denotes the time for one inverse computation; T_m defines the time for one modular multiplication computation; and T_h denotes the time for executing the adopted one-way hash function in one's scheme. Note that the time needed for computing modular addition and subtraction is ignored, since it is much smaller than T_e,T_i,T_m and T_h.

Table 1:Comparisons of two forward-secure blind signature schemes

	Our scheme	Duc. et al. scheme
Computations for the requester	$2T_e+3T_m+T_i+T_h$	$6T_e+15T_m+T_h$
Computations for the signer	T_e	$4T_e+5T_m$
Computations for the signature verification	$2T_e+T_m+T_h$	$4T_e+3T_m+T_h$
Computations for the key update in each time period	$5T_m$	T_e+11T_m

We summarize the comparisons of our forward-secure blind signature scheme with Duc *et al.*, scheme[6] in Table 1. In our scheme, the computational complexity for the requester (user), the signer and the signature verification are 2 T_e+3 T_m+T_i+T_h,T_e and $2T_e+T_h+T_m$, respectively. It is more efficient than Duc *et al.*'s scheme. Also, as shown in Table 1, no modular exponentiation and inverse computations are required for the key update in our scheme; only five modular multiplications are required for the key update procedure. Compared with Duc *et al.*'s scheme, the proposed scheme can reduce a large number of computations required for the key update in each time period. Because the proposed scheme can provide a fast key update algorithm, the signer (bank) can provide more efficient and safe services to the signature requester. On the other hand, Duc *et al.*'s method requires three rounds of communications in the signature generation protocol. However, the proposed method requires only two rounds of communications. Hence, the proposal has less round complexity.

In addition, if we take away the time period and the key update algorithm, our forward-secure blind signature scheme can still be used in the same way as the ordinary blind signature schemes. And it only needs four extra space requirements for four random numbers T, K, r and V to update the secret key for each time period. The increased storage is not significantly affected by a comparison of the ordinary blind signature schemes. Since the master public key V remains the same over its lifetime, the proposed method does not certify the current public (secret) key for each time period. Thus, in our forward-secure blind signature scheme, both the signing protocol and the verification procedure are almost as efficient as in the ordinary blind signature schemes.

CONCLUSION

In this study, we proposed a novel forward-secure blind signature scheme based on Chaum's blind signature scheme. It preserves the validity of past signatures and prevents a forger from forging signatures for past time periods even if the current secret key has been compromised. In our scheme, both the signing protocol and the verification procedure are as efficient as the ones underlying ordinary blind signature schemes and the storage space for the keys and signatures is almost the same as in those ordinary blind signature schemes. Moreover, only five modular multiplications are required in our key update procedure and it has less round complexity in the signing generation stage. Hence, the fast key update algorithm and simple signing protocol make our scheme very attractive for electronic applications.

REFERENCES

1. Bellare, M. and S. Miner, 1999. A forward-secure digital signature scheme, advances in cryptology-CRYPTO'99, LNCS 1666, pp: 431-448.
2. Itkis, G. and L. Reyzin, 2001. Forward-secure signatures with optimal signing and verifying, advances in cryptology-CRYPTO 2001, LNCS 2139, pp: 332-354.
3. Guillou, L.S. and J.J. Quisquater, 1988. A Paradoxical Identity-Based Signature Scheme Resulting from Zero-Knowledge, Advances in Cryptolgy-CRYPTO, Springer-Verlag, LNCS 403, pp: 216-231.
4. Malkin, T., D. Micciancio and S. Miner, 2002. Efficient generic forward-secure signatures with an unbounded number of time periods, Advances in Cryptology-EUROCRYPT 2002, Springer-Verlag, LNCS 2332, pp: 400-417.
5. Chaum, D., 1982. Blind Signature for Untraceable Payments, Advances in Cryptology-CRYPTO'82, Plenum, pp: 199-204.
6. Duc, D.N., J.H. Cheon and K. Kim, 2003. A Forward-Secure Blind Signature Scheme Based on the Strong RSA Assumption, Proceedings of ICICS2003, Lecture Notes in Computer Science (ICICS2003), Springer-Verlag, LNCS 2836, pp: 11-21.
7. Pointcheval, D. and J. Stern, 1996. Provably Secure Blind Signature Scheme, Advances in Cryptology-ASICRYPT' 96, Springer-Verlag, LNCS 1163, pp: 252-265.
8. Okamoto, T., 1992. Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes, Advances in Cryptology-CRYPTO'92, Springer-Verlag, LNCS 740, pp: 31-53.
9. Rivest, R.L., A. Shamir and L. Adlemsan, 1978. A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of ACM, 21: 33-39.