International Journal of Innovative Computing, Information and Control
Volume **7**, Number **9**, September **2011**

 ISSN 1349-4198
pp. 5403–5416

A BLIND SIGNATURE BASED ON DISCRETE LOGARITHM PROBLEM

Victor R. L. Shen[1], Yu Fang Chung[2], Tzer Shyong Chen[3] and Yu An Lin[4]

[1]Department of Computer Science and Information Engineering
[4]Graduate Institute of Electrical Engineering
National Taipei University
No. 151, University Rd., San Shia District, New Taipei City 23741, Taiwan
rlshen@mail.ntpu.edu.tw

[2]Department of Electrical Engineering
[3]Department of Information Management
Tunghai University
No. 181, Section 3, Taichung Port Rd., Taichung City 40704, Taiwan
{ yfchung; arden }@thu.edu.tw

Received May 2010; revised September 2010

Abstract. *The concept of a blind signature scheme deals with the request that the signer should sign on a blind message. The characteristic of blind signatures is that the requester enables to derive the signature but the signer disables to link a pair of signatures when the requester releases the signature pair in public. This study proposes a new blind signature scheme based on the discrete logarithm problem and the generalized ElGamal-type digital signature scheme by Harn. With high security, the proposed blind signature scheme meets the requirements like correctness, blindness, unforgeability and untraceability.*
Keywords: Blind signature, Digital signature, Discrete logarithm problem

1. **Introduction.** Because the digital signature provides authentication, non-repudiation, data integrity and unforgeability within the world of modern cryptography, it has become a very important research topic [2]. Especially in the large network system, key distributions, authentications and electronic commerce can utilize the digital signature. The blind signature is a variant of the digital signature. In 1983, Dr. D. Chaum first proposed the concept of the blind signature and devised a scheme based on the RSA algorithm [6,8,26,34]. The blind signature can protect people's privacy within a network, especially in an electronic cash payment system [7] or electronic voting system [10]. In the digital signature scheme, there are two participants, namely, the signer and the verifier. The signer first uses a private key to sign a message and then sends this signature to the verifier. After the verifier receives the signature, he/she can use a public key to verify the legitimacy of the signature. In the blind signature scheme, there are three participants, namely, the requester, the signer and the verifier. First, the requester blinds the message and sends the blind message to the signer. After receiving the blind message, the signer can use a private key to sign it and send the blind signature back to the requester. Once the requester receives it, he/she "unblinds" the blind signature to obtain the signature and sends it to the verifier. After the verifier receives the signature, he/she can use a public key to verify the legitimacy of the signature.

The main differences between the digital signature and the blind signature are shown as follows [6,8].

(1) In the blind signature scheme, the content of the message should be blind to the signer.
(2) When the public knows the message-signature pair, the signer should not be able to trace the message-signature pair.

The blind signature schemes must meet the following requirements, namely, correctness, blindness, unforgeability and untraceability [6,13,19,20,33]. This paper provides details of these requirements in Section 2 and proposes a novel blind signature scheme based on the discrete logarithm and the generalized ElGamal type digital signature scheme [17]. This study proposes the blind signature scheme that can be useful for private protection of the Internet. The organization of the rest of this paper is described as follows.

Section 2 is a review of the literature and a presentation of the hash function, public cryptosystems, including RSA public cryptosystem [26] and ElGamal public cryptosystem [12], RSA digital signature, and ElGamal digital signature. In the last subsection of Section 2, it presents the research of the blind signature. In Section 3, it proposes the blind signature scheme based on discrete logarithm and the generalized ElGamal type digital signature. In Section 4, it examines the requirements, namely, correctness, blindness, unforgeability and untraceability of a digital signature. The conclusion and the future work for this research are described in Section 5.

2. Related Work.

In this section, the hash function [3], public cryptosystem [11], digital signature [2], the concept of blind signature [6,8] and other related blind signature schemes are introduced.

2.1. Hash function.

The hash function plays an important role in modern cryptography. The hash function $h(g)$ of this equation $h = h(m)$ generates a hash value of h. The value m is a variable-length message and the hash value h is the fixed-length message digest. Electronic mails, message authentication and other applications widely deploy the hash function [29].

The requirements for a hash function used in digital signatures [24] are listed as follows.

(1) A block of data of any size can be applied to the hash function $h(g)$ and produces a fixed-length output (message digest).
(2) The hash function $h(m)$ is relatively easy to compute for any given m, making both hardware and software implementations practical.
(3) The hash function used in digital signature must be a one-way hash function. For collision resistance, it is computationally infeasible to find any pair (m_1, m_2) such that $h(m_1) = h(m_2)$.
(4) Public cryptosystems always use the hash function. By using the hash function in public cryptosystem, it can reduce the computation time and increase the efficiency. Therefore, the hash function also plays an important role in the public cryptosystem, digital signature and blind signature.

2.2. Public cryptosystem based on factoring problem and discrete logarithm problem.

In 1976, Dr. W. Diffie and Dr. M. Hellman proposed the concept of a public key cryptosystem [11]. Factoring problems or discrete logarithms are the base for the public cryptosystem. RSA public cryptosystem [26] is based on factoring problem. Discrete logarithm is the basis for the ElGamal public cryptosystem [12]. In this subsection, the RSA public cryptosystem and ElGamal public cryptosystem were briefly presented.

(1) RSA Public-key Cryptosystem: In 1978, R. L. Rivest, A. Shamir and L. Adleman proposed RSA public cryptosystem based on factoring problem [26]. The process was presented in the following. In RSA public cryptosystem, there were two participants,

namely, the receiver and the sender. In the following example, the receiver is called Alice, and the sender Bob. During the key generation phase, Alice chooses two big primes p and q, and computes $n = p * q$, $\phi(n) = (p-1) * (q-1)$. Then, she chooses an integer e, such that $1 < e < \phi(n)$ and $GCD(e, \phi(n)) = 1$, and computes $d = e^{-1}(\mathrm{mod}\phi(n))$. She obtains two keys, namely, public key (e, n) and private key (d, n). Bob wants to send the message M to Alice and uses Alice's public key to encrypt the message M, and then he gets the cipher text C ($C = M^{\varepsilon} \bmod n$) and sends it to Alice. When Alice receives the cipher text C, she can use the private key to decrypt cipher text C. She then receives the message M ($M = C^d \bmod n$). The factoring problem was the basis for the security of RSA public cryptosystem. In the RSA public cryptosystem, the signer must keep the values p, q and $\phi(n)$ secure. In D. Boneh's paper [4], he suggested that the length of n should be greater than 1024 bits, and the two primes p and q differ in length by only few bits. In addition, the value d could not be less than $n^{1/4}$. If $d < n^{1/4}$, d was easily determined [31].

(2) ElGamal Public-key Cryptosystem: Dr. T. ElGamal proposed the ElGamal public cryptosystem [12], based on the discrete logarithm problem, in 1985. In the ElGamal public cryptosystem, there were two participants, namely, the receiver and the sender. For example, the name of the receiver is Alice, and the sender is Bob. First, Alice chooses a big prime p and α, the primitive root of p. She then randomly chooses the value x ($x < p$) and computes $y = \alpha^x \bmod p$. She obtains the public key (y, α, p) and the private key x. Bob wants to send the message M to Alice, so he chooses a random number k ($0 \le k \le p-2$) and computes $a = \alpha^k \bmod p$, $b = y^k M \bmod p$. After computation, he sends (a, b) to Alice. When Alice receives (a, b), she can use the private key to decrypt the message M ($M = b * (a^x)^{-1}(\mathrm{mod}p)$).

2.3. **Digital signatures.** The digital signature plays a very important role in modern cryptography. A digital signature can provide the following requirements, namely, authentication, non-repudiation, data integrity and unforgeability. In this subsection, the RSA digital signature and ElGamal digital signature are briefly described.

(1) RSA Digital Signatures: R. L. Rivest, A. Shamir and L. Adleman proposed RSA digital signature [26] in 1978. The sender, Alice, wants to sign the message M and sends the signature to the receiver, Bob. Alice has a public key (e, n), a private key, (d, n) and a hash function $h(g)$. Alice computes $s^* = h(M)^d \bmod n$ and sends the message-signature pair (M, s^*) to Bob. When Bob receives the message-signature pair (M, s^*), he can use the public key (e, n) and hash function $h(g)$ to compute $V_1 = h(M) \bmod n$ and $V_2 = (s^*)^{\varepsilon} \bmod n$. If $V_1 = V_2$, the verification then passes; else the verification fails.

(2) ElGamal Digital Signature: As stated previously, the discrete logarithm problem was the basis for the ElGamal digital signature [12]. The sender Alice wants to sign the message M and send to the receiver, Bob. Alice has the public key (y, α, p), a private key x and a hash function $h(g)$. Alice randomly selects an integer k, such that $GCD(k, \phi(p)) = 1$, then she computes $r = \alpha^k \bmod p$ and $s^* = k^{-1}(h(M) - ar) \bmod \phi(p)$. After computation, she sends the digital signature $s = (M, r, s^*)$ to Bob. When Bob receives the digital signature $s = (M, r, s^*)$, he can use the public key (y, α, p) to compute $V_1 = y^r r^{s^*} \bmod p$ and $V_2 = g^{h(M)} \bmod p$. If $V_1 = V_2$, then the verification passes; else the verification fails.

(3) Generalized ElGamal Type Digital Signature Scheme Based on Discrete Logarithm: L. Harn and Y. Xu proposed the generalized ElGamal type digital signature based on discrete logarithm problem in 1994 [17]. In their research, without loss of generality, they expressed the generalized equation for all ElGamal type digital signature

schemes as $ax = bk+c \bmod \phi(p)$. Where (a, b, c) were the three parameters from the set of values (m, r, s). In the discussion, each parameter could be a mathematical combination of (m, r, s). For instance, the parameter a could be rm or r, etc. The verification equation could be $y^a = r^b\alpha^c \bmod p$. In the following, this paper briefly presents the restrictions applied to parameters (a, b, c) for security considerations [17].

For the security reasons, parameters s and m cannot be combined with any of parameters (a, b, c). For instance, if the signature equation is $x = rk+sm \bmod \phi(p)$, then only by modifying the partial signature s of a legitimate signature (m, r, s) corresponding to the message m can it forge a signature (m', r, s') of another message m' $(m' = \beta m \bmod \phi(p))$ and $s' = \beta^{-1}s \bmod \phi(p)$. For security reasons, parameters s and r cannot be combined together. For example, if the signature equation is $mx = k + rs \bmod \phi(p)$, the verification equation is $y^m = r\alpha^{rs} \bmod p$. The attacker can randomly select an integer R and then computes r' to satisfy $y^m = r'\alpha^R \bmod p$. The forged signature is (m, r', s'), where $r's' = R \bmod \phi(p)$.

There must be three separate terms as specified in the signature equation. For instance, if the signature equation is $mx = rk + s \bmod \phi(p)$, then it can forge signature (m', r, s') for another message m', where $m-m' = \beta \bmod \phi(p)$ and $s' = (1-\beta(m+r)^{-1})s \bmod \phi(p)$. Based on the above considerations, L. Harn and Y. Xu proposed a complete list of 18 ElGamal type digital signature schemes as shown in Table 1 [17].

Table 1. Generalized ElGamal type signature schemes

	Signature Equation	Signature Verification Equation	Comment
1	$mx = rk + s \bmod \phi(p)$	$y^m = r^r\alpha^r \bmod p$	Harn scheme [15,36,37]
2	$mx = sk + r \bmod \phi(p)$	$y^m = r^s\alpha^r \bmod p$	
3	$rx = mk + s \bmod \phi(p)$	$y^r = r^m\alpha^s \bmod p$	
4	$rx = sk + m \bmod \phi(p)$	$y^r = r^r\alpha^m \bmod p$	ElGamal scheme [12]
5	$sx = rk + m \bmod \phi(p)$	$y^s = r^r\alpha^m \bmod p$	AMV scheme [1]
6	$sx = mk + r \bmod \phi(p)$	$y^s = r^m\alpha^r \bmod p$	
7	$rmx = k + s \bmod \phi(p)$	$y^{rm} = r\alpha^s \bmod p$	Schnorr scheme [27,35]
8	$x = mrk + s \bmod \phi(p)$	$y = r^{mr}\alpha^s \bmod p$	Yen and Laih scheme [32]
9	$sx = k + mr \bmod \phi(p)$	$y^s = r\alpha^{mr} \bmod p$	
10	$x = sk + rm \bmod \phi(p)$	$y = r^s\alpha^{rm} \bmod p$	
11	$rmx = sk + 1 \bmod \phi(p)$	$y^{rm} = r^s\alpha \bmod p$	
12	$sx = rmk + 1 \bmod \phi(p)$	$y^s = r^{rm}\alpha \bmod p$	
13	$(r + m)x = k + s \bmod \phi(p)$	$y^{r+m} = r\alpha^s \bmod p$	Harn scheme [16]
14	$x = (m + r)k + s \bmod \phi(p)$	$y = r^{(m+r)}\alpha^s \bmod p$	
15	$sx = k + (m + r) \bmod \phi(p)$	$y = r^{(m+r)}\alpha^s \bmod p$	
16	$x = sk + (r + m) \bmod \phi(p)$	$y = r^s\alpha^{r+m} \bmod p$	
17	$(r + m)x = sk + 1 \bmod \phi(p)$	$y^{r+m} = r^s\alpha \bmod p$	
18	$sx = (r + m)k + 1 \bmod \phi(p)$	$y^s = r^{(r+m)}\alpha \bmod p$	

2.4. **Blind signatures and applications.** Dr. D. Chaum introduced the concept of the blind signature [6] in 1983. The blind signature was a special form of digital signature because, unlike a normal digital signature scheme, the signer did not know the content of message in the signing phase. Because the blind signature could meet the following requirements, namely, correctness, blindness, unforgeability and untraceability

[6,13,19,20,33], the blind signature could protect people's privacy in the network transaction. In this subsection, Dr. D. Chaum's blind signature and other blind signatures based on factoring problems or discrete logarithm problems are presented.

(1) **The concept of blind signatures**: Dr. D. Chaum was the first scholar to propose the concept of the blind signature scheme in 1982 [6]. The blind signature scheme is a method, which guarantees the anonymity of the participants. The blind signature scheme as a cryptographic protocol contains two parties, namely, the requester A and the signer B. The requester A wants to obtain the signature of the signer B on the message M. First, A blinds the message M into M' and sends M' to B. B generates the s' on M' and returns s' to A. When the requester A receives the s', the requester unblinds s' into s and outputs s as the signature on the message M. In this scheme, A can protect the content of message M. In addition, whenever B assigns a signature pair of (M, s), B cannot determine when, or for whom he/she signed that message. This concept is widely used in electronic voting systems and electronic payment systems.

In the next year, Dr. D. Chaum proposed the blind signature scheme based on RSA [8]. In Chaum's blind signature scheme, there were three participants in this scheme, namely, the requester, the signer and the verifier. There were five phases in this scheme, including (1) initialization phase, (2) blinding phase, (3) signing phase, (4) unblinding phase and (5) verifying phase. The blind signature scheme is described as follows.

Initialization phase: The signer randomly chooses two large primes p and q and then computes $n = p * q$ and $\phi(n) = (p-1) * (q-1)$. The signer chooses large numbers $e(GCD(e, \phi(n)) = 1)$ and computes $d(d = e^{-1} \bmod \phi(n))$. Let (e, n) be the signer's public key, and (d, n) be the signer's private key. He/she then publishes (e, n) and a one-way hash function $h(g)$.

Blinding phase: The requester has a message m and wants to have it signed by the signer. The requester randomly chooses an integer r as the blinding factor, and then computes and sends $\alpha = r^{\varepsilon} gh(m) \bmod n$ to the signer.

Signing phase: When the signer receives α from the requester, the signer computes $t = \alpha^d \bmod n$ and sends t to the requester.

Unblinding phase: After receiving t from the signer, the requester computes $s = tgr^{-1} \bmod n$ and sends the message-signature pair (m, s) to the verifier.

Verifying phase: When the verifier receives the message-signature pair (m, s), the verifier can use $h(g)$ and (e, n) to verify the legitimacy of the signature by checking whether $s^{\varepsilon} \equiv h(m) \bmod n$ exists.

Over the past few decades of research work on blind signature, it has been found that the blind signature schemes must meet the following requirements, namely, correctness, blindness, unforgeability and untraceability [6,13,19,20,33].

Correctness: Everyone with the signer's public key can check the signature of the message signed by using the blind signature scheme.

Blindness: The content of the message should be blind to the signer. In other words, when the signer signs the message, he/she does not know the content of the message.

Unforgeability: The signature is the proof of the signer and no one else can derive any forged signature and pass verification.

Untraceability: The signer of the blind signature scheme is unable to link the message-signature pair even when the public can read the signature.

(2) **The blind signatures based on factoring problem**: H. Y. Chien, J. K. Jan and Y. M. Tseng proposed the blind signature based on the RSA algorithm in 2001 [9]. In the proposed blind signature schemes, there were three participants, namely, the

requester, the signer, and the verifier. The scheme consists of four phases, namely, (1) initialization, (2) requesting, (3) signing and (4) extraction and verification.

Initialization phase: The signer randomly chooses two large primes, p and q, and computes $n = p * q$ and $\phi(n) = (p-1)(q-1)$. The signer computes d such that $d = e^{-1} \bmod \phi(n)$, where $e = 3$. Let (e, n) be the signer's public key and (d, p, q) be the private key. The signer publishes (e, n) and also chooses a secure one-way hash function such as SHA-1 [25] or MD5 [3].

Requesting phase: According to the predefined format, the requester has a message m and the common information a. The requester also chooses two numbers, r and u, such that $r \in Z_n^*$ and $u \in Z_n^*$. Then, he/she computes $\alpha = r^{\varepsilon} h(m)(u^2+1) \bmod n$ and sends the tuple (a, α) to the signer. After receiving the tuple (a, α), the signer verifies the common information a. The signer then randomly chooses a positive integer x, less than n, and sends x to the requester. When the requester receives x from the signer, the requester randomly chooses an integer r' and lets $b = r * r'$. Then the requester computes $\beta = b^{\varepsilon}(u - x) \bmod n$ and sends β to the signer.

Signing phase: After the signer receives β from the requester, the signer computes $\beta^{-1} \bmod n$ and $t = h(a)^d(\alpha(x^2+1)\beta^{-2})^{2d} \bmod n$ and then sends (β^{-1}, t) to the requester.

Extraction and verification phase: Upon receiving (β^{-1}, t), the requester acquires the signature by computing $c = (ux+1) * \beta^{-1} * b^{\varepsilon} = (ux+1)(u-x)^{-1} \bmod n$ and $s = t * r^2 * r'^4 \bmod n$. The tuple (a, c, s) is a signature on the message, and the requester sends the message-signature pair $((a, c, s), m)$ to the verifier. The verifier can use the public key (e, n) to verify this message-signature pair by checking whether $s^{\varepsilon} \equiv h(a)h(m)^2(c^2 + 1)^2 \bmod n$ exists.

In 2003, M. S. Hwang, C. C. Lee and Y. C. Lai proposed an untraceable blind signature scheme [19] based on RSA and Extended Euclidean algorithm [3]. There were three participants in this scheme, namely, the requester, the signer and the verifier. The scheme contained five phases, including (1) initialization phase, (2) blinding phase, (3) signing phase, (4) unblinding phase and (5) verifying phase. The blind signature scheme is described as follows:

Initialization phase: The signer randomly chooses two large primes p and q and computes $n = p * q$ and $\phi(n) = (p-1)(q-1)$. The signer chooses a number e, such that $GCD(e, \phi(n)) = 1$. Then, he/she computes $d = e^{-1} \bmod \phi(n)$. Let (e, n) be the public key and (p, q, d) be the private key. The signer publishes the public key (e, n) and a hash function $h(g)$.

Blinding phase: The requester has a message m and wants to have it signed by the signer, but he/she does not want the signer to know the content of this message. The requester randomly selects two distinct numbers r_1, r_2 as the blinding factors. He/she then randomly chooses two distinct primes a_1, a_2, such that $GCD(a_1, a_2) = 1$. He/she then computes the blinded message $\alpha_1 = r_1^{\varepsilon} g h(m)^{a_1} \bmod n$ and $\alpha_2 = r_2^{\varepsilon} g h(m)^{a_2} \bmod n$ and sends blinded messages (α_1, α_2) to the signer.

Signing phase: After receiving the blinded messages (α_1, α_2) from the requester, the signer randomly chooses two distinct primes, b_1 and b_2, such that $GCD(b_1, b_2) = 1$. The signer then computes $t_1 = \alpha_1^{b_1 d} \bmod n$ and $t_2 = \alpha_2^{b_2 d} \bmod n$ and sends (t_1, t_2, b_1, b_2) to the requester.

Unblinding phase: The requester receives (t_1, t_2, b_1, b_2) from the signer and computes $a_1 b_1$, $a_2 b_2$. Due to $GCD(a_1, a_2) = 1$ and $GCD(b_1, b_2) = 1$, $GCD(a_1 b_1, a_2 b_2) = 1$, there must be two values, w and t, satisfying the equation $a_1 b_1 w + a_2 b_2 t = 1$. It is called the extended Euclidean algorithm [3]. The four values (a_1, a_2, w, t) must remain secure. The requester computes $s_1 = t_1 g r_1^{-b_1} = h(m)^{a_1 b_1 d} \bmod n$ and $s_2 = t_2 g r_2^{-b_2} = h(m)^{a_2 b_2 d} \bmod n$.

Then, he/she can obtain the signature s by computing $s = s_1^w g s_2^t \bmod n$ and the message-signature pair is (m, s).

Verifying phase: After the verifier receives the message-signature pair (m, s), he/she can use the signer's public key (e, n) and hash function $h(g)$ to verify the legitimacy of the signature by using the equation $s^\varepsilon \equiv h(m) \bmod n$.

(3) **The blind signatures based on discrete logarithm problem:** J. L. Camenisch, J. M. Priveteau and M. A. Stadler first proposed the blind signature based on discrete logarithm problems in 1994 [5]. In their paper, they presented two new blind signature schemes. The first blind signature scheme originated from a variation of the DSA (Digital Signature Algorithm) [14]. The Nyberg-Rueppels signature scheme [21] was the basis for the second blind signature scheme. The first blind signature scheme derived from a variation of the DSA [14] is presented in the following.

Initialization phase: The signer selects a big prime p, a prime factor q of $p-1$, and g, where g is a primitive root of p. He/she chooses a random number x, where $x \in Z_q$. He/she then computes y, where $y = g^x \bmod p$. The signer gets a private key x and a public key y.

Blinding phase: The requester sends a request to the signer. After receiving the request, the signer randomly chooses a number $\tilde{k}$, where $\tilde{k} \in Z_q$. He/she then computes $\tilde{R} = g^{\tilde{k}} \bmod p$ and checks $\gcd(\tilde{R}, q)$. If $\gcd(\tilde{R}, q) = 1$, he/she sends $\tilde{R}$ to the requester; otherwise he/she must choose another $\tilde{k}$. When the requester receives the value $\tilde{R}$, he/she must check if $\gcd(\tilde{R}, q) = 1$. Then he/she randomly chooses α, $\beta \in Z_q$ and computes $R = \tilde{R}^\alpha g^\beta \bmod p$. The requester checks $\gcd(R, q)$. If $\gcd(R, q) = 1$, then he/she computes $\tilde{m} = \alpha m \tilde{R} R^{-1} \bmod q$ and sends $\tilde{m}$ to the signer; else, he/she must choose another α and β.

Signing phase: After receiving $\tilde{m}$, the signer computes $\tilde{s} = \tilde{k}\tilde{m} + \tilde{R}x \bmod q$ and sends $\tilde{s}$ to the requester.

Unblinding phase: When the requester receives $\tilde{s}$ from the signer, he/she computes $s = \tilde{s} R \tilde{R}^{-1} + \beta m \bmod q$ and $r = R \bmod q$.

Finally, the requester gets the message-signature pair (m, r, s).

Verifying phase: The verifier can use the public key to verify the legitimacy of the signature. He/she then computes $T = (g^s y^{-r})^{m^{-1}} = g^{(\tilde{s}R\tilde{R}^{-1} + \beta m - xr)m^{-1}} = g^{\tilde{k}\alpha + \beta} = R \bmod p$ and checks the equation $r = T \bmod q$.

Below is the second blind signature scheme based on the Nyberg-Rueppel signature scheme [21].

Initialization phase: The signer selects a big prime$p$, a prime factor q of $p-1$, and g, where g is a primitive root of p. He/she then randomly chooses a number x, where $x \in Z_q$. He/she then computes y, where $y = g^x \bmod p$. The signer gets a private key x and a public key y.

Blinding phase: The requester sends the request to the signer. After receiving the request, the signer chooses a number $\tilde{k} \in Z_q$ and computes $\tilde{r} = g^{\tilde{k}} \bmod p$. Then he/she sends $\tilde{r}$ to the requester. When the requester receives the value $\tilde{r}$, he/she randomly chooses $\alpha \in Z_q$, $\beta \in Z_q^*$ and computes $r = m g^\alpha \tilde{r}^\beta \bmod p$, $\tilde{m} = r\beta^{-1} \bmod q$. He/she then sends $\tilde{m}$ to the signer.

Signing phase: After receiving $\tilde{m}$, the signer computes $\tilde{s} = \tilde{m}x + \tilde{k} \bmod q$ and sends $\tilde{s}$ to the requester.

Unblinding phase: When the requester receives the value $\tilde{s}$, he/she computes $s = \tilde{s}\beta + \alpha \bmod q$. He/she gets the message-signature pair (m, r, s) and sends message-signature pair to the verifier.

Verifying phase: After receiving the message-signature pair (m, r, s), the verifier can verify the legitimacy of the signature by checking $g^{-s}y^r r = mg^{-\tilde{s}\beta-\alpha+xr+\tilde{k}\beta+\alpha} = mg^{-\tilde{m}x\beta-\tilde{k}\beta+xr+\tilde{k}\beta} = m \bmod p$

Cryptanalysis [18]: In 1995, Dr. L. Harn pointed out that the first blind signature derived from a variation of the DSA did not provide true blind signature [18]. The signer keeps the record $(\tilde{m}, \tilde{R}, \tilde{k}, \tilde{s})$ for all blinding signatures. After the requester reveals the message-signature pair (m, r, s) to the public, the signer will try to compute a pair of integers $\alpha' = \tilde{m}m^{-1}\tilde{R}^{-1}r \bmod q$ and $\beta' = m^{-1}(s - \tilde{s}r\tilde{R}^{-1}) \bmod q$ and check if $r = \tilde{R}^{\alpha'}g^{\beta'} \bmod p$ can trace the true blind signature. Therefore, Carmenisch et al. proposed a blind signature scheme that did not satisfy the untraceability. E. Mogammed, A. E. Emarah and K. EL-Shennawy [23] proposed another blind signature based on discrete logarithm problem. Their proposed blind signature had the advantage of less computational complexity and was faster than the blind signature based on the RSA algorithm. The details of blind signatures are presented in the following:

Initialization Phase: The signer generates a public and private key.

Blinding phase: The requester randomly chooses k $(1 < k < p-1)$, where $\gcd(k, p-1) = 1$. He/she computes $r = \alpha^k \bmod (p-1)$, then chooses a blind factor h, where $\gcd(h, p-1) = 1$ and computes $m' = h * m \bmod (p-1)$. After computation, he/she sends m' and r to the signer.

Signing Phase: After receiving m', the signer computes $s' = (m' - xr) * k^{-1} \bmod (p-1)$, and then sends s' to the requester.

Unblinding phase: When the requester receives s', he/she computes the signature $s = xrk^{-1}(h^{-1}-1)+h^{-1}s' \bmod (p-1)$, and then sends the message-signature pair (m, r, s) to the requester.

Verifying phase: After receiving the message-signature pair (m, r, s), the verifier can use the public key to verify the legitimacy of the message-signature pair (m, r, s) by checking whether $\alpha^m \equiv y^r r^s \bmod p$.

Cryptanalysis: In the blind signature scheme proposed by E. Mogammed et al., the requester obtained the set of values (s', m', r, k^{-1}) during the unblinding phase, when he/she could easily locate the private key x. Therefore, E. Mogammed et al. proposed a blind signature scheme, which did not meet the unforgeability. The blind signature scheme is now unsecure.

3. The Proposed Blind Signature.

The discrete logarithm problem and the generalized ElGamal type digital signature schemes proposed by Dr. L. Harn [17] are the base for the proposed blind signature schemes. In this section, we describe how to transform the generalized ElGamal type digital signature schemes to the blind signature scheme. The last part in this section presents the usability in the proposed blind signature scheme.

3.1. The construction of our proposed scheme.

There are 18 generalized ElGamal type digital signature schemes shown in Table 1. In this subsection, the new blind signature derived from the generalized ElGamal type digital signature scheme No.15 is presented as follows. Table 1 shows the generalized ElGamal type digital signature scheme No.15. The signature equation is shown below.

$$sx = k + (m + r) \tag{1}$$

In the proposed blind signature scheme, there are four different parameters between the signature equation in the generalized ElGamal type digital signature and the signature equation in the proposed blind signature. The proposed signature equation is shown

TABLE 2. Parameters of our proposed scheme

Requester		Signer	
Parameter	Explanation	Parameter	Explanation
a, b, c	Choose randomly, a, b, c are relatively prime to $\phi(p)$	p	Big prime
m	Message	α	Primitive root of p
$\tilde{m}$	Blinded message	y	$y = \alpha^x \bmod p$
k	$k = a\tilde{k} + bx + c$	x	Private key, $2 < x < (p-2)$
r	$r = \tilde{r}^a y^b \alpha^c \bmod p$	$\tilde{k}$	Integer, $\gcd(\tilde{k}, p-1) = 1$
s	Digital signature	$\tilde{r}$	$\tilde{r} = \alpha^{\tilde{k}} \bmod p$
		$\tilde{s}$	Blind signature
		$h(g)$	Hash function

below.

$$\tilde{s}x = \tilde{k} + (\tilde{m} + \tilde{r}) \tag{2}$$

From (2),

$$x = \tilde{k}\tilde{s}^{-1} + (\tilde{m} + \tilde{r})\tilde{s}^{-1} \bmod \phi(p) \tag{3}$$

can be obtained. Let $k = a\tilde{k} + bx + c$. Substituting (3) into $k = a\tilde{k} + bx + c$ results in

$$k = a\tilde{k} + b\tilde{k}\tilde{s}^{-1} + b(\tilde{m} + \tilde{r})\tilde{s}^{-1} + c \tag{4}$$

From (1),

$$sx = k + (m + r) \Rightarrow sx - k - (m + r) = 0 \tag{5}$$

is obtained. Substituting (3) and (4) into (5),

$$\begin{aligned} & sx - k - (m + r) = 0 \\ & \Rightarrow s\tilde{k}\tilde{s}^{-1} + s(\tilde{m} + \tilde{r})s^{-1} - a\tilde{k} - b\tilde{k}\tilde{s}^{-1} - b(\tilde{m} + \tilde{r})\tilde{s}^{-1} - c - (m + r) = 0 \\ & \Rightarrow k(s\tilde{s}^{-1} - a - b\tilde{s}^{-1}) + s(\tilde{m} + \tilde{r})\tilde{s}^{-1} - b(\tilde{m} + \tilde{r})\tilde{s}^{-1} - c - (m + r) = 0 \end{aligned} \tag{6}$$

is obtained. According to (6),

$$s(\tilde{m} + \tilde{r})\tilde{s}^{-1} - b(\tilde{m} + \tilde{r})\tilde{s}^{-1} - c - (m + r) = 0 \tag{7}$$

$$s\tilde{s}^{-1} - a - b\tilde{s}^{-1} = 0 \tag{8}$$

are obtained. From (7),

$$\tilde{m} = a^{-1}(c + m + r) - \tilde{r} \tag{9}$$

is obtained. From (8),

$$s = a\tilde{s} + b \tag{10}$$

is obtained, where (9) is the blind equation and (10) is the unblind equation in the proposed blind signature scheme.

3.2. **Blind signature based on generalized ElGamal type digital signature schemes.** The novel blind signature schemes derived from the generalized ElGamal type digital signature are presented. In the proposed blind signature scheme, there are three participants, namely, the requester, the signer, and the verifier; and five phases, namely, (1) initialization phase, (2) blinding phase, (3) signing phase, (4) unblinding phase and (5) verification phase. Below are the details of the proposed scheme. The generalized ElGamal type digital signature scheme No.15 (see Table 1) is the basis for the proposed blind signature scheme 1. The details of the proposed scheme are described in the following.

Initialization phase: The signer chooses a large prime p and α as a primitive root model p. In addition, he/she randomly chooses a number x $(2 < x < (p-2))$ and then

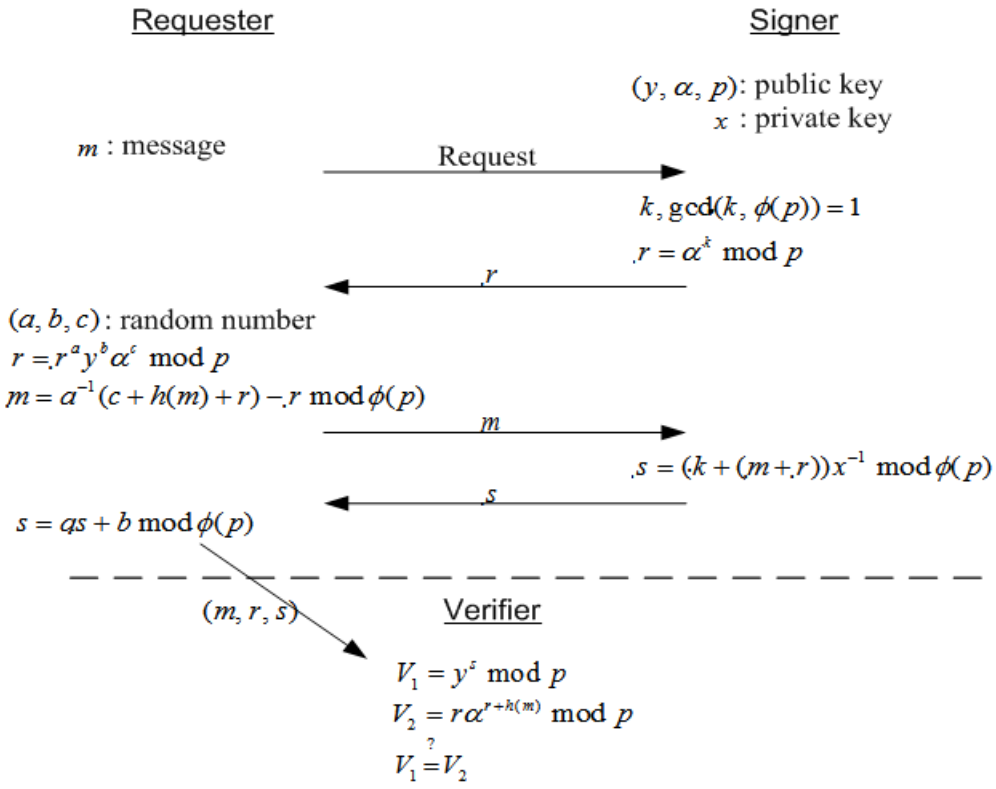

FIGURE 1. Protocol diagram of novel blind signature scheme

computes $y = \alpha^x \bmod p$. The signer publishes (y, α, p) as the public key, keeps x as the private key, and chooses a one-way hash function $h(g)$ such as SHA-1 [25] or MD5 [3].

Blinding phase: The requester has a message m and wants to have it signed by the signer. First, the requester sends a request to the signer for signing a message. The signer then randomly chooses a number $\tilde{k}$, such that $\gcd(\tilde{k}, \phi(p)) = 1$. The signer computes $\tilde{r} = \alpha^{\tilde{k}} \bmod p$. After computing $\tilde{r}$, the signer sends $\tilde{r}$ to the requester. When the requester receives $\tilde{r}$ from the signer, he/she randomly chooses the set of values (a, b, c), such that parameters (a, b, c) are relatively prime to the value $\phi(p)$. The requester then computes $r = \tilde{r}^a y^b \alpha^c \bmod p$ and the hash value $h(m)$ generated by the hash function $h(g)$. The requester then blinds the value $h(m)$ with the blind equation $\tilde{m} = a^{-1}(c + m + r) - \tilde{r} \bmod \phi(p)$. After the blinding phase, the requester sends the value $\tilde{m}$ to the signer.

Signing phase: When the signer receives the value $\tilde{m}$, he/she computes $\tilde{s} = (\tilde{k} + (\tilde{m} + \tilde{r}))x^{-1} \bmod \phi(p)$. The signer then sends the value $\tilde{s}$ to the requester.

Unblinding phase: After receiving $\tilde{s}$ from the signer, the requester computes $s = a\tilde{s} + b \bmod \phi(p)$ and obtains the message-signature (m, r, s). The requester can then send the message-signature pair (m, r, s) to the verifier.

Verifying phase: When the verifier receives the message-signature pair (m, r, s), he/she can use the one-way hash function $h(g)$ and the public key (y, α, p) to verify the legitimacy of the signature by checking $V_1 = V_2$, such that,

$$V_1 = y^s \bmod p$$
$$V_2 = r\alpha^{r+h(m)} \bmod p$$

If $V_1 = V_2$, then the verification passes; else the verification fails.

4. **Discussions.** In general, the blind signature should meet the four requirements, namely, correctness, blindness, unforgeability and untraceability. In this section, it examines the requirements of our proposed blind signature scheme. Four main equations are included in the following:

Signature Equation: $\tilde{s}x = \tilde{k} + (\tilde{m} + \tilde{r}) \bmod \phi(p)$
Blind Equation: $\tilde{m} = a^{-1}(c + h(m) + r) - \tilde{r} \bmod \phi(p)$
Unblind Equation: $s = a\tilde{s} + b \bmod \phi(p)$
Verification Equation: $y^s = r\alpha^{h(m)+r} \bmod p$

4.1. **Correctness.** Let message-signature pair (m, r, s) be in the new blind signature scheme. In the following, we prove the verification equation $y^s \equiv r\alpha^{h(m)+r} \bmod p$.

$$
\begin{aligned}
& y^s \equiv r\alpha^{h(m)+r} \bmod p \\
\Leftrightarrow\ & \alpha^{xs} \equiv \alpha^k \alpha^{r+h(m)} \bmod p \\
\Leftrightarrow\ & xs \equiv k + r + h(m) \bmod \phi(p) \\
\Leftrightarrow\ & x(a\tilde{s} + b) \equiv a\tilde{k} + bx + c + r + h(m) \bmod \phi(p) \\
\Leftrightarrow\ & xa\tilde{s} \equiv a\tilde{k} + c + r + h(m) \bmod \phi(p) \\
\Leftrightarrow\ & a(x\tilde{s} - \tilde{k}) \equiv c + h(m) + r \bmod \phi(p) \quad \text{multiplied simultaneously by } a^{-1} \\
\Leftrightarrow\ & (x\tilde{s} - \tilde{k}) \equiv a^{-1}(c + h(m) + r) \bmod \phi(p) \quad \text{subtracted simultaneously by } \tilde{r} \\
\Leftrightarrow\ & x\tilde{s} - \tilde{k} - \tilde{r} \equiv a^{-1}(c + h(m) + r) - \tilde{r} \bmod \phi(p) \\
\Leftrightarrow\ & x\tilde{s} - \tilde{k} - \tilde{r} \equiv \tilde{m} \bmod \phi(p) \\
\Leftrightarrow\ & \tilde{s}x \equiv \tilde{k} + \tilde{m} + \tilde{r} \bmod \phi(p)
\end{aligned}
$$

4.2. **Blindness.** In this experiment, blindness means that the signer does not know the content of the message when he/she signs the message. This is a very important requirement in the blind signature. In the new blind signature scheme, the blind equation is

$$\tilde{m} = a^{-1}(c + h(m) + r) - \tilde{r} \bmod \phi(p)$$

In this equation, the signer has three unknown parameters, namely, a, c and r. Therefore, the signer cannot know the content of the message in this blind signature scheme.

4.3. **Unforgeability.** The discrete logarithm problem and the generalized ElGamal one are the base for the digital signature in the proposed blind signature scheme. The security of the proposed scheme relies on the difficulty of solving the discrete logarithm problem. It is very difficult to forge a valid signature s that can pass the verification equation $y^s = r\alpha^{h(m)+r} \bmod p$.

4.4. **Untraceability.** Untraceability is also an important requirement in the blind signature scheme. The signer is unable to link the signature with the message when publishing the message-signature pair (m_i, r_i, s_i).

In the proposed blind signature scheme, if the signer wants to track the blind signature, he/she keeps the set of values $(\tilde{m}_i, \tilde{r}_i, \tilde{s}_i)$. When the requester publishes the message-signature pair (m_i, r_i, s_i) in public, the signer cannot get any information from the set of values that he/she keeps. Because the signer does not know the values including a, b, c and r, he/she cannot trace the relationship between the message-signature pair and the blind signature.

This paper mainly applies the concept of digital signature including the requirements, namely, (1) authentication, (2) non-repudiation, (3) data integrity and (4) unforgeability. In addition, for the demands of environmental applications, the technology and concept

of blind signature are also proposed, where the blind signature is mostly based on the spirit and concept of digital signature. In order to reinforce the demand of blind signature features and improve the blind signature proposed by Harn, this method proposes a new blind signature protocol to solve the application problems on blind signature. The existing methods for blind signature did not present good efficacy. For this reason, in order to improve the efficacy of blind signature, this paper also reinforces the requirements, namely, (1) correctness, (2) blindness, (3) unforgeability and (4) untraceability.

In consideration of the requirements on flexibility and efficacy in application contexts, the proposed method also takes security and efficacy into account, further improves them, selects the simplification of parameters, and, at the same time, reduces the loading in the protocol. Moreover, it simplifies parameters at the phases of Requester and Signer so that the purpose of verification can be easily achieved at verifier. It also selects appropriate algorithms, such as choosing SHA-1 or MD5 as the hash function at Initialization phase, so that the method is suitable in various application contexts. Furthermore, based on the mathematical difficulty of discrete logarithm problem, it presents a certain degree of security. In other words, the proposed method can reduce the processing time of communication and can be applied to various contexts, like electronic commerce systems, electronic balloting systems, or auction systems.

5. **Conclusion and Future Work.** This study proposes a new blind signature scheme based on discrete logarithm problem and generalized type digital signature schemes. The proposed blind signature can meet the requirements, namely, correctness, blindness, unforgeability, and untraceability. It is expected that the network systems, such as electronic cash payment system and electronic voting systems, can apply the proposed blind signature scheme.

In 1992, Solms and Naccache presented a perfect crime by using the untraceability property of blind signature [30]. They indicated that it became easy to blackmail and launder money by using the untraceability properties of the blind signature. In 1993, Micali introduced the concept of fair cryptosystems [22] and Stadler, Piveteau and Camenisch presented the fair blind signature scheme in 1995 [28]. In the fair blind signature scheme, there was an additional participant called a judge. The judge could deliver information, which allowed the signer to link the message-signature pair. In the future work, the proposed blind signature will be transformed into the fair blind signature to avoid the perfect crime situation that Solms et al. proposed.

Acknowledgement. The authors are very grateful to the anonymous reviewers for their constructive comments which improved the quality of this paper. This work was supported by National Science Council of Taiwan, under grant NSC 99-2221-E-029-023.

REFERENCES

[1] G. B. Agnew, R. C. Mullin and S. A. Vanstone, Improved digital signature scheme based on discrete exponentiation, *Electronics Letters*, vol.26, pp.1024-1025, 1990.
[2] S. G. Aki, Digital signatures: A tutorial survey, *Computer*, vol.16, no.2, pp.15-24, 1983.
[3] J. M. Alfred, A. V. Scott and C. V. O. Paul, *Handbook of Applied Cryptography*, CRC Press, 1996.
[4] D. Boneh, Twenty years of attacks on the RSA cryptosystem, *Notices of the American Mathematical Society*, vol.46, no.2, pp.203-213, 1999.
[5] J. L. Camenisch, J. M. Piveteau and M. A. Stadler, Blind signatures based on the discrete logarithm problem, *Lecture Notes in Computer Science*, pp.428-432, 1995.
[6] D. Chaum, Blind signatures for untraceable payments, *Advances in Cryptology-Crypto'82*, pp.199-203, 1982.
[7] D. Chaum, A. Fiat and M. Naor, Untraceable electronic cash, *Proc. on Advances in Cryptology*, Santa Barbara, CA, pp.319-327, 1990.

[8] D. L. Chaum, Blind signature systems, *US Patent 4759063*, 1988.
[9] H. Y. Chien, J. K. Jan and Y. M. Tseng, RSA-based partially blind signature with low computation, *Proc. of the 8th IEEE International Conference on Parallel and Distributed Systems*, pp.385-389, 2001.
[10] D. Chaum, Untraceable electronic mail, return addresses, and digital pseudonyms, *Communications of the ACM*, vol.24, no.2, pp.84-88, 1981.
[11] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, vol.22, pp.644-654, 1976.
[12] T. Elgamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory*, vol.31, no.4, pp.469-472, 1985.
[13] C. I. Fan, W. K. Chen and Y. S. Yeh, Randomization enhanced Chaum's blind signature scheme, *Computer Communications*, vol.23, no.11, pp.1677-1680, 2000.
[14] *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication (FIPS PUB) 186-2, National Institute of Standards and Technology (NIST), 2000.
[15] L. Harn, Group-oriented (t,n) threshold digital signature scheme and digital multisignature, *IEEE Proc. on Computers and Digital Techniques*, vol.141, no.5, pp.307-313, 1994.
[16] L. Harn, New digital signature scheme based on discrete logarithm, *Electronics Letters*, vol.30, no.5, pp.396-398, 1994.
[17] L. Harn and Y. Xu, Design of generalised ElGamal type digital signature schemes based on discrete logarithm, *Electronics Letters*, vol.30, no.24, pp.2025-2026, 1994.
[18] L. Harn, Cryptanalysis of the blind signatures based on the discrete logarithm problem, *IEE Electronics Letters*, vol.31, no.14, pp.1136-1137, 1995.
[19] M. S. Hwang, C. C. Lee and Y. C. Lai, An untraceable blind signature scheme, *IEICE Trans. Fundam Electron Commun. Comput. Sci. (Inst. Electron Inf. Commun. Eng.)*, vol.E86-A, no.7, pp.1902-1906, 2003.
[20] W. S. Juang and C. L. Lei, Partially blind threshold signatures based on discrete logarithm, *Computer Communications*, vol.22, no.1, pp.73-86, 1999.
[21] N. Kaisa and A. R. Rainer, A new signature scheme based on the DSA giving message recovery, *The 1st ACM Conference on Computer and Communications Security*, Fairfax, VA, pp.58-61, 1993.
[22] S. Micali, Fair cryptosystems, *Technical Report: TR-579b*, Massachusetts Institute of Technology, 1995.
[23] E. Mohammed, A. E. Emarah and K. El-Shennawy, A blind signature scheme based on ElGamal signature, *EUROCOMM 2000: Information Systems for Enhanced Public Safety and Security*, pp.51-53, 2000.
[24] J. Nechvatal, Public-key cryptography, in *Contemporary Cryptology – The Science of Information Integrity*, G. J. Simmons (ed.), IEEE Press, 1992.
[25] *Secure Hash Standard*, Federal Information Processing Standards Publication (FIPS PUB) 180-1, National Institute of Standards and Technology (NIST), 1995.
[26] R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, vol.21, pp.120-126, 1978.
[27] C. P. Schnorr, Efficient identification and signatures for smart cards, *Advances in Cryptology-CRYPTO'89, LNCS*, vol.435, pp.239-252, 1990.
[28] M. Stadler, J. M. Piveteau and J. Camenisch, Fair blind signatures, *Advances in Cryptology-Eurocrypt'95*, vol.921, pp.209-219, 1995.
[29] G. Tsudik, Message authentication with one-way hash functions, *The 11th Annual Joint Conference of the IEEE Computer and Communications Societies*, vol.3, pp.2055-2059, 1992.
[30] S. V. Solms and D. Naccache, On blind signatures and perfect crimes, *Computers and Security*, vol.11, no.6, pp.581-583, 1992.
[31] M. J. Wiener, Cryptanalysis of short RSA secret exponents, *IEEE Transactions on Information Theory*, vol.36, pp.553-558, 1990.
[32] S. M. Yen and C. S. Laih, New digital signature scheme based on discrete logarithm, *Electronics Letters*, vol.29, no.12, pp.1120-1121, 1993.
[33] Z. H. Shao, Improved user efficient blind signatures, *Electronics Letters*, vol.36, no.16, pp.1372-1374, 2000.
[34] C. I. Fan, C. I. Wang and W. Z. Sun, Fast randomization schemes for Chaum blind signatures, *International Journal of Innovative Computing, Information and Control*, vol.5, no.11(A), pp.3887-3900, 2009.

[35] Y. M. Tseng, T. Y. Wu and J. D. Wu, An efficient and provably secure ID-based signature scheme with batch verifications, *International Journal of Innovative Computing, Information and Control*, vol.5, no.11(A), pp.3911-3922, 2009.
[36] L. J. Wang and J. J. R. Chen, Novel digital multisignature scheme, *ICIC Express Letters*, vol.4, no.4, pp.1251-1256, 2010.
[37] M. S. Hwang, S. F. Tzeng and S. F. Chiou, A non-repudiable multi-proxy multi-signature scheme, *ICIC Express Letters*, vol.3, no.3(A), pp.259-264, 2009.