New Multisignature Schemes with Distinguished Signing Authorities

Minh Nguyen Hieu[1] and Hung Dao Tuan[2]
[1]Le Qui Don Technical University, Ha Noi, Viet Nam
[2]Vietnam Information Security Laboratory, Ha Noi, Viet Nam
Email: hieuminhmta@ymail.com

Abstract - **In this paper, we propose two multisignature schemes with distinguished signing authorities. The two schemes are based on the discrete logarithm problem and based on the difficulty of finding the *k*th roots modulo a large prime *p*. Our schemes provide individual evidence to prevent confusion over authority due to malice and provide generation of the multisignature possessing internal integrity. Moreover, the difference between our schemes and Hwang et al.'s scheme is the method of exchange of data during the multisignature generation process. Comparisons show that the new schemes allow reducing computation and communication costs, so they can be used widely in E-applications.**

Keywords - **Digital signature, discrete logarithm problem, multisignature scheme, internal integrity.**

I. INTRODUCTION

Digital signature schemes is a method which allows one party, the signer, to sign messages in such a way that everyone can verify the validity of authentic signatures, but no one can forge signatures of other messages [12]. These schemes provide authentication, integrity and non-repudiation to digital communications. Digital signatures can be classified into two main categories: single signature and multiple signatures. The digital multisignature is analogous to an ordinary digital signature. Instead of generating the digital signature by an individual signer with the knowledge of a single private key, the digital multisignatures are generated by multiple group members with the knowledge of multiple private keys [2]. Digital multisignatures can be classified into two classes: the multisignatures with undistinguished signing authorities and the multisignatures with distinguished signing authorities.

The first multisignature scheme was introduced by Itakura and Nakamura [1], however in that scheme, all group members hold the same responsibilities of signing the document. In fact, there are some applications that need to use multisignatures with distinguished signing responsibilities. The first multisignature scheme with distinguished signing authorities was introduced by Harn [2], and has been followed by many other research works [4-8].

Harn [2] has proposed a multisignature scheme with distinguished signing authorities based on the discrete logarithm problem. In [4] proposed two ID-based multisignatures with distinguished signing authorities based on the difficulty of the factorization problem. In [6] proposed two multisignature schemes with distinguished signing authority based on RSA and the discrete logarithm with composite modulus. However, those schemes were not a strong secure ones [9-13].

Li et al. [9] showed that Harn's scheme is not secure against their attack. Moreover, in Harn's scheme, no one is able to prove his own distinguished signing authority though he actually signed only for his partial content [5]. To guard against Li et al.'s attack without the help of CA (Certificate authority), a new multisignature scheme with distinguished signing authorities is proposed [5]. However, in their scheme, the computation and communication costs for generation of the multisignature will be significantly affected by the number of signers in the group. It is very time-consuming for generation of the multisignature when the number of group members increases.

In this paper, we propose two multisignature schemes with distinguished signing authorities. The two schemes are based on the difficulty of the discrete logarithm problem (DLP) [14, 15] and based on the difficulty of finding roots modulo prime [16, 17]. Our schemes provide individual evidence to prevent confusion over authority due to malice. The new schemes also provide generation of the multisignature possessing internal integrity. Nobody participating in the schemes are able to form a valid multisignature that corresponds to reduced number of the signers. Moreover, the difference between our schemes and Hwang et al.'s scheme is a method of exchange of data during the multisignature generation process. Proposed method allows reducing computation and communication costs.

We will organize this paper as follows: In section II, discrete logarithm problem, computing roots modulo prime and Hwang et al.'s scheme are reviewed. In section III, our new schemes are proposed. In Section IV, we provide a formal proof that our schemes are security and then performance evaluation. Section V concludes the paper.

II. PRELIMINARIES

A. *Discrete Logarithm Problem* [18]

Let p and q be two large primes satisfying $q|p-1$, and α a generator of order q over Z_p. The discrete logarithm problem is, given an instance (y, p, q, α), where $y = \alpha^x \bmod p$ for some $x \in Z_q$, to derive x.

B. *Computing Roots Modulo Prime* [16,17]

Difficulty of finding roots modulo a composite number is used in some of the known DSSes: RSA and Rabin's DSS [18].

978-1-4673-4352-7/12/$31.00 ©2012 IEEE

The main difference between the RSA and Rabin's DSS consists in the following [16, 17].

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) ≠ 1 and gcd(2, q – 1) ≠ 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 kth 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 $\Delta'' = \Delta'^{-1} \bmod p - 1$. Then we have:

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

With high probability the value d is sufficiently small and the dth root can be easily found, for example, using the method described in [16].

If $k^2 \mid p-1$, then 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 kth roots is difficult [16].

C. Review of Hwang et al.'s Scheme [5]

In this section, we brief describe the multisignature scheme in [5]. The scheme consists of four phases: the key generation phase, the multisignature generation phase, the multisignature verification phase and evidence verification phase

C.1. The Key Generation Phase

Let p and q be two large primes satisfying $q|p-1$, and α a generator of order q over Z_p.

Assume that the signing group is $\{U_1, U_2, \ldots, U_n\}$.

$x_i \in Z_q^*$: Secret key of each member U_i.

$y_i = \alpha^{x_i} \bmod p$: Public key of each member U_i.

$Y = \prod_{i=1}^{n} y_i^{y_i} \bmod p$: The group public key.

C.2. The Multisignature Generation Phase

Supposed that the signing group $\{U_1, U_2, \ldots, U_n\}$ and the message m_i be the partial message that U_i is responsible for.

1) **Step 1**. Each member U_i selects a random integer $k_i \in Z_q^*$ and computes $r_i = \alpha^{k_i} \bmod p$ and $h(m_i)$ for i = 1, 2, …, n. Then each member U_i broadcasts $(r_i, h(m_i))$ to the other n-1 members and a predetermined clerk C.
2) **Step 2**. Each member U_i computes the commitment value $r = \prod_{i=1}^{n} r_i^{h(h(m_i), r_i)} \bmod p$. The clerk also computes the commitment value r.
3) **Step 3**. Each member U_i finds the solution s_i satisfying $s_i = (x_i y_i H + r k_i h(h(m_i), r_i)) \bmod q$, where $H = h(h(m_1) \| h(m_2) \ldots \| h(m_n))$. Then each member U_i transmits his individual signature (r_i, s_i) to the clerk.
4) **Step 4**. The clerk verifies each the individual signature (r_i, s_i) by means of the equation $\alpha^{s_i} \equiv y_i^{y_i H} r_i^{r h(h(m_i), r_i)} \bmod q$ after receiving all of the individual signatures (r_i, s_i)'s. If all of the individual signatures are legal, then the clerk generates the multisignature (r, s) by computing $s = \sum_{i=1}^{n} s_i \bmod q$.

Finally, (r, s) is the multisignature for the message $M = m_1 || m_2 || \ldots || m_n$.

C.3. The Multisignature Verification Phase

The multisignature (r, s) is verified by means of the equation $\alpha^s \equiv Y^H r^r \bmod p$.

C.4. The Evidence Verification Phase

All of the individual signatures (r_i, s_i) can be used as evidence in the evidence verification phase.

III. The Proposed Schemes

A. Our First Scheme

Suppose that the signing group $\{U_1, U_2, \ldots, U_n\}$ wants to generate the multisignature for the message $M = m_1 || m_2 || \ldots || m_n$. The member U_i is only responsible for the partial content m_i, for i = 1, 2, …, n.

A.1. The Key Generation Phase

Assuming a group of n signers and a trusted clerk, the following parameters are defined:

1) **Step 1**: A trusted clerk chooses a large prime p, a prime divisor q correspondingly with $q|(p-1)$, and a one-way hash function such as SHA-1 ($H = h(M)$) [18].
2) **Step 2**: $x_1, x_2, \ldots, x_n$: group members' secret keys such that $1 < x_i < q$, x_i is selected randomly and known only by the member U_i.
3) **Step 3**: $y_1, y_2, \ldots, y_n$: group members' public keys such that $y_i = \alpha^{x_i} \bmod p$ is computed and published by the group members U_i (α is generator of the cyclic group of

order $q \in Z_p^*$). Adding/deleting a member i requires adding/deleting the corresponding y_i by the clerk.

4) **Step 4**: The clerk computes group public key Y for all signers: $Y = \prod_{i=1}^{n} y_i^{y_i} \bmod p$.

A.2. The Multisignature Generation Phase

The scheme requires the clerk and other signing group members to carry out an exchange of data during the multisignature generation process.

1) **Step 1**: Each signer selects random number $k_i \in Z_q^*$ and computes $r_i = \alpha^{k_i} \bmod p$. Then each signer U_i sends r_i to the clerk.

2) **Step 2**: The clerk computes the common randomization value $R = \prod_{i=1}^{n} r_i^{h(m_i)} \bmod p$ and computes the values $E = h(R \| M)$ and $H = h(h(m_1) \| h(m_2) \| ... \| h(m_n))$. Then he sends (E, H) to each of the signers.

3) **Step 3**: Each signer computes its signature share s_i as follows $s_i = (k_i h(m_i) H + x_i y_i E) \bmod q$. Then each signer U_i sends s_i to the clerk.

4) **Step 4**: Once the clerk receives the individual signature (r_i, s_i) from i signers, he needs to verify the validity of this individual signature. The clerk check the signature of the individual as follows $\alpha^{s_i} \equiv y_i^{y_i E} r_i^{h(m_i)H} \bmod p$. If all of the individual signatures are legal, then the clerk generates the multisignature (R, S) by computing $S = \sum_{i=1}^{n} s_i \bmod q$.

Finally, (R, S) is the multisignature for the message $M = m_1 || m_2 || \ldots || m_n$.

A.3. The Multisignature Verification Phase

Prior to verifying the signature of a signed message, the parameters (p, α, Y) are made available to the verifier in an authenticated manner.

Verification of the multisignature is performed using the group public key Y.

1) **Step 1**: Using the multisignature (R, S) to compute $\alpha^{S'} \equiv Y^E R^H \bmod p$.

2) **Step 2**: Compare values S' and S. If $S' = S$, then the signature is valid. Otherwise the signature is false.

The partial contents of the message $m_1 || m_2 || \ldots || m_n$ 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 $h(m_1) || h(m_2) || \ldots || h(m_{i-1}) || m_i || h(m_{i+1}) || \ldots || h(m_n)$ to verify the multisignature (R, S).

A.4. The Evidence Verification Phase

All of the individual signatures (r_i, s_i) can be used as evidence. To show that member U_i is responsible for signing only for the partial content m_i, (R, S), (r_i, s_i) and $M = m_1 || m_2 || \ldots || m_n$ are verified by $\alpha^S \equiv Y^E R^H \bmod p$ and $\alpha^{s_i} \equiv y_i^{y_i E} r_i^{h(m_i)H} \bmod p$. If the two equations are satisfied, member U_i is responsible for signing only for the partial content m_i because the equation $\alpha^{s_i} \equiv y_i^{y_i E} r_i^{h(m_i)H} \bmod p$ shows the relationship between the whole document, the partial content m_i, and member U_i.

B. Our Second Scheme

Suppose that the signing group $\{U_1, U_2, \ldots, U_n\}$ wants to generate the multisignature for the message $M = m_1 || m_2 || \ldots || m_n$. The member U_i is only responsible for the partial content m_i, for $i = 1, 2, \ldots, n$.

B.1. The Key Generation Phase

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

Assuming a group of n signers and a trusted clerk, the following parameters are defined:

1) **Step 1**: A trusted clerk generates a large prime p, a prime divisor q having the structure $p = Nq^2 + 1$ correspondingly with $q^2 | (p-1)$, and a one-way hash function such as SHA-1 ($H = h(M)$).

2) **Step 2**: $x_1, x_2, \ldots, x_n$: group members' secret keys such that $1 < x_i < q$, x_i is selected randomly and known only by the member U_i.

3) **Step 3**: $y_1, y_2, \ldots, y_n$: group members' public keys such that $y_i = x_i^{q} \bmod p$ is computed and published by the group members U_i. Adding/deleting a member i requires adding/deleting the corresponding y_i by the clerk.

4) **Step 4**: The clerk computes group public key Y for all signers: $Y = \prod_{i=1}^{n} y_i^{y_i} \bmod p$.

B.2. The Multisignature Generation Phase

The scheme requires the clerk and other signing group members to carry out an exchange of data during the multisignature generation process.

1) **Step 1**: Each signer selects random number $k_i \in Z_q^*$ and computes $r_i = k_i^{q} \bmod p$. Then each signer U_i sends r_i to the clerk.

2) **Step 2**: The clerk computes the common randomization value $R = \prod_{i=1}^{n} r_i^{h(m_i)} \bmod p$ and computes the values

$E = h(R \| M)$ and $H = h(h(m_1) \| h(m_2) \| ... \| h(m_n))$. Then he sends (E, H) to each of the signers.

3) **Step 3**: Each signer computes its signature share s_i as follows $s_i = x_i^E k_i^H \bmod p$ and then each signer U_i sends s_i to the clerk.

4) **Step 4**: Once the clerk receives the individual signature (r_i, s_i) from i signers, he needs to verify the validity of this individual signature. The clerk check the signature of the individual as follows $s_i^q \equiv y_i^{y_i E} r_i^{h(m_i)H} \bmod p$. If all of the individual signatures are legal, then the clerk generates the multisignature (R, S) by computing $S = \prod_{i=1}^{n} s_i \bmod p$

Finally, (R, S) is the multisignature for the message $M = m_1 || m_2 || \ldots || m_n$.

B.3. The Multisignature Verification Phase

Prior to verifying the signature of a signed message, the parameters (p, q, Y) are made available to the verifier in an authenticated manner.

Verification of the multisignature is performed using the group public key Y.

1) **Step 1**: Using the multisignature (R, S) to compute $S'^q \equiv Y^E R^H \bmod p$.

2) **Step 2**: Compare values S' and S. If $S' = S$, then the signature is valid. Otherwise the signature is false.

The partial contents of the message $m_1 || m_2 || \ldots || m_n$ 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 $h(m_1) || h(m_2) || \ldots || h(m_{i-1}) || m_i || h(m_{i+1}) || \ldots || h(m_n)$ to verify the multisignature (R, S).

B.4. The Evidence Verification Phase

All of the individual signatures (r_i, s_i) can be used as evidence. To show that member U_i is responsible for signing only for the partial content m_i, (R, S), (r_i, s_i) and $M = m_1 || m_2 || \ldots || m_n$ are verified by $S^q = Y^E R^H \bmod p$ and $s_i^q \equiv y_i^{y_i E} r_i^{h(m_i)H} \bmod p$. If the two equations are satisfied, member U_i is responsible for signing only for the partial content m_i because the equation $s_i^q \equiv y_i^{y_i E} r_i^{h(m_i)H} \bmod p$ shows the relationship between the whole document, the partial content m_i, and member U_i.

IV. Analysis of Our Schemes and Disscusion

A. Correctness

Theorem 1 (our first scheme): The signature (R, S) is a valid multisignature for the message $M = m_1 || m_2 || \ldots || m_n$.

Proof: Indeed, using $\alpha^{S'} \equiv Y^E R^H \bmod p$ we get:

$$\alpha^{S'} = \alpha^{\sum_{i=1}^{n} s_i} = \alpha^{\sum_{i=1}^{n} (h(m_i)k_i H + x_i y_i E)} = \alpha^{\sum_{i=1}^{n} k_i h(m_i) H} \alpha^{\sum_{i=1}^{n} x_i y_i E}$$

$$= \prod_{i=1}^{n} \alpha^{k_i h(m_i) H} \prod_{i=1}^{n} \alpha^{x_i y_i E} = \prod_{i=1}^{n} r_i^{h(m_i)H} \prod_{i=1}^{n} y_i^{y_i E}$$

$$= R^H Y^E \bmod p = \alpha^S$$

$$\Rightarrow S' = S.$$

Theorem 2 (our second scheme): The signature (R, S) is a valid multisignature for the message $M = m_1 || m_2 || \ldots || m_n$.

Proof: Indeed, using $S'^q \equiv Y^E R^H \bmod p$ we get:

$$S'^q = \prod_{i=1}^{n} (x_i^E k_i^H)^q = \prod_{i=1}^{n} (x_i^E)^q (k_i^H)^q$$

$$= Y^E R^H = Y^E R^H \bmod p = S^q$$

$$\Rightarrow S' = S.$$

B. Security Analysis of Our Schemes

Our schemes can prevent Li et al.'s attack, as showed [3, 5].

For our schemes, the participants of the schemes have significant more possibilities to attack the schemes than outsiders.

B.1. The First Scheme

The first attack: Suppose that $n - 1$ signers that share some multisignatue (R, S) with the n-th signer are attackers trying to calculate the secret key of the n-th signer. The attackers know the values r_n and s_n generated by the n-th signer. This values satisfy the equation $\alpha^{s_n} = y_n^{y_n E} r_n^{h(m_n)H} \bmod p$, where the values r_n and E are out of the attackers control, since the value $r_n = \alpha^{k_n} \bmod p$, where k_n is a random number generated by the n-th signer, and E is the output of the hash function algorithm. 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 DLP, i.e., i) to find $k_n = \log_\alpha r_n$ and then compute $x_n = (y_n E)^{-1}(s_n - k_n h(m_i) H) \bmod q$ or ii) to compute $x_n = \log_\alpha y_n \bmod p$. If attackers determines the value of k_n (or x_n) first, then attackers has to overcome the challenges of the discrete logarithm problem and one-way hash function.

The second 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 $R^H = \alpha^S Y^{-E} \bmod p = \alpha^S (Y' y_n^{y_n})^{-E} \bmod p$. 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 (R^*, S^*) is individual signature of the n-th user and 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 [3, 5].

In this scheme, the signers generates only its share in the multisignature that corresponds exactly to the given document and to the assigned set of n users. Besides it is computationally difficult to manipulate with shares $s_1, s_2, \ldots, s_n$, and compose another signatures, relating to some different set of users. This fact imparts on the scheme the property of the internal integrity.

B.2. The Second Scheme

The proof is similar to the proof in the first scheme.

C. Performance Evaluation

C.1. Computational Costs

In this subsection, we use notations as showed in [5]. ME_p denotes one modular exponentiation operation modular p. MM_q (MM_p) denotes one modular multiplication operation modular q (or p). T_H denotes the computation cost of the hash function H. The computational costs required in the our proposed schemes are measured by the total caculations for group public key generation, multisignatures generation, and multisignatures verification, respectively.

1) Our first scheme

Group public key generation: $n(ME_p)$

Multisignatures generation: $n(ME_p)$; $n(ME_p) + (n + 2)(T_H)$; $2(MM_q) + n(T_H)$; $3n(ME_p) + 3n(MM_q) + n(T_H)$.

Mutisignature verification: $3(ME_p) + 1(MM_q) + 2(T_H)$.

2) Our second scheme

Group public key generation: $n(ME_p)$

Multisignatures generation: $n(ME_p)$; $n(ME_p) + (n + 2)(T_H)$; $n(ME_p) + 2(MM_p)$; $3n(ME_p) + 3n(MM_p) + n(T_H)$.

Mulsignature verification: $3(ME_p) + 1(MM_p) + 2(T_H)$.

3) Hwang et al.'s scheme

Group public key generation: $n(ME_p)$

Multisignatures generation: $n(ME_p) + n(T_H)$; $n(n + 1)(ME_p) + 2n(n + 1)(T_H)$; $2(MM_q) + n(T_H)$; $3n(ME_p) + 3n(MM_q) + 2n(T_H)$.

Mutisignature verification: $3(ME_p) + 1(MM_q) + 2(T_H)$.

Comparison of computational costs between the proposed schemes and the scheme of [5] is shown in Table I.

TABLE I. COMPUTATIONAL COMPARISON OF THE PROPOSED SCHEMES AND THE SCHEME OF [5]

Scheme	Total
The first scheme	$(6n + 3)(ME_p) + (3n + 3)(MM_q) + (3n + 4)(T_H)$
The second scheme	$(7n + 3)(ME_p) + (3n + 3)(MM_p) + (2n + 4)(T_H)$
Hwang et al.'s scheme	$(n^2 + 6n + 3)(ME_p) + (3n + 3)(MM_q) + (2n^2 + 5n + 4)(T_H)$

C.2. Size of Our Schemes

Our proposed schemes has two options for use of the multisignature.

If using value R as the first part of the multisignature, then the pair of numbers (R, S) is the multisignature.

The size of the first scheme is $|R| + |S| \approx |p| + |q|$.

The size of the second scheme is $|R| + |S| \approx |p| + |p|$.

If using value E as the first part of the multisignature, then the pair of numbers (E, S) is the multisignature.

The size of the first scheme is $|E| + |S|$.

The size of the second scheme is $|E| + |S|$.

Comparison of size of the multisignature between the proposed schemes and the scheme of [5] is shown in Table II.

TABLE II. COMPARISON OF SIZE OF THE MULTISIGNATURE BETWEEN THE PROPOSED SCHEMES AND THE SCHEME OF [5]

Scheme	The first option	The second option
The first scheme	$\|R\| + \|S\|$	$\|E\| + \|S\|$
The second scheme	$\|R\| + \|S\|$	$\|E\| + \|S\|$
Hwang et al.'s scheme	$\|R\| + \|S\|$	

C.3. Communication Costs

The communication costs required in the proposed schemes are measured by the total number of data transmission during the multisignature generation process (i.e. requires the clerk and other signing group members to carry out an exchange of data during the multisignature generation process).

Comparison of total number of data exchange between the proposed schemes and the scheme of [5] is shown in Table III.

TABLE III. COMPARISON OF TOTAL NUMBER OF DATA EXCHANGE BETWEEN THE PROPOSED SCHEMES AND THE SCHEME OF [5]

Scheme	Total
The first scheme	$3n$
The second scheme	$3n$
Hwang et al.'s scheme	$n^2 + n$

V. CONCLUSION

In this paper, we proposed two multisignature schemes with distinguished signing authorities. Our new schemes provide individual evidence to prevent confusion over authority due to malice. Moreover, the new schemes provide generation of the multisignature possessing with internal integrity.

In summary, as compared to Hwang et al.'s scheme, the proposed schemes have the following advantages:

1) Allow to reduce computation and communication costs as showed in Table I and Table III.

2) The size of the multisignatures are flexible as showed in Table II.

REFERENCES

[1] K. Itakura, K. Nakamura, "A public-key cryptosystem suitable for digital multisignatures," NEC Res. Dev., 1983, 71:1-8.

[2] L. Harn, "Digital multisignatures with distinguished signing authorities," Electr. Lett., 1999, 35(4):294-295.

[3] L. Harn, "Group-oriented (t, n) threshold digital signature scheme and digital multisignatures," IEE Proceedings: Computers and Digital Techniques, 1994, 141(5):307-313.

[4] T. S. Wu, C. L. Hsu, "ID-based multisignatures with distinguished signing authorities for sequential and broadcasting architectures," Appl. Math. Comput., 2002, 132(2):349-356.

[5] S. J. Hwang, M. S. Hwang, S. F. Tzeng, "A New Digital Multisignature Scheme With Distinguished Signing Authorities," J. Inform. Sci. Eng., 2003, 19(5):881-887.

[6] H. F. Huang, C. C. Chang, "Multisignatures with distinguished signing authorities for sequential and broadcasting architectures," Comput. Stand. Interfaces., 2005, 27(2):169-176.

[7] C. Popescu, "A Digital Multisignature Scheme with Distinguished Signing Responsibilities," Studies in Informatics and Control, 2003, 12(3):227-231.

[8] L. H. Dung, N. H. Minh, "New Digital Multisignature Scheme with Distinguished Signing Responsibilities," Int. J. Compt. Sci. Network Security, 2010, 10(1):51-57.

[9] Z. C. Li, L. C. K. Hui, K. P. Chow, C. F. Chong, H. H. Tsang, H. W. Chan, "Cryptanalysis of Harn digital multisignature scheme with distinguished signing authorities," Electr. Lett., 2000, 36(4):314-315.

[10] H. Y Chien, "Comments on ID-based multisignatures with distinguished signing authorities," Appl. Math. Comput., 2005, 170(2):1284-1289.

[11] E. J. Yoon and K. Y. Yoo, "Cryptanalysis of Two Multisignature Schemes with Distinguished Signing Authorities," 2006 International Conference on Hybrid Information Technology - Vol2 (ICHIT'06), 2006, p.492-495.

[12] J. Zhang and V. Zou, "On the Security of Huang-Chang Multisignature Schemes," Int. J. Network Security., 2007, 5(1):62-65.

[13] W. C. Yang, J. S. Jhou. "Known Signature Attack of ID-Based Multisignature Schemes," The 5th Inter. Conf. on Information Assurance and Security (IAS09), 2009, p.341-343.

[14] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inform. Theory., 1985, 31(4):469-472.

[15] L. Harn, "New digital signature scheme based on discrete logarithm," IET Electr. Lett., 1994, 30(5):396-398.

[16] N. A. Moldovyan, "Digital Signature Scheme Based on a New Hard Problem," Comput. Sci. J. Moldova, 2008, 16(2):163-182.

[17] N. H. Minh, N. A. Moldovyan, N. L. Minh, "New Multisignature Protocols Based on Randomized Signature Algorithms," 2008 IEEE International Conference on Research, Innovation and Vision for the Future in computing & Communication Technologies, 2008, p.124-127 (Hard copy).

[18] W. Stallings. Cryptography and Network Security Principles and Practices. Fourth Edition, Prentice Hall, 2005, p.592.