Send Orders for Reprints to reprints@benthamscience.ae

248 *The Open Cybernetics & Systemics Journal,* 2014, *8,* 248-253

Open Access

Secret Sharing Member Expansion Protocol Based on ECC

Yujie Wu[1], Daofeng Li[2] and Feng Wang[1,*]

[1]*College of Mathematical Sciences, Dezhou University, Dezhou Shan dong, China;* [2]*School of Computer and Electronics Information, Guangxi University, Nanning Guanxi, China*

Abstract: The protocols for member expansion in secret sharing schemes are very useful for key management in dynamic topology networks. In order to reduce the computation complexity of the existed protocols for member expansion in secret sharing schemes, a new protocol is proposed based on the problem of elliptic curve discrete logarithm. This paper examines fifteen most recent patens that were awarded in the area of secret sharing. Unlike traditional detailed patent reviews that are focused on applying the simple secret sharing method, the proposed protocol has the following merits: 1) there is no trust center ; 2) only requesting broadcast $2t+1$ times to generate the sub-secret for the new participant and the new participant can verify the truth of the sub-secret; 3) the old participants can verify the new sub-secret by the non-interactive zero-knowledge proof protocol; 4) In the sub-secret generation stage, not only sub-secrets of old participants but also the sub-secret of new participant is secure. Compared to the existed protocols, the proposed protocol has lower computational complexity and less communications. Therefore, the proposed protocol has higher performance and is suitable for resource-constrained terminals of dynamic networks.

Keywords: Elliptic curve, mobile Ad hoc networks, secret sharing, zero-knowledge proof.

1. INTRODUCTION

In 1979, Shamir and Blakley respectively proposed threshold secret sharing scheme based on different mathematic theory [1, 2]. Shamir's scheme was based on the Lagrange interpolating polynomial [1], while Blakley's scheme was based on linear projective geometry [2]. Subsequently, secret sharing becomes an important research field of modern cryptography and information security, a lot of researches have been proposed [3-7]. Secret sharing can prevent the abuse of power, therefore, it is applied to realize the trust recommendation of trust management in the mobile Ad hoc networks (MANETs) [8]. However, in practical application, the set of the participants may change frequently in MANETs, in order to ensure the security, it is needed to redistribute the secret to update each participant's share, this is not only difficult for key management but also increases the system's computing complexity and communication costs. To solve this problem, Dong *et al.* [9] proposed a protocol for member expansion in secret sharing schemes with broadcast channel in 2005. However, Jin *et al.* [10] pointed out that Dong *et al.*'s scheme cannot resist the attack of the old dishonest members. In order to improve the security and reduce communication of Dong *et al.*'s scheme, the references [11, 12] respectively proposed protocols for member expansion in secret sharing schemes without the trust center, and greatly reduce the communication costs. Reference [13] add public verification on the basis of the protocol [11, 12], not only the new participant can verify his/her share, but also other old participants can verify the new share without revealing, therefore it improves the level of security. However, the security of the above protocols are all based on the discrete logarithm problem of finite field, the computation of those protocols is very large, so they are not suitable for resource-constrained platform terminals of the wireless networks.

In order to reduce the computation of the protocols for member expansion in secret sharing schemes, a new protocol for member expansion in secret sharing scheme is proposed based on elliptic curve discrete logarithm problem, the protocol not only significantly reduces the computation, but also improves the security. The rest of this paper is organized as follows, section 2 introduces the current patents applying secret sharing; section 3 introduces the elliptic curve discrete logarithm problem and a protocol of Non-interactive zero-knowledge proof, section 3 describes the proposed protocol for member expansion, section 4 gives the security analysis and performance analysis of the proposed protocol, section V concludes our work.

2. PATENTS APPLYING SECRET SHARING

Through examining the patents applying secret sharing [14-19], the method of sharing secret is very simple. For example, U.S. Patent 20,130,173,910 titled "Method for sharing secret values between sensor nodes in multi-hop wireless communication network" [17] proposed a method for sharing a secret key between a source node and a destination node which includes (a) adding, at each forward intermediate node, a secret key between the forward intermediate node and a node before the forward intermediate node to the secret key sharing request message; (b) generating a shared secret key between the source node and the destination node from the secret key between the forward interme-

1874-110X/14 2014 Bentham Open

diate node and the node before the forward intermediate node added in the secret key sharing request message; (c) adding, at each backward intermediate node, a secret key between the backward intermediate node and a node before it to the secret key sharing response message; and (d) generating the shared secret key between the destination node and the source node from the secret key between the backward intermediate node and the node before it added in the secret key sharing response message. U.S. Patent 20,130,022,235 titled "Interactive secret sharing" [19] proposed an Interactive secret sharing that includes receiving video data from a source and interpreting the video data to track an observed path of a device.

3. PRELIMINARIES

In this section, we will introduce the elliptic curve discrete logarithm problem and a protocol of Non-interactive zero-knowledge proof.

3.1. The Elliptic Curve Discrete Logarithm Problem

Definition 1: E is a elliptic curve which defines on finite F_p, $E(F)$ is a rational subgroup of extension field F. P, Q are two random points of $E(F)$, if there is a integer m that satisfies $Q = mP$, then the number m is the elliptic curve discrete logarithm (ECDL) of the point Q, relative to point Q. Point P is called the base point (base point); From the equation $Q = mP$ and P, Q to resolve the m, is the elliptic curve discrete logarithm problem (ECDLP).

Let elliptic curve equation E: $y^2 = x^3 + ax = b \;\; a,b \in F_p$. The point operation of the elliptic curve is as follows:

(1) The inverse operation $P = (x, y) \in E(F), -P = (x, -y)$;

(2) Addition operation

Let $P = (x_1, y_1), Q = (x_2, y_2) \in E(F)\; P \neq -Q$, and $P + Q = R = (x, y)$, $x = \lambda^2 - x_1 - x_2, y = \lambda(x_1 - x_2) - y_1$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1}, P = Q, \text{The number multiplied's definition} \end{cases}$$

3.2. Non-interactive Zero-knowledge Proof

Zero-knowledge proof is one protocol by which a verifier can verify if a thesis is correct without knowing any useful information. The non-interactive zero-knowledge proof is a one-way, non-interactive protocol in which the verifier and the prover do not need to interact in the certification process. Here is a non-interactive zero-knowledge proof protocol.

Prover A, wants to prove that he/she knows the secret s to the verifier B, $H(\cdot)$ is a one-way hash function, g_1 and g_2 are two generators of the cyclic group G_p.

Prover A, computes: $h_1 = g_1^{\,s}, h_2 = g_2^{\,s}$ and publicizes (g_1, g_2, h_1, h_2). Then prover A randomly selects a number $\alpha \in Z^*$ and computes $b_1 = g_1^{\,\alpha}, b_2 = g_2^{\,\alpha}$, $c = H(b_1 \| b_2)$, $r = \alpha - sc$, then A publicizes (r, c) as evidence that shows he knows s.

Verifier B verifies the equation $c = H(g_1^r h_1^c \| g_2^r h_2^c)$, if the equation is established, B believes A.

4. PROTOCOL FOR MEMBER EXPANSION

A new verifiable protocol for member expansion is proposed based on the elliptic curve discrete logarithm problem in this section. The proposed protocol consists of three parts: (1) the system initialization phase; (2) a new sub-secret generation phase; (3) a new sub-secret validation phase.

4.1. System Initialization Phase

$\mathrm{P}_1, \mathrm{P}_2, \ldots, \mathrm{P}_n$ are the participants of the system to share the secret s; $GF(p)$ is a finite field and p is a large prime number; $E_p(a,b)$ is an elliptic curve defined on $GF(p)$, and G is the generator of $E_p(a,b)$, g_1 and h are two generators of $GF(p)$, $H(\cdot)$ is a one-way hash functions, there is a polynomial $f(x) = s + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$ $a_1, a_2 \text{£} \neg \text{£} \neg a_{t-1} \in GF(p)$ to distribute sub-secrets for participants P_i $i = 1, 2, \cdots, n$ by $s_i = f(i)$, s is the shared secret, any t members of n participants can construct the $f(x)$ by the Lagrange interpolation formula:

$$f(x) = \sum_{j=1}^{t} \left\{ f(i_j) \prod_{h \neq j} \frac{(x - i_h)}{(i_j - i_h)} \right\}.$$

Let, $\omega_j = \prod_{h \neq j} \dfrac{(x - i_h)}{(i_j - i_h)}$, the new participant is P_{n+1}, his/her private key and public key is d and $R = dG$, $g_2 = h^d$. $g(M) = y$ is a two variables function and $M = (x, y)$. The protocol requires broadcasting authentication information $\{G, E_p(a,b), sG, g_1, g_2\}$ for new member and other members to verify the new sub-secret.

4.2. New sub-secret Generation Phase

(1) $\mathrm{P}_1, \mathrm{P}_2, \ldots, \mathrm{P}_t$ are any t old members of n participants, they calculate and broadcast $Q_j = s_j \omega_j(0) G$, $U_j = s_j \omega_j(n+1) G$ $j = 1, 2, \cdots t$ (t broadcasts with $2t$ data);

(1) The i^{th} member P_i receives the other older members' broadcasting information and verifies their truth by $sG = \sum_{i=1}^{t} Q_i$. Then he/she computes:

$$M_{ij} = \begin{cases} s_i \omega_i(0) Q_j & i > j \\ (0,0) & i = j \\ -s_i \omega_i(0) Q_j & i < j \end{cases} \quad j = 1, 2 \cdots t, \; M_i = \sum_{j=1}^{t} g(M_{ij})$$

P_i randomly chooses point $T_i = (x_i, y_i) \in E_p(a,b)$ and computes: $W_i = T_i + s_i \omega_i(0) R$, $C_i = [s_i \omega_i(n+1) + M_i] x_i + y_i$, then he/she broadcasts cW_i C_i (t broadcast with $2t$ data).

(3) P_{n+1} receives the broadcast of the old members and calculates $W_i + (-d)Q_i$ to obtain $T_i = (x_i, y_i)$, then computes his/her sub-secret by $s_{n+1} = f(n+1) = \sum_{i=1}^{t} \frac{C_i - y_i}{x_i}$.

After that, P_{n+1} randomly selects $\alpha \in GF(p)$ and calculates evidence of s_{n+1} as follows:

$b_1 = g_1^{\alpha}, b_2 = g_2^{\alpha}$

$c = H(b_1 \| b_2)$,

$r = \alpha - cg(s_{n+1}G)$,

$X = g_1^{g(s_{n+1}G)}, Y = g_2^{g(s_{n+1}G)}$

Then P_{n+1} public (X, Y, r, c).

In the new sub-secret generating step, there are total of $2t+1$ broadcasts with $4t+4$ data.

4.3. Verification of the New sub-secret

P_{n+1} can verify his/her sub-secret s_{n+1} by the public information $(G, E_p(a,b), sG, Q_j)$ and the equation $s_{n+1}\omega_{n+1}(0)G = sG - \sum_{i=1}^{t-1} Q_j$. If the equation does not hold, P_{n+1} can find out s_{n+1} is incorrect.

Every one can verify the validity of the new sub-secret s_{n+1} by the non-interactive zero-knowledge proof protocol: first calculating $X = g_1^{g(\sum_{i=1}^{t} Q_i)}$, and then verifying $c = H(g_1^r X^c \| g_2^r Y^c)$, if the equation establishes, then the new sub-secret s_{n+1} is valid, otherwise it is invalid.

5. ANALYSIS OF THE PROTOCOL

In this section, we will analysis the protocol from three aspects: the truth, security and performance. In the truth analysis, we will give the demonstration of the equation in the verification of the protocol; in the security analysis, we will show the new participant's sub-secret and the old participants' sub-secrets are all secure; in the performance analysis, will show that the proposed protocol is more efficient than the existing protocol.

5.1. Truth Analysis

1) The old members can verify the information broadcasted by the other old members through the equation $sG = \sum_{i=1}^{t} Q_i$.

Assuming, P_k receives the other members' $Q_j = s_j\omega_j(0)G$ $j = 1, 2 \cdots t$ and $j \neq k$, he/she can compute $s_k\omega_k(0)G = sG - \sum_{i=1}^{k-1} Q_i - \sum_{i=k+1}^{t} Q_i$, because $Q_k = s_k\omega_k(0)G$, so, P_k can get $sG = \sum_{i=1}^{t} Q_i$, If the broadcasting information is false, then the equation does not hold, it can prevent the deception of the old members.

As the same, new member P_{n+1} can verify the old members through the equation $sG = \sum_{i=1}^{t} Q_i$ so the new member can also prevent the deception of the old members.

2) New member P_{n+1} can compute his/her sub-secret by the equation $s_{n+1} = f(n+1) = \sum_{i=1}^{t} \frac{C_i - y_i}{x_i}$

The new protocol is proposed based on Shamir secret sharing scheme. If the new member's sub-secret s_{n+1} is truth, s_{n+1} will meet the polynomial $s_{n+1} = f(n+1)$.

The verification of the new sub-secret is as follows:

Because

$$\begin{aligned} W_i + (-d)\mathrm{Q}_i &= T_i + \mathrm{s}_i\omega_i(0)R + (-d)\mathrm{Q}_i \\ &= T_i + \mathrm{s}_i\omega_i(0)(dG) + (\text{-}d)\mathrm{s}_i\omega_i(0)\mathrm{G} \\ &= T_i = (x_i, y_i) \end{aligned}$$

$C_i = [s_i\omega_i(n+1) + M_i]x_i + y_i$

So $\frac{C_i - y_i}{x_i} = s_i\omega_i(n+1) + M_i$,

By $M_{ij} = \begin{cases} s_i\omega_i(0)Q_j & i > j \\ (0,0) & i = j \ \ j = 1, 2 \cdots t \\ \text{-}s_i\omega_i(0)Q_j & i < j \end{cases}$, we can get $M_{ij} = -M_{ji}$

By the operation property of Elliptic curve point $-(x,y) = (x,-y)$, $g(M_{ij}) = -g(M_{ji})$, $M_i = \sum_{j=1}^{t} g(M_{ij})$,

So,

$\sum_{i=1}^{t} M_i = \sum_{i=1}^{t}\sum_{j=1}^{t} g(M_{ij}) = 0$,

Then,

$$\begin{aligned} \sum_{i=1}^{t} \frac{C_i - y_i}{x_i} &= \sum_{i=1}^{t} (s_i\omega_i(n+1) + M_i) \\ &= \sum_{i=1}^{t} (s_i\omega_i(n+1)) + \sum_{i=1}^{t} M_i \\ &= \sum_{i=1}^{t} (s_i\omega_i(n+1)) = f(n+1) \\ &= s_{n+1} \end{aligned}$$

P_{n+1} can verify the correctness of new sub-secret s_{n+1} by

$s_{n+1}\omega_{n+1}(0)G = (sG - \sum_{i=1}^{t-1} \mathrm{s}_i\omega_i(0)G)$.

Because

$s = \sum_{i=1}^{t-1} \mathrm{s}_i\omega_i(0) + s_{n+1}\omega_{n+1}(0)$,

So,

$sG = \sum_{i=1}^{t-1} s_i \omega_i(0)G + s_{n+1}\omega_{n+1}(0)G$,

Then,

$s_{n+1}\omega_{n+1}(0)G = (sG - \sum_{i=1}^{t-1} s_i \omega_i(0)G)$.

Every one can publicly verify the new sub-secret by $c = H(g_1^r X^c \| g_2^r Y^c)$

In order to ensure the security of the new sub-secret and let old members verify the new sub-secret, a non-interactive zero-knowledge proof protocol is utilized by verifying the equation: $c = H(g_1^r X^c \| g_2^r Y^c)$.

P_i computes,

$g_1^{g(\sum_{j=1}^{t} Q_j)} = g_1^{g(\sum_{j=1}^{t} s_j \omega_j(n+1))} = g_1^{g(s_{n+1}G)} = X$, because of; $r = \alpha - cg(s_{n+1}G)$, $Y = g_2^{g(s_{n+1}G)}$,

So, $g_1^r X^c = g_1^{\alpha - cg(s_{n+1}G)}(g_1^{g(s_{n+1}G)})^c = g_1^{\alpha} = b_1$, $g_2^r Y^c = g_2^{\alpha - cg(s_{n+1}G)}(g_2^{g(s_{n+1}G)})^c = g_2^{\alpha} = b_2$,

By the equation;

$b_1 = g_1^{\alpha}, b_2 = g_2^{\alpha}$, $c = H(b_1 \| b_2)$,

So,

$c = H(g_1^r X^c \| g_2^r Y^c)$.

5.2. Security Analysis

The security of the proposed protocol is based on the problem of elliptic curve discrete logarithm. The protocol can generate the sub-secret for new participant without threatening the security of the shared secret and the old members' sub-secrets. In the generation progress, the new participant and the old members cooperate to generate the new sub-secret without trust center. Not only the new participant but also the old members can verify the new sub-secret.

(1) The new sub-secret is security

In the generation progress, only the new participant can generate the new sub-secret. However, the old members can get nothing about the new sub-secret. P_i received the other members' broadcast information cW_i C_i, and $W_j = T_j + s_j \omega_j(0)R$, $C_j = [s_j \omega_j(n+1) + M_j]x_j + y_j$, if P_i can get $s_j \omega_j(n+1)$ from C_j, he/she will generate the new sub-secret, however, P_i can not get $s_j \omega_j(n+1)$ from C_j. Because it needs to get T_j from W_j by $s_j \omega_j(0)R = s_j \omega_j(0)(dG)$, which will face the problem of elliptic curve discrete logarithm.

In addition, the old members can get nothing about the new sub-secret in the public verification progress. For example, P_i wants to get s_{n+1} from (X, Y, r, c), $X = g_1^{g(s_{n+1}G)}$, $Y = g_2^{g(s_{n+1}G)}$, however, it will not only be faced with the problem of discrete logarithm over finite fields but also the problem of elliptic curve discrete logarithm. If P_i wants to get s_{n+1} from $r = \alpha - cg(s_{n+1}G)$, he/she must know the random number α. So P_i cannot get $g(s_{n+1}G)$; even if P_i gets $g(s_{n+1}G)$, he/she has to face the problem of the elliptic curve discrete logarithm to get s_{n+1}.

(2) The old members' sub-secrets are security

At first, P_i receives the broadcasting information cW_i C_i from P_j, if he/she wants to get P_j 's sub-secret, he/she must get $s_j \omega_j(0)$ from $s_j \omega_j(0)R = s_j \omega_j(0)(dG)$, which will face the problem of elliptic curve discrete logarithm.

Second, after the new participant P_{n+1} receives the broadcasting information $Q_j = s_j \omega_j(0)G$, he/she must resolve the problem of elliptic curve discrete logarithm to get the sub-secret s_j.

The new participant P_{n+1} also cannot get the sub-secret s_j from the broadcasting information cW_i C_i, because P_{n+1} can only compute $s_j \omega_j(n+1) + M_j$ by W_j and C_j, in order to get $s_j \omega_j(n+1)$, P_{n+1} has to get M_j, however because $M_j = \sum_{i=1}^{t} g(M_{ij})$,

$$M_{ij} = \begin{cases} s_i \omega_i(0) Q_j & i > j \\ (0,0) & i = j \ j = 1, 2 \cdots t \\ -s_i \omega_i(0) Q_j & i < j \end{cases}$$

、 $Q_j = s_j \omega_j(0)G$, so P_{n+1} must get M_{ij} to obtain M_j, which will face the problem of elliptic curve discrete logarithm.

5.3. Performance Analysis

In this section, we compare the system performances of our scheme with the current protocols in Table **1**. As the result shown in Table **1**, Ref [11] broadcasts $3t+2$, $9t+6$ data, Ref [12] broadcasts $2t$, $3t$ data, Ref [13] and our protocol both broadcast $2t+1$, $4t+4$ data, so the Ref [12] is the most efficient, however, Ref [12] cannot publicly verify the new sub-secret, and our protocol can release public verifiability. In the new sub-secret generated and verifiable computational complexity, Ref [11] is $13tT_m + (13t+4)T_e$ and $11T_m + 8T_e$, Ref [12] is $t(t+5)T_m + 2t(t+5)T_e$ and $tT_m + T_e$. Ref [13] is $(4t+7)T_m + t(t+7)T_e$ and $(t+1)T_m + 5T_e$. Our protocol is $4T_e + (t^2+t+1)T_m + (t^2+t+2)T_{ec}$ and $4tT_e + 2tT_m$. Through the comparison of the new sub-secret generated and verifiable computational complexity, we can find that the Ref [11, 12] all need a lot of modular exponentiation computation, and our protocol only performs $4tT_e$. So the protocols of Ref [11-13] cannot apply for the lower communication and computation networks. However, our protocol mainly performs modular multiplication computation and elliptic curve product computation, the amount calculation of the protocol is less, so the proposed protocol is suitable for mobile communications encryption, e-commerce, and so on. In addition, the protocol can realize public verifiability to avoid new member

Table 1. Performance comparison between our protocol and Ref. [11-13].

	Ref [11]	Ref [12]	Ref [13]	Our Protocol
The number of broadcasts	$3t+2$	$2t$	$2t+1$	$2t+1$
Broadcast data	$9t+6$	$3t$	$4t+4$	$4t+4$
Trust Center	*No*	*No*	*No*	*No*
Publicly verify	*No*	*No*	*Yes*	*Yes*
New sub-secret generating complexity	$13tT_m+(13t+4)T_e$	$t(t+5)T_m+2t(t+5)T_e$	$(4t+7)T_m+t(t+7)T_e$	$4T_e+(t^2+t+1)T_m+(t^2+t+2)T_{ec}$
New sub-secret verifiable complexity	$11T_m+8T_e$	tT_m+T_e	$(t+1)T_m+5T_e$	$4T_e+3T_m+T_{ec}$

T_e : the time for performing a modular exponentiation computation; T_m : the time for performing a modular

deceiving. In general, our proposed protocol outperforms the current schemes and has more functions.

6. CURRENT & FUTURE DEVELOPMENTS

This paper reviewed the current protocols for member expansion in secret sharing and pointed out their problems. Taking all these problems into consideration, a new public verifiable protocol for member expansion in secret sharing based on the problem of elliptic curve discrete logarithm was proposed. The proposed protocol remains the merits of the current protocols such as not needing trust centers and less communication. Because of mainly performing modular multiplication computation and elliptic curve product computation, the computation of the proposed protocol is greatly reduced. Through the security analysis, the sub-secrets of the new participant and the old participants are all secure. Except that, the proposed protocol can release public verifiability and withstand the conspiracy attack of the new participant, so improving the level of the security. In general, the proposed protocol outperforms the current schemes in performance and security. Therefore the proposed protocol is suitable for application in mobile communication encryption, e-commerce of wireless networks. In the future, we will further reduce the computation of the proposed protocol and design a new scheme without modular exponentiation computation.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

We would like to thank the editors for their detailed and valuable advice. This research is supported by Scientific and Technological Research Program of Chongqing Municipal Education Commission (Grant No.KJ120504), National Nature Science Foundation of China (Grant No.60970135, No.61170282).

REFERENCES

[1] A. Shamir, "How to share a secret", *Commun. ACM*, vol. 22, no.11, pp. 612-613, 1979.

[2] G. R. Blakley, "Safeguarding cryptographic keys", in: Proceedings of AFIPS'79, vol. 48, pp.313-317, 1979.

[3] C. Guo, Z. H. Wang, C. C. Chang C. Qin, "A secret image sharing scheme with high quality shadows based on exploiting modification direction", *J. Multimedia,* vol. 6, no. 4, pp. 341-348, 2011.

[4] H. B. Zhang, X. F. Wang, Y. P. Huang, "A novel ideal contrast visual secret sharing scheme with reversing", *J. Multimedia*, vol. 4, no. 3, pp. 104-111, 2009.

[5] F. Wang, L. Z. Gu, S. H. Zheng, Y. X. Yang, Z. M. Hu, "A verifiable multi-policy secret sharing scheme", *J. Beijing Univ. Posts Telecommun.*, vol. 33, no. 6, pp. 72-75, 2010.

[6] Y. Q. Cai, Z. H. L, Y. Yang. "Rational multi-secret sharing scheme based on bit commitment protocol", *J. Netw.*, vol. 7, no. 4, pp. 738-745, 2012.

[7] F. Wang, J. Z. Zhang, "Dynamic verified threshold multi-secret sharing scheme based on RSA cryptosystem", *Appl. Res. Comput.*, vol. 25, no. 6, pp. 1806-1808, 2008.

[8] O. Mawloud, C. Yacine, A. Bouabdallah, "Reliable and fully distributed trust model for mobile ad hoc networks", *Comput. Security*, vol.28, pp. 199-214, 2009.

[9] P. Dong, X. H. Kuang, X. C. Lu, "A non-interactive protocol for member expansion in secret sharing scheme", *J. Softw.*, vol. 16, no. 1, pp. 116-120, 2005.

[10] Y. M. Jin, Q. L. Xu, "Cryptanalysis of a secret sharing protocol for member expansion", *Comput. Eng. Appl.*, vol. 21, no. 27, pp. 94-95, 2006.

[11] F. Wang, J. Z. Zhang, "New verifiable protocol for member expansion in secret sharing schemes", *Comput. Eng. Appl.*, vol. 42, no. 28, pp. 122-124, 2007.

[12] J. F. Xu, G. H. Cui, Q. Cheng, Z. Zhang "Cryptanalysis of a non-interactive protocol for member expansion in a secret sharing scheme", *J. Commun.*, vol. 30, no. 10, pp. 118-123, 2009.

[13] L. Li, L. P. Mo, K. Q. Zhou, "A publicly verifiable secret sharing new member expansion protocol", *Comput. Appl. Softw.*, vol. 28, no. 5, pp. 123-125, 2011.

[14] K. Masanobu. "*Secret sharing system, apparatus, and storage medium*". U.S. Patent 20140013439, Jan 9, 2014.

[15] E. P. Alan, "*Change-Tolerant Method of Generating an Identifier for a Collection of Assets in a Computing Environment Using a Secret Sharing Scheme*", U.S. Patent 20140007252, Jan 2, 2014.

[16] H. Koki, "*Secret sharing system, secret sharing apparatus, secret sharing method, secret sorting method, secret sharing program*", U.S. Patent 20130182836, Jul 18, 2013.

[17] H. C. Seon, "*Method for sharing secret values between sensor nodes in multi-hop wireless communication network*", U.S. Patent 20130173910, Jul 4, 2013.

[18] N. Ryo, "*Secret sharing system , sharing apparatus , share management apparatus, acquisition apparatus, secret sharing method, program and recording medium*", U.S. Patent 20130114815, May 9, 2013.

[19] P. B. Robert, "*Interactive secret sharing*", U.S. Patent 20130022235, Jan 24, 2013.

Received: September 22, 2014 Revised: November 30, 2014 Accepted: December 02, 2014