Asian Journal of Information Technology, 4 (9): 861-867, 2005

Secrets Sharing Method for Real Time Applications

[1]Kuo Feng Hwang, [2]I-En Liao and [2]Po-Whei Huang
[1]Department of Applied Mathematics, [2]Department of Computer Science,
National Chung Hsing University, Taiwan

Abstract: In this study, each mobile agent can shares secrets with other agents by holding only his secret key and can on-line dynamic change access structure for real time applications. It provides great capabilities for many practical cases on flexible workflow technology driving the networked economy applications. Only the qualified subset of agents or agents can get the share secrets that suit for e-commerce distributed systems for real time applications. Each participant or agent is allowed to check whether another participant provides the true information or not in the recovery phase. We proposed a new solution based on systematic block codes can dynamic change access structure with m share secrets that prepare the generator matrix G(2m+1, m+1) which can be pre-computed and suit for VLSI design in hardware using in real time distributed systems. We can increase efficient and security on the process of e-market information system for real time applications.

Key words: Generalized secrets sharing, information security, RSA cryptosystem, E-commerce

INTRODUCTION

A generalized secret sharing scheme is an important issue of Web-based competitive agents for the negotiating, buying and selling in e-commerce. A secret sharing scheme is a technique to share a secret among a group of agents or agents. The dealer assigns some subsets of agents as qualified subsets have the following two properties[1-6]:

- If all the agents of a qualified subset provide their shadows, they can recover the shared secret easily.
- If all the agents of an unqualified subset provide their shadows, they reveal no knowledge about the shared secret.

The set contains all the qualified subset is named the access structure£F.

There are extended to a generalized secret sharing model and a secrets sharing model by Blundo *et al.*[7,8]. Cachin[9] defined an on-line secret sharing scheme with general access structures. Cachin's scheme is based on a computational assumption that the agents can be added or deleted dynamically without redistributing new shadows secretly to the old agents. Unfortunately, Cachin's scheme does not allow the shadows to be reused after the shared secret is recovered. In succession, Pinch [6] proposed a modified version of Cachin's scheme. Pinch's scheme allows an arbitrary number of shared secrets to be recovered where each participant only holds one shadow. However, in Pinch's scheme, the agents of the qualified subset have to cooperate to recover the shared secret in a specific order for the sake of security. In Cachin's and Pinch's schemes, the dealer has to store the shadow of each participant to maintain the 'on-line' property. This makes the dealer record a too heavy load of secret data.[10-12]

This study propose a new computationally secure on-line secret sharing scheme with general access structures. Present scheme allows the agents to share many secrets although each one of them only holds one secret key. In present scheme, the agents may be dynamically added or deleted without having to redistribute new shadows secretly to the older agents. The dealer can also share new secrets among the agents at any them without changing or redistributing new shadows secretly. Additionally, present scheme also provides the capability to detect and identify of cheaters. Altogether, the scheme we shall propose here overcomes the drawbacks of the previous schemes and provides great capabilities for many applications.

We know that Ayanoglu *et al.*[13] designed a special type of linear block codes in the error control coding theory. Deng *et al.*[14] used the (2(m+n)-1, m+n) systematic block codes, where n is the number of agents and m is the number of secrets to be distributed. This study, we propose an efficient generalized secrets sharing scheme by using the (2m+1, m+1) systematic block codes where m is the number of secrets to be distributed in the number of n agents.

Corresponding Author: Mr. Kuo Feng Hwang, Department of Information Management, The Overseas Chinese Institute of Technology, No. 100, Chiao Kwang Road Taichung 40721, Taiwan
Tel: 886 4 2701 6855 2131 Fax: 886 4 2707 5420

THE SYSTEMATIC BLOCK CODES

A G (N,K), where N is the length and K is the dimension. D = $(d_1, d_2, \ldots, d_K)^T$ to be a vector of K information symbols, where d_i are in GF(2^m). V=GD=$(v_1,v_2, \ldots, v_N)$ is the corresponding code word. A systematic block code is a linear block code where the first K elements are identical to the information symbols ($d_1, d_2, \ldots, d_K$) and the last N-K elements denoted as ($c_1, c_2, \ldots, c_{N-K}$) are parity symbols.[15] Ayanoglu *et al.*[15] designed a systematic block code generator matrix G(N, K) =[I : P] where I is the KxK identity matrix and P is a GF(2^m) matrix in GF(2^m) where N=2(p+n)-t, K=p+n, p the number of secrets, n is the number of agents and t is the threshold value for these secrets[15]. The generator matrix G (2 (p+n) -t, p+n) as follows:

$$G(2(p+n)-t,p+n) = \begin{bmatrix} I \\ M \end{bmatrix} \quad (1)$$

D=$(d_1, d_2, \ldots, d_{p+n})^t$ is a vector of p+n unknown symbols which consist of secrets and pseudo shadows of agents, where V=GD=$(d_1,d_2, \ldots, d_{p+n}, c_1, c_2, \ldots, c_{p+n-t})$,

$$c_i = \sum_{j=1}^{p+n} g^{(i-1)(j-1)} d_j, \quad \text{where} \quad 1 \le i \le p+n-t \quad (2)$$

Mobile agents keep ($d_1, d_2, \ldots, d_{p+n}$) secret but public values ($c_1, c_2, \ldots, c_{p+n-t}$), there are p+n-t linear equations with p+n unknown symbols. We given these p+n-t equations, these unknown symbols can not be uniquely determined since p+n-t < p+n. [15]

THE PROPOSED GENERALIZED MOBILE AGENTS SECRETS SHARING METHOD

Our generalized mobile agents secrets sharing method can apply in single secret. Our secret sharing method contains four phases: the initialization phase, the construction phase, the recovery phase and the reconstruction/renew phase. We assume that there are n agents, $p_1, p_2, \ldots, p_n$ using secret key K_0 to recover a sharing a secret M_1 within the access structure $\Gamma = \{\gamma_1, \gamma_2, \ldots, \gamma_r\}$

Initialization phase: The original signer must prepare the following parameters:

- Two large primes p and q and their product N=p*q, where N is strong enough to combat a factoring attack and L=lcm((p-1),(q-1)).
- An element g which is a primitive root over both GF(p) and GF(q).
- A large prime Q, which is larger than N.
- The identify number of participant p_i is ID_i.

Then the dealer publishes (N, g, Q) and all (ID_i, y_i) as the public keys and he keep (p, q) as the secret keys. Each participant p_i has a key pair (x_i, y_i) where x_i is a secret key chosen by the participant p_i and the public key $y_i = g^{x_i} \bmod N$.

Construction phase: In this phase, the dealer computes and publishes some information for each qualified subset in access structure $\Gamma = \{\gamma_1, \gamma_2, \ldots, \gamma_r\}$. The dealer does not need to distribute any information to any participant secretly. The dealer only needs to publish some information on the public bulletin. The agents of any qualified subset y_i can cooperate for the secret key K_0 to get the share secret M_1 by using these information and some values generated from their shadows in the recovery phase to recover share secret M_1. The dealer generates the public information as follows.

- Randomly selects an integer S_0 from the interval [2,n] for the secret key K_0 to recover a sharing secret M_1 such that S_0 is relatively prime to (p-1) and (q-1).
- Compute $P_0 = g^{S0} \bmod N$.
- Generate an integer h_0 such that $S_0 * h_0 = 1 \bmod L$.
- Publish P_0 and h_0 for the secret key K_0 for recovery share secret M_1 on the public bulletin.
- For each qualified subset $y_i = \{p_{j1}, p_{j2} \ldots p_{jt}\}$ of Γ. The dealer computes T_j, the public information, as follows:
  Compute

$$H_j = K_0 \oplus (y_{j1}^{S_0} \bmod N) \oplus (y_{j2}^{S_0} \bmod N) \oplus \ldots \oplus (y_{jr}^{S_0} \bmod N)$$

- Use t + 1 points:

$$(0, H_j), (ID_{j1}, y_{j1}^{S_0}), (ID_{j2}, y_{j2}^{S_0}), \ldots, (ID_{jt}, y_{jt}^{S_0})$$

and Lagrange interpolation[11] to construct a t-degree polynomial $f_j(X)$:

$$f_j(X) = \sum_{L=1}^{t} [(y_{jL}^{S_0} \bmod N)(X / ID_{jL}) \prod_{\substack{k=1 \\ k \ne L}}^{t} \frac{(X - ID_{jk})}{ID_{jL} - ID_{jk}}] \bmod Q \quad (3)$$

Where t is the number of the agents in qualified subset.

- Compute and publish $T_j = f_j(1)$ on the public bulletin.
- The G is the generator matrix for systematic block codes (2*1+1,1+1).
- The dealer prepares the information vector D = (M_1, K_0).

We computes V=GD=(M_1, K_0, c_1) and Finally, the system publishes public values (P_0, c_1) in an authenticated manner [3,8,16], where c_1 can be represented as $c_1 = M_1 + K_0$. We know that the generator matrix G can be pre-computed

and the generator matrix with lager dimension can be easily constructed by extending from a generator matrix with smaller dimension. All the public values for secret M_1 are listed as $M_1 : (P_0, h_0, N, T_1, T_2, \ldots, T_r, c_1)$

Secret reconstruction phase: When members want to recover the secret M_1 there must be in the access structure $\Gamma = \{\gamma_1, \gamma_2, \ldots, \gamma_r\}$. Within the qualified subset $y_j = \{p_{j1}, p_{j2}, \ldots\ldots, p_{jt}\}$ of Γ for each p_{ji}, he computes his shadow $(P_0)^{xji}$. The agents of the minimal qualified subset cooperates to recover the shared secret K.

- Each participant gets $(P_0, h_0, N, T_1, T_2, \ldots, T_r, c_1)$ from the public bulletin.
- Each participant p_{ji}, computes and provides $S'_{ji}$where x_{ji} is the secret key of p_{ji}.
- Any body can verify S'_{ji} provided by p_{ji}, if $S'^{h0}_{ji} \bmod N = y_{ji}$then S'_{ji} is true; otherwise, S'_{ji} is false and may be a cheater. The y_{ji} is public value of participant p_{ji}.
- Get T_j from the public bulletin and use r+1 points $(1, T_j)$, (ID_{j1}, S'_{j1}) (ID_{j2}, S'_{j2}), …, (ID_{jt}, S'_{jt}) and use Lagrange interpolation to reconstruct the t-degree polynomial $f_j(X)$:

$$f_j(X) = \sum_{L=1}^{t}[S'_{jL}(X-1)/(ID_{jL}-1)\prod_{\substack{k=1\\k\neq L}}^{t}\frac{(X-ID_{jk})}{ID_{jL}-ID_{jk}}]\bmod Q \quad (4)$$

- Compute $H_j = f_j(0)$s
- Recover the secret key $K_0 = H_j \oplus S'_{j1} \oplus S'_{j2} \oplus \ldots \oplus S'_{jt}$
- The equations $c_1 = M_1 + K_0$. We know c_1 and K_0 then the share secret M_1 can be uniquely determined.

Multiple share secrets for generalized access structure: Now we considered the case there are multiple secrets to be shared within generalized access structure

Public value broadcasting phase: We assume that there are m share secrets $(M_1, M_2, \ldots, M_m)$ the system executes the following jobs.

The dealer generates the public information as follows.

- Randomly selects an integer S_i from the interval[2, N] for the secret key K_i to recover m sharing secrets $(M_1, M_2, \ldots, M_m)$ such that S_i is relatively prime to (p-1) and (q-1).
- Compute $P_i = g^{Si} \bmod N$.
- Generate an integer h_i such that $S_i * h_i = 1 \bmod L$.
- Publish P_i and h_i for the secret key K_i for recovery share secrets $(M_1, M_2, \ldots, M_m)$ on the public bulletin.
- For each qualified subset $Y_j = \{p_{j1}, p_{j2}, \ldots\ldots, p_{jt}\}$ of T. The dealer computes $T_j = f_j(1)$ the public information, as follows:

Compute

$$H_j = K_i \oplus (y_{j1}^{Si} \bmod N) \oplus (y_{j2}^{Si} \bmod N) \oplus \ldots \oplus (y_{jt}^{Si} \bmod N)$$

- Use t + 1 points:$(0, H_j)$, (ID_{j1}, y^{si}_{j1}), (ID_{j2}, y^{si}_{j2}),…, (ID_{jt}, y^{si}_{jt}) and Lagrange interpolation[10] to construct a t-degree polynomial $f_j(X)$:

$$f_j(X) = \sum_{L=1}^{t}[(y_{jL}^{Si} \bmod N)(X/ID_{jL})\prod_{\substack{k=1\\k\neq L}}^{t}\frac{(X-ID_{jk})}{ID_{jL}-ID_{jk}}]\bmod Q$$

Where r is the number of the agents in qualified subset.

- Compute and publish $T_j = f_j(1)$ on the public bulletin.
- Prepare the generator matrix G(2m+1, m+1) which can be pre-computed.
- The dealer prepares the information vector $D = (M_1, M_2, \ldots, M_m, K_i)$.

We computes $V = GD = (M_1, M_2, \ldots, M_m, K_i, c_1, c_2, \ldots, c_m)$, where c_j can be represented as follows.

$$c_j = \sum_{L=1}^{k} g^{(j-1)(L-1)} M_j + K_i \text{ , where } 1 \le j \le m \quad (5)$$

Publish $(P_i, h_i, N, T_1, T_2, \ldots, T_r, c_1, c_2, \ldots, c_m)$ all the public values are in an authenticated manner.

Secret reconstruction phase: When members want to recover the share secret list $(M_1, M_2, \ldots, M_m)$, there must be a co-operation among access structure.

The agents of any qualified subset, y_j, can cooperate to get secret key K_i to recover the share secret $(M_1, M_2, \ldots, M_m)$ by providing the information generate from their shadows and getting the public information on the bulletin. Note that agents do not need to provide their secret key directly. He only provides information generated from his secret key. Nobody can trace the real secret key of each participant with this provided information. At the same time, in the phase, on can also check whether the information that was provided by each participant is true or not. Now we show how each minimal qualified subset $y_j = \{p_{j1}, p_{j2}, \ldots\ldots, p_{jt}\}$ of Γ, the agents of the minimal qualified subset cooperate for the secret key K to recover the share secret list $(M_1, M_2, \ldots, M_m)$.

- Each participant gets (P_i, h_i, N) from the public bulletin.
- Each participant p_{ji}, computes and provides $S'_{ji} = P_0^{x_{ji}} \bmod N$ where x_{ji} is the secret key of p_{ji}.
- Any body can verify S'^{hi}provided by p_{ji}, if $S'^{hi}_{ji} \bmod N = y_{ji}$ then S'_{ji} is true; otherwise, S'_{ji} is false and may be a cheater.
- Get T_j from t he public bulletin and use r+1 points $(1, T_j)$, (ID_{j1}, S'_{j1}) (ID_{j2}, S'_{j2}), …, (ID_{jt}, S'_{jt}) and use

Lagrange interpolation to reconstruct the t degree polynomial $f_j(X)$:

$$f_j(X) = \sum_{L=1}^{t}[S'_{jL}(X-1)/(ID_{jL}-1)\prod_{\substack{k=1\\k\neq L}}^{t}\frac{(X-ID_{jk})}{ID_{jL}-ID_{jk}}]\bmod Q$$

- Compute $H_j=f_j(0)$
- Recover the secret key $K_0 = H^j \oplus S'_{j1} \oplus S'_{j2} \oplus \ldots \oplus S'_{jt}$
- For each qualified subset $y_j = \{p_{j1}, p_{j2}, \ldots\ldots, p_{jt}\}$ of T that the secret key K_i for recovery share secrets (M_1, M_2, …, M_m).

$$c_j = \sum_{L=1}^{k} g^{(j-1)(L-1)} M_j + K_i \text{ , where } 1 \le j \le m$$

For each p_{ji}, he computes his shadow $(P_i)^{xji}$ and then contributes this shadow to the qualified subset. Now the number of missing symbols is 1, which is the secret key K_i. So the share secret list (M_1, M_2, …, M_m) can be uniquely determined.

Reconstruction/renew phase: There are many practical applications in situations where the access structure and the agents, or even the shared secret itself, have to be changed; for example, when agents quit or new agents join the group. In this phase, the shadow of each participant in the proposed scheme can be reused when the group dynamically absorbs or disenrolls agents in real time system. These capabilities are gained by publishing additional information on the public bulletin. We shall show how the proposed scheme achieves these objectives in the following.

The generalized access structure $T = \{\gamma_1, \gamma_2, \ldots, \gamma_r\}$ is easily changeable.

Case 1: adding a new qualified subset $\{y_{r+1}\}$

If the new qualified subset contains an old minimal qualified subset in the access structure $T = \{\gamma_1, \gamma_2, \ldots, \gamma_r\}$ The dealer should perform the construction phase to publish information $T_{r+1}=f_{r+1}(1)$ for the new qualified subset on the public bulletin.

The dealer publish (P_i, h_i, N, T_1, T_2,…, T_r, T_{r+1}, c_1 , c_2 , …, c_m) all the public values are in an authenticated manner.

Case 2: canceling qualified subsets $\{y_r\}$

Suppose we have to cancel the qualifications of some qualified subsets. If the new qualified subset in the access structure $T = \{\gamma_1, \gamma_2, \ldots, \gamma_r\}$. For the sake of security, the secret key should be renewed. In this case, the dealer performs the construction phase to alter the information corresponding to the renewed shared secret on the public bulletin for the reset of the qualified subsets. In this way, the public information of each canceled qualified subset can be removed from the public bulletin.

The dealer publish (P'_i, h'_i, N, T'_1, T'_2,…, T'_{r-2}, T'_{r-1}, c_1 , c_2 , …, c_m) all the public values are in an authenticated manner. For the sake of security, the P'_i and h'_i should be renewed.

Cheaters can be detected and identified easily

Each participant gets (P_i, h_i, N) from the public bulletin. The participant p_{ji}, computes and provides $S'_{ji} = P_0^{x}{}_{ji} \bmod N$ where x_{ji} is the secret key of p_{ji}.. Any body can verify S'_{ji} provided by p_{ji}, if S'^{hi}_{ji}, then S'_{ji} is true; otherwise, S'_{ji} is false and may be a cheater. Because y_{ji} is the public key well known by all of the group members.

The agents are easily changeable in generalized access structure

Case 1: Add new agents, p_{L1}, p_{L2}, …, p_{Lv}

When add new agents, p_{L1}, p_{L2}, …, p_{Lv}, join the group in generalized access structure. Let $T = \{\gamma_1, \gamma_2, \ldots, \gamma_r\}$ be the set of the new minimal qualified subsets, which are included in the access structure. Each ne\w participant p_{Li} randomly selects an integer x_{Li} from the interval[2,N] as his x_{Li} secretly and provides $y_{Li}=g^{XLi} \bmod N$ as well as his identity number ID_{Li} to the dealer in the initialization phase. Then the dealer performs the construction phase to publish information for each new minimal qualified subset. Note that the older agents do not alter their shadows in this case.

The dealer publish $(P'_i, h'_i, N, T'_1, T'_2, \ldots, T'_r, c_1, c_2, \ldots, c_m)$ all the public values are in an authenticated manner. For the sake of security, the $P'_i, h'_i, T'_1, T'_2, \ldots, T'_r$ should be renewed.

Case 2: Agents p_{U1}, p_{U2}, …, p_{UV} disenrolled

When agents p_{U1}, p_{U2}, …, p_{UV} disenrolled. That some corresponding minimal qualified subsets should be deleted from the a ccess structure. Let $T = \{\gamma_1, \gamma_2, \ldots, \gamma_r\}$ be the set of the new minimal qualified subsets, which are included in the access structure. The secret key should be renewed for security consideration. The dealer performs the construction phase to publish some information of the renewed shared secret on the public bulletin for each qualified subset in the alternative access structure. At the same time, the rest of the authorized qualified agents still hold the old shadows.

The dealer publish (P'_i, h'_i, N, T'_1, T'_2,…, T'_r, c_1 , c_2 , …, c_m) all the public values are in an authenticated manner. For the sake of security, the P'_i, h'_i, T'_1, T'_2,…, T'_r should be renewed.

The generalized secrets share scheme is easily changeable

Case 1: Change secret key K_i

When the security department find something wrong or maybe have intruder or plotter. The dealer need to change the secret key K_i.

- After restructure the qualified subsets, which are included in the access structure.
- After adjust agents in the qualified subsets.

The dealer publish (P'_i, h'_i, N, T'_1, T'_2,…, T'_r, c'_1 , c'_2 , … , c'_m) all the public values are in an authenticated manner. For the sake of security, the P'_i, h'_i, T'_1, T'_2,…, T'_r should be renewed.

Case 2: Change the share secret list (M_1, M_2, …, M_m, M_{m+1}…, m_V)

The dealer performs the construction phase to add some information of the new shared secret (M_{m+1}, …, M_{m+v}) on the public bulletin.

The dealer publish (P_i, h_i, N, T_1, T_2,…, T_r, c'_1 , c'_2 , …, c'_m ,c'_{m+1} , …, c'_{m+v}) all the public values are in an authenticated manner.

DISCUSSION

The proposed scheme is based on some secure properties of the RSA cryptosystem[6,12] and Shamir's (t, n) threshold scheme [6,12]. Obeying the kernel spirit of the (t, n) threshold scheme we shall discuss the security analysis of the scheme we propose. The property we would like to mention is that each participant selects his secret key by himself in present scheme. The dealer does not need to distribute the shadows to the agents each. Each participant p_i only provides a piece of corresponding public information to the dealer in the initialization phase. Not only the other agents but also the dealer is unable to derive the secret key of the participant p_i unless he can break the decryption function of the RSA cryptosystem. With this property, the security damage caused by distributing shadows is eliminated. The proposed scheme does not need a secure channel to distribute shadows.

Attack 1: The intruder use publish data (P_i, h_i, N, T_1, T_2,…, T_r, c_1 , c_2 , … , c_m) and the unqualified subset of agents to acquire the share message list (M_1, M_2, …, M_m)

Analysis the attack: Given the public values (P_i, h_i, N, T_1, T_2,…, T_r, c_1 , c_2 , … , c_m) in

$$f_j(X) = \sum_{L=1}^{t}[S'_{jL}(X-1)/(ID_{jL}-1)\prod_{\substack{k=1\\k\neq L}}^{t}\frac{(X-ID_{jk})}{ID_{jL}-ID_{jk}}]\bmod Q$$

and $\quad c_j = \sum_{L=1}^{k} g^{(j-1)(L-1)}M_j + K_i$, where $1 \le j \le m$

we can see that the number of unknown symbols is larger than the numbers of linear equations. Obeying the kernel spirit of the (t, n) threshold scheme, the security analysis of the scheme match present requirement. So, an adversary has no way to derive the secrets. The proposed scheme is based on some secure properties of Shamir's (t, n)-threshold scheme.

The fact that the unqualified subset of agents cannot cooperate to recover the secret key K_i is the basic requirement of a secret sharing scheme. Our scheme, any unqualified subset of wanting to get the secret key K_i to get the share secrets (M_1, M_2, …, M_m) have to face the difference value below$H_j = K^J \oplus (Y^{si}_{j1} \bmod N) \oplus (Y^{si}_{j2} \bmod N) \oplus .... \oplus Y^{si}_{j} \bmod N)$.

The unqualified subset may intend to derive its difference value from the difference values of qualified subsets. Due to the fact that one can reconstruct the polynomial $f_j(X)$, only when he can collect r + 1 points (X_i, Y_i) which satisify $Y_i=f_j(X_i)$[10], it is difficult for any unqualified subset without r points (ID_w,P^{sw}_i) to get the difference value of any qualified subset y_i as they hold t-1 or fewer points to break Shamir's(t, n)-threshold scheme[13]. The difference value can be retrieved only by the cooperation of the agents of the corresponding qualified subset. So, any unqualified subset cannot derive a correct difference value to get the secret key K_i. In other words, they cannot recover the share secrets (M_1, M_2, …, M_m)

Attack 2: The intruder use publish data (P_i, h_i, N, T_1, T_2,…, T_r, c_1 , c_2 , … , c_m) and y_i to acquire the secret key of participant p_i

Analysis the attack: Present scheme will not disclose participant p_i secret key x_i even after multiple secret reconstruction. The intruder has $S'^1_i=p^{xi}_1$, $S'^2_i=p^{xi}_2$,…, $S'^n_i=p^{xi}_n$, It is hard to find x_i from S_i' because this is a discrete logarithm problem.

Theorem 1: Let the participant p_{ji} provide S_i'. If $S^{h'}_{ji} \bmod N = P^{ji}$ then S'_{ji} is true; otherwise S'_{ji} is false and may be a cheater

Proof: The dealer generates h_i such that $S_i * h_i = 1 \bmod L$ in the construction phase. We know that the equation $S'^{h}_{ji} \bmod N = P_{ji}$ can be rewritten as

$$S'^{h}_{ji} \bmod N = (P_0^{S_{ji}})^h \bmod N = (g^{S_0 * h})^{S_{ji}} \bmod N = (g^{S_0 * h \bmod L})^{S_{ji}}$$

$$\bmod N = (g\ )^{S_{ji}} \bmod N = P_{ji}S'_{ji}$$

if S'_{ji} is true, this equation must hold. It is clear that anyone can check whether the participant p_{ji} provides the true value or not.

The proposed scheme requires a public bulletin for the dealer to publish information. All agents can access the information and yet the integrity and the authenticity of such information are still assured. It is common sense

that such a public bulletin is necessary for all existing secrets sharing schemes nowadays and it contains at least the access structure and the number of agents'[6]. By using the public bulletin sufficiently in the proposed scheme there can be no communications between the dealer and each participant, which is necessary for most secret sharing schemes.

CONCLUSIONS

In this study we propose an efficient generalized secrets sharing scheme in distributed systems for real time applications. The proposed scheme can on-line dynamic change access structure provides many functions for practical on flexible workflow technology driving the networked economy applications. Only the qualified subset of agents can get the share secrets that suit for e-commerce distributed systems. It is a computational secure secret sharing scheme with general access structures. In this study, based on systematic block codes that prepare the generator matrix G(2m+1, m+1) which can be pre-computed and suit for VLSI design in hardware using in real time system, we have proposed a secure dynamic change access structure in secrets sharing scheme. The security of the proposed scheme is the same as the decryption function of the RSA cryptosystem and Shamir's (r,n)-threshold scheme.

Inspired by Ayanoglu *et al.*'s work, Deng *et al.*[10] proposed an efficient broadcasting scheme by using the (2(m+n)-1, m+n) systematic block codes, where n is the number of agents and m is the number of secrets to be distributed. In this paper, we propose an efficient generalized secrets sharing scheme by using the (2m+1, m+1) systematic block codes where m is the number of secrets to be distributed in the number of n agents. Deng *et al*'s[14] size G(2(m+n)-1, m+n) but also our scheme can on-line dynamic change in access structure than their is static for real time applications.

Enterprise information systems using workflow technology will play an increasingly critical role in providing a competitive edge to organizations in the networked economy for real time applications. They like all agents using generalized secrets sharing scheme in reality, the deadline of the contract, product brokering, merchant brokering, negotiation the purchase and the price of electronic funds transaction. We can increase efficient and security on the process of e-market information system. The proposed scheme has the following properties:

- The secret key of each participant or agent need not change when agents or agents are joining or quitting, with the shared secret ready to be renewed and the access structure ready to be altered dynamically.
- Each participant or agent is able to check whether another participant or agent provides the true information or not in the recovery phase.
- The dealer shares new secrets or renews shared secrets among these n agents or agents without collecting their shadows.
- No secret communication exists between the dealer and the agents or agents.

REFERENCES

1. Elgamal, T., 1995. A public-key cryptosystem and a signature scheme based on discrete logarithm. IEEE Trans. Inform. Theory, 31: 469-472.
2. Tan, K.J., H.W. Zhu and S.J. Gu, 1999. Cheater identification in (t,n) threshold scheme. Computer Communications, 22: 762-765.
3. Wei-Bin Lee and Chin-Chen Chang, 1998. A dynamic secret sharing scheme based on the factoring and Diffie-Hellman problem. IEICE Trans. Fundamentals E81-A. pp: 1733-1738.
4. Harn, L., 2003. Efficient sharing (broadcasting) of multiple secrets. IEE Proc. Comput. Digit. Techol., 142: 237-240.
5. Blakey, B., G.R. Blakley, A.H.Cha and J.L. Massey, 1993. Threshold scheme with disenrollment, In: Advances in Cryptology-Crypto, Springer-Verlag, Berlin, pp: 540-548.
6. Pinch, R.G.E., 1996. On-line multiple secret sharing. Electronics Letters, pp: 1987-1088.
7. Blundo, C., A. Cresti. D. Santis and U. Vaccaro, 1994. Fully dynamic secret sharing schemes, Advances in Cryptolo Gy-crypto, Springer-Verlag, Berlin, pp: 110-125.
8. Blundo, C., D. Santis, D. Crescenoz, A.G. Gaggia and U. Vaccaro, 1994. Secrets sharing schemes. Advances in Cryptology-Crypto, Springer-Verlag, Berlin, pp: 190-198.
9. Cachin, C., 1994. On-line secret sharing, Cryptography and Coding. Springer-Verlag, Berlin, pp: 150-163.
10. Chang, C.C., H.J. Horug and D.J. Buehrer, 1995. A cascade exponentiation evaluation scheme based on the Lempel-Zie-Welch compression algorithm. J. Inform. Sci. and Eng., 11: 417-431.
11. Lin, W.D. and J.K. Jan, 2000. An automatic signature scheme using a compiler in distributed systems. IEICE Trans. Communications, E83-B pp: 935-941.
12. Stinson, D.R., 1995. Cryptography: Theory and Practice, CRC Press, Boca Raton.

13. Krawczyk, H., 1994. Secret sharing made short. Advances in Cryptology-crypto, Springer-Verlag, Berlin, pp: 113-138.
14. Deng, R.H., L. Gong, A. A. Lazar and W. Guo, 2000. Authenticated key distribution and secure broadcast using no conventional encryption: A unified approach based on block codes. IEEE GLOBECOM, pp: 1193-1197.
15. Chien, H.Y., J.K. Jan and Y.M. Tseng, 2000. A practical (t,n) multi-secret sharing scheme. IEICE Trans. Fundamental. E83-A. pp: 2762-2765.
16. Lin, W.D., 2003. EC Transactions use different web-based platforms. Lecture Notes in Computer Science, 2658: 1059-1068.