DYNAMIC THRESHOLD SCHEME BASED ON THE DEFINITION OF CROSS-PRODUCT IN AN N-DIMENSIONAL LINEAR SPACE

CHI-SUNG LAIH*, LEIN HARN**, JAU-YIEN LEE* and Tzonelih Hwang***

* Department of Electrical Engineering
National Cheng Kung University
Tainan, Taiwan, Republic of China
** Computer Science Program
University of Missouri-Kansas City
Kansas City, MO 64110, U.S.A.
*** Institute of Information Engineering
National Cheng Kung University
Tainan, Taiwan, Republic of China

ABSTRACT

This paper investigates the characterizations of threshold /ramp schemes which give rise to the time-dependent threshold schemes. These schemes are called the "dynamic threshold schemes" as compared to the conventional time-independent threshold scheme. In a (d, m, n, T) dynamic threshold scheme, there are n secret shadows and a public shadow, p^j, at time $t=t_j$, $1 \le t_j \le T$. After knowing any m shadows, $m \le n$, and the public shadow, p^j, we can easily recover d master keys, K_1^j, K_2^j, ..., and K_d^j. Furthermore, if the d master keys have to be changed to K^{j+1}_1, K^{j+1}_2, ..., and K^{j+1}_d for some security reasons, only the public shadow, p^j, has to be changed to p^{j+1}. All the n secret shadows issued initially remain unchanged. Compared to the conventional threshold/ramp schemes, at least one of the previous issued n shadows need to be changed whenever the master keys need to be updated for security reasons. A (1, m, n, T) dynamic threshold scheme based on the definition of cross- product in an N-dimensional linear space is proposed to illustrate the characterizations of the dynamic threshold schemes.

This work was sponsored by the National Science Council, Republic of China, under Contract NSC79-0408-E006-02.

G. Brassard (Ed.): Advances in Cryptology - CRYPTO '89, LNCS 435, pp. 286-298, 1990.

I INTRODUCTION

A threshold scheme is used to ensure that the information needed careful protection does not get lost, destroyed, or into wrong hands. As described by Denning [1, pp.179-185], an (m, n) threshold scheme is designed to break the single master key K into n different "shadows" such that:

(1) With knowledge of any m shadows, $m \leq n$, the master key K can be easily derived; and
(2) With knowledge of any m-1 or fewer "shadows", it is impossible to derive the master key K.

The idea of threshold schemes (or sometimes referred as key safeguarding schemes or secret sharing schemes) was introduced independent by Blakley [2] and Shamir [3]. Since then, threshold schemes have been well-studied over the past decade [4-7]. In 1984, the relationships between these schemes and a generalized linear scheme are established by Kothari [8]. However, as shown by Blakley and Meadows [9], although (m, n) linear threshold schemes provide Shannon perfect security up to threshold value, unfortunately they require a very large data expansion. That is, m shadows are needed to reclaim one secret which is very inefficient as a conveyor of information. In order to overcome this drawback, Blakley and Meadows presented the idea of (d, m, n) ramp schemes. In a (d, m, n) linear ramp scheme, it is designed to allow d secrets and m-d other predetermined types of secrets to be combined to produce n "shadows", in such a fashion that these d secrets can be reconstructed from any m shadows. However, there is a predetermined level of uncertainty (also called Shannon relative security) regarding the secrets if only j, $j<m$, shadows are known. It has been observed by Blakley and Meadows that $1 \leq d \leq m \leq n$. It is obvious that many conventional (m, n) threshold schemes are just the special case of the (1, m, n) ramp scheme.

We observe that the (d, m, n) ramp scheme is just the space expansion (with d times) of the conventional threshold schemes. In this paper, we will consider the time expansion of the threshold/ramp schemes. We will call them the "dynamic threshold schemes" (or, briefly, a (d, m, n, T) dynamic scheme, where T indicates time).

Any threshold/ramp scheme can be referred to as an "m out of secret sharing system." The one or d secrets can be divided into n shadows and securely distributed to n trustees in such a way that any m of them can reconstruct the secrets, but any m-1 of fewer of them cannot learn anything about it. However, it seems that two time-dependent phenomena are not discussed in the previous papers:

(1) When any m out of n trustees recover the secrets, whether the secrets are known by these trustees or not.

If these secrets can be known by m trustees when they are

reconstructed at time t^j, then the threshold/ramp schemes can be used only before time t^j. However, in practice applications, we may assume that these m trustees do not known these secrets. For example, in the access control system, any m trustees may simply insert their magnetic strip cards which contain the shadow information into the card reader and the system calculates these secrets to decide whether the door can be opened or not. In that case, these secrets are not known by m trustees when they get together to reconstruct these secrets, and therefore, the scheme can be used continually. But, conventional threshold/ramp schemes still exist the following disadvantage.

(2) Whenever these secrets under protection by threshold/ramp schemes need to be updated for some security reasons, at least one of the previously issued n shadows need to be changed.

This paper will focus on investigating the characterizations of threshold/ramp schemes which give rise to the time-dependent threshold/ramp schemes. We call the time-dependent threshold/ramp schemes the "dynamic threshold/ramp schemes" (or, more precisely, the (d, m, n, T) threshold /ramp schemes, where d, m, and n are the number of secrets, threshold value of shadows, and number of all shadows, respectively, and T indicates time). A (1, m, n, T) dynamic threshold scheme based on the definition of cross-product in an n-dimensional linear space is used to explain the characteristics of the dynamic threshold scheme.

II THE CHARACTERIZATIONS OF DYNAMIC THRESHOLD/RAMP SCHEMES

The security of a (d, m, n, T) dynamic threshold/ramp scheme is based on the following assumption:

Whenever any m of n trustees are combined to recover d secrets, the secrecy of those shadows held by these m trustees is still maintained.

Under practical implementation, this is a reasonable assumption, since the trustees may simply insert their magnetic strip cards which contain the shadow information into a card reader consecutively and the system calculates these secrets automatically . Therefore, the shadows are still kept secret for each individual trustee. Under this assumption, a dynamic threshold/ramp scheme may achieve the following characteristics:

Whenever these secrets under protection by a threshold/ramp scheme need to be updated for security reasons, all the previously issued n shadows do not need to be changed.

Since these secrets under protection are time-dependent and all previously issued shadows are time-independent, a time-dependent variable which we call the public shadow, P^j, have to be inserted into the system. The model of the dynamic threshold

scheme is shown in Fig.(1). A (1, m, n, T) dynamic threshold scheme can be expressed by a function F such that

$$F(W_1, W_2, \ldots, W_m, P^j)=K^j \quad (1)$$

where K^j is the secret under protection at time t^j,

$W_1, W_2, \ldots, W_m \in$ {the set of all n shadows},

P^j is the public shadow at time t_j.

As shown in Eq.(1), knowing any m shadows, and the public shadow, P^j, at time t_j, it is sufficient to recover the secret (or master key) K^j. Whenever the master key, K^j, needs to be changed to K^{j+1} for some security reasons, only the public shadow, P^j, need to be changed to P^{j+1}. All the n secret shadows may remain unchanged.

In the ideal situation, the dynamic threshold/ramp schemes must satisfy the following characteristics:

(1) At the beginning of the time, $t_j=1$, dynamic threshold/ramp schemes, like conventional threshold/ramp schemes, provide perfect security [9] up to the threshold value. For the master key K^j, j=1, conveyed by the scheme, we have

probability (K^j/given that m-1 (or fewer) shadows and the public shadow, p^j, are known) = Probability (K^j)

(2) If the previous master keys, K^j, j=1, 2, ..., v-1, are kept secret, the scheme also provides Shannon perfect security for the following master keys, K^j, $j\geq v$. More clearly, knowing any u (even $u\geq m$) public shadows, P^i, i=1, 2, ..., u, cannot provide any information to derive any new master keys, K^j, $j\geq v$. That is

Probability (any new master keys K^j, $j\geq v$,/given that any u public shadows, p^i, i=1, 2, ..., u, are known) = Probability (any new master keys K^j, $j\geq v$)

(3) Knowing any v-1 previous master keys K^j, j=1, 2, ..., v-1, the scheme also provides Shannon perfect security for the following new master keys K^j, $j\geq v$. That is, knowing all v-1

($\geq$m) previous master keys K^j, j=1, 2, ..., v-1, cannot provide any information to derive the following new master keys K^j, $j \geq v$, i.e.,

Probability (any new master keys K^j, $j \geq v$/given that all K^j, $j<v$, and p^1, i=1, 2, ..., u) = Probability (any new master keys K^j, $j \geq v$)

In general, it is very difficult to design an ideal dynamic threshold/ramp scheme to satisfy the characteristics (1)-(3). Alternatively, we define the "relative dynamic threshold/ramp scheme" which satisfies the above characteristics (1)-(2). That is, knowing v-1 previous master keys K^j, j=1, 2, ..., v-1, and u (>v) public shadows p^i, i=1, 2, ..., u, the scheme provides Shannon relative security for the following master keys K^j, $j \geq v$, (the threshold number of shadows is decreased to m-v from m.) Note that the relative dynamic/ramp scheme is sufficient to the practice applications (e.g. the access control system discussed in the above section.) A dynamic threshold scheme based on the definition of cross-product in an N-dimensional space is proposed to illustrate the characteristics of relative dynamic threshold schemes. We encourage readers to propose any scheme which satisfies the characteristics of ideal threshold/ramp scheme.

III. THE DYNAMIC THRESHOLD SCHEME BASED ON THE DEFINITION OF CROSS-PRODUCT IN N-DIMENSIONAL SPACE

Our proposed (1, m, n, T) dynamic threshold scheme is based on the following definition.

Definition : The cross-product of s-1 linearly independent s-dimensional row vectors $Z_1, Z_2, \ldots, Z_{s-1}$ is defined as :

$$Z_1 \times Z_2 \times \cdots \times Z_{s-1} =$$

$$\left(\begin{vmatrix} z_2^1 & z_3^1 & \cdots & z_s^1 \\ z_2^2 & z_3^2 & \cdots & z_s^2 \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ z_2^{s-1} & z_3^{s-1} & \cdots & z_s^{s-1} \end{vmatrix}, \begin{vmatrix} z_3^1 & z_4^1 & \cdots & z_s^1 & z_1^1 \\ z_3^2 & z_4^2 & \cdots & z_s^2 & z_1^2 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ z_3^{s-1} & z_4^{s-1} & \cdots & z_s^{s-1} & z_1^{s-1} \end{vmatrix}, \cdots, \begin{vmatrix} z_1^1 & z_2^1 & \cdots & z_{s-1}^1 \\ z_1^2 & z_2^2 & \cdots & z_{s-1}^2 \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ z_1^{s-1} & z_2^{s-1} & \cdots & z_{s-1}^{s-1} \end{vmatrix} \right)$$

with $Z_i = (z_1^i, z_2^i \ldots, z_s^i)$ (2)

The determinants of (s-1)*(s-1) matrices in Eq. (2) can be computed by using the probabilistic algorithm proposed by Wiedemann [10]. Given a r*r matrix, Wiedemann showed that the probabilistic algorithm for finding the determinant required an expected O(r(w+r)) number of field operations, where w is approximately the number of field operations needed to apply the matrix to a test vector. Since Eq. (2) contains s determinants, the complexity of Eq. (2) is about O(s(s-1)(w+s-1)) operations.

Now, assume that n is the total number of "shadows" need to be constructed and m is the threshold value which works with the public shadow, P^j, to recover the single master key, K^j. The scheme is described as follows :

Shadows generation:

For j=1 to T repeat step 1-3.

Step 1 : The key generation center randomly selects m+1 linearly independent (m+2)-dimensional row vectors V_1, V_2, ..., V_m and V_{m+1}^j.

Step 2 : The center then evaluates a new vector $U^j=(u_1^j, u_2^j, \ldots, u_{m+2}^j) = V_1 X V_2 X \ldots X V_t X V_{m+1}^j$, and system master key, K^j, at the time t_j, $1 \le j \le T$, is obtained from U^j as follows :

$$K^j = \prod_{i=2}^{m+2} abs(u_i^j)$$

where abs(x) means the absolute value of x. The master key, K^j, is kept secret, but the first element, u_1^j, of the vector U^j is made public (system security is not affected by revealing this element). u_1^j will be used for normalizing purposes, as described later as part of the master key computation and it cannot to be zero.

Step 3 : The n "shadows" S_i, i=1, 2, ..., n, and the public shadow, P^j, are constructed by randomly selecting an (n+1)*(m+1) matrix A^j and then executing the following operation :

$$\begin{bmatrix} S_1 \\ S_2 \\ . \\ . \\ . \\ S_n \\ P^j \end{bmatrix} = \begin{bmatrix} a_{11}, & a_{12}, & \cdots, & a_{1m}, & 0 \\ a_{21}, & a_{22}, & \cdots, & a_{2m}, & 0 \\ . & . & \cdots & . & . \\ . & . & \cdots & . & . \\ . & . & \cdots & . & . \\ a_{n1}, & a_{n2}, & \cdots, & a_{nm}, & 0 \\ b_1^j, & b_2^j, & \cdots, & b_m^j, & b_{m+1}^j \end{bmatrix} \begin{bmatrix} V_1 \\ V_2 \\ . \\ . \\ . \\ V_m \\ V_{m+1}^j \end{bmatrix} \qquad (3)$$

where in matrix A^j, any m row vectors (excluding the (m+1)-th column) need to be a full rank square matrix and $b_{m+1}^j \neq 0$.

The key center then secretly distributes these n secret shadows S_i, $1 \leq i \leq n$, one to each trustee publishes the public shadow, P^j.

Master key recomputation:

Knowledge of any m "shadows" W_i, i=1, 2, ..., m, from S_1, S_2, ..., S_n, and the public shadow, P^j uniquely determines the master key K^j as follows :
First, evaluate

$$W_1 \chi W_2 \chi \ldots \chi W_m \chi P^j = (w_1^j, w_2^j, \ldots, w_{m+2}^j), \qquad (4)$$

where $W_k \in \{S_i, i=1, 2, \ldots, n\}$, k=1, 2, ..., m.

Then the system master key can be calculated as

$$K^j = \prod_{i=2}^{m+2} [abs(w_i^j/h^j)], \text{ with } h^j = w_1^j/u_1^j. \qquad (5)$$

From Eq.(3), it can be seen that the n secret shadows, S_i, $1 \leq i \leq n$, can be used for computing different master keys, K^j, j=1, 2, ..., T.

Example : Let t=2, n=5.

The key generation center randomly selects V_1=(1, 2, 3, 4), V_2=(5, 6, 7, 8) and V_3^1=(2, 2, 1, 1) and evaluates $U^1=V_1 \chi V_2 \chi V_3^1$=(-4, -4, 4, 4). The system master key at t=1 is calculated as K^1=4*4*4=64. The first element of the row +vector U^1, which is -4, is made public. Next, the key generation center randomly selects

a 6*3 matrix A^1, as for example

$$A^1 = \begin{bmatrix} 1, & 2, & 0 \\ -1, & 1, & 0 \\ 4, & 5, & 0 \\ 2, & 3, & 0 \\ 2, & -3, & 0 \\ 4, & 1, & -2 \end{bmatrix}$$

Then the n shadows and the public shadow P^1 are generated as

S_1 = (11, 14, 17, 20),
S_2 = (4, 4, 4, 4),
S_3 = (29, 38, 47, 56),
S_4 = (17, 22, 27, 32),
K_5 = (-13, -14, -15, -16),

and P^1 = (5, 10, 17, 22).

Knowing any two "shadows" and the public shadow, P^1, one can reconstruct the master key K^1. For example, $S_1 \chi S_5 \chi P^1$ = (24, 24, -24, -24), and h^1=24/(-4)=-6. Thus K^1 = (24/6) * (24/6) * (24/6) = 64.

If the master key needs to be updated at t=2, then the key center randomly selects V_3^2=(1, 2, 1, -1), b_1^2, b_2^2, and b_3^2 = (-2, 1,1) (as shown in Eq.(3)). It evaluates $U^2=V_1 \chi V_2 \chi V_3^2$=(4, 16, 20, 8) and P^2=(4, 4, 2, -1). The new master key is calculated as K^2=16*20*8=2560. Next, the system publishes the first element of the new row vector U^2, which is 4, and the new public shadow P^2. Then knowing any two shadows and P^2 can reconstruct K^2. For example, $S_4 \chi S_5 \chi P^2$ = (-48, 192, -240, -96), and h^2=48/4=12. Thus K^2= (192/12)*(240/12)*(96/12) = 2560.

IV SECURITY ANALYSIS AND DISCUSSIONS

The dynamic threshold scheme proposed in the section III is satisfied the requirements of relative dynamic threshold schemes. We will discuss this scheme as follows:

(1) At the beginning time, t_j=1, the scheme provides Shannon perfect security.

It is obvious that the master key K^1, is concealed in the

vector U^1, which is perpendicular to the original vectors V^1, V^2, ..., V^m and the time dependent vector V^1_{m+1}. Hence U^1 can be evaluated by at least m+1 independent vectors which are linearly combined by the vectors V_1, V_2, ..., V^1_{m+1}. If only r shadows, r<m, and the public shadow, P^1, are known (as shown in Eq.(3)) then the combination of those r shadows and the public shadow, P^1, cannot evaluate U^1 since they cannot construct m+1 independent vectors which are linearly combined by the vectors V_1, V_2, ..., V_m and V_{m+1}. On the other hand, if only r shadows, r<m, are known, then the cross-product of these r shadows with the public shadow, P^1, is meaningless (i.e., these cannot form m+2 square submatrices as required in the definition). Therefore, the scheme provide Shannon perfect security at the beginning time, t_j=1.

(2) If the previous v-1 master keys, K^j, j=1, 2, ...,v-1, are kept secret, then this scheme also provide Shannon perfect security.

Without loss of generality, we assume that m-1 trustees want to use their shadows, W_j, $1 \le j \le m-1$, to derive the new master key, K^v, with some of the public shadows, p^1 and p^k. Then these m-1 trustees can compute $W_1 X W_2 X \ldots X W_{m-1} X P^i X P^k$ which is a cross-product of vectors within the vectors space spanned by V_1, V_2, concealed by the vector $U^j = V_1 X V_2 X \ldots X V_m X V^v_{m+1}$, which is a cross-product of vectors within the vector space spanned by V_1, V_2, ..., V_m, and V^v_{m+1} only. Therefore, even v=i or k, the cardinality of $W_1 X W_2 X \ldots X W_{m-1} X P^i X P^k$ is larger than the cardinally of the new master key, K^v by at least one. It implies that the scheme provide Shannon perfect security, if all the previous master keys are kept secret.

(3) Knowing any v previous secrets K^j, j=1, 2, ..., V, the scheme provide Shannon relative security. It implies that knowing any v previous master keys, the threshold value is decreased, from m to m-v.

At first, we assume that the previous master key, K^1, is known. If we know m-1 shadows, W^j, j=1, 2, ..., m-1, we can construct the following cross-product form

$$U^1 = W_1 X W_2 X \ldots X W_{M-1} X P^1 X Y = (u_1^1, u_2^1, \ldots, u_{m+2}^1) =$$

$$\left(\begin{vmatrix} w_2^1, & w_3^1, & \ldots, & w_{m+2}^1 \\ w_2^2, & w_3^2, & \ldots, & w_{m+2}^2 \\ \ldots & \ldots & \ldots & \ldots \\ w_2^{m-1}, & w_3^{m-1}, & \ldots, & w_{m+2}^{m-1} \\ p_2^1, & p_3^1, & \ldots, & p_{m+2}^1 \\ y_2, & y_3, & \ldots, & y_{m+2} \end{vmatrix} \begin{vmatrix} w_1^1, & w_3^1, & \ldots, & w_{m+2}^1 \\ w_1^2, & w_3^2, & \ldots, & w_{m+2}^2 \\ \ldots & \ldots & \ldots & \ldots \\ w_1^{m-1}, & w_3^{m-1}, & \ldots, & w_{m+2}^{m-1} \\ p_1^1, & p_3^1, & \ldots, & p_{m+2}^1 \\ y_1, & y_3, & \ldots, & y_{m+2} \end{vmatrix} \ldots \begin{vmatrix} w_1^1, & w_2^1, & \ldots, & w_{m+1}^1 \\ w_1^2, & w_2^2, & \ldots, & w_{m+1}^2 \\ \ldots & \ldots & \ldots & \ldots \\ w_1^{m-1}, & w_2^{m-1}, & \ldots, & w_{m+1}^{m-1} \\ p_1^1, & p_2^1, & \ldots, & p_{m+1}^1 \\ y_1, & y_2, & \ldots, & y_{m+1} \end{vmatrix} \right) \tag{6}$$

where $Y=(y_1, y_2, \ldots, y_{m+2})$ is an unknown shadow. Eq.(6) can be reformulated to the following (m+2) linear equations:

$$\begin{aligned} 0 + b_{12}y_2 + b_{13}y_3 + \ldots + b_{1,m+2}y_{m+2} &= u_1^1 \\ b_{21}y_1 + 0 + b_{23}y_3 + \ldots + b_{2,m+2}y_{m+2} &= u_2^1 \\ \ldots & \quad \vdots \\ \ldots & \quad \vdots \\ \ldots & \quad \vdots \\ b_{m+2,1}y_1 + b_{m+2,2}y_2 + \ldots + b_{m+1,m+2}y_{m+1} + 0 &= u_{m+2}^1 \end{aligned} \tag{7}$$

Since U_1^1 is public and $K^1 = \prod_{j=2}^{m+2} \mathrm{abs}(u_j^1)$ is known, it is possible to evaluate u_j^1, for j=2, 3, ..., m+2. Thus one secret shadow Y can be derived from Eq.(7). Once the secret shadow Y was derived, then knowing other m-1 shadows and the following public shadow, p^i, $i \geq 2$, can evaluate any following master key, K^i, $i \geq 2$. The same ideas can be extended to more general cases. In general, knowing any v previous master keys, the threshold value of this dynamic threshold scheme is decreased, from m to m-v. If v previous master keys are known, then the level of uncertainly is decreased to zero. It is why the assumption

$$1 \leq T < m \leq n$$

is implicit in the linear dynamic threshold scheme.

V CONCLUSION

In this paper, the model of a time-dependent threshold/ramp scheme is proposed. We call the time-dependent threshold/ramp

scheme a "dynamic threshold/ramp scheme", as compared to the conventional threshold/ramp scheme. If the previous master keys are not known by all trustees, the dynamic threshold/ramp scheme is similar to the conventional threshold/ramp scheme at any time $t=t_j$. However, the dynamic threshold/ramp scheme has the major advantage, that is, whenever the master key, K^j, needs to change to k^{j+1} for some security reasons, the system needs to change only the public shadow, p^j, to p^{j+1}. All the n trustees do not need to be notified since all the n secret shadows issued initially do not need to be changed.

We have defined the characterizations of the ideal and relative threshold/ramp scheme. The unique difference between ideal and relative threshold/ramp schemes is that the ideal scheme can provide Shannon perfect security at any time regardless how many previous master keys and public shadows are known. However, the relative scheme just can provide Shannon relative security when some of the previous master keys are known. As shown in the section IV, knowing any v previous master keys, the threshold value of the dynamic threshold/ramp scheme is decreased from m to m-v. Notice that, the conventional threshold/ramp scheme is useless in this assumption, i.e., if the master key can be known by any m trustees when they get together at time t, then anyone of these m trustees do not need to cooperate with other m-1 trustees after the time t.

Since almost all proposed threshold schemes are linear, it seems very difficult to propose an ideal dynamic threshold scheme. Instead, we propose a (1, m, n, T) dynamic threshold scheme based on the definition of cross-product in an N-dimensional dimensional space which satisfies the characterizations of the relative dynamic threshold scheme. The ideal dynamic threshold schemes may or may not exit, we encourage readers to further study and investigate the applications about this field.

REFERENCES

[1] D.E.R. Denning, Cryptography and Data Security, (Addison-Wesley Reading Mass., 1982.

[2] G.R. Blakley, Safeguarding crytographic keys, Proc. NCC, Vol.48, AFIPS Press, Montvale, N.J., 1979, pp. 313-317.

[3] A. Shamir, How to share a secret, Comm. ACM, vol.22, no.11, 1979, pp.612-613.

[4] G.I. Davida, R.A. Demillo and R.J. Liption, "Protecting shared cryptographic keys," Proc. Symp. on security and privacy, IEEE computer society, 1980, pp.100-102.

[5] D.E. Denning and F.B. Schneider, "Master keys for group sharing, " Information Processing Letters, vol.12, no.1, pp.23-25, 1981.

[6] E.D. Karnin, J.W. Greene and M.E. Hellman, "On secret sharing systems, " IEEE Trans. on Inform. Theory, vol.IT-29, no.2, pp.208-210, 9183.

[7] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," IEEE Trans. on Inform. Theory, vol.IT-29, no2, pp.208-210, 1983.

[8] S.C Kothari, Generalized linear threshold scheme, Proc. of crypto 84, Springer-Verlag, 9185, pp.231-241.

[9] G.R. Blakley and C. Meddows, "Security of Ramp Schemes," Advances in Cryptology: Proceeding of CRYPTO'84, Springer-Verlag.

[10] D.H. Wiedemann, "Solving sparse linear equations over finite fields," IEEE Trans. Information Theory, vol.IT-32, pp.54-62, 1986.

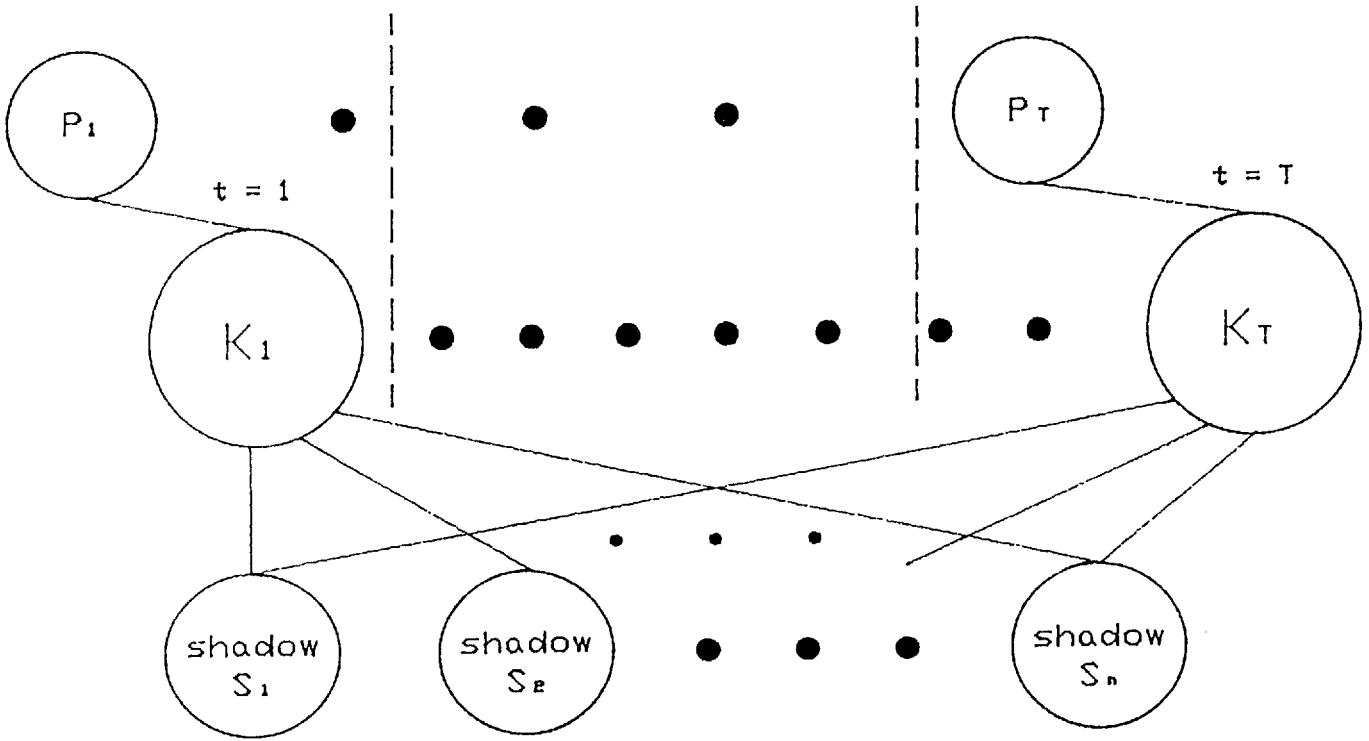

Fig.(1) The model of dynamic threshold/ramp scheme