Partial Key Escrow Monitoring Scheme

Jiang shaoquan and Zhang yufeng
State Key Lab. of Information Security
Graduate School of USTC, Bejing 100039
Email: jiangshq@hotmail.com
Tel: 8610-68213046 Fax: 8610-68213046

Abstract

During (partial) key escrow, how to monitor a user safely and efficiently is a very important problem. This paper initially proposes a monitoring scheme of a typical partial key escrow scheme. In this scheme, the escrowed key of a user is not compromised even if the user has been monitored for many times.

1 Introduction

Shamir [1] proposed a new kind of key escrow scheme- 'partial key escrow' whose purpose is to prevent the government from a large scale decryption. In his scheme, a user's private key c is divided into two parts x, a, such that $c = x + a$,a is a number of short length and x is the escrowed key. x is divided into shares of which each is hold by a different Key Escrow Agency(KEA). Only more than certain number KEAs can collaborate to recover x. When the law enforce agency(LEA) intends to monitor the user, he asks enough KEAs to deliver their shares of x. He then calculates x. But to get c, he must carry out brute search for a.

From the description above, we can see that once LEA has monitored a user, he knows the user's private key c for ever. That will cause abuse. Of course, for general key escrow schemes, such problem exists, too. We call it monitoring problem. [2] proposes a new partial key escrow scheme, which avoids such a problem. But it leaves open for partial key escrow. In this paper, although we are not intend to propose a new escrow scheme, we construct a new monitoring scheme. And the escrow scheme is based on [5]. When monitoring, an escrow agency offers not his share to LEA , but some useful information. And the information is only useful in current monitoring. If LEA wants to monitor the same user next time, he must repeat the procedure above,i.e., he must depend on LEA's. The detail will be presented in the following content. We will also prove the security and feasibility of this scheme.

2 Partial Key Escrow Scheme

We present some parameters that will be used in this paper. $T_i,\ 1 \le i \le n$ denotes all key escrow agencies; l denotes the number of the honest key escrow agencies;t is the limit number of KEAs that can't recover the user's escrowed key (we always assume $l \ge t+1$); $p,\ q$ are large prime numbers and $q|(p-1)$; $\beta\ \gamma$ are elements of Z_p of order q, and log_β^γ is unknown (That $\beta\ \gamma$ are secretly generated by different persons separately can achieve this); d is the bit length of the partial private key a which is not escrowed; c is the user's private key; x_0 is the escrowed key of the user; Y is the user's public key.

2.1 Typical Partial Key Escrow System

In this section, we introduce a well known partial key escrow system [5], which, we think, is feasible and secure except for monitoring problem. In the rear sections, when we introduce our monitoring scheme, we base the system. More partail key escrow systems appear in [3],[4]. To meet our need, I make some inessential modifications, *i.e.* (2),(3),(4). Here is the system.

1. User A selects $c \in F_q^*$, computes $Y = \beta^c$, and publishes Y.
2. User A randomly selects $d+2$ numbers $a, u, u_0, u_1, \cdots, u_{d-1} \in F_q$, where
$$a = \sum_{i=0}^{d-1} a_i 2^i,\ a_i \in \{0, 1\}$$
is an d-bit number. Computes
$$x_0 = c - a \pmod q,\ X = \beta^{x_0}\gamma^u \pmod p),$$

and

$$A_i = \beta^{a_i}\gamma^{u_i} \pmod p,\ i = 0, 1, \cdots, d-1,$$

$$w = u + \sum_{i=0}^{d-1} u_i 2^i.$$

And then he sends X, A_i, w to KEAs.

3. KEAs check whether

$$Y\gamma^w = X \prod_{i=0}^{d-1} A_i^{2^i}.$$

If true, they use Bit-Commitment Protocol(readers can refer to [5]) to verify that a is really a d-bit number. After all these are verified successfully, they publish X.

4. User A checks whether X is proper. If true, he selects two polynomials

$$f(x) = x_0 + \sum_{i=1}^{t} f_i x^i,$$

and

$$v(x) = u + \sum_{i=1}^{t} v_i x^i \ \in Z_q[x],$$

where $f_i,\ v_i$ are randomly selects from F_q with $f_t,\ v_t \neq 0$.

A calculates

$$s_i = v(i),\ x_i = f(i) \pmod q,\ i = 1, 2, \cdots, n$$

$$F_i = \beta^{x_i}\gamma^{s_i},\ i = 1, 2, \cdots, n. \quad (1)$$

Publishes $F_i,\ i = 1, 2, \cdots, n$, and sends (s_i, x_i) to T_i secretly.

5. The ith key escrow agency T_i,$i = 1, 2, \cdots, n$ calculates the matrix

$$(b_{ij})_{0\le i<n, 1\le j\le n} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & n & \cdots & n^{n-1} \end{pmatrix}^{-1},$$

and checks whether

$$F_i = \beta^{x_i}\gamma^{s_i} \pmod p, \quad (2)$$

$$X = \prod_{i=1}^{n} F_i^{b_{0i}} \pmod p, \quad (3)$$

$$\prod_{i=1}^{n} F_i^{b_{ji}} = 1 \pmod p, \quad (4)$$

where $j = t+1, \cdots, n-1$. If (2)(3)(4) hold, then T_i's accept that the private key of user A is escrowed successfully.

2.2 Communication phase

In this paper, we suppose communications between users as follow. E is a known encrypt algorithm and D is the corresponding decrypt algorithm.

If user B wants to send a message to user A, they follow the steps below:

1. B randomly selects $\tau \in F_q,\ K \in Z_p$, and computes

$$y_1 = \beta^\tau \pmod p,\ \textit{and} \quad y_2 = KY^\tau \pmod p.$$

If $LEAF = (y_1,\ y_2)$, then encrypts message M with a random session key K, $C = E(M, K)$.

B sends $(C, LEAF)$ to user A.

2. User A calculates K from $LEAF$ with his private key c by $K = y_2 y_1^{-c}\ mod\ p$, then decrypts message M by $M = D(C, K)$.

3 monitoring Scheme

In this section, we construct a new monitoring scheme which is secure based on Discrete Logarithm Problem[7] and Diffie Hellman Problem[6]. We first introduce our scheme,then analyze it. If LEA wants to monitor user A, he can follow the steps below:

1. LEA randomly selects $t+1$ key escrow agencies

$$T_{j_1}, \cdots, T_{j_{t+1}},$$

and sends the certificate to them. For every $i \in \{j_1, \cdots, j_{t+1}\}$, LEA and T_i carry out item 2-8,separately.

2. T_i computes

$$B_i = \beta^{x_i} \pmod p,$$

and sends (B_i, s_i) to LEA.

3. LEA checks whether

$$B_i = F_i\gamma^{-s_i} \pmod p. \quad (5)$$

If this equation holds, LEA accepts B_i as right, else goto step 9.

4. LEA randomly selects

$$\lambda_1,\ \lambda_2 \in F_q^*,$$

computes

$$\theta_1 = \beta^{\lambda_1} y_1^{\lambda_2} \pmod p,$$

and sends θ_1 to T_i.

5. T_i sends
$$\theta_1' = \theta_1^{x_i} \pmod p$$
to LEA.

6. LEA randomly selects
$$\lambda_3,\ \lambda_4 \in F_q^*,$$
s.t.,
$$\lambda_1\lambda_4 \neq \lambda_2\lambda_3 \pmod q,$$
computes
$$\theta_2 = \beta^{\lambda_3} y_1^{\lambda_4} \pmod p,$$
and sends θ_2 to T_i.

7. T_i sends
$$\theta_2' = \theta_2^{x_i} \pmod p$$
to LEA.

8. LEA computes
$$\begin{pmatrix} \lambda_1' & \lambda_2' \\ \lambda_3' & \lambda_4' \end{pmatrix} = \begin{pmatrix} \lambda_1 & \lambda_2 \\ \lambda_3 & \lambda_4 \end{pmatrix}^{-1}$$
$$= (\lambda_1\lambda_4 - \lambda_2\lambda_3)^{-1} \begin{pmatrix} \lambda_4 & -\lambda_2 \\ -\lambda_3 & \lambda_1 \end{pmatrix} \pmod q$$
If
$$B_i = \theta_1'^{\lambda_1'} \theta_2'^{\lambda_2'} \pmod p \qquad (6)$$
then calculates
$$z_i = \theta_1'^{\lambda_3'} \theta_2'^{\lambda_4'} \pmod p. \qquad (7)$$

9. If a key escrow agency has not passed 2-8, replace him with another KEA until $t+1$ KEA's pass 2-8. (Note we have supposed that there are at least $t+1$ honest agencies at the beginning of section 2.) Without loss of generality, we suppose these KEA's are still $T_{j_1}, \cdots, T_{j_{t+1}}$.

10. LEA calculates the first row numbers of matrix
$$\begin{pmatrix} 1 & j_1 & \cdots & j_1^t \\ 1 & j_2 & \cdots & j_2^t \\ \vdots & \vdots & \ddots & \vdots \\ 1 & j_{t+1} & \cdots & j_{t+1}^t \end{pmatrix}^{-1} \pmod q$$
that are denoted by
$$(b_{j_1}, b_{j_2}, \cdots, b_{j_{t+1}}),$$
and computes
$$\eta = Y(\prod_{k=1}^{t+1} B_{j_k}^{b_{j_k}})^{-1} \pmod p, \qquad (8)$$
searches for a such that $\eta = \beta^a$. Then the session key K can be calculated by
$$K = y_2(\prod_{k=1}^{t+1} z_{j_k}^{b_{j_k}})^{-1} y_1^{-a} \pmod p. \qquad (9)$$
Then LEA can use this key to decrypt the message $M = D(C, K)$.

4 Feasibility and Security of the Scheme

In this section, we are going to prove the security and feasibility of the scheme.
Feasibility: If all attendants are honest,then carrying out this scheme will result in successfull monitoring.
Security:

1. This scheme is verifiable. Dishonest users or dishonest KEA's can be detected.
2. Once a user is monitored, his private key x is not compromised.

Feasibility
Now we will show if all attendants are honest, the monitoring scheme will result in successful monitoring.In fact, we only need to keep guarantee the validity of (5) and (6) and assure the exactness of z_i in (7),η in (8),K in (9).
(i) At (5),
$$F_i\gamma^{-s_i} = \beta^{x_i}\gamma^{s_i}\gamma^{-s_i} = \beta^{x_i}$$
Therefore,(5) holds.
(ii) At (6),because
$$\begin{aligned} \theta_1{}' &= \theta_1^{x_i} = \beta^{\lambda_1 x_i}\beta^{\tau\lambda_2 x_i} \\ &= \beta^{x_i(\lambda_1,\lambda_2)(1,\tau)^T}, \end{aligned}$$
$$\begin{aligned} \theta_2{}' &= \theta_2^{x_i} = \beta^{\lambda_3 x_i}\beta^{\tau\lambda_4 x_i} \\ &= \beta^{x_i(\lambda_3,\lambda_4)(1,\tau)^T}, \end{aligned}$$
we get
$$\begin{aligned} \theta_1'^{\lambda_1'}\theta_1'^{\lambda_2'} &= \beta^{\lambda_1' x_i(\lambda_1,\lambda_2)(1,\tau)^T + \lambda_2' x_i(\lambda_3,\lambda_4)(1,\tau)^T} \\ &= \beta^{(\lambda_1',\lambda_2')\begin{pmatrix} \lambda_1 & \lambda_2 \\ \lambda_3 & \lambda_4 \end{pmatrix}(1,\tau)^T x_i}. \end{aligned}$$
Noticing that
$$\begin{pmatrix} \lambda_1' & \lambda_2' \\ \lambda_3' & \lambda_4' \end{pmatrix} = \begin{pmatrix} \lambda_1 & \lambda_2 \\ \lambda_3 & \lambda_4 \end{pmatrix}^{-1},$$

we get

$$\begin{pmatrix} \lambda'_1 & \lambda'_2 \\ \lambda'_3 & \lambda'_4 \end{pmatrix} \begin{pmatrix} \lambda_1 & \lambda_2 \\ \lambda_3 & \lambda_4 \end{pmatrix} = I_2,$$

which implies

$$(\lambda'_1, \lambda'_2) \begin{pmatrix} \lambda_1 & \lambda_2 \\ \lambda_3 & \lambda_4 \end{pmatrix} = (1,0).$$

Therefore,

$$\theta_1'^{\lambda'_1} \theta_2'^{\lambda'_2} = \beta^{(1,0)(1,\tau)^T x_i} = \beta^{x_i} = B_i.$$

So (6) holds.

(iii) Let's compute z_i . Similar to (ii),

$$\begin{aligned} z_i &= \theta_1'^{\lambda'_3} \theta_2'^{\lambda'_4} \\ &= \beta^{(0,1)(1,\tau)^T x_i} \\ &= \beta^{x_i \tau} = y_1^{x_i}. \end{aligned}$$

(iv) Now we will compute η. From $x_i = f(i)$, we derive

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & n & \cdots & n^{n-1} \end{pmatrix} \begin{pmatrix} x_0 \\ f_1 \\ \cdots \\ f_t \\ 0 \\ \cdots \\ 0 \end{pmatrix}, \quad (10)$$

which includes

$$\begin{pmatrix} x_{j_1} \\ x_{j_2} \\ \vdots \\ x_{j_{t+1}} \end{pmatrix} = \begin{pmatrix} 1 & j_1 & \cdots & j_1^t \\ 1 & j_2 & \cdots & j_2^t \\ \vdots & \vdots & \ddots & \vdots \\ 1 & j_{t+1} & \cdots & j_{t+1}^t \end{pmatrix} \begin{pmatrix} x_0 \\ f_1 \\ \vdots \\ f_t \end{pmatrix},$$

i.e.

$$\begin{pmatrix} x_0 \\ f_1 \\ \vdots \\ f_t \end{pmatrix} = \begin{pmatrix} 1 & j_1 & \cdots & j_1^t \\ 1 & j_2 & \cdots & j_2^t \\ \vdots & \vdots & \ddots & \vdots \\ 1 & j_{t+1} & \cdots & j_{t+1}^t \end{pmatrix}^{-1} \begin{pmatrix} x_{j_1} \\ x_{j_2} \\ \vdots \\ x_{j_{t+1}} \end{pmatrix}$$

If the first row of the matrix

$$\begin{pmatrix} 1 & j_1 & \cdots & j_1^t \\ 1 & j_2 & \cdots & j_2^t \\ \vdots & \vdots & \ddots & \vdots \\ 1 & j_{t+1} & \cdots & j_{t+1}^t \end{pmatrix}^{-1}$$

is

$$(b_{j_1}, \cdots, b_{j_{t+1}}),$$

then

$$x_0 = \sum_{k=1}^{t+1} b_{j_k} x_{j_k} \pmod q. \quad (11)$$

Therefore,

$$\beta^{x_0} = \prod_{k=1}^{t+1} (\beta^{x_{j_k}})^{b_{j_k}} = \prod_{k=1}^{t+1} B_{j_k}^{b_{j_k}},$$

$$\eta = Y(\prod_{k=1}^{t+1} B_{j_k}^{b_{j_k}})^{-1} = Y\beta^{-x_0} = \beta^a \pmod p$$

(v) From $z_i = \beta^{x_i \tau}$ and (10),we have

$$\begin{aligned} \prod_{k=1}^{t+1} z_{j_k}^{b_{j_k}} &= \prod_{k=1}^{t+1} \beta^{b_{j_k} x_{j_k} \tau} \\ &= \beta^{\sum_{k=1}^{t+1} b_{j_k} x_{j_k}} = \beta^{\tau x_0} = y_1^{x_0} \end{aligned}$$

$$y_2(\prod_{k=1}^{t+1} z_{j_k}^{b_{j_k}})^{-1} y_1^{-a} = y_2 y_1^{-x_0} y_1^{-a} = y_2 y_1^{-c} = K$$

Security

Let's consider the security of the scheme. Firstly,we will prove a Key Escrow Agency who pass the monitoring scheme's item 2-8 can't cheat.

(i) Seeing that (2)(3)(4)in Section 2.1 are different from [5],we have to prove that their security,*i.e.*,no cheat from User and T_i's. In fact, because $log_\beta \gamma$ is know to nobody. Based on Discrete Logarithm Problem,(3)(4) implies

$$\begin{cases} \prod_{i=1}^n \beta^{x_i b_{0i}} & = \beta^{x_0} \\ \prod_{i=1}^n \beta^{x_i b_{ji}} & = 1, j = t+1, \cdots, n-1 \end{cases}$$
$$\begin{cases} \prod_{i=1}^n \gamma^{s_i b_{0i}} & = \gamma^u \\ \prod_{i=1}^n \gamma^{s_i b_{ji}} & = 1, j = t+1, \cdots, n-1 \end{cases}$$

Furthermore,it is equalent to

$$\begin{aligned} &\sum_{i=1}^n x_i b_{0i} = x_0, \sum_{i=1}^n x_i b_{ji} = 0, \\ &\sum_{i=1}^n s_i b_{0i} = u, \sum_{i=1}^n s_i b_{ji} = 0, j = t+1, \cdots, n-1. \end{aligned}$$

Let

$$\sum_{i=1}^n x_i b_{ji} = f'_j, \sum_{i=1}^n s_i b_{ji} = v'_j,$$

then these equations can be expressed as

$$\begin{pmatrix} b_{01} & b_{02} & \cdots & b_{0n} \\ b_{11} & b_{12} & \cdots & b_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n-1,1} & b_{n-1,2} & \cdots & b_{n-1,n} \end{pmatrix} \begin{pmatrix} x_1 & s_1 \\ x_2 & s_2 \\ \vdots & \vdots \\ x_n & s_n \end{pmatrix} = \begin{pmatrix} x_0 & f_1' & \cdots & f_t' & 0 & \cdots & 0 \\ u & v_1' & \cdots & v_t' & 0 & \cdots & 0 \end{pmatrix}^T$$

Noticing that

$$(b_{ij}) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & n & \cdots & n^{n-1} \end{pmatrix}^{-1},$$

(3)(4) is equivalent to

$$\begin{pmatrix} x_1 & s_1 \\ x_2 & s_2 \\ \vdots & \vdots \\ x_n & s_n \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & n & \cdots & n^{n-1} \end{pmatrix} \begin{pmatrix} x_0 & u \\ f_1' & v_1' \\ \cdots & \cdots \\ f_t' & v_t' \\ 0 & 0 \\ \cdots & \cdots \\ 0 & 0 \end{pmatrix}$$

That is to say, The choose of $s_i, x_i, i = 1, 2, \cdots, n$ in item 5 of Section 2.1 is legal. Thus we complete the proof of the validity of (3)(4).

Definition If data B can only derive from A via the protocol steps stated in this paper(i.e. can not be a forgery),then data B is called to match with A.

From the validity of (3)(4), (x_i, s_i) in $F_i, i = 1, 2, \cdots, n$ matches with (x_0, u) in the expression of X. Because Bit-Commitment verifies a is a d-bit number, (x_0, a) matches with c.

(ii) T_i's who pass items 2-8 of monitoring scheme can't cheat.

From (2) we know F_i matches with (x_i, s_i). On the other hand, Because $\lambda_i, 1 \leq i \leq 4$, are random and θ_1, θ_2 are independently,randomly chosen from $< \beta >$,the multiple group 0generated by β, we only need to consider (5)(6). If T_i has cheated at(6) successfully,he must construct equation

$$B_i = \theta_1'^{\lambda_1'} \theta_2'^{\lambda_2'} \qquad (*)$$

Case 1: If he has cheated at (3),then at item 2 he must sent (B_i, s_i') with $B_i = \beta^{x_i'} = \beta^{x_i}\gamma^{s_i - s_i'}$. Because $log_\gamma \beta$ is unknown, he can't know x_i'. So if his construction (θ_1', θ_2')must satisfies

$$(i) \quad \theta_1' = \theta_1^{x_i'}, \theta_2' = \theta_2^{x_i'} \ or;$$
$$(ii) \quad \theta_1' \neq \theta_1^{x_i'}, \theta_2' \neq \theta_2^{x_i'}.$$

Constructing (i) requires him to compute Discrete Logarithm $log_\beta B_i$. It's impossible. As to case (ii),

P(successfully construct $\theta_1' \neq \theta_1^{x_i'}, \theta_2' \neq \theta_2^{x_i'}$,which satisfies(*))

$\leq$ P(successfully construct $\theta_1' \neq \theta_1^{x_i'}, \theta_2' \neq \theta_2^{x_i'}$,which satisfies(*) $|x_i'$)

=P(successfully construct $\theta'(\neq 1)$ and $\theta''(\neq 1), s.t., \theta'^{\lambda_1'} = \theta''^{\lambda_2'}$),

Because

$$(\lambda_1', \lambda_2') = (\lambda_1\lambda_4 - \lambda_2\lambda_3)(\lambda_4, -\lambda_2) \pmod q,$$

The probability above equals

P(successfully construct $\theta'(\neq 1)$ and $\theta''(\neq 1), s.t., \theta'^{\lambda_4} = \theta''^{-\lambda_2}$).

But from Discrete Logarithm Problem T_i can't drive any information of relation between λ_2, λ_4 from θ_1, θ_2. Therefore, his construction is not efficient.

Case 2: if $s_i' = s_i$,successfully constructing (*) with $\theta_1 \neq \theta_1^{x_i}, \theta_2 \neq \theta_2^{x_i}$, equals constructing $\theta', \theta''(\neq 1), s.t., \theta'^{\lambda_1'} = \theta''^{\lambda_2'}$. Similar to the proof in (ii) of Case 1, it's difficult. **(iii)** Security of x_0

The two following theorems show

(a) x_0 is secure;

(b) Communication between users is secure.

Theorem 1 Less than $t + 1$ key escrow agencies can not derive a user's session key K or his escrowed private key x_0. And LEA can't derive x_0, too.

Proof : It's obvious that less than $t + 1$ KEA's can't derive K or x_0. As to LEA, information available is at most

$$\beta^{\tau x_i}, \beta^{x_i}, \beta^{x_0}, i = 1, 2, \cdots, n.$$

But τ is random in F_q^*. Therefore, the information is equivalent to $\beta^{x_i}, \beta^{x_0}, i = 1, 2, \cdots, n$. So for any $t+1 < j \leq n \ or \ j = 0$, LEA can easily derive $(h_{j1}, \cdots, h_{j,t+1})$ from (10),$s.t.$,

$$\beta^{x_j} = \prod_{i=1}^{t+1} (\beta^{x_i})^{h_{ji}}.$$

Therefore, the above information is equivalent to $\beta^{x_i}, \beta^{x_0}, i = 1, 2, \cdots, t$. On the other hand,$x_1, x_2, \cdots, x_t and x_0$ are independent, because random tuple

$$(x_1, x_2, \cdots, x_t) \in F_q^t,$$

can correspond to a unique $f(x)$ $\in$F[x],with $x_i = f(i), i = 1, 2, \cdots, t$, and the constant item of $f(x)$ is x_0. Therefore, the above information is further equivalent to β^{x_0}. But if it's difficult to derive x_0 from β^{x_0}.

Theorem 2 After monitoring a user for several times, LEA can not derive the user's session key K in the next monitoring only by himself.

Proof : we adopt reduction to absurdity. Suppose LEA has monitored a user for J times, then the information available to him is at most $\tau_1, \tau_2, \cdots, \tau_J$ and $\beta, \beta^{x_0}, \cdots, \beta^{x_n}$. Since $\tau_1, \tau_2, \cdots, \tau_J$ are random, this information is equivalent to $\beta, \beta^{x_0}, \cdots, \beta^{x_n}$. If LEA can derive the $(J+1)th$ session key, he can derive $\beta^{\tau x_0}$ from $\beta, \beta^{\tau}, \beta^{\tau x_1}, \cdots, \beta^{\tau x_t}$. From the proof of theorem 1,$x_1, x_2, \cdots, x_t$ are independent of each other and each is uniformly distributed in F_q* as a variable. So from τ being random, we know

$$\beta^{\tau}, \beta, \beta^{x_0}, \cdots, \beta^{x_t}$$

are independent of each other. Therefore, deriving $\beta^{\tau x_0}$ from $\beta^{\tau}, \beta, \beta^{x_0}, \cdots, \beta^{x_t}$ is equivalent to derive $\beta^{\tau x_0}$ from $\beta^{\tau}, \beta, \beta^{x_0}$. It's Diffe-Hellman Problem[6], which is difficult.

5 Conclusion

This paper solves an important problem of partial key escrow system i.e., how to devise monitoring scheme to guarantee private key security of monitored users. And we modulate parameter d to make the scheme efficient. Furhter more, we have guaranteed Escrow Agencies are honest. So failed monitoring must be due to the user.

Authors would like to thank Prof.Z.D.Dai for her useful suggestions.

References

[1] A. Shamir, " Partial key escrow," *Key escrow conference,* September 15, 1995.

[2] M. Burmester, Y. Desmedt, and J. Seberry, "Equitable key escrow with limited time span (or How to enforce time expiration cryptographically)," *Advances in Cryptology-Asiacrpt'98*, LNCS 1514, pp 380-391, Springer-Verlag, New York, 1998.

[3] S. Micali, "Guaranteed Partial key escrow," *MIT laboratory of computer science,* Technical Memo 537, September, 1995.

[4] S. Micali and A. Shamir," Partial key escrow," *Manuscript February*, 1996.

[5] M. Bellare and S. Goldwasser," Verifiable partial key escrow," *Proceeding of Fourth Annual Conference on computer and communications Security, ACM,* 1997.

[6] Diffie,W.,Hellman,M.E. "New directions in cryptography,"*IEEE Trans. Inform. Theory,* IT-22(6), 1976, pp644-654.

[7] T.Elgalmal, "A subexpotential-time algorithm for computing discrete logrithms over $GF(q^2)$," *IEEE trans. Inform. Thoery,* Vol.IT-31, No. 4, July, 1985, pp 473-481.