ISSN1000-9825 Journal of Software 软件学报 2000,11(8):1133~1137

部分密钥托管的监听体制*

蒋绍权 张玉峰

(中国科学技术大学研究生院信息安全国家重点实验室 北京 100039)

E-mail: jiangshq@hotmail.com

摘要 在(部分)密钥托管中,监听阶段是一个关键阶段.因此,如何安全而有效地实施监听是一个重要的问题.按照以前的监听方案,用户被监听后,他的整个私钥就暴露了.这对于诚实守法的用户来说是不公平的.该文提出部分密钥托管中的监听方案.在这个方案下,即使用户被监听多次,其托管密钥也不会受到危害.

关键词 监听方案,托管代理,监听机构,密钥,安全性.

中图法分类号 TP309

1995年,Shamir提出部分密钥托管的方案,其目的是为了在监听时延迟恢复密钥,从而阻止了政府大规模实施监听事件的发生.所谓部分密钥托管,就是把整个私钥 c 分成两个部分 x_0 和 a,使得 $c=x_0+a$,其中 a 是小比特数,x_0 是被托管的密钥.x_0 被分成许多份子密钥,它们分别被不同的托管机构托管,只有足够多的托管机构合在一起才能恢复 x_0.监听机构在实施监听时依靠托管机构只能得到 x_0,要得到用户的私钥 c,就需穷搜出 a.

从上面的描述可以看出,一旦监听机构对某个用户实施监听后,他就知道了用户的私钥 c.这样,用户不得不重新申请密钥.这对诚实合法的用户来说是不公平的.对于一般的托管系统,这样的麻烦同样存在.我们称此为监听问题.M. Bellare, Y. Desmedt 和 J. Seberry[1]提出了一个新的托管体制,避免了这样的问题.但对于部分密钥托管来说,还没有解决方案.本文针对一个典型的部分密钥托管方案[2],构造了一个监听方案.在这个方案下,用户的私钥不被暴露.若监听机构想再次监听同一用户时,他必须依靠同样多的托管机构.

1 部分密钥托管系统

下面是本文将用到的参数:T_i 代表第 i 个托管代理;n 代表托管代理 T_i 的总数;l 代表诚实代理 T_i 的数目;t 代表托管门限(假定 $l\geqslant t+1$);p 是大素数,q 是大素数且 $q|p-1$;γ 和 β 是 Z_p 中的 q 阶元,且 $\log_\gamma\beta$ 未知(两个人独立秘密产生 γ,β 即可);d 代表未经托管的部分私钥 a 的长度.

1.1 典型的部分密钥托管系统

在这节,我们首先介绍一个典型的托管系统,其内容除托管代理验证部分(式(2)~(4))外都来自文献[2],更多的托管方面的知识可以参考文献[3,4].

(1) 用户 A 随机选择 $c\in F_q^*$,计算 $Y=\beta^c$,并公开 Y.

(2) 用户 A 随机选取 $d+2$ 个数:$u,w,u_0,\ldots,u_{d-1}\in F_q$,其中 $a=\sum_{i=0}^{d-1}a_i2^i$,$a_i\in\{0,1\}$.

计算 $x_0=c-a \bmod q$,$X=\beta^{x_0}\gamma^w \bmod p$,$A_i=\beta^{u_i}\gamma^{w_i} \bmod p$,$i=0,1,\ldots,d-1$,$w=u+\sum_{i=0}^{d-1}u_i2^i$,把 $X,A_i,w,i=0,1,\ldots,d-1$ 传给每个托管机构.

(3) 托管机构验证:$Y\gamma^w=X\prod_{i=0}^{d-1}A_i^{2^i}$ 是否成立.若成立,则进行比特协议[5];若不成立,则让用户重传数据,直

---

* 作者蒋绍权,1972年生,硕士,主要研究领域为密码学.张玉峰,1976年生,硕士,主要研究领域为密码学.

本文通讯联系人:蒋绍权,成都 610041,成都 622 信箱 220 分箱

本文 1999-04-05 收到原稿,1999-07-20 收到修改稿

到这个等式成立为止.在一切验证通过后,公开 X.

(4) 用户 A 构造多项式 $f(x)=x_0+\sum_{i=1}^{t}f_ix^i\in Z_q[x]$,$v(x)=u+\sum_{i=1}^{t}v_ix^i\in Z_q[x]$,其中 $v_i,f_i(1\leqslant i\leqslant t)$ 随机取自 F_q,计算

$$s_i=v(i),x_i=f(i)\bmod q,\ i=1,\ldots,n, \tag{1}$$

$F_i=\beta^{x_i}\gamma^{s_i},i=1,\ldots,n$.公开 $F_i,i=1,2,\ldots,n$,并把 (s_i,x_i) 秘密传给托管代理 T_i.

(5) 第 i 个托管机构 $T_i,i=1,2,\ldots,n$,计算矩阵 $(b_{ij})_{0\leqslant i<n,1\leqslant j\leqslant n}=((i+1)^{j-1})^{-1}$,验证下面几式是否成立:

$$F_i=\beta^{x_i}\gamma^{s_i}, \tag{2}$$

$$X=\prod_{i=1}^{n}F_i^{b_{0i}}, \tag{3}$$

$$\prod_{i=1}^{n}F_i^{b_{ji}}=1,\ j=t+1,\ldots,n-1. \tag{4}$$

若成立,则密钥申请成功;否则,让用户重传数据,直到成功为止.

1.2 用户间的通信

这一节我们假定用户 A 和 B 按如下方式进行通信[2].

(1) B 随机选取 $r\in(0,q)$,$K\in Z_p$,计算 $y_1=\beta^r\bmod(p)$ 和 $y_2=KY^r\bmod(p)$,令 $LEAF=(y_1,y_2)$,以会话密钥 K 加密明文 M 为 $C=E(M,K)$,将 $(LEAF,C)$ 传给 A.

(2) A 计算 $K\equiv y_2(y_1^x)^{-1}\bmod p$,解出 $M=D(C,K)$.

2 监听方案

这一节介绍我们的监听方案.我们将证明该方案基于离散对数难题[3]和 Diffie Hellman 难题[4]是安全的.本节所用符号与前面保持一致.

2.1 监听方案

(1) 监听机构随机指定 $t+1$ 个代理,不妨设为 $T_{j_1},T_{j_2},\ldots,T_{j_{t+1}}$,分别执行步骤(2)~(8).

(2) T_i 计算 $B_i=\beta^{s_i}\bmod p$,将 (B_i,s_i) 传给监听机构.

(3) 监听机构验证

$$B_i=F_i\gamma^{-s_i}\bmod p \text{ 是否成立.} \tag{5}$$

若成立,则接受 B_i;否则,进行步骤(9).

(4) 监听机构随机选取 $\lambda_1,\lambda_2\in Z_q^*$,计算 $\theta_1=\beta^{\lambda_1}y_1^{\lambda_2}$ 到底 $\bmod p$,把 θ_1 传给 T_i.

(5) T_i 计算 $\bar{\theta}_1=\theta_1^{x_i}$,并把 $\bar{\theta}_1$ 传给监听机构.

(6) 监听机构随机选取 $\lambda_3,\lambda_4\in Z_q\backslash\{0\}$,使 $\lambda_1\lambda_4\neq\lambda_2\lambda_3$,计算 $\theta_2=\beta^{\lambda_3}y_1^{\lambda_4}$,并传给 T_i.

(7) T_i 计算 $\bar{\theta}_2=\theta_2^{x_i}$,把它传给监听机构.

(8) 监听机构计算

$$\begin{pmatrix}\bar{\lambda}_1 & \bar{\lambda}_2\\ \bar{\lambda}_3 & \bar{\lambda}_4\end{pmatrix}=\begin{pmatrix}\lambda_1 & \lambda_2\\ \lambda_3 & \lambda_4\end{pmatrix}^{-1}=(\lambda_1\lambda_4-\lambda_2\lambda_3)^{-1}\begin{pmatrix}\lambda_4 & -\lambda_2\\ -\lambda_3 & \lambda_1\end{pmatrix}\bmod q,\text{验证}$$

$$B_i=\bar{\theta}_1^{\bar{\lambda}_1}\bar{\theta}_2^{\bar{\lambda}_2} \tag{6}$$

是否成立,若成立,则计算

$$z_i=\bar{\theta}_1^{\bar{\lambda}_3}\bar{\theta}_2^{\bar{\lambda}_4}\bmod p. \tag{7}$$

(9) 若有某代理在步骤(3)或步骤(8)的验证中没被通过,则另选一个代理代替之,并重复步骤(2)~(8).直到有 $t+1$ 个代理通过步骤(3)~(8)为止(由于诚实代理数 $l\geqslant t+1$,故一定存在这样的 $t+1$ 个代理),不妨仍设这 $t+1$ 个代理为 $T_{j_1},T_{j_2},\ldots,T_{j_{t+1}}$.

(10) 监听机构计算 $\begin{pmatrix}1 & j_1 & \cdots & j_1^t\\ 1 & j_2 & \cdots & j_2^t\\ & & \cdots & \\ 1 & j_{t+1} & \cdots & j_{t+1}^t\end{pmatrix}^{-1} \bmod q$ 的第 1 行，记作 $(b'_{j_1},\cdots,b'_{j_{t+1}})$，计算

$$\eta=Y\Big(\prod_{k=1}^{t+1}B_{j_k}^{b'_{j_k}}\Big)^{-1}\bmod p, \tag{8}$$

穷搜出 a，使得 $\eta+\beta^a$，计算出会话密钥

$$K=y_2\Big(\prod_{k=1}^{t+1}z_{j_k}^{b'_{j_k}}\Big)^{-1}y_1^{-a}, \tag{9}$$

并用 k 解出明文 $M=D(C,K)$.

2.2 新方案的可行性与安全性

这一节我们将证明体制的可行性与安全性.

可行性是指若所有的参加者是诚实的，则能成功实施监听.

安全性是指：(1) 体制是可验证的. 不诚实的用户或托管机构将被查出；(2) 用户被监听后，他的私钥 c 没有暴露.

2.2.1 可行性

我们将证明若所有的参加者是诚实的，则能成功实施监听. 事实上，只需保证式(5)和式(6)的验证以及式(7)中的 z_i，式(8)中的 η，式(9)中的 K 的正确性.

(1) 式(5)中，$F_i\gamma^{-x_i}=\beta^{x_i}\gamma^{-x_i}=\beta^{x_i}$，故式(5)成立.

(2) 对于式(6)，$\overline{\theta}_1=\theta_1^{x_i}=\beta^{\lambda_1x_i}\beta^{\lambda_2x_i}=\beta^{x_i(\lambda_1,\lambda_2)(1,r)^T}$，$\overline{\theta}_2=\theta_2^{x_i}=\beta^{\lambda_3x_i}\beta^{x_i\lambda_4x_i}=\beta^{x_i(\lambda_3,\lambda_4)(1,r)^T}$. 故 $\overline{\theta}_1^{\lambda_1}\overline{\theta}_2^{\lambda_2}=\beta^{(\lambda_1,\lambda_2)\begin{pmatrix}\lambda_1 & \lambda_2\\ \lambda_3 & \lambda_4\end{pmatrix}(1,r)^Tx_i}$. 由于 $\begin{pmatrix}\lambda_1 & \lambda_2\\ \lambda_3 & \lambda_4\end{pmatrix}*\begin{pmatrix}\lambda_1 & \lambda_2\\ \lambda_3 & \lambda_4\end{pmatrix}^{-1}=I_2$，所以，$\overline{\theta}_1^{\lambda_1}\overline{\theta}_2^{\lambda_2}=\beta^{(1,0)(1,r)^Tx_i}=\beta^{x_i}=B_i$，因此，式(6)成立.

(3) 现在来计算 z_i，与(2)类似，$\overline{\theta}_3^{\lambda_3}\overline{\theta}_4^{\lambda_4}=\beta^{(0,1)(1,r)^Tx_i}=\beta^{x_ir}=y_1^{x_i}$，所以，$z_i=y_1^{x_i}$.

(4) 由 $x_i=f(i)$ 可知，

$$\begin{pmatrix}x_1\\ x_2\\ \vdots\\ x_n\end{pmatrix}=\begin{pmatrix}1 & 1 & \cdots & 1\\ 1 & 2 & \cdots & 2^{n-1}\\ \vdots & & \ddots & \vdots\\ 1 & n & \cdots & n^{n-1}\end{pmatrix}(x_0\ f_1\cdots f_t\ 0\cdots0)^T. \tag{10}$$

设通过监听体制的代理为 $T_{j_1},\cdots,T_{j_{t+1}}$，因而

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

令 $\begin{pmatrix}1 & j_1 & \cdots & j_1^t\\ 1 & j_2 & \cdots & j_2^t\\ \vdots & & \ddots & \vdots\\ 1 & j_{t+1} & \cdots & j_{t+1}^t\end{pmatrix}^{-1}$ 的第 1 行为 $(b'_{j_1},\cdots,b'_{j_{t+1}})$，则 $x_0=\sum_{k=1}^{t+1}b'_{j_k}x_{j_k}$，所以，$\beta^{x_0}=\prod_{k=1}^{t+1}(\beta^{x_{j_k}})^{b'_{j_k}}=\prod_{k=1}^{t+1}B_{j_k}^{b'_{j_k}}$，因此，$\eta=Y\beta^{-x_0}=\beta^a$.

(5) 由于有 $z_i=\beta^{x_ir}$ 及式(10)，我们有

$$\prod_{k=1}^{t+1}z_{j_k}^{b'_{j_k}}=\prod_{k=1}^{t+1}\beta^{b'_{j_k}x_{j_k}r}=\beta^{rx_0}=y_1^{x_0}，\text{所以，}y_2\Big(\prod_{k=1}^{t+1}z_{j_k}^{b'_{j_k}}\Big)^{-1}y_1^{-a}=y_2y_1^{-x_0}y_1^{-a}=K.$$

2.2.2 安全性

现在，我们来考虑体制的安全性. 首先，通过了步骤(3)～(8)的代理，则不可能有欺骗.

(1) 我们先证明(2)~(4)式的安全性. 由于 $\log_\beta \gamma$ 未知,由离散对数难题,它们等价于 $\sum_{i=1}^{n} x_i b_{0i} = x_0$, $\sum_{i=1}^{n} x_i b_{ji} = 0$, $\sum_{i=1}^{n} s_i b_{0i} = u$ 及 $\sum_{i=1}^{n} s_i b_{ji} = 0$, $j = t+1, \ldots, n-1$. 令 $\sum_{i=1}^{n} s_i b_{ji} = \tilde{v}_j$, $\sum_{i=1}^{n} x_i b_{ji} = f_j$, $j = 1, \ldots, t$,则把这几个等式写成矩阵形式就是:

$$\begin{pmatrix} b_{01} & b_{02} & \ldots & b_{0n} \\ b_{11} & b_{12} & \ldots & b_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n-1,1} & b_{n-1,2} & \ldots & b_{n-1,n} \end{pmatrix} \begin{pmatrix} x_1 & s_1 \\ x_2 & s_2 \\ \vdots & \vdots \\ x_n & s_n \end{pmatrix} = \begin{pmatrix} x_0 & f_1 & \ldots & f_t & 0 & \ldots & 0 \\ u & \tilde{v}_1 & \ldots & \tilde{v}_t & 0 & \ldots & 0 \end{pmatrix}^T, \text{即}$$

$$\begin{pmatrix} x_1 & s_1 \\ x_2 & s_2 \\ \vdots & \vdots \\ x_n & s_n \end{pmatrix} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & 2 & \ldots & 2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & n & \ldots & n^{n-1} \end{pmatrix} \begin{pmatrix} x_0 & f_1 & \ldots & f_t & 0 & \ldots & 0 \\ u & \tilde{v}_1 & \ldots & \tilde{v}_t & 0 & \ldots & 0 \end{pmatrix}^T.$$

也就是说,$s_i, x_i, i = 1, 2, \ldots, n$ 的计算是合法的.

如上所述,若数据 B 只能按第 2~4 的协议所述的步骤方法从 A 得到,而不能伪造,则我们称数据 B 匹配于数据 A.

由于式(3)、式(4)验证有效,故 X 和 F_i 中 (x_i, s_i) 匹配于 (x_0, u) $(i = 1, 2, \ldots, n)$,又由于比特协议验证了 a 是 d 比特数,故 (x_0, a) 匹配于 c.

(2) 步骤(3)及步骤(8)验证通过的 T_i 不可能欺骗. 由于式(2)式验证了 F_i 匹配于 (x_i, s_i),故 T_i 掌握真实的分享密钥;另一方面,由于 $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ 是随机的,θ_1, θ_2 可以独立、随机、均匀地送取于乘法群 $\langle\beta\rangle$,故 T_i 要构造步骤(8)中的 $\tilde{\lambda}_1, \tilde{\lambda}_2$,只可能从 B_i 中得到信息,使得

$$B_i = \bar{\theta}_1^{\lambda_1} \bar{\theta}_2^{\lambda_2}. \qquad (*)$$

情形 1. T_i 在步骤(2)中使用 $\tilde{s}_i \neq s_i$,则为了通过步骤(3)的验证,必须计算 $B_i = \beta^{x_i} \gamma^{s_1 - \tilde{s}_i}$,由于离散对数 $\log_\gamma \beta$ 未知,故不可能知道 $\tilde{x}_i$,所以,若构造了(*),其构造必满足(i) $\bar{\theta}_1 = \theta_1^{\tilde{x}_i}$,或(ii) $\bar{\theta}_1 \neq \theta_1^{\tilde{x}_i}, \bar{\theta}_2 \neq \theta_2^{\tilde{x}_i}$;(i) 要求能求出 mod p 的离散对数,但这不可能;(ii) P(成功构造 $\bar{\theta}_1 \neq \theta_1^{\tilde{x}_i}, \bar{\theta}_2 \neq \theta_2^{\tilde{x}_i}$ 满足(*)) $\leqslant P$(成功构造 $\bar{\theta}_1 \neq \theta_1^{\tilde{x}_i}, \bar{\theta}_2 \neq \theta_2^{\tilde{x}_i}$ 满足(*)$|\tilde{x}_i$) $= P$(成功构造 $\theta' (\neq 1), \theta'' (\neq 1), \theta'^{\lambda_1} = \theta''^{\lambda_2}$,由于 $(\tilde{\lambda}_1, \tilde{\lambda}_2) = (\lambda_1\lambda_4 - \lambda_2\lambda_3)^{-1}(\lambda_4, -\lambda_2)$ mod q,故此概率为 P(成功构造 $\theta' (\neq 1), \theta'' (\neq 1), \theta'^{\lambda_4} = \theta''^{\lambda_2}$,但由离散对数难题 T_i 从 θ_1, θ_2 得不到 λ_4, λ_2 之间关系的信息;故此概率为 $1/q$.

情形 2. 当 $\tilde{s}_i = s_i$ 时,构造(*),使 $\bar{\theta}_1 \neq \theta_1^{\tilde{x}_i}$ 或 $\bar{\theta}_2 \neq \theta_2^{\tilde{x}_i}$,等价于构造 $\theta', \theta'' \neq 1$ 使 $\theta'^{\lambda_1} = \theta''^{\lambda_2}$,与情形 1 中(ii)的后一部分证明类似,这也是不可行的.

下面的两个定理说明:

(a) x_0 安全的. (b) 用户间的通信是安全的.

定理 1. x_0 没有泄漏.

证明:在整个监听过程中,监听机构至多获得 β^{x_0},而从 β^{x_0} 算出 x_0 是困难的.

定理 2. 如果少于 $t+1$ 个代理参与监听方案,监听机构要想成功地算出会话密钥 K,在计算上是不可行的.

证明:假定命题不对,通过 J 次对某用户监听后,监听机构至多得到了 $\tau_1, \tau_2, \ldots, \tau_J, \beta, \beta^{x_0}, \ldots, \beta^{x_n}$,实施第 $J+1$ 次监听时,他必须从 $\beta^\tau, \beta^{x\tau_1}, \ldots, \beta^{x\tau_t}$ 中计算出 $\beta^{x\tau_0}$,注意:产生 $x_1, x_2, \ldots, x_n$ 的多项式 $f(x)$ 是随机的、未知的,而随机选择 $\beta^{x_1}, \ldots, \beta^{x_t}$ 可以决定 $f(x)$,并且 $f(x)$ 对监听机构来说也是随机的,故问题等价于从 $\beta, \beta^\tau, \beta^{x_0}$ 中计算出 $\beta^{x\tau_0}$,τ 是随机的,故等价于从 β, y, β^{x_0} 中计算出 y^{x_0},这里,β, y 独立;这在计算上是不可行的.

3 结束语

本文注意并解决了一个广为忽视但又十分重要的问题,即如何才能使用户在被监听后,能安全地使用密钥. 由于 a 的比特数 d 是可以调整的,故体制的有效性也得到了保证. 若监听中产生欺骗,由于我们的监听方案防止

了来自托管代理的欺骗,故欺骗者只可能是用户.

致谢 作者衷心感谢导师戴宗铎教授的热忱关心与支持.

参考文献

1 Burmester M, Desmedt Y, Seberry J. Equitable key escrow with limited time span (or how to enforce time expiration cryptographically). In: Pei Ding-yi ed. Advances in Cryptology-Asiacrypt'98. LNCS 1514, New York: Springer-Verlag, 1998. 380~391

2 Bellare M, Goldwasser S. Verifiable Key escrow. In: Proceedings of the 4th Annual Conference on Computer and Communications Security. New York: ACM Press, 1997

3 Diffie, Hellman W M E. New direction in cryptography. IEEE Transactions on Information Theory, 1976, IT-22(6): 644~654

4 Elgamal T. A subexpotential-time algorithm for computing discrete algorithms over $GF(q^2)$. IEEE Transactions on Information Theory, 1985, IT-31(4): 473~481

Partial Key Escrow Monitoring Scheme

JIANG Shao-quan ZHANG Yu-feng

(State Key Laboratory of Information Security Graduate School University of Science and Technology of China Beijing 100039)

Abstract During (partial) key escrow, monitoring is a vital phase. So how to monitor a user safely and efficiently is a very important problem. According to the known monitoring schemes, after a user is monitored, his secret key is known. It is unfair to an honest user. In this paper, the authors propose 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.

Key words Monitor scheme, trustee, law enforce agency, secret key, security.