一种安全的群签名方案 [1]

王晓明 * ** 符方伟 *

*(南开大学数学科学学院 天津 300071)
**(青岛大学自动化学院 青岛 266071)

摘 要 对 Tseng-Jan(1999) 的群签名方案提出了一种新的伪造攻击，任何人利用这种攻击都能伪造出有效的群签名. 针对该文提出的伪造攻击和 Z.C.Li 等人 (2000) 提出的伪造攻击，对 Tseng-Jan 的群签名方案进行了改进，提出了一种新的安全群签名方案. 新方案不仅能抵抗各种伪造攻击，而且保留了 Tseng-Jan 方案的主要优点，并且增加了群成员可注销的特性.

关键词 密码学，群签名，伪造攻击，可注销群成员
中图号 TN918.1

1 引 言

1998 年， Lee 和 Chang 提出了一个群签名方案 [1]，此方案具有匿名性，群权威 T 可以辨认签名者身份和高效等特性，但这个方案具有关联性. Tseng 和 Jan 对 Lee-Chang 的方案进行了改进，提出了两种改进的群签名方案 [2,3]，然而 Tseng-Jan 提出的两种改进的群签名方案也是不安全的. 最近， Z.C.Li 等人对 Tseng-Jan 方案提出了两种伪造攻击 [4]，任何人利用这两种伪造攻击，都可以伪造出有效的群签名. 本文对 Tseng-Jan 方案的安全性进行了分析，提出了一种新的伪造攻击方法，并针对本文和 Z.C.Li 等人提出的伪造攻击，对 Tseng-Jan 的方案进行了改进，提出了一种新的安全群签名方案. 新方案能抵抗各种伪造攻击，并保留了 Tseng-Jan 的方案的优点，还增加了可注销群成员的特性.

2 Tseng-Jan 的群签名方案 1(简称 TJ1)[2]

2.1 安全参数

(1) p, q 为两个大素数，且 $q|(p-1)$， g 是 GF(p) 中阶为 q 的生成元. 公开 p, q, g .

(2) 群中的每一个成员 u_i 的私钥为 $x_i \in Z_q^*$ ，公钥为 $y_i = g^{x_i} \bmod p$ ，群权威 T 的私钥为 $x_T \in Z_q^*$ ，公钥为 $y_T = g^{x_T} \bmod p$.

(3) 安全的 Hash 函数 h ，公开 h .

2.2 群签名产生过程

(1) T 随机选取 $k_i \in Z_q^*$ ，并计算 $r_i = g^{-k_i} y_i^{k_i} \bmod p$ ， $s_i = k_i - r_i x_T \bmod q$. 秘密送 (s_i, r_i) 给 u_i .

(2) u_i 接到 (s_i, r_i) 后，验证 $g^{s_i} y_T^{r_i} r_i = (g^{s_i} y_T^{r_i})^{x_i} \bmod p$ ，如等式成立，则 (s_i, r_i) 是 T 对每一个成员 u_i 的有效签名，否则是无效签名.

(3) u_i 选取随机数 $a, b, t \in Z_q^*$ ，并计算

$$A = r_i^a \bmod p, \quad B = s_i - b \bmod q, \quad C = r_i a \bmod q, \quad D = g^a \bmod p, \quad E = g^{ab} \bmod p,$$

$$\alpha_i = D^B y_T^C E \bmod p, \quad R = \alpha_i^t \bmod p, \quad s = t^{-1}[h(m) - Rx_i] \bmod q$$

[1] 2001-07-22 收到， 2002-08-23 改回
国家自然科学基金资助 (No.60172060)

m 为待签名的消息。送 (s,R,A,B,C,D,E,m) 给签名验证者。

2.3 群签名的验证过程

群签名验证者首先计算 $\alpha_i = D^B y_T^C E \bmod p$， $\delta_i = \alpha_i A \bmod p$，然后验证

$$\alpha_i^{h(m)} = \delta_i^R R^s \bmod p \tag{1}$$

如 (1) 式成立，则 (s,R,A,B,C,D,E,m) 是 u_i 对消息 m 的有效签名。

3 Tseng-Jan 群签名方案 2(简称 TJ2)[3]

3.1 安全参数

与 2.1 节一样。

3.2 群签名产生过程

(1) 与 2.2 节中的 (1),(2) 一样。

(2) u_i 选取随机数 $a,b,d,t \in Z_q^*$，并计算

$$A = r_i^a \bmod p,\quad B = as_i - bh(A,C,D,E) \bmod q,\quad C = r_i a - d \bmod q,\quad D = g^b \bmod p,$$
$$E = y_T^d \bmod p,\quad \alpha_i = g^B y_T^C E D^{h(A,C,D,E)} \bmod p,\quad R = \alpha_i^t \bmod p,\quad s = t^{-1}[h(m,R) - Rx_i] \bmod p,$$

m 为待签名的消息。送 (s,R,A,B,C,D,E,m) 给签名验证者。

3.3 群签名的验证过程

群签名验证者首先计算 $\alpha_i = g^B y_T^C E D^{h(A,C,D,E)} \bmod p$， $\delta_i = \alpha_i A \bmod p$，然后验证

$$\alpha_i^{h(m,R)} = \delta_i^R R^s \bmod p \tag{2}$$

如 (2) 式成立，则 (s,R,A,B,C,D,E,m) 是 u_i 对消息 m 的有效签名。

4 伪造攻击

4.1 对 TJ1 的伪造攻击 (攻击 1)

攻击者任意选取 B, C, D, E，并选取随机数 $t \in Z_q^*$，计算

$$\alpha_i = D^B y_T^C E \bmod p,\quad A = \alpha_i^{x_i - 1} \bmod p,\quad R = \alpha_i^t \bmod p,\quad s = t^{-1}[h(m) - Rx_i] \bmod q \tag{3}$$

则 (s,R,A,B,C,D,E,m) 是伪造的群签名。

伪造的群签名 (s,R,A,B,C,D,E,m) 能通过 (1) 式的验证，因为由 (3) 式得

$$\alpha_i^{h(m)} = \alpha_i^{x_i R} \alpha_i^{ts} = (\alpha_i^{x_i - 1} \alpha_i)^R R^s = (\alpha_i A)^R R^s = \delta_i^R R^s \bmod p$$

则 (s,R,A,B,C,D,E,m) 是一个有效的群签名。

4.2 对 TJ2 的伪造攻击 (攻击 2)

攻击者任意选取 C, U，并选取随机数 t, $b \in Z_q^*$，计算

$$E = y_T^{-C} U \bmod p,\quad A = U^{x_i - 1} \bmod p,\quad D = g^b \bmod p,\quad B = -bh(A,C,D,E) \bmod q,$$
$$\alpha_i = g^B y_T^C E D^{h(A,C,D,E)} \bmod p,\quad R = \alpha_i^t \bmod p,\quad s = t^{-1}[h(m,R) - Rx_i] \bmod p,$$

则 (s,R,A,B,C,D,E,m) 是伪造的群签名。

伪造的群签名 (s,R,A,B,C,D,E,m) 能通过 (2) 式的验证，因为

$$\alpha_i = g^{-bh(A,C,D,E)} y_T^C y_T^{-C} U g^{bh(A,C,D,E)} = U \bmod p,$$
$$\alpha_i^{h(m,R)} = (U^{x_i-1}U)^R R^s = (A\alpha_i)^R R^s = \delta_i^R R^s \bmod p,$$

则 (s,R,A,B,C,D,E,m) 是一个有效的群签名。

5 Z. C. Li 等人提出的伪造攻击 [4]

5.1 对 TJ1 的伪造攻击 (攻击 3)

攻击者选取随机数 $U, V, X, Y \in Z_q^*$，并计算

$$D = y_T^U \bmod p, \quad E = y_T^V \bmod p, \quad A = y_T^X \bmod p, \quad R = y_T^Y \bmod p.$$

攻击者随机选取 B 和 C，并从下面方程解出 s。

$$Uh(m)B + h(m)C + Vh(m) = UBR + CR + VR + XR + sY \bmod q \tag{4}$$

则 (s,R,A,B,C,D,E,m) 是伪造的群签名。

伪造的群签名 (s,R,A,B,C,D,E,m) 能通过 (1) 式的验证，因为

$$\alpha_i = D^B y_T^C E = y_T^{UB} y_T^C y_T^V \bmod p, \qquad \delta_i = \alpha_i A = y_T^{UB} y_T^C y_T^V y_T^X \bmod p,$$
$$\alpha_i^{h(m)} = y_T^{UBh(m)+h(m)C+h(m)V} \bmod p, \qquad \delta_i^R R^s = y_T^{UBR+CR+VR+XR+sY} \bmod p$$

因为 s 是从 (4) 式中解出的，所以 (s,R,A,B,C,D,E,m) 可以使 $\alpha_i^{h(m)} = \delta_i^R R^s \bmod p$ 成立 (见 (1) 式)，则伪造的 (s,R,A,B,C,D,E,m) 是一个有效的群签名。

5.2 对 TJ2 的伪造攻击 (攻击 4)

攻击者选取 5 对随机数 $(U_A,V_A),(U_C,V_C),(U_D,V_D),(U_E,V_E),(U_R,V_R) \in Z_q^*$，并计算

$$A = g^{U_A} y_T^{V_A} \bmod p, \quad D = g^{U_D} y_T^{V_D} \bmod p, \quad C = g^{U_c} y_T^{V_c} \bmod p, \quad R = g^{U_R} y_T^{V_R} \bmod p,$$
$$E = g^{U_E} y_T^{V_E} \bmod p, \qquad h = h(m,R), \qquad H = h(A,C,D,E).$$

攻击者解下面方程，求出 s, B

$$Bh + U_E h + U_D hH = BR + U_E R + U_D HR + U_A R + U_R s \bmod q \tag{5}$$
$$Ch + V_E h + V_D hH = CR + V_E R + V_D HR + V_A R + V_R s \bmod q \tag{6}$$

则 (s,R,A,B,C,D,E,m) 是伪造的群签名。

伪造的群签名 (s,R,A,B,C,D,E,m) 能通过 (2) 式的验证，因为

$$\alpha_i = g^B y_T^C g^{U_E} y_T^{V_E} g^{U_D H} y_T^{V_D H} \bmod p,$$
$$\delta_i = g^B y_T^C g^{U_E} y_T^{V_E} g^{U_D H} y_T^{V_D H} g^{U_A} y_T^{V_A} \bmod p,$$
$$\alpha_i^{h(m,R)} = g^{Bh+U_E h+U_D Hh} y_T^{Ch+V_E h+V_D Hh} \bmod p,$$
$$\delta_i^R R^s = g^{BR+U_E R+U_D HR+U_A R+U_R s} y_T^{CR+V_E R+V_D HR+V_A R+V_R s} \bmod p.$$

根据 (5), (6) 式知，伪造的 (s,R,A,B,C,D,E,m) 满足 $\alpha_i^{h(m,R)}=\delta_i^R R^s \bmod p$(见 (2) 式)，则 (s,R,A,B,C,D,E,m) 是一个有效的群签名。

6 新的群签名方案

6.1 安全参数

(1) p, q 为两个大素数，且 $q|(p-1)$， g 是 GF(p) 中阶为 q 的生成元。公开 p, q, g。

(2) 群中的每一个成员 u_i 选择随机数 $x_i\in Z_q^*$ 作为私钥，计算 $y_i=g^{x_i}\bmod p$ 作为公钥，群权威 T 选择随机数 $x_T\in Z_q^*$ 作为私钥，计算 $y_T=g^{x_T}\bmod p$ 作为公钥。

(3) 安全的 Hash 函数 h，公开 h。

6.2 群成员的加入

当 u_i 想成为群的一个成员，需作如下步骤：

(1) T 随机选取 $k_i\in Z_q^*$，并计算

$$r_i=g^{-k_i}y_i^{k_i}\bmod p,\qquad s_i=k_i-r_i x_T \bmod q \tag{7}$$

秘密送 (s_i,r_i) 给 u_i，并存储 (s_i,r_i,k_i)。

(2) u_i 接到 (s_i,r_i) 后，验证

$$g^{s_i}y_T^{r_i}r_i=(g^{s_i}y_T^{r_i})^{x_i}\bmod p \tag{8}$$

如 (8) 式成立，u_i 接收 (s_i,r_i)。(8) 式成立的原因为：由 (7) 式得

$$g^{s_i}=g^{k_i}g^{-r_i x_T}\bmod p,\qquad g^{s_i}y_T^{r_i}=g^{k_i}\bmod p,$$
$$g^{s_i}y_T^{r_i}r_i=g^{k_i}g^{-k_i}y_i^{k_i}=y_i^{k_i}=(g^{s_i}y_T^{r_i})^{x_i}\bmod p.$$

6.3 群签名的产生过程

设待签名的消息为 m, u_i 随机选取 $a,b,d,t\in Z_q^*$，并计算

$$\left.\begin{aligned}
&C=r_i a-d\bmod q,\quad A=y_i^b\bmod p,\quad D=g^b\bmod p,\\
&E=r_i^a(1+g^{-s_i a}y_T^{-r_i a})^{x_i}\bmod p,\quad F=y_T^d\bmod p,\\
&B=s_i a-bh(A,C,D,E,F)+bh(E,D,F)\bmod q,\\
&\alpha_i=[D^{h(E,D,F)}+g^B y_T^C F D^{h(A,C,D,E,F)}]\bmod p,\\
&R=\alpha_i^t\bmod p,\qquad s=t^{-1}[h(m,R)-x_i R]\bmod q
\end{aligned}\right\} \tag{9}$$

送 (s,R,A,B,C,D,E,m) 给签名验证者。

6.4 群签名的验证

群签名验证者计算

$$\alpha_i=D^{h(E,D,F)}+g^B y_T^C F D^{h(A,C,D,E,F)}\bmod p,$$
$$\delta_i=A^{h(E,D,F)}[\alpha_i D^{-h(E,D,F)}-1]E\bmod p,$$

验证

$$\alpha_i^{h(m,R)}=\delta_i^R R^s\bmod p \tag{10}$$

如 (10) 式成立，则 (s,R,A,B,C,D,E,F,m) 是 u_i 对消息 m 的有效签名。

(10) 式成立的原因为：由 (7) 式中的 s_i，(9) 式中的 C, D, F 和 B 得

$$\begin{aligned}\alpha_i &= g^{bh(E,D,F)} + g^{s_i a} g^{-bh(A,C,D,E,F)} g^{bh(E,D,F)} g^{x_T r_i a} g^{-x_T d} g^{x_T d} g^{bh(A,C,D,E,F)} \\ &= g^{bh(E,D,F)}(1 + g^{s_i a} g^{x_T r_i a}) = g^{bh(E,D,F)}(1 + g^{k_i a}) \bmod p \end{aligned} \tag{11}$$

由 (7) 式中的 r_i，(9) 式中的 A, α_i, s 和 (11) 式得

$$\begin{aligned}\alpha_i^{h(m,R)} &= \alpha_i^{x_i R} \alpha_i^{ts} = [g^{bh(E,D,F)x_i} g^{k_i a x_i}(1 + g^{-k_i a})^{x_i}]^R R^s \\ &= [A^{h(E,D,F)} g^{k_i a} r_i^a (1 + g^{-s_i a} y_T^{-r_i a})^{x_i}]^R R^s \\ &= [A^{h(E,D,F)}(\alpha_i g^{-bh(E,D,F)} - 1) r_i^a (1 + g^{-s_i a} y_T^{-r_i a})^{x_i}]^R R^s = \delta_i^R R^s \bmod p. \end{aligned}$$

6.5 群成员的识别

群权威 T 已存有每一个群成员的 (s_i, r_i, k_i)，T 可以预先计算

$$v_i = s_i^{-1} k_i \bmod q, \qquad w_i = g^{v_i} \bmod p \tag{12}$$

并将 (v_i, w_i) 与 (s_i, r_i, k_i) 一起存储。如需要打开某一个群签名，T 可以查询已存的 (s_i, r_i, k_i) 和 (v_i, w_i)，这里 $i = 1, 2, \cdots, n$，n 是群成员个数，判断那个群成员对应的 (v_i, w_i) 满足

$$g^B y_T^C F D^{h(A,C,D,E,F)} = w_i^B D^{[h(A,C,D,E,F)v_i - h(E,D,F)v_i + h(E,D,F)]} \bmod p \tag{13}$$

于是 T 就能确定签名者的身份。

(13) 式成立的原因为：由 (7) 式中的 s_i，(9) 式中的 C, D, F, B 和 (12) 式得

$$\begin{aligned}&g^B y_T^C F D^{h(A,C,D,E,F)} = g^{k_i a} g^{bh(E,D,F)} \bmod p, \\ &w_i^B D^{[h(A,C,D,E,F)v_i - h(E,D,F)v_i + h(E,D,F)]} \\ &\quad = (g^{s_i^{-1} k_i})^{[s_i a - bh(A,C,D,E,F) + bh(E,D,F)]} g^{bh(A,C,D,E,F) s_i^{-1} k_i} g^{-bh(E,D,F) s_i^{-1} k_i} g^{bh(E,D,F)} \\ &\quad = g^{k_i a} g^{bh(E,D,F)} \bmod p \end{aligned}$$

6.6 群成员的注销

如果要注销某个群成员，群权威 T 查询出要注销群成员对应的 (v_i, w_i)，并公布 (v_i, w_i) 为注销群成员。当签名验证者接到群签名时，首先从公布的注销群成员名单中取出 (v_i, w_i)，判断

$$g^B y_T^C F D^{h(A,C,D,E,F)} = w_i^B D^{[h(A,C,D,E,F)v_i - h(E,D,F)v_i + h(E,D,F)]} \bmod p \tag{14}$$

如 (14) 式成立，则此群签名无效，否则，继续验证群签名的有效性，即进行群签名的验证，从而实现了群成员的注销。

6.7 性能分析

(1) 新方案能抵抗本文和 Z.C. Li 等人提出的伪造攻击

攻击 1 因为 $\alpha_i = D^{h(E,D,F)} + g^B y_T^C F D^{h(A,C,D,E,F)} \bmod p$，所以攻击者无法取 A 或 D 与 α_i 有关的数，因此攻击 1 对新方案无效。

攻击 2 如攻击者任意取 C，选取随机数 $b \in Z_q^*$，并计算

$$F = y_T^{-C} \bmod p, \quad A = D = g^b \bmod p, \quad B = -bh(A,C,D,E,F) \bmod q,$$

则 $\alpha_i = D^{h(E,D,F)} + g^{-bh(A,C,D,E,F)} y_T^C y_T^{-C} g^{bh(A,C,D,E,F)} = D^{h(E,D,F)} + 1 \bmod p$,
$\delta_i = A^{h(E,D,F)}[(D^{h(E,D,F)}+1)D^{-h(E,D,F)} - 1]E = A^{h(E,D,F)} D^{-h(E,D,F)} E = E \bmod p$.
为了能使伪造的群签名通过 (2) 式验证，则攻击者就必须取 $E = [1 + D^{h(E,D,F)}]^{x_i} \bmod p$ ，但从此式可知，攻击者无法求出 E, 则攻击者在不知道 (s_i, r_i) 时，无法伪造出能通过 (2) 式验证的 $(s, R, A, B, C, D, E, F, m)$. 因此攻击 2 对新方案无效.

攻击 3 攻击者选取随机数 $U, V, X, Y, W \in Z_q^*$ ，并计算

$$A = y_T^U \bmod p, \quad E = y_T^V \bmod p, \quad D = y_T^X \bmod p, \quad F = y_T^Y \bmod p, \quad R = y_T^W \bmod p,$$
$$\alpha_i^{h(m,R)} = [y_T^{Xh(E,D,F)} + g^B y_T^{C+Y+Xh(A,C,D,E,F)}]^{h(m,R)} \bmod p,$$
$$\delta^R R^s = g^{BR} y_T^{[Uh(E,D,F)R+CR+YR+XRh(A,C,D,E,F)-XRh(E,D,F)+VR+sW]} \bmod p$$

根据 $\alpha_i^{h(m,R)} = \delta_i^R R^s \bmod p$ ，即

$$[y_T^{Xh(E,D,F)} + g^B y_T^{C+Y+Xh(A,C,D,E,F)}]^{h(m,R)} = g^{BR} y_T^{[Uh(E,D,F)R+CR+YR+XRh(A,C,D,E,F)-XRh(E,D,F)+VR+sW]} \bmod p$$

得不到能解出 s 的方程，所以攻击者无法伪造 s ，则 Z.C. Li 等人提出的伪造攻击 3 对新方案攻击无效.

攻击 4 攻击者随机选取 5 对数 $(U_A, V_A), (U_D, V_D), (U_E, V_E), (U_F, V_F), (U_R, V_R) \in Z_q^*$

$$A = g^{V_A} y_T^{U_A} \bmod p, \quad D = g^{U_D} y_T^{V_D} \bmod p, \quad E = g^{U_E} y_T^{V_E} \bmod p, \quad R = g^{U_R} y_T^{V_R} \bmod p,$$
$$F = g^{U_F} y_T^{V_F} \bmod p, \quad H = h(A, C, D, E, F), \quad h = h(E, D, F),$$
$$\alpha_i^{h(m,R)} = [g^{U_D h} y_T^{V_D h} + g^{B+U_F+U_D H} y_T^{C+V_F+V_D H}]^{h(m,R)} \bmod p,$$
$$\delta^R R^s = g^{[V_A h+B+U_F+U_D H-V_D h+U_E]R+U_R s} y_T^{[V_A h+C+V_F+V_D H-V_D h+V_E]R+V_R s} \bmod p$$

根据 $\alpha_i^{h(m,R)} = \delta_i^R R^s \bmod p$ ，即

$$[g^{U_D h} y_T^{V_D h} + g^{B+U_F+U_D H} y_T^{C+V_F+V_D H}]^{h(m,R)} = g^{[V_A h+B+U_F+U_D H-U_D h+U_E]R+U_R s} y_T^{[V_A h+C+V_F+V_D H-V_D h+V_E]R+V_R s} \bmod p$$

得不到解出 s 的方程，所以攻击者无法伪造 s ，则 Z.C. Li 等人提出的伪造攻击 4 对新方案攻击无效.

(2) 新方案比 Tseng-Jan 的群签名方案 [2,3] 增加了可注销群成员的特性 (见 6.6 节) . 通过群权威 T 公布注销群成员的 (v_i, w_i) ，群签名验证者根据接收的群签名中 $g^B y_T^C F D^{h(A,C,D,E,F)}$ 是否与 $w_i^B D^{[h(A,C,D,E,F)v_i - h(E,D,F)v_i + h(E,D,F)]}$ 相等 (见 (14) 式) 来判断接收的群签名是否是注销群成员签发的，使注销群成员不能再行使群签名的权力，从而实现了群成员的注销. 同时由于公布的是注销群成员的 (v_i, w_i) ，并没有泄露 (s_i, r_i) ，所以没有破坏原来所做群签名的安全性，匿名性，不关联性，群权威 T 可辨认群签名者的身份等特性.

(3) 与文献 [2,3] 一样分析，新方案具有群签名者匿名性，不关联性，群权威 T 可辨认群签名者的身份和高效等特性.

7 结 束 语

Tseng-Jan 的群签名方案具有匿名性，不关联性. 群权威 T 可辨认签名者身份和高效等特性，但它是不安全的，不能抵抗本文和 Zichen Li 等人提出的伪造攻击。本文提出的安全群签名方案能抵抗各种伪造攻击，保留了 Tseng-Jan 的方案已有优点，还增加了可注销群成员的特性。

参 考 文 献

[1] W. Lee, C. Chang, Efficient group signature scheme based on the discrete logarithm, IEE Proc.-Comput. Digital Techniques, 1998, 145(1), 15–18.

[2] Y. M. Tseng, J. K. Jan, Improved group signature based on discrete logarithm problem, Electronics Letters, 1999, 35(1): 37–38.

[3] Y. M. Tseng, J. K. Jan, Reply: Improved group signature scheme based on discrete logarithm problem, Electronics Letters, 1999, 35(6), 1324–1325

[4] Z. C. Li, L. C. K. Hui, *et al.*, Security of Tseng-Jan's group signature schemes, Information Processing Letters, 2000, 75(5), 187–189.

A SECURE GROUP SIGNATURE SCHEME

Wang Xiaoming* **　　Fu Fangwei*

*(*School of Mathematics Science, Nankai University, Tianjin* 300071, *China*)

**(*College of Automatization, Qingdao University, Qingdao* 266071, *China*)

Abstract　A new forgery attack is proposed to Tseng-Jan's group signature scheme(1999), anyone can produce a valid group signature with this forgery attack. In this paper, a new modified and secure group signature scheme is presented in point of the forgery attacks proposed by this paper and Z.C. Li, *et al.*(2000). The new scheme can not only resist all kinds of forgery attacks, but also preserve the main merits in Tseng-Jan's scheme. Furthermore, the new scheme can revoke group member according to need.

Key words　Cryptography, Group signature, Forgery attack, Revocation group member

王晓明：　女，1960 年生，副教授，博士生，主要从事现代密码学，计算机网络安全等方面的研究工作.

符方伟：　男，1963 年生，教授，博士生导师，主要从事信息论，现代密码学，编码理论，计算机网络安全等方面的研究工作.