- C 检查列表 $List_{key}$:若 $List_{key}$ 中存在数组 $\left(\omega_{ID_\varsigma,\bar{I}}, ID_\varsigma, \{T_{\bar{I},j}, S_{\bar{I},j}\}_{j\in\omega_{ID_\varsigma,\bar{I}}\cup\Omega_{\bar{I}}^*}, P_{\bar{I}}\right)$,则将 $\{T_{\bar{I},j}, S_{\bar{I},j}\}_{j\in\omega_{ID_\varsigma,\bar{I}}\cup\Omega_{\bar{I}}^*}$ 和 $P_{\bar{I}}$ 作为对 $(\omega_{ID_\varsigma,\bar{I}}, ID_\varsigma)$ 进行密钥解析询问的应答发送给 A.
- 否则,若 $|\omega_{ID_\varsigma,\bar{I}}\cap\omega_{\bar{I}}^*|<t_{\bar{I}}$,$C$ 随机选取缺省属性集合 $\Omega_{\bar{I}}^*$,满足 $|\Omega_{\bar{I}}^*|=d_{\bar{I}}-t_{\bar{I}}$. 定义 3 个属性集合 $\Gamma_{\bar{I}},\Gamma'_{\bar{I}},S_{\bar{I}}$,其中,$\Gamma_{\bar{I}}\subseteq\Gamma'_{\bar{I}}\subset S_{\bar{I}}, \Gamma_{\bar{I}}=\omega_{ID_\varsigma,\bar{I}}\cap\omega_{\bar{I}}^*\cup\Omega_{\bar{I}}^*, |\Gamma'_{\bar{I}}|=d_{\bar{I}}-1, S_{\bar{I}}=\Gamma'_{\bar{I}}\cup\{0\}$.由拉格朗日插值公式可知,$a_0=\sum_{k\in\Psi\cup\bar{I}}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)$,由于 A 已经攻破集合 Ψ 中所有属性授权机构,因此,$AA_{\bar{I}}$ 的部分密钥满足等式 $a_{\bar{I},0}=\dfrac{a_0-\sum_{k\in\Psi}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)}{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}$.

对于属性 $j_{\bar{I}}\in\Gamma'_{\bar{I}}$,$C$ 首先随机选取 $x'_{\bar{I}},\tau_{j,\bar{I}},t_{j,\bar{I}}\in Z_q^*$,等价于隐性地令 $q_{\bar{I}}(j)=\tau_{j,\bar{I}}$,然后分别对 ID_ς 和 $j_{\bar{I}}$ 进行预言机询问得到 $H_1(\lambda_\varsigma)$ 和 $H_2(j_{\bar{I}})$ 的仿真结果,最后 C 生成相应属性的密钥.

$$\{S_{1,j,\bar{I}}=H_2(j)^{t_{j,\bar{I}}}g_2^{H_1(\lambda_{\varsigma,\bar{I}})\tau_{j,\bar{I}}}\}_{j\in\Gamma'},S_{2,\bar{I}}=g_1^{-x'_{\bar{I}}}g_2^{\frac{-(H_1(\lambda_{\varsigma,\bar{I}})+1)\cdot\sum_{k\in\Psi}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)}{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}},\{T_{1,j,\bar{I}}=g^{t_{j,\bar{I}}}\}_{\xi\in\Gamma'},P_{\bar{I}}=g_1^{x'_{\bar{I}}}.$$

正确性验证:令 $x_{\bar{I}}=\dfrac{(H_1(\lambda_{\varsigma,\bar{I}})+1)\cdot b_0}{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}+x'_{\bar{I}}$,则下列等式成立.

$$S_{2,\bar{I}}=g_1^{-x'_{\bar{I}}}g_2^{\frac{-(H_1(\lambda_{\varsigma,\bar{I}})+1)\cdot\sum_{k\in\Psi}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)}{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}}=g_1^{-\left(x_{\bar{I}}-\frac{(H_1(\lambda_{\varsigma,\bar{I}})+1)\cdot b_0}{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}\right)}g_2^{\frac{-(H_1(\lambda_{\varsigma,\bar{I}})+1)\cdot\sum_{k\in\Psi}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)}{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}}=g_1^{-x_{\bar{I}}}g_2^{H_1(\lambda_{\varsigma,\bar{I}})a_{\bar{I},0}+a_{\bar{I},0}}.$$

对于属性 $\xi_{\bar{I}}\notin\Gamma'$,为了确保等式 $q_{\bar{I}}(0)=a_{\bar{I},0}$ 成立,C 随机选取 $t'_{\xi,\bar{I}}\in Z_p^*$,计算相应的属性密钥:

$$S_{1,\xi,\bar{I}}=(g_1^{-\beta_{\bar{I},\xi}}g^{\gamma_{\bar{I},\xi}})^{t'_{\xi,\bar{I}}}g_2^{\gamma_{\bar{I},\xi}\cdot\frac{H_1(\lambda_{\varsigma,\bar{I}})\Delta_{0,S_{\bar{I}}}(\xi)}{\beta_{\bar{I},\xi}\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}+H_1(\lambda_{\varsigma,\bar{I}})\left(\sum_{j\in\Gamma'_{\bar{I}}}q_{\bar{I}}(j)\Delta_{j,S_{\bar{I}}}(\xi)-\frac{\sum_{k\in\Psi}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)}{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}\Delta_{0,S_{\bar{I}}}(\xi)\right)},T_{1,\xi,\bar{I}}=g_2^{\frac{H_1(\lambda_{\varsigma,\bar{I}})\Delta_{0,S_{\bar{I}}}(\xi)}{\beta_{\bar{I},\xi}\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}}g^{t'_{\xi,\bar{I}}}.$$

正确性验证:令 $t_{\xi,\bar{I}}=\dfrac{H_1(\lambda_{\varsigma,\bar{I}})\Delta_{0,S_{\bar{I}}}(\xi)}{\beta_{\bar{I},\xi}\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}\cdot b_0+t'_{\xi,\bar{I}}$,由于 $q_{\bar{I}}(\xi)=\sum_{j\in\Gamma'_{\bar{I}}}q_{\bar{I}}(j)\Delta_{j,S_{\bar{I}}}(\xi)+q_{\bar{I}}(0)\Delta_{0,S_{\bar{I}}}(\xi)$,故下列等式成立.

$$\begin{aligned}S_{1,\xi,\bar{I}}&=(g_1^{-\beta_{\bar{I},\xi}}g^{\gamma_{\bar{I},\xi}})^{t'_{\xi,\bar{I}}}g_2^{\gamma_{\bar{I},\xi}\cdot\frac{H_1(\lambda_{\varsigma,\bar{I}})\Delta_{0,S_{\bar{I}}}(\xi)}{\beta_{\bar{I},\xi}\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}+H_1(\lambda_{\varsigma,\bar{I}})\left(\sum_{j\in\Gamma'_{\bar{I}}}q_{\bar{I}}(j)\Delta_{j,S_{\bar{I}}}(\xi)-\frac{\sum_{k\in\Psi}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)}{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}\Delta_{0,S_{\bar{I}}}(\xi)\right)}\\&=(g_1^{-\beta_{\bar{I},\xi}}g^{\gamma_{\bar{I},\xi}})^{t_{\xi,\bar{I}}-\frac{H_1(\lambda_{\varsigma,\bar{I}})\Delta_{0,S_{\bar{I}}}(\xi)}{\beta_{\bar{I},\xi}\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}\cdot b_0}g_2^{\gamma_{\bar{I},\xi}\cdot\frac{H_1(\lambda_{\varsigma,\bar{I}})\Delta_{0,S_{\bar{I}}}(\xi)}{\beta_{\bar{I},\xi}\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}+H_1(\lambda_{\varsigma,\bar{I}})\left(\sum_{j\in\Gamma'_{\bar{I}}}q_{\bar{I}}(j)\Delta_{j,S_{\bar{I}}}(\xi)-\frac{\sum_{k\in\Psi}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)}{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}\Delta_{0,S_{\bar{I}}}(\xi)\right)}\\&=(g_1^{-\beta_{\bar{I},\xi}}g^{\gamma_{\bar{I},\xi}})^{t_{\xi,\bar{I}}}g_2^{H_1(\lambda_{\varsigma,\bar{I}})q_{\bar{I}}(\xi)}.\end{aligned}$$

把相应密钥集合发送给 A,并将数组 $\left(\omega_{ID_\varsigma,\bar{I}}, ID_\varsigma, \{T_{j,\bar{I}}, S_{j,\bar{I}}\}_{j\in\omega_{ID_\varsigma,\bar{I}}\cup\Omega_{\bar{I}}^*}, P_{\bar{I}}\right)$ 存入列表 $List_{key}$.

- 否则,$|\omega_{ID_\varsigma,\bar{I}}\cap\omega_{\bar{I}}^*|\geqslant t_{\bar{I}}$,$C$ 停止仿真,将该事件记为 E_1.

e) 签名询问:A 输入 $(\omega_{ID_\varsigma}, ID_\varsigma, m_\varsigma)$ 进行签名询问,C 进行如下操作.

- 若 $|\omega_{ID_\varsigma,\bar{I}}\cap\omega_{\bar{I}}^*|<t_{\bar{I}}$,$C$ 通过对 $(\omega_{ID_\varsigma,k}, ID_\varsigma)_{k\in\psi\cup\bar{I}}$ 进行密钥解析询问,获得相应属性的密钥,对 m_ς 进行 H_3 询问得到 $H_3(m_\varsigma)$ 的仿真结果,直接利用签名算法得到 m_ς 相应的签名,并发送给 A.
- 否则,$|\omega_{ID_\varsigma,\bar{I}}\cap\omega_{\bar{I}}^*|\geqslant t_{\bar{I}}$,若 $H_3(m_\varsigma)\neq g^{\eta_\delta}$,$C$ 首先随机选取属性集合 $\{\omega'_{ID_\varsigma,k}\}_{k\in\psi\cup\bar{I}}$ 和缺省属性集合 $\{\Omega_k^*\}_{k\in\psi\cup\bar{I}}$,其中,$\omega'_{ID_\varsigma,k}\subseteq\{\omega_{ID_\varsigma,k}\cap\omega_k^*\}$ 且 $|\omega'_{ID_\varsigma,k}\cup\Omega_k^*|=d_k$;然后,选随机数 $z,v'\in Z_q^*$ 和随机数集合 $\{r_{j,k}\in Z_q^*\}_{k\in\Psi\cup\bar{I},j\in\omega_k^*\cup\Omega_k^*}$;最后,通过下述方法生成 m_ς 对应的签名 $\sigma_\varsigma=\langle\sigma_1^\varsigma,\sigma_2^\varsigma,\sigma_3^\varsigma,\{\sigma_{4,j,k}^\varsigma\}_{j\in\omega_k^*\cup\Omega_k^*,k\in\psi\cup\bar{I}}\rangle$,其中,

$$\sigma_1 = g_2^{z-\frac{\eta_\varsigma \cdot H_1(\lambda_{i,\bar{I}})}{\theta_\varsigma}+\sum_{k\in\Psi}(H_1(\lambda_{i,k})-H_1(\lambda_{i,\bar{I}}))a_{k,0}\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}(g_1^{\theta_\varsigma}g^{\eta_\varsigma})^{v'}\prod_{k\in\Psi\cup\bar{I}}\left(\prod_{j\in\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(H_2(j)^{t_{j,k}})^{\Delta_{j,\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(0)\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}\prod_{j\in\omega_k^*\cup\Omega_k^*}H_2(j)^{r_{j,k}}\right),$$

$$\sigma_2 = g_2^{z-(H_1(\lambda_\varsigma)+1)\cdot\sum_{k\in\Psi}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)}\prod_{k\in\Psi}(g_2^{H_1(\lambda_i)a_{k,0}+a_{k,0}})^{\Delta_{k,\Psi\cup\bar{I}}(0)},$$

$$\sigma_3 = g_2^{-\frac{H_1(\lambda_{\varsigma,\bar{I}})}{\theta_\varsigma}}g^{v'}\left\{\sigma_{4,j,k}=(T_{j,k})^{\Delta_{j\in\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(0)\Delta_{k\in\Psi\cup\bar{I}}(0)}g_2^{r_{j,k}}\right\}_{j\in\omega'_{ID_\varsigma,k}\cup\Omega_k^*,k\in\Psi\cup\bar{I}}\{\sigma_{4,j,k}=g_2^{r_{j,k}}\}_{j\in\omega_k^*\setminus\omega'_{ID_\varsigma,k},k\in\psi\cap\bar{I}}.$$

正确性验证:令 $v=-\frac{H_1(\lambda_{\varsigma,\bar{I}})}{\theta_\varsigma}\cdot b_0+v'$,则下列等式成立.

$$\sigma_1 = g_2^{z-\frac{\eta_\varsigma \cdot H_1(\lambda_{\varsigma,\bar{I}})}{\theta_\varsigma}+\sum_{k\in\Psi}(H_1(\lambda_{\varsigma,k})-H_1(\lambda_{\varsigma,\bar{I}}))a_{k,0}\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}(g_1^{\theta_\varsigma}g^{\eta_\varsigma})^{v'}\prod_{k\in\Psi\cup\bar{I}}\left(\prod_{j\in\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(H_2(j)^{t_{j,k}})^{\Delta_{j,\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(0)\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}\prod_{j\in\omega_k^*\cup\Omega_k^*}H_2(j)^{r_{j,k}}\right)$$

$$= g_2^{z-\frac{\eta_\varsigma \cdot H_1(\lambda_{\varsigma,\bar{I}})}{\theta_\varsigma}+\sum_{k\in\Psi}(H_1(\lambda_{\varsigma,k})-H_1(\lambda_{\varsigma,\bar{I}}))a_{k,0}\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}(g_1^{\theta_\varsigma}g^{\eta_\varsigma})^{v+\frac{H_1(\lambda_{\varsigma,\bar{I}})}{\theta_\varsigma}\cdot b_0}$$

$$\prod_{k\in\Psi\cup\bar{I}}\left(\prod_{j\in\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(H_2(j)^{t_{j,k}})^{\Delta_{j,\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(0)\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}\prod_{j\in\omega_k^*\cup\Omega_k^*}H_2(j)^{r_{j,k}}\right)$$

$$= g_2^{z+\sum_{k\in\Psi}(H_1(\lambda_{\varsigma,k})-H_1(\lambda_{\varsigma,\bar{I}}))a_{k,0}\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}(g_1^{\theta_\varsigma}g^{\eta_\varsigma})^{v}g_2^{H_1(\lambda_{\varsigma,\bar{I}})\cdot\sum_{k\in\Psi\cup\bar{I}}a_{k,0}\cdot\Delta_{k,\Psi\cup\bar{I}}(0)};$$

$$\prod_{k\in\Psi\cup\bar{I}}\left(\prod_{j\in\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(H_2(j)^{t_{j,k}})^{\Delta_{j,\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(0)\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}\prod_{j\in\omega_k^*\cup\Omega_k^*}H_2(j)^{r_{j,k}}\right)$$

$$= g_2^{z+\sum_{k\in\Psi\cup\bar{I}}H_1(\lambda_{\varsigma,k})\cdot a_{k,0}\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}(g_1^{\theta_\varsigma}g^{\eta_\varsigma})^{v}\prod_{k\in\Psi\cup\bar{I}}\left(\prod_{j\in\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(H_2(j)^{t_{j,k}})^{\Delta_{j,\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(0)\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}\prod_{j\in\omega_k^*\cup\Omega_k^*}H_2(j)^{r_{j,k}}\right)$$

$$= g_2^z H_3(m)^v\prod_{k\in\Psi\cup\bar{I}}\left(\prod_{j\in\omega'_{ID_\varsigma,k}\cup\Omega_k^*}S_{1,j,k}^{\Delta_{j,\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(0)\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}\prod_{j\in\omega_k^*\cup\Omega_k^*}H_2(j)^{r_{j,k}}\right),$$

$$\sigma_2 = g_2^{z-(H_1(\lambda_\varsigma)+1)\cdot\sum_{k\in\Psi}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)}\prod_{k\in\Psi}(g_2^{H_1(\lambda_i)a_{k,0}+a_{k,0}})^{\Delta_{k,\Psi\cup\bar{I}}(0)} = g_2^z(P_{\bar{I}}S_{2,\bar{I}})^{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}\prod_{k\in\Psi}(P_kS_{2,k})^{\Delta_{k,\Psi\cup\bar{I}}(0)} = g_2^z\prod_{k\in\Psi\cup\bar{I}}(P_kS_{2,k})^{\Delta_{k,\Psi\cup\bar{I}}(0)},$$

$$\sigma_3 = g_2^{-\frac{H_1(\lambda_{\varsigma,\bar{I}})}{\theta_\varsigma}}g^{v'} = g^{-\frac{H_1(\lambda_{\varsigma,\bar{I}})}{\theta_\varsigma}\cdot b_0+v'} = g_2^v.$$

- 否则,C 停止仿真,将该事件记为 E_2.

3) 伪造阶段:攻击者 A 在挑战断言 $\{\Upsilon_{t_k,\omega_k^*}(\cdot)\}_{k\in\psi\cup\bar{I}}$ 和缺省属性集合 $\{\bar{\Omega}_k\}_{k\in\psi\cup\bar{I}}$ 的条件下,成功地伪造了消息 m_ς^* 的签名 $\sigma_\varsigma^*=\langle\sigma_{1,\varsigma}^*,\sigma_{2,\varsigma}^*,\sigma_{3,\varsigma}^*,\{\sigma_{4,j,k}^*\}_{k\in\Psi\cup\bar{I},j\in\omega_k^*\cup\bar{\Omega}_k}\rangle$. 如果 $H_3(m_\varsigma^*)=g^{\eta_\delta}$ 且 $\{\bar{\Omega}_k=\Omega_k^*\}_{k\in\psi\cup\bar{I}}$,则下列等式成立.

$$\frac{e(g,\sigma_{2,\varsigma}^*)e(g^{\eta_\delta},\sigma_{3,\varsigma}^*)\prod_{k\in\psi\cup\bar{I}}\prod_{j\in\omega_k^*\cup\Omega_k^*}e(g^{\beta_{k,j}^*},\sigma_{4,j,k}^*)}{e(g,\sigma_{1,\varsigma}^*)} = Z = e(g,g^{a_0\cdot b_0}).$$

因此,C 可以成功地解决 CDH 困难问题,其中, $g^{a_0\cdot b_0}=\frac{\sigma_{2,\varsigma}^*\cdot\sigma_{3,\varsigma}^{*\eta_\delta}\cdot\prod_{k\in\Psi\cup\bar{I}}\prod_{j\in\omega_k^*\cup\Omega_k^*}\sigma_{4,j,k}^{*\beta_{k,j}^*}}{\sigma_{1,\varsigma}^*}$.

下面分析 C 成功解决 CDH 困难问题的优势.

在伪造过程中要求 $H_3(m_\varsigma^*)=g^{\eta_\delta^*},\{\bar{\Omega}_k=\Omega_k^*\}_{k\in\psi\cup\bar{I}}$ 且 $H_2(j)$已知,因为$|\Omega_k|=d_k-1$,进行 H_2,H_3 预言仿真的次数分

别为 q_{H_2},q_{H_3},所以 C 成功解决 CDH 困难问题的优势为 $\varepsilon' \approx \dfrac{\varepsilon}{q_{H_2}q_{H_3}\prod\limits_{k\in\psi\cup\bar{I}}\binom{d_k-t_k}{d_k-1}}$. 证毕. □

定理 3(适应性选择消息和断言攻击下抗合谋攻击). 本文所提出的分布式无中心授权的属性基可变门限环签名方案在适应性选择消息和断言攻击下可以抵抗合谋攻击.

证明:假设存在攻击者 A 分别可以进行 $q_{H_1},q_{H_2},q_{H_3},q_k,q_s$ 次 $H_i(i=1,2,3)$预言仿真、密钥解析预言仿真和签名预言仿真.若该攻击者 A 能够在适应性选择消息和断言攻击的条件下,以一个不可忽略的优势ε在多项式时间内攻破本方案,则存在算法 C 可以在多项式时间内以不可忽略的优势ε'解决 CDH 困难问题,其中,

$$\varepsilon' \approx \frac{\varepsilon}{q_{H_2}q_{H_3}\prod\limits_{k\in\psi\cup\bar{I}}\binom{d_k-t_k}{d_k-1}}.$$

1) 系统建立

同定理 2 的系统建立过程.

2) 预言仿真阶段

同定理 2 的预言仿真阶段.

3) 挑战阶段

攻击者 A 在挑战断言 $\{\Upsilon_{t_k,\omega_k^*}(\cdot)\}_{k\in\psi\cup\bar{I}}$ 和缺省属性集合 $\{\bar{\Omega}_k\}_{k\in\psi\cup\bar{I}}$ 的条件下,挑战该方案的抗合谋攻击性.

A 首先随机选取用户 ID_1(属性集合为ω_1),ID_2(属性集合为ω_2),满足 $\Upsilon_{t_{\bar{I}},\omega_{\bar{I}}^*}(\omega_1)\neq 1,\Upsilon_{t_{\bar{I}},\omega_{\bar{I}}^*}(\omega_2)\neq 1$,且存在属性集合 $\omega'_{1,\bar{I}}\subseteq\omega_{1,\bar{I}},\omega'_{2,\bar{I}}\subseteq\omega_{2,\bar{I}}$,满足 $\Upsilon_{t_{\bar{I}},\omega_{\bar{I}}^*}(\omega'_{1,\bar{I}}\cup\omega'_{2,\bar{I}})=1$;

然后,分别对 $(ID_1,AA_{\bar{I}}),(ID_2,AA_{\bar{I}})$ 进行 H_1 询问,得到 $H_1(\lambda_{1,\bar{I}}),H_1(\lambda_{2,\bar{I}})$ 的仿真结果 $\alpha_{1,\bar{I}}$ 和 $\alpha_{2,\bar{I}}$;

对 $(\omega'_{1,\bar{I}},ID_1),(\omega'_{2,\bar{I}},ID_2)$ 进行密钥解析询问得到密钥集合:

$$\{S^1_{1,j,\bar{I}}=H_2(j)^{t_{j,\bar{I}}}g_2^{\alpha_{1,\bar{I}}\cdot q_{\bar{I}}(j)},S^1_{2,\bar{I}}=g_1^{-x_{\bar{I}}}g_2^{\alpha_{1,\bar{I}}\cdot a_{\bar{I},0}+a_{\bar{I},0}},T_{j,\bar{I}}=g^{t_{j,\bar{I}}},P_{\bar{I}}=g_1^{x_{\bar{I}}}\}_{j\in\omega'_{1,\bar{I}}\cup\bar{\Omega}_{1,\bar{I}}},$$

$$\{S^2_{1,j,\bar{I}}=H_2(j)^{t_{j,\bar{I}}}g_2^{\alpha_{2,\bar{I}}\cdot q_{\bar{I}}(j)},S^2_{2,\bar{I}}=g_1^{-x_{\bar{I}}}g_2^{\alpha_{2,\bar{I}}\cdot a_{\bar{I},0}+a_{\bar{I},0}},T_{j,\bar{I}}=g^{t_{j,\bar{I}}},P_{\bar{I}}=g_1^{x_{\bar{I}}}\}_{j\in\omega'_{2,\bar{I}}\cup\bar{\Omega}_{2,\bar{I}}};$$

其次,为用户 ID_2 生成新的属性密钥集合:

$$\left\{S^{2'}_{1,j,\bar{I}}=S^2_{1,j,\bar{I}}{}^{\frac{\alpha_{1,\bar{I}}}{\alpha_{2,\bar{I}}}}=H_2(j)^{t_{j,\bar{I}}\cdot\frac{\alpha_{1,\bar{I}}}{\alpha_{2,\bar{I}}}}g_2^{\alpha_{1,\bar{I}}\cdot q_{\bar{I}}(j)},S^{2'}_{2,\bar{I}}=S^1_{2,\bar{I}}=g_1^{-x_{\bar{I}}}g_2^{\alpha_{1,\bar{I}}\cdot a_{\bar{I},0}+a_{\bar{I},0}},T'_{j,\bar{I}}=T^{\frac{\alpha_{1,\bar{I}}}{\alpha_{2,\bar{I}}}}_{j,\bar{I}}=g^{t_{j,\bar{I}}\cdot\frac{\alpha_{1,\bar{I}}}{\alpha_{2,\bar{I}}}},P_{\bar{I}}=g_1^{x_{\bar{I}}}\right\}_{j\in\omega'_{2,\bar{I}}\cup\bar{\Omega}_{2,\bar{I}}};$$

最终,A 可以获得签名密钥集合 $\{S^1_{1,j,k}\cup S^{2'}_{1,j,\bar{I}},S^1_{2,k},T_{j,k}\cup T'_{j,\bar{I}},P_k\}_{j\in\omega'_{1,k}\cup\omega'_{2,\bar{I}}\cup\bar{\Omega}_k,k\in\psi\cup\bar{I}}$.

4) 伪造阶段

攻击者 A 在挑战断言 $\{\Upsilon_{t_k,\omega_k^*}(\cdot)\}_{k\in\psi\cup\bar{I}}$ 和缺省属性集合 $\{\bar{\Omega}_k\}_{k\in\psi\cup\bar{I}}$ 的条件下,成功地伪造消息 m^*的签名$\sigma^*=\langle\sigma_1^*,\sigma_2^*,\sigma_3^*,\{\sigma_{4,j,k}^*\}_{j\in\omega_k^*\cup\bar{\Omega}_k,k\in\psi\cup\bar{I}}\rangle$,并将$\sigma^*$发送给 C 进行验证.如果 $H_3(m^*)=g^{\eta_\delta}$ 且 $\{\bar{\Omega}_k=\Omega_k^*\}_{k\in\psi\cup\bar{I}}$,则下列等式成立:

$$\frac{e(g,\sigma_2^*)e(g^{\eta_\delta},\sigma_3^*)\prod\limits_{k\in\psi\cup\bar{I}}\prod\limits_{j\in\omega_k^*\cup\Omega_k^*}e(g^{\beta_{k,j}},\sigma_{4,j,k}^*)}{e(g,\sigma_1^*)}=Z=e(g,g^{a_0\cdot b_0}).$$

因此,C 可以成功地解决 CDH 困难问题,其中, $g^{a_0\cdot b_0}=\dfrac{\sigma_2^*\cdot\sigma_3^{*\eta_\delta}\cdot\prod\limits_{k\in\psi\cup\bar{I}}\prod\limits_{\xi\in\omega_k^*\cup\Omega_k^*}\sigma_{4,j,k}^{*\beta_{k,j}}}{\sigma_1^*}$.

正确性验证如下:

$$\frac{e(g,\sigma_2^*)e(H_3(m^*),\sigma_3^*)\prod_{k\in\psi\cup\bar{I}}\prod_{j\in\omega_k^*\cup\Omega_k^*}e(H_2(j),\sigma_{4,j,k}^*)}{e(g,\sigma_1^*)}=$$

$$\frac{e\left(g,\prod_{k\in\psi\cup\bar{I}}(P_kS_{2,k}^1)^{\Delta_{k,\psi\cup\bar{I}}(0)}\right)\prod_{k\in\psi\cup\bar{I}}\left(\prod_{j\in\omega_{1,k}'\cup\Omega_k^*}e\left(H_2(j),T_{j,k}^{\Delta_{j,\omega_{1,k}'\cup\omega_{2,\bar{I}}'\cup\Omega_k^*(0)\cdot\Delta_{k,\psi\cup\bar{I}}(0)}}\right)\prod_{j\in\omega_{2,\bar{I}}'}e\left(H_2(j),T_{j,\bar{I}}'^{\Delta_{j,\omega_{1,\bar{I}}'\cup\omega_{2,\bar{I}}'\cup\Omega_{\bar{I}}^*(0)\cdot\Delta_{\bar{I},\psi\cup\bar{I}}(0)}}\right)\prod_{j\in\omega_k^*\cup\Omega_k^*}e(H_2(j),g^{r_{k,j}})\right)}{e\left(g,\prod_{k\in\psi\cup\bar{I}}\left(\prod_{j\in\omega_{1,k}'\cup\Omega_k^*}S_{1,j,k}^{1\ \Delta_{j,\omega_{1,k}'\cup\omega_{2,\bar{I}}'\cup\Omega_k^*(0)\cdot\Delta_{k,\psi\cup\bar{I}}(0)}}\prod_{j\in\omega_{2,\bar{I}}'}S_{1,j,\bar{I}}^{2'\ \Delta_{j,\omega_{1,\bar{I}}'\cup\omega_{2,\bar{I}}'\cup\Omega_{\bar{I}}^*(0)\cdot\Delta_{\bar{I},\psi\cup\bar{I}}(0)}}\prod_{j\in\omega_k^*\cup\Omega_k^*}H_2(j)^{r_{k,j}}\right)\right)}=$$

$$\frac{e\left(g,\prod_{k\in\psi\cup\bar{I}}(g_2^{\alpha_{1,k}\cdot a_{k,0}+a_{k,0}})^{\Delta_{k,\psi\cup\bar{I}}(0)}\right)\prod_{k\in\psi\cup\bar{I}}\left(\prod_{j\in\omega_{1,k}'\cup\Omega_k^*}e\left(H_2(j),g^{t_{j,k}\cdot\Delta_{j,\omega_{1,k}'\cup\omega_{2,\bar{I}}'\cup\Omega_k^*(0)\cdot\Delta_{k,\psi\cup\bar{I}}(0)}}\right)\right)\prod_{j\in\omega_{2,\bar{I}}'}e\left(H_2(j),g^{t_{j,k}\cdot\frac{\alpha_{1,\bar{I}}}{\alpha_{2,\bar{I}}}\Delta_{j,\omega_{1,\bar{I}}'\cup\omega_{2,\bar{I}}'\cup\Omega_{\bar{I}}^*(0)\cdot\Delta_{\bar{I},\psi\cup\bar{I}}(0)}}\right)}{e\left(g,\prod_{k\in\psi\cup\bar{I}}\left(\prod_{j\in\omega_{1,k}'\cup\Omega_k^*}(H_2(j)^{t_{j,k}}g_2^{\alpha_{1,k}\cdot q_k(j)})^{\Delta_{j,\omega_{1,k}'\cup\omega_{2,\bar{I}}'\cup\Omega_k^*(0)\cdot\Delta_{k,\psi\cup\bar{I}}(0)}}\prod_{j\in\omega_{2,\bar{I}}'}\left(H_2(j)^{t_{j,k}\cdot\frac{\alpha_{1,\bar{I}}}{\alpha_{2,\bar{I}}}}g_2^{\alpha_{1,\bar{I}}\cdot q_{\bar{I}}(j)}\right)^{\Delta_{j,\omega_{1,\bar{I}}'\cup\omega_{2,\bar{I}}'\cup\Omega_{\bar{I}}^*(0)\cdot\Delta_{\bar{I},\psi\cup\bar{I}}(0)}}\right)\right)}=$$

$$\frac{e\left(g,g_2^{a_0}\prod_{k\in\psi\cup\bar{I}}g_2^{\alpha_{1,\bar{I}}\cdot a_{k,0}\cdot\Delta_{k,\psi\cup\bar{I}}(0)}\right)\prod_{k\in\psi\cup\bar{I}}\left(\prod_{j\in\omega_{1,k}'\cup\Omega_k^*}e\left(H_2(j),g^{t_{j,k}\cdot\Delta_{j,\omega_{1,k}'\cup\omega_{2,\bar{I}}'\cup\Omega_k^*(0)\cdot\Delta_{k,\psi\cup\bar{I}}(0)}}\right)\right)\prod_{j\in\omega_{2,\bar{I}}'}e\left(H_2(j),g^{t_{j,k}\cdot\frac{\alpha_{1,\bar{I}}}{\alpha_{2,\bar{I}}}\cdot\Delta_{j,\omega_{1,\bar{I}}'\cup\omega_{2,\bar{I}}'\cup\Omega_{\bar{I}}^*(0)\cdot\Delta_{\bar{I},\psi\cup\bar{I}}(0)}}\right)}{e\left(g,\prod_{k\in\psi\cup\bar{I}}\left(g_2^{\alpha_{1,\bar{I}}\cdot a_{k,0}\cdot\Delta_{k,\psi\cup\bar{I}}(0)}()\prod_{j\in\omega_{1,k}'\cup\Omega_k^*}H_2(j)^{t_{j,k}\cdot\Delta_{j,\omega_{1,k}'\cup\omega_{2,\bar{I}}'\cup\Omega_k^*(0)\cdot\Delta_{k,\psi\cup\bar{I}}(0)}}\right)\prod_{j\in\omega_{2,\bar{I}}'}H_2(j)^{t_{j,k}\cdot\frac{\alpha_{1,\bar{I}}}{\alpha_{2,\bar{I}}}\cdot\Delta_{j,\omega_{1,\bar{I}}'\cup\omega_{2,\bar{I}}'\cup\Omega_{\bar{I}}^*(0)\cdot\Delta_{\bar{I},\psi\cup\bar{I}}(0)}}\right)}=$$

$e(g,g_2^{a_0})=e(g,g^{a_0\cdot b_0})$.

下面分析 C 成功解决 CDH 困难问题的优势.

在合谋攻击过程中,要求 $H_3(m^*)=g^{\eta_\delta},\{\bar{\Omega}_k=\Omega_k^*\}_{k\in\psi\cup\bar{I}}$,$H_2(j)$ $H_2(j)$,由于$|\Omega_k|=d_k-1$,进行 H_2,H_3 预言仿真的次数分别为 q_{H_2},q_{H_3},因此,C 成功解决 CDH 困难问题的优势为 $\varepsilon'\approx\dfrac{\varepsilon}{q_{H_2}q_{H_3}\prod_{k\in\psi\cup\bar{I}}\binom{d_k-t_k}{d_k-1}}$. 证毕. □

5 效率比较与性能分析

本节将从效率和性能两方面与现有方案进行对比,进而得出本方案的综合评估结果.评估过程所用符号及其定义见表 1,效率比较见表 2,性能比较见表 3.

Table 1 Definition of related symbols

表 1 相关符号定义

符号	定义	符号	定义
A	签名者拥有属性集合	d	预定义数值
B	断言声明属性集合	t	断言中声明的门限值
D	系统缺省属性集	T_p	双线性对运算所需时间复杂度
T	签名所需 AA_k 组成的集合	T_e	倍点运算所需时间复杂度
A	签名者拥有属性集合	–	–

Table 2 Efficiency comparison of ABRS schemes

表 2 ABRS 方案效率比较

方案	密钥长度/bit	签名长度/bit	签名计算量	验证计算量
文献[13]中方案	$2(\|A\|+d-1)\|G_1\|$	$3d\|G_1\|$	$5dT_e$	dT_e+3dT_p
文献[14]中方案	$2\|A\|\|G_1\|$	$3\|A\|\|G_1\|$	$(2\|A\|+1)T_e$	$3dT_p+(d+1)T_e$
文献[16]中方案	$(\|A\|+d+1)\|G_1\|$	$2\|G_1\|$	$4T_e$	$3T_p+1T_e$
文献[17]中方案	$2(\|A\|+d-1)\|G_1\|$	$(\|B\|+d-t+2)\|G_1\|$	$(2\|B\|+4d-2t+2)T_e$	$(\|B\|+d-t+2)T_p$
文献[18]中方案	$(\|A\|+d)\|G_1\|$	$3\|G_1\|$	$5T_e$	$4T_p+1T_e$
文献[19]中方案	$(\|A\|+d-1)(\|B\|+d-t)\|G_1\|$	$3\|G_1\|$	$(2d+4)T_e$	$3T_p$
文献[20]中方案	$(\|A\|+d)\|G_1\|$	$(\|B\|+d-t+2)\|G_1\|$	$(\|B\|+2d-2t+2)T_e$	$(\|B\|+d-t+2)T_p+(\|B\|+d-t)T_e$
文献[21]中方案	$(2\|A\|+\|T\|^2)\|G_1\|$	$(\|B\|+2)\|G_1\|$	$(2\|B\|+2d+2)T_e$	$(\|B\|+2)T_p$
本文方案	$(\|A\|+d-1+\|T\|)\|G_1\|$	$(\|B\|+d-t+3)\|G_1\|$	$(2\|B\|+4d-2t+4+\|T\|)T_e$	$(\|B\|+d-t+3)T_p$

Table 3 Performance comparison of ABRS schemes

表 3 ABRS 方案性能比较

方案	不可伪造性	匿名性	抗合谋攻击性	签名门限可变	属性密钥托管问题	批验证	安全模型
文献[13]中方案	CDH	弱匿名性	×	√	存在	×	标准模型
文献[14]中方案	CDH	强匿名性	×	×	存在	×	标准模型
文献[16]中方案	SDH	弱匿名性	×	×	存在	×	标准模型
文献[17]中方案	CDH	强匿名性	×	√	存在	×	标准模型#
文献[18]中方案	CDH	弱匿名性	×	×	存在	×	标准模型
文献[19]中方案	q-DHE	强匿名性	×	√	存在	×	标准模型
文献[20]中方案	CDH	计算匿名性	√	√	存在	×	ROM
文献[21]中方案	CDH**	强匿名性	√#	×	不存在	√	ROM
本文方案	CDH	强匿名性	√	√	不存在	√	ROM

注:×代表不支持该性能,√代表支持该性能,**代表形式化证明不完整,#代表未给出形式化证明.

综合表 2 和表 3 的结果可知,虽然文献[20,21]中的方案和本文方案的形式化安全证明均基于随机预言机模型,但是目前仅有这 3 个方案可以抵抗合谋攻击,因此下面主要针对这 3 个方案进行分析.当$|T|=1$时,即本文所提出的方案与文献[20]中的方案均使用单属性授权机构为相应属性分发密钥,此时,本方案密钥长度与文献[20]中的方案相等,签名长度仅比文献[20]中的方案多 $1|G_1|$bit,虽然就签名效率而言本方案不占优势,但是由于本文提出了一种高效地批验证方法,因此验证效率很高,且即便仅对单个签名进行验证,本方案的计算量也比文献[20]中的方案少$(|B|+d-t)T_e-1T_p$;同时,本方案匿名性明显优于文献[20]中的方案,且当$|T|\neq 1$ 时,本方案可以解决文献[20]中的方案存在的属性密钥托管问题.

若不考虑动态门限的实现,本方案签名长度和验证计算量与文献[21]中的方案相差不大,比文献[21]中的方案分别多 $1|G_1|$bit 和 $1T_p$,虽然签名计算量比文献[21]中的方案高$(2+|T|)T_e$,但是文献[21]中的方案引入了密钥匿名分发协议,因此就密钥长度而言,比本方案长$(|A|-|T|+|T|^2)|G_1|$bit,导致其 AA 与用户之间的通信代价很大.此外,该方案只能在单属性授权机构,即存在的属性密钥托管问题的安全模型下,被证明具备匿名性和不可伪造性,并未给出抗合谋攻击的形式化安全证明.而本文方案可以在克服密钥长度过长这一前提下,在假设存在 $l-1$ 个不可信授权属性机构的安全模型下,被证明同时具备无条件强匿名性、不可伪造性和抗合谋攻击性.

上述分析表明,综合考虑安全性和效率两方面性能,本文方案较现有方案具有更大优势.

6 总 结

本文针对现有基于属性的门限环签名方案无法同时具备无条件强匿名性和抗合谋攻击性,并且存在属性密钥托管、验证效率低、签名门限固定等问题,通过采用分布式密钥生成协议以及在属性密钥和签名中分别嵌入用户身份标识和用户身份模糊因子的方式,提出了一个分布式无中心授权的属性基可变门限环签名方案.该方案同时具备无条件强匿名性和抗合谋攻击性.在假设存在 $l-1$ 个不可信属性授权机构的前提下,该方案被证明在适应性选择消息和断言攻击下是存在性不可伪造的,并且能够抵抗由拥有互补属性集合的恶意用户发动合谋攻击.另外,还提出了一种适用于本方案的批验证算法,有效地提高了验证效率.

References:

[1] Sahai A, Waters B. Fuzzy identity-based encryption. In: Proc. of the 24th Annual Int'l Conf. on Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2005. 457−473. [doi: 10.1007/11426639_27]

[2] Attrapadung N, Libert B, De Panafieu E. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In: Proc. of the 14th Int'l Conf. on Practice and Theory in Public Key Cryptography (PKC 2011). Berlin: Springer-Verlag, 2011. 90−108. [doi: 10.1007/978-3-642-19379-8_6]

[3] Han F, Qin J, Zhao H, Hu J. A general transformation from KP-ABE to searchable encryption. Future Generation Computing Systems, 2014,30(1):107−115. [doi: 10.1016/j.future.2013.09.013]

[4] Rouselakis Y, Waters B. Practical constructions and new proof methods for large universe attribute-based encryption. In: Proc. of the 2013 ACM SIGSAC Conf. on Computer and Communications Security. Berlin: ACM Press, 2013. 463−474. [doi: 10.1145/2508859.2516672]

[5] Bethencourt J, Sahai A, Waters B. Ciphertext-Policy attribute-based encryption. In: Proc. of the 2007 IEEE Symp. on Security and Privacy (SP 2007). Berkeley: IEEE Press, 2007. 321−334. [doi: 10.1109/SP.2007.11]

[6] Goyal V, Jain A, *et al*. Bounded ciphertext policy attribute based encryption. In: Proc. of the 35th Int'l Colloquium on Automata, Languages and Programming. Berlin: Springer-Verlag, 2008. 579−591. [doi: 10.1007/978-3-540-70583-3_47]

[7] Hong H, Sun Z, Liu X. A key-insulated CP-ABE with key exposure accountability for secure data sharing in the cloud. KSII Trans. on Internet and Information Systems, 2016,10(5):2394−2406. [doi: 10.3837/tiis.2016.05.024]

[8] Burnett A, Duffy A, Dowling T. A biometric identity based signature scheme. 2004. http://eprint.iacr.org/2004/176

[9] Guo SQ, Zeng YP. Attribute-Based signature scheme. In: Proc. of the 2nd Int'l Conf. on Information Security and Assurance. Busan. IEEE Press, 2008. 509−511. [doi: 10.1109/ISA.2008.111]

[10] Maji H, Prabhakaran M, Rosulek M. Attribute-Based signatures: Achieving attribute privacy and collusion-resistance. 2008. http://eprint.iacr.org/2008/328

[11] Rivest R, Shamir A, Tauman Y. How to leak a secret. In: Proc. of the Advances in Cryptology (ASIACRYPT 2001). Gold Coast: Springer-Verlag, 2001. 552−565. [doi: 10.1007/3-540-45682-1_32]

[12] Li J, Kim K. Attribute-Based ring signatures. 2008. http://eprint.iacr.org/2008/394

[13] Li J, Kim K. Hidden attribute-based signatures without anonymity revocation. Information Sciences, 2010,180(9):1681−1689. [doi: http://dx.doi.org/10.1016/j.ins.2010.01.008]

[14] Shahandashti SF, Safavi-Naini R. Threshold attribute-based signatures and their application to anonymous credential systems. In: Proc. of the Cryptology-Africacrypt 2009, Vol.5580. Berlin: Springer-Verlag, 2009. 198−216. [doi: 10.1007/978-3-642-02384-2_13]

[15] Wang WQ, Chen SZ. An efficient attribute-based ring signature scheme. In: Proc. of the Int'l Forum on Computer Science-Technology and Applications, Vol.1. Chongqing: IEEE Press, 2009. 147−150. [doi: 10.1109/IFCSTA.2009.43]

[16] Toluee R, Asaar MR, Salmasizadeh M. Attribute-Based ring signatures: Security analysis and a new construction. In: Proc. of the 10th Int'l ISC Conf. on Information Security and Cryptology (ISCISC). IEEE Press, 2014. 1−6. [doi: 10.1109/ISCISC.2013.6767342]

[17] Li J, Au MH, Susilo W, *et al*. Attribute-Based signatures and its applications. In: Proc. of the 5th ACM Symp. on Information, Computer and Communications Security (ASIACCS 2010). Beijing: ACM Press, 2010. 978−987.

[18] Wang WQ, Chen SZ. Attribute-Based ring signature scheme with constant-size signature. IET Information Security, 2010,4(2):104−110. [doi: 10.1049/iet-ifs.2009.0189]

[19] Ge AJ, Ma CG, Zhang ZF. Attribute-Based signature scheme with constant size signature in the standard model. Journal of IET Information Security, 2012,6(2):47−54. [doi: 10.1049/iet-ifs.2011.0094]

[20] Chen Z, Zhang WF, Wang XM. Attribute-Based alterable threshold ring signature scheme with conspiracy attack immunity. Journal on Communications, 2015,36(12):212−222 (in Chinese with English abstract).

[21] Li J, Chen XF, Huang XY. New attribute-based authentication and its application in anonymous cloud access service. Int'l Journal of Web and Grid Services, 2015,11(1):125−141. [doi: http://dx.doi.org/10.1504/IJWGS.2015.067161]

[22] Chase M. Multi-Authority attribute based encryption. In: Proc. of the 4th Theory of Cryptography Conf. Berlin: Springer-Verlag, 2007. 515−534. [doi: 10.1007/978-3-540-70936-7_28]

[23] Chase M, Chow S. Improving privacy and security in multi-authority attribute-based encryption, In: Proc. of the 16th ACM Conf. on Computer and Communications Security. Chicago: ACM Press, 2009. 121−130. [doi: 10.1145/1653662.1653678]

[24] Lin H, Cao ZF, Liang XH, *et al*. Secure threshold multi-authority attribute based encryption without a central authority. Journal of Information Sciences, 2010,180(13):2618−2632. [doi: http://doi.org/10.1016/j.ins.2010.03.004]

[25] Sun CX, Ma WP, Chen HF. Provable secure multi-authority attribute-based signature without a central authority. Journal of University of Electronic Science and Technology of China, 2012,41(4):552−556 (in Chinese with English abstract).

[26] Ferrara A, Green M, Hohenberger S, Pedersen M. Practical short signature batch verification. 2008. http://eprint.iacr.org/2008/015

附中文参考文献:

[20] 陈桢,张文芳,王小敏.基于属性的抗合谋攻击可变门限环签名方案.通信学报,2015,36(12):212−222.

[25] 孙昌霞,马文平,陈和风.可证明安全的无中心授权的多授权属性签名.电子科技大学学报,2012,41(4):552−556.

刘旭东(1990－),男,内蒙古呼和浩特人,硕士,主要研究领域为基于属性密码的密码体制,环签名.

张文芳(1978－),女,博士,副教授,主要研究领域为密码学,信息安全,分布式系统认证,密钥协商.

王小敏(1974－),男,博士,教授,博士生导师,主要研究领域为信息安全,轨道交通信息系统安全.