

前向安全的单向门限代理重签名

杨小东,王彩芬

(西北师范大学 数学与信息科学学院,兰州 730070)

(y200888@163.com)

摘要:为了降低重签名密钥被泄露所带来的损失,提出了一个前向安全的单向门限代理重签名(FSTPRS)方案,使得重签名密钥随时间段单向进化,而验证签名的公钥在整个有效时间段内保持不变,以保证即使重签名密钥被泄露,攻击者不能恢复在此之前的重签名密钥,也无法伪造在此之前的任何时间段的签名。在标准模型下证明了该方案的安全性,分析表明在计算性 Diffie-Hellman 假设下该方案是健壮的,并且能抵抗适应性选择消息攻击。

关键词:单向门限;代理重签名;前向安全;可证安全;标准模型

中图分类号: TP309.7 **文献标志码:** A

Forward-secure unidirectional threshold proxy re-signature

YANG Xiao-dong, WANG Cai-fen

(College of Mathematics and Information Science, Northwest Normal University, Lanzhou Gansu 730070, China)

Abstract: To reduce the loss caused by the leakage of the re-signature key, a scheme of forward-secure unidirectional threshold proxy re-signature (FSTPRS) was proposed in this paper. The re-signature key was updated in each period by one-way function while the public key remains fixed. As a result, even if the current re-signature key was exposed, the adversary could not recover the re-signature key before the current time period or forge any signatures pertaining to the past. The security of scheme was proved in the standard model. The analysis result shows that it is robust and secure against the existing forgery under the adaptive chosen message attack, under the condition of the computational Diffie-Hellman.

Key words: unidirectional threshold; proxy re-signature; forward security; provably secure; standard model

0 引言

在代理签名中,委托者必须高度信任代理者。为了分散代理者的签名权利,Blaze 等人^[1]提出了代理重签名(Proxy Re-Signature, PRS)的概念。在代理重签名中,一个拥有重签名密钥的半可信代理者可将受托者的签名转换为委托者对同一消息的签名(也称重签名),但这个代理者不能自己单独生成受托者或委托者的任何签名。代理重签名在简化证书管理、管理群签名、提供遍历的路径证明、构造审查系统和数字版权管理系统等方面有广泛的应用前景^[2]。一旦重签名密钥被泄露,攻击者可用重签名密钥将受托者的任何签名转换为委托者的签名。门限代理重签名^[3]可将重签名密钥以门限方式分散给多个代理者管理,不仅能降低破译重签名密钥成功的概率,还可防止代理者滥用代理签名权,但门限代理重签名的研究才刚刚起步。Canetti 等人^[4]发现,一个在随机预言模型下可证安全的密码系统,当使用一个真正哈希函数实现时,却是完全不安全的。所以,研究标准模型下可证安全的门限代理重签名方案更具有实际意义。

单向门限代理重签名比双向门限代理重签名更具有优越性,因为后者可以用两个不同的前者来构成,而前者不能由后者构成。本文提出了一个在标准模型下可证安全的前向安全的单向门限代理重签名(forward-secure unidirectional threshold proxy re-signature, FSTPRS)方案。重签名密钥随着时间段的推移进行阶段性地更新,而相应的公钥在整个有效时间段内

保持不变。将重签名的有效时间分为 T 个时间段,分别记为 $1, 2, \dots, T$ 。即使第 k 时间段的重签名密钥 $rk_{A \rightarrow B}^k$ 被泄露,攻击者无法推出第 $k-1$ 时间段的重签名密钥 $rk_{A \rightarrow B}^{k-1}$,也无法伪造第 k 时间段之前的签名。前向安全的门限代理重签名为重签名密钥提供了强大的保护,使重签名密钥被泄露所造成的损失降到最小。

1 预备知识

1.1 双线性对

设 G_1 和 G_2 是两个阶为素数 p 的循环群, g 是 G_1 的生成元,定义两个群 G_1 和 G_2 上的双线性映射 $e: G_1 \times G_1 \rightarrow G_2$, 且满足以下性质。

- 1) 双线性性。对任意的 $a, b \in Z_p$, 有 $e(g^a, g^b) = e(g, g)^{ab}$ 。
- 2) 非退化性。 $e(g, g)$ 不等于 G_2 的单位元。
- 3) 可计算性。对任意的 $g_1, g_2 \in G_1$, 存在一个高效的算法计算 $e(g_1, g_2)$ 。

可利用超奇异椭圆曲线上的 Weil 配对或 Tate 配对来构造双线性对^[2]。

1.2 计算性 Diffie-Hellman 假设

定义 1 计算性 Diffie-Hellman (Computational Diffie-Hellman, CDH) 问题。设 G_1 是阶为素数 p 的循环群, g 是 G_1 的生成元, 已知 $g, g^a, g^b \in G_1$, 其中 a, b 是从 Z_p 中随机选取的, 计算 g^{ab} 。

定义 2 计算性 Diffie-Hellman 假设。如果没有一个概率

多项式时间算法在时间 t 内以至少 ε 的概率解决群 G_1 上的 CDH 问题, 则称群 G_1 上的 (t, ε) -CDH 假设成立。

1.3 双线性 Diffie-Hellman 假设

定义 3 双线性 Diffie-Hellman (Bilinear Diffie-Hellman, BDH) 问题。设 G_1 和 G_2 是两个阶为素数 p 的循环群, g 是 G_1 的生成元, 已知 (g, g^a, g^b, g^c) , 计算 $e(g, g)^{abc} \in G_2$, 其中 a, b, c 是从 Z_p 中随机选取的。

定义 4 双线性 Diffie-Hellman 假设。如果没有一个概率多项式时间算法在时间 t 内以至少 ε 的概率解决双线性 Diffie-Hellman 问题, 则称 BDH 假设成立。

1.4 前向安全的单向门限代理重签名方案及其安全性

前向安全的单向门限代理重签名体制涉及到 4 方: 一个受托者、一个委托者、一个可信第三方 (Trusted Third Party, TTP) 和 n 个半可信的代理者组成的签名者集合 $P = \{P_1, \dots, P_n\}$ 。

定义 5 前向安全的单向门限代理重签名。一个 (t, n) 前向安全的单向门限代理重签名方案 $FSTPRS = (\text{Setup}, \text{RekeyUpd}, \text{Sign}, \text{ShareResign}, \text{Combine}, \text{Verify})$ 由以下 6 个算法组成。

1) Setup 是系统参数生成算法。输入一个安全参数 1^κ , 输出系统参数 $params$ 和公私钥对 (pk, sk) 。

2) RekeyUpd 是门限重签名密钥更新算法。输入一个受托者的公私钥对 (pk_A, sk_A) , 一个委托者的公私钥对 (pk_B, sk_B) 和一个时间段参数 $k-1$, 输出第 k 时间段的重签名密钥 $rk_{A \rightarrow B}^k$ 。代理者 P_i 在第 k 时间段的重签名子密钥记为 $rk_{A \rightarrow B}^{k,i}$, 同时产生相应的验证公钥 $vk_{k,i}$ 检验 $rk_{A \rightarrow B}^{k,i}$ 的合法性。

3) Sign 是签名生成算法。输入一个消息 m 和一个私钥 sk , 输出一个消息 m 的签名 σ 。可用对应的公钥 pk 来验证签名 σ 的合法性。

4) ShareResign 是部分重签名生成算法。输入一个时间段参数 k , 一个重签名子密钥 $rk_{A \rightarrow B}^{k,i}$, 一个消息 m , 一个公钥 pk_A 和一个签名 σ_A , 该算法首先验证 σ_A 的合法性, 如果 $\text{Verify}(k, pk_A, m, \sigma_A) = 1$, 输出一个对应于公钥 pk_B 的消息 m 的部分重签名 $\sigma_{B,i}$; 否则, 输出 \perp 。

5) Combine 是门限重签名生成算法。输入 t 个合法的消息 m 的部分重签名 $\sigma_{B,i_1}, \dots, \sigma_{B,i_t}$, 输出一个对应于公钥 pk_B 的消息 m 的门限重签名 σ_B 。

6) Verify 是签名验证算法。输入一个时间段参数 k , 一个消息 m , 一个公钥 pk 和一个签名 σ , 如果 σ 是第 k 时间段对应于公钥 pk 的消息 m 的合法签名, 输出 1; 否则, 输出 0。

攻击模型 攻击者在游戏开始前必须确定已被攻陷的代理者, 攻击游戏分三个阶段进行。首先是选择消息攻击阶段, 攻击者可以适应性地向挑战者进行用户的私钥询问、重签名密钥询问、签名询问和部分重签名询问, 挑战者响应攻击者所发起的各种询问请求, 并将询问结果返回给攻击者。这个阶段的安全性定义与一般的门限代理重签名的安全性定义基本相同。在这个阶段结束时, 攻击者可以选择继续留在该阶段或进入超门限阶段。其次是超门限阶段, 攻击者可以攻陷当前时间段的 t 个或更多的代理者。这就意味着攻击者可以获得当前时间段的重签名密钥。最后是伪造阶段, 攻击者输出一个伪造, 即一个消息/签名对。

攻击者决定从选择消息攻击阶段的时间段 T_a 转到超门限阶段的时间段 T_b , 如果攻击者能生成一个新消息 m 在第 T_a 时间段的合法签名, 或攻击者能伪造在时间段 T_b 以前任何时

间段的新消息的合法签名, 那么就说攻击者伪造成功。

攻击者在上面的游戏中的优势可以定义 $Adv_A = \Pr[A \text{ succeeds}]$, 这个概率完全取决于挑战者和攻击者之间的抛币概率。

定义 6 不可伪造性。如果没有一个攻击者在多项式时间内以不可忽略的优势赢得上述游戏, 则称一个前向安全的单向门限代理重签名方案 (FSTPRS) 在适应性选择消息攻击下能抵抗存在性伪造 (Unforgeability-Forward Secure Threshold Proxy Re-Signature-Chosen Message Attack, UF-FSTPRS-CMA)。

定义 7 强壮性。在一个 (t, n) 前向安全的单向门限代理重签名方案中, 如果一个恶意的攻击攻陷了 $t-1$ 个代理者, 门限代理重签名方案仍能输出一个正确的重签名, 则称 FSTPRS 方案具有强壮性。

如果一个前向安全的单向门限代理重签名是安全的, 则至少满足不可伪造性和强壮性。

2 前向安全的单向门限代理重签名方案

对于不同长度的用户公钥比特串和签名消息比特串, 使用两个抗碰撞的哈希函数分别将它们映射到方案所要求的长度, 即 $H_1: \{0, 1\}^* \rightarrow \{0, 1\}^{n_k}$ 和 $H_2: \{0, 1\}^* \rightarrow \{0, 1\}^{n_m}$ 。本文的方案由以下 7 个算法组成。

1) Setup。输入一个安全参数 1^κ , 选择两个阶为素数 p 的循环群 G_1 和 G_2 , g 和 h 是 G_1 的生成元, 定义一个双线性映射 $e: G_1 \times G_1 \rightarrow G_2$ 。选取 $u \in G_1$, 一个 n_m 维向量 $\vec{u} = (u_i)$ 和一个 n_k 维向量 $\vec{v} = (v_j)$, 其中 $u_i \in G_1, v_j \in G_1$ 。设 $q_1 = q_2 = 3 \pmod{4}$ 是两个大素数且 $N_q = q_1 q_2$ 。任选一个随机数 $x \in Z_p^*$ 为私钥 sk , 计算公钥 $pk = e(g, g)^x$ 。将重签名密钥的有效期分为 T 个时间段, 公开系统参数 $params = (G_1, G_2, p, e, g, h, u, \vec{u}, \vec{v}, N_q, T)$ 。

2) RekeyUpd。输入一个时间段参数 $k-1$, 一个受托者的公私钥对 $(pk_A, sk_A) = (e(g, g)^a, \alpha)$ 和一个委托者的公私钥对 $(pk_B, sk_B) = (e(g, g)^b, \beta)$, 如果 $k > T$ 或 $k < 0$, 输出 \perp ; 否则, 一个可信的分发者执行如下操作。

① 在 Z_p^* 中选取 $t-1$ 个随机数 $f_{k,1}, \dots, f_{k,t-1}$, 构造一个 $t-1$ 次多项式 $f_k(x) = \sum_{i=0}^{t-1} f_{k,i} x^i$, 使得 $f_{k,0} = \beta^{T+k} \pmod{N_q}$ 。

② 选取 $s_k \in_R Z_p^*$, 计算 $rk_{A \rightarrow B}^{k,i} = (rsk_{A \rightarrow B}^{k,i}, rp_{A \rightarrow B}^{k,i}) = (g^{f_k(i)-\alpha} J(pk_B)^{s_k}, g^{s_k}), i = 1, 2, \dots, n$, 其中 $J(pk_B) = v \prod_{i=1}^{n_k} v_i^{pk'_{B,i}}$ 和 $pk'_B = H_1(pk_B) = (pk'_{B,1}, \dots, pk'_{B,n_k}) \in \{0, 1\}^{n_k}$; 通过一个秘密渠道将重签名子密钥 $(i, rk_{A \rightarrow B}^{k,i})$ 分发给代理者 P_i 。

③ 广播验证公钥 $vk_{k,j} = e(g, g)^{f_k(j)}, j = 1, 2, \dots, n$ 。

④ 每个代理者 $P_i (1 \leq i \leq n)$ 通过式 (1) 验证 $rk_{A \rightarrow B}^{k,i} = (rsk_{A \rightarrow B}^{k,i}, rp_{A \rightarrow B}^{k,i})$ 的合法性:

$$e(rsk_{A \rightarrow B}^{k,i}, g) = vk_{k,i} \cdot pk_A^{-1} \cdot e(J(pk_B), rp_{A \rightarrow B}^{k,i}) \quad (1)$$

3) Sign。输入一个私钥 $sk = \alpha$ 和一个 n_m 比特的消息 $m = (m_1, \dots, m_{n_m}) \in \{0, 1\}^{n_m}$, 输出一个 m 的签名 $\sigma = (\sigma_1, \sigma_2) = (g^\alpha \varpi^{r_m}, g^{r_m})$, 这里 $r_m \in_R Z_p$ 且 $\varpi = u \prod_{i=1}^{n_m} (u_i)^{m_i}$ 。

4) ShareResign。输入一个时间段参数 k , 一个重签名子密钥 $rk_{A \rightarrow B}^{k,i} = (rsk_{A \rightarrow B}^{k,i}, rp_{A \rightarrow B}^{k,i})$, 一个 n_m 比特的消息 m , 一个公钥 pk_A 和一个签名 $\sigma_A = (\sigma_{A,1}, \sigma_{A,2})$, 如果 $\text{Verify}(0, pk_A, m,$

$\sigma_A) = 0$, 输出 \perp ; 否则, 每个代理者 P_i 选取一个随机数 $r_i \in_R Z_p$, 计算一个对应于公钥 pk_B 的消息 m 的部分重签名:

$$\sigma_{B,i} = (\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}) = (\sigma_{A,1} \cdot rsk_{A \rightarrow B}^{k,i} \cdot \varpi^{r_i}, rpk_{A \rightarrow B}^{k,i}, \sigma_{A,2} \cdot g^{r_i})$$

5) Combine. 假定 D 是一个指定的部分重签名的合成者 (可以是任意一个代理者)。 D 收到部分重签名 $\sigma_{B,i} = (\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3})$ 后, 通过式(2) 验证其合法性:

$$e(\sigma_{i,1}, g) = vk_{k,i} \cdot e(J(pk_B), \sigma_{i,2}) \cdot e(\varpi, \sigma_{i,3}) \quad (2)$$

这里 $vk_{k,i}$ 是代理者 P_i 在第 k 时间段的验证公钥。为了不失去一般性, 假定 D 收到 t 个合法的部分重签名 $\sigma_{B,i} = (\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}), i = 1, 2, \dots, t$, 则消息 m 的门限重签名:

$$\sigma_B = (\sigma_{B,1}, \sigma_{B,2}, \sigma_{B,3}) = \left(\prod_{i=1}^t (\sigma_{i,1})^{\lambda_{0,i}}, \prod_{i=1}^t (\sigma_{i,2})^{\lambda_{0,i}}, \prod_{i=1}^t (\sigma_{i,3})^{\lambda_{0,i}} \right)$$

其中 $\lambda_{0,i}$ 是 Lagrange 插值多项式的系数。

6) Verify(0, pk, m, σ)。输入一个 n_m 比特长的消息 m , 一个 n_k 比特长的公钥 pk 和一个签名 $\sigma = (\sigma_1, \sigma_2)$, 如果 $e(\sigma_1, g) = pk \cdot e(\sigma_2, \varpi)$, 输出 1; 否则, 输出 0。

7) Verify(k, pk, m, σ)。输入一个时间段参数 $k (0 < k \leq T)$, 一个 n_m 比特长的消息 m , 一个 n_k 比特长的公钥 pk 和一个签名 $\sigma = (\sigma_1, \sigma_2, \sigma_3)$, 如果 $e(\sigma_1, g) = pk^{2^{T+k}} e(J(pk), \sigma_2) e(\varpi, \sigma_3)$, 输出 1; 否则, 输出 0。

3 签名方案分析

3.1 正确性分析

本方案的正确性可以通过以下方程得到验证。

1) 第 k 时间段的重签名子密钥的正确性验证:

$$\begin{aligned} e(rsk_{A \rightarrow B}^{k,i}, g) &= e(g^{f_k(i)-\alpha} J(pk_B)^{s_k}, g) = e(g^{f_k(i)}, g) e(g^{-\alpha}, g) \\ &= e(g, g)^{f_k(i)} e(g, g)^{-\alpha} e(J(pk_B), g^{s_k}) \\ &= vk_{k,i} \cdot pk_A^{-1} \cdot e(J(pk_B), rpk_{A \rightarrow B}^{k,i}) \end{aligned}$$

2) 第 k 时间段的部分重签名的正确性验证:

$$\begin{aligned} e(\sigma_{i,1}, g) &= e(\sigma_{A,1} \cdot rsk_{A \rightarrow B}^{k,i} \cdot \varpi^{r_i}, g) = \\ &= e(g^{\alpha} \varpi^{r_m} g^{f_k(i)-\alpha} J(pk_B)^{s_k} \varpi^{r_i}, g) = \\ &= e(g^{f_k(i)} J(pk_B)^{s_k} \varpi^{r_m+r_i}, g) = \\ &= e(g^{f_k(i)}, g) e(J(pk_B)^{s_k}, g) e(\varpi^{r_m+r_i}, g) = \\ &= e(g, g)^{f_k(i)} e(J(pk_B), g^{s_k}) e(\varpi, g^{r_m+r_i}) = \\ &= vk_{k,i} \cdot e(J(pk_B), \sigma_{i,2}) \cdot e(\varpi, \sigma_{i,3}) \end{aligned}$$

3) 第 k 时间段的门限重签名的正确性验证:

$$\begin{aligned} \sigma_{B,2} &= \prod_{i=1}^t (\sigma_{i,2})^{\lambda_{0,i}} = \prod_{i=1}^t (rpk_{A \rightarrow B}^{k,i})^{\lambda_{0,i}} = \\ &= \prod_{i=1}^t (g^{s_k})^{\lambda_{0,i}} = g^{\sum_{i=1}^t s_k \lambda_{0,i}} \\ \sigma_{B,3} &= \prod_{i=1}^t (\sigma_{i,3})^{\lambda_{0,i}} = \prod_{i=1}^t (\sigma_{A,2} g^{r_i})^{\lambda_{0,i}} = \\ &= \prod_{i=1}^t (g^{r_m+r_i})^{\lambda_{0,i}} = g^{\sum_{i=1}^t (r_m+r_i) \lambda_{0,i}} \\ e(\sigma_{B,1}, g) &= e\left(\prod_{i=1}^t (\sigma_{i,1})^{\lambda_{0,i}}, g\right) = e\left(\prod_{i=1}^t (g^{f_k(i)} J(pk_B)^{s_k} \varpi^{r_m+r_i}), g\right) = \\ &= e\left(g^{\sum_{i=1}^t f_k(i) \lambda_{0,i}} J(pk_B)^{\sum_{i=1}^t s_k \lambda_{0,i}} \varpi^{\sum_{i=1}^t (r_m+r_i) \lambda_{0,i}}, g\right) = \\ &= e\left(g^{\sum_{i=1}^t f_k(i) \lambda_{0,i}}, g\right) e\left(J(pk_B)^{\sum_{i=1}^t s_k \lambda_{0,i}}, g\right) e\left(\varpi^{\sum_{i=1}^t (r_m+r_i) \lambda_{0,i}}, g\right) \end{aligned}$$

$$\begin{aligned} g) &= e\left(g^{\sum_{i=1}^t f_k(i) \lambda_{0,i}}, g\right) e\left(J(pk_B)^{\sum_{i=1}^t s_k \lambda_{0,i}}, g\right) e\left(\varpi^{\sum_{i=1}^t (r_m+r_i) \lambda_{0,i}}, g\right) = \\ &= pk_B^{2^{T+k}} e(J(pk_B), \sigma_{B,2}) e(\varpi, \sigma_{B,3}) \end{aligned}$$

3.2 安全性分析

定理 1 若 $n \geq 2t - 1$, 则本文所提的前向安全的单向门限代理重签名方案 FSTPRS 是强壮的。

证明 在重签名密钥更新算法 RekeyUpd 中, 选择一个 $t-1$ 次多项式 $f_k(x)$ 分发 $f_{k,0} = \beta^{2^{T+k}} \pmod{N_q}$ 。所以, 任何 $t-1$ 个或更少的代理者不能生成合法的 $f_{k,0}$, 只有 t 个或更多的代理者才能重构合法的 $f_{k,0}$ 。即使攻陷了 $t-1$ 个代理者, 攻击者仍然不能生成一个合法的 $f_{k,0}$ 。只要有 t 个合法的代理者就能生成合法的 $f_{k,0}$, 从而保证 RekeyUpd 算法的正确执行。

在门限重签名生成算法 Combine 中, 如果有恶意的代理者提供不正确的信息, 则通过相应的验证等式 $e(\sigma_{i,1}, g) = vk_{k,i} \cdot e(J(pk_B), \sigma_{i,2}) \cdot e(\varpi, \sigma_{i,3})$ 很容易确认出恶意代理者的公钥 $vk_{k,i}$ 。任何 $t-1$ 个或更少的代理者不能生成合法的门限重签名, 只有 t 个或更多的代理者共同参与才能生成合法的门限重签名。所以, 即使攻陷了 $t-1$ 个代理者, 攻击者仍然不能生成一个合法的门限重签名。至少需要 t 个诚实的代理者, 才能保证 Combine 算法的正确执行。

因此, 在允许 $t-1$ 个代理者被攻陷的情况下, 为了保证 RekeyUpd 算法和 Combine 算法的正确执行, 至少需要 t 个诚实的代理者, 所以当 $n \geq 2t - 1$ 时, 本文所提的 FSTPRS 方案是强壮的。

定理 2 本文所提的 FSTPRS 方案是前向安全的。

证明 本文所提方案的重签名密钥更新算法——RekeyUpd 所使用的单向函数是基于二次剩余问题的困难性^[4]。即对于某个时间段 $k, \beta^{2^{T+k}} = (\beta^{2^{T+(k-1)}})^2 \pmod{N_q}$ 。如果攻击者在第 k 时间段攻陷了 t 个代理者, 那么攻击者可以重构出第 k 时间段的重签名密钥 $rk_{A \rightarrow B}^{k,i} = \beta^{2^{T+k}} / \alpha \pmod{N_q}$, 但无法重构出第 k 时间段以前时间的重签名密钥, 也不能伪造时间段 $j (j < k)$ 的签名。在重签名的验证算法中添加了时间段参数 k , 这样可保证重签名的前向安全性。

Yang 等人定义了门限代理重签名的模拟性^[3,5], 并证明了门限代理重签名和代理重签名之间的关系。

定理 3 如果一个 (t, n) 门限代理重签名方案 (Threshold Proxy Re-Signature, TPRS) 是可模拟的, 并且关联于 TPRS 的代理重签名方案 (Proxy Re-Signature, PRS) 是不可伪造的, 则这个门限代理重签名方案也是不可伪造的^[3,5]。

门限代理重签名的安全性证明可采用“模拟”的证明方法, 而这个方法与“前向安全”属性是独立的, 所以为了证明前向安全的单向门限代理重签名方案的不可伪造性, 只需证明 FSTPRS 方案是可模拟的和 PRS 方案是不可伪造的。本文的单向 FSTPRS 方案是基于 Chow-Phan 代理重签名方案, 而 Chow-Phan 代理重签名方案已被证明在标准模型下在适应性选择消息攻击下是不可伪造的^[2]。因此, 只需证明 FSTPRS 方案是可模拟的。

命题 1 本文所提的 FSTPRS 方案是可模拟的。

证明 给定一个时间段参数 k , 一个受托者和一个委托者的公钥 (pk_A, pk_B) , 构造一个门限重签名密钥更新算法 RekeyUpd 的模拟器 $SIM_{RekeyUpd}$ 。知道已被攻陷代理者的验证公钥 $vk_{k,i}$ 和重签名子密钥 $rk_{A \rightarrow B}^{k,i} (i = 1, 2, \dots, t-1)$ 。

然后计算未被攻陷代理者的验证公钥:

$$vk_{k,j} = (pk_B^{2^{T+k}})^{\lambda_{j,0}} \prod_{i=1}^{t-1} vk_{k,i}^{\lambda_{j,i}}; j = t, \dots, n$$

这里 $\lambda_{j,i}$ 是 Lagrange 插值多项式的系数。从攻击者的角度来看,模拟器 $SIM_{RekeyUpd}$ 的模拟过程与 RekeyUpd 算法的执行过程是不可区分的。所以,RekeyUpd 算法是可模拟的。

给定一个时间段参数 k , 一个受托者和一个委托者的公钥 (pk_A, pk_B) , 一个 n_m 比特的消息 m , 一个原始签名 $\sigma_A = (\sigma_{A,1}, \sigma_{A,2})$ 和一个重签名 $\sigma_B = (\sigma_{B,1}, \sigma_{B,2}, \sigma_{B,3})$, 以及 $t-1$ 个已被攻陷的重签名子密钥 $rk_{A \rightarrow B}^{k,i} = (rsk_{A \rightarrow B}^{k,i}, rpk_{A \rightarrow B}^{k,i})$, 构造一个部分重签名生成算法 ShareResign 的模拟器 $SIM_{ShareResign} \circ SIM_{ShareResign}$ 在 Z_p^* 选取 $t-1$ 个随机数 r_1, \dots, r_{t-1} , 代表 $t-1$ 个已被攻陷的代理者计算相应的部分重签名:

$$\sigma_{B,i} = (\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}) = (\sigma_{A,1} \cdot rsk_{A \rightarrow B}^{k,i} \cdot \sigma^{r_i}, rpk_{A \rightarrow B}^{k,i}, \sigma_{A,2} \cdot g^{r_i}); i = 1, 2, \dots, t-1$$

然后, $SIM_{ShareResign}$ 计算未被攻陷的代理者的部分重签名

$$\sigma_j = (\sigma_{j,1}, \sigma_{j,2}, \sigma_{j,3}) = ((\sigma_{B,1})^{\lambda_{j,0}} \prod_{i=1}^{t-1} (\sigma_{i,1})^{\lambda_{j,i}}, (\sigma_{B,2})^{\lambda_{j,0}} \prod_{i=1}^{t-1} (\sigma_{i,2})^{\lambda_{j,i}}, (\sigma_{B,3})^{\lambda_{j,0}} \prod_{i=1}^{t-1} (\sigma_{i,3})^{\lambda_{j,i}}); j = t, \dots, n$$

这里 $\lambda_{j,i}$ 是 Lagrange 插值多项式的系数。因此, $SIM_{ShareResign}$ 能模拟 ShareResign 算法的执行, 即本文所提的 FSTPRS 方案是可模拟的。

结合定理 1, 2, 3, 命题 1 和 Chow-Phan 代理重签名的不可伪造性, 可得定理 4。

定理 4 在标准模型下, 本文所提的 FSTPRS 方案在 CDH 假设下是 UF-FSTPRS-CMA 安全的; 如果 $n \geq 2t-1$, 那么本文方案也是强壮的。

(上接第 800 页)

参考文献:

- [1] MOLNAR D, WAGNER D. Privacy and security in library RFID, issues, practices and architectures [C]// ACM Conference on Communications and Computer Security. New York: ACM Press, 2004: 210-219.
- [2] PERIS-LOPEZ P, HERNANDEZ-CASTRO J C, ESTEVEZ-TAPIA-DOR J M, et al. RFID systems: A survey on security threats and proposed solutions [C]// PWC'06: Proceedings of the 11th IFIP International Conference on Personal Wireless Communications, LNCS 4217. Berlin: Springer, 2006: 159-170.
- [3] MA CHANGSHE, LI YINGJIU, DENG R H. RFID privacy: Relation between two notions, minimal condition and efficient construction [C]// Proceedings of the 16th ACM Conference on Computer and Communications Security. New York: ACM Press, 2009: 54-65.
- [4] BRESSON E, CHEVASSUT O, POINTCHEVAL D. New security results on encrypted key exchange [C]// PKC 2004: Proceedings of the 7th International Workshop on Theory and Practice in Public Key Cryptography. Berlin: Springer, 2004: 145-148.
- [5] BRESSON E, CHEVASSUT O, POINTCHEVAL D. Security proofs for an efficient password-based key exchange [C]// Proceedings of ACM Computer and Communications Security. New York: ACM Press, 2003: 241-250.
- [6] 姜丽芬, 李章林, 辛运伟. 一种实用的轻量级 RFID 安全协议研究[J]. 计算机科学, 2009, 36(6): 105-107.
- [7] GARFINKEL S L, JUELS A, PAPPU R. RFID privacy: An over-

4 结语

本文提出了一种在标准模型下可证安全的前向安全的单向门限代理重签名方案。在门限代理重签名中引入了前向安全的思想, 使得当前重签名密钥的泄露也不会影响以前时间段签名的安全性。签名验证算法中加入时间段参数, 不仅确保了重签名密钥的前向安全性, 还可保证重签名的前向安全性。该方案可容忍 $t \leq n/2 + 1$ 个代理者被攻击者攻陷, 在 CDH 假设下能抵抗适应性选择消息攻击。

参考文献:

- [1] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography [C]// Proceedings of Eurocrypt'98, LNCS 1403. Berlin: Springer, 1998: 127-144.
- [2] CHOW S S M, PHAN R C W. Proxy re-signatures in the standard model [C]// ISC 2008: Proceedings of the 11th International Conference on Information Security, LNCS 5222. Berlin: Springer, 2008: 260-276.
- [3] YANG P, CAO Z, DONG X. Threshold proxy re-signature [C]// IPCCC 2008: Proceedings of the 27th IEEE International Performance Computing and Communications Conference. Austin, Texas: [s.n.], 2008: 450-455.
- [4] CANETTI R, HALEVI S, KATZ J. A forward-secure public-key encryption scheme [C]// Eurocrypt'03: Proceedings of the 22nd International Conference on Theory and Applications of Cryptographic Techniques, LNCS 2656. Berlin: Springer-Verlag, 2003: 255-274.
- [5] YANG XIAODONG, WANG CAIFEN. Threshold proxy re-signature schemes in the standard model [J]. Chinese Journal of Electronics, 2010, 19(2): 345-350.
- [6] view of problems and proposed solutions [J]. IEEE Security and Privacy, 2005, 3(3): 34-43.
- [8] JUELS A, WEIS S A. Define strong privacy for privacy for RFID [C]// Proceedings of the Fifth IEEE International Conference on Pervasive Computing and Communications Workshops. Washington, DC: IEEE Computer Society, 2007: 342-347.
- [9] RHEE K, KWAK J, KIM S, et al. Challenge-response based RFID authentication protocol for distributed database environment [C]// SPC 2005: Proceedings of the Second International Conference on Security in Pervasive Computing, LNCS 3450. Berlin: Springer, 2005: 70-84.
- [10] HA J H, MOON S J, ZHOU J Y, et al. A new formal proof model for RFID location privacy [C]// ESORICS'08: Proceedings of the 13th European Symposium on Research in Computer Security, LNCS 5283. Berlin: Springer, 2008: 267-281.
- [11] van DEURSEN T, RADOMIROVIC S. On a new formal protocol model for RFID location privacy [J]. Information Processing Letters, 2009, 110(2): 57-61.
- [12] SHOUP V. Sequences of games: A tool for taming complexity in security proofs [EB/OL]. (2006-01-01) [2010-05-20]. <http://eprint.iacr.org/2004/332>. Revised.
- [13] AVOINE G. Adversarial model for radio frequency identification [EB/OL]. (2005-01-01) [2010-05-15]. <http://eprint.iacr.org>.