文章编号:1001 - 9081(2011)03 - 0798 - 03
doi:10.3724/SP.J.1087.2011.00798

Molnar 协议的安全性证明

邓强东,王立斌
(华南师范大学 计算机学院,广州 510631)
(lbwang@scnu.edu.cn)

摘　要:Molnar 协议是射频识别(RFID)系统中读写器与标签之间的双边认证协议,同时强调能够保护标签的位置隐私,而协议安全性尚未得到形式化的分析和证明。在 eHa 模型下,严格地证明了 Molnar 协议具有不可预测的强隐私性,并得到确切的安全界。协议的证明使用了基于 Game 的方法,将协议的隐私性紧致地归约到伪随机函数的输出与随机函数的输出多项式时间不可区分的假设上,对分析和解决 RFID 系统安全性问题有效而通用。

关键词:射频识别;安全模型;强隐私性;可证明安全
中图分类号: TP309.1　　**文献标志码**:A

Security proof of Molnar protocol

DENG Qiang-dong, WANG Li-bin
(*School of Computer, South China Normal University, Guangzhou Guangdong* 510631, *China*)

Abstract: Molnar protocol is a scheme for mutual authentication between tags and readers in Radio Frequency Identification (RFID) system, which emphasizes protecting privacy for the tag; however, its security has not been proved formally. By using the eHa model, a formal proof was given, in which the output of the Molnar protocol maintain unpredictable, denoted as un-privacy. Moreover, the accurate security boundary of the Molnar protocol was computed. The privacy of protocol was reduced tightly on the assumption that the output of pseudorandom functions was indistinguishable from the output of random functions in polynomial time by utilizing the game-based technique. This technique is a powerful tool for analyzing and solving the privacy problem of RFID system, and provides an effective and universal solution.

Key words: Radio Frequency Identification (RFID); security model; strong privacy; provable security

0　引言

Molnar 等人为射频识别(Radio Frequency Identification, RFID)系统设计了一种双边认证协议(简称 Molnar 协议)[1],该协议不仅实现了读写器与标签之间的双向认证,还试图保护标签的位置隐私。Molnar 协议使用了简单的异或操作与伪随机函数来实现安全保护,效率较高,因此受到了广泛的关注,成为了解决 RFID 系统隐私问题的一种重要方案[2]。长期以来,并没有针对 Molnar 协议的攻击的报道,但其安全性也一直没有得到形式化的分析与证明。

本文旨在形式化证明 Molnar 协议具有强隐私性。首先,使用 eHa 模型[3]描述了一个能够完全控制通信信道的攻击者。其次,将协议的隐私性定义为协议的输出副本与随机数的不可区分性[3](不可预测的强隐私性)。为此使用基于 Game 的方法[4-5],将协议不可预测的强隐私性紧致地归约到伪随机函数的输出与随机函数输出多项式时间不可区分的假设上。

伪随机函数假设是指不存在多项式时间的攻击者,能够有效地区分伪随机函数的输出和随机函数的输出。协议的隐私性建立在这个假设上,即如果存在多项式时间的攻击者 A 以不可忽略的概率攻破协议的隐私性,则可以利用 A 构造算法以不可忽略的概率区分伪随机函数与随机函数,从而与伪随机函数假设矛盾。

传统的反证归约法[6]虽然能够证明协议的隐私性,但是无法得到确切的安全界。本文在 eHa 模型和不可预测强隐私性定义下,通过定义一系列不可区分的 Game,最终证明攻击者以可忽略的概率攻破协议的隐私性,并得到了确切的安全界。该证明技术有望成为未来分析和解决 RFID 系统的安全性问题的一种通用而有效的解决方法。

为了解决 RFID 系统的隐私性问题[2,7],不同的安全模型与安全定义相继被提出。Juels 等人描述了一个能够控制通信信道的攻击者,并且提出了一个相对简单的强(弱)隐私性定义[8],这个隐私性定义基于的是两个标签的不可区分性(不可区分强隐私性)。同时,Juels 等人利用这个模型证明了 hash-lock 协议具有不可区分强隐私性,然而 hash-lock 协议却被发现容易暴露标签的位置信息[9]。2008 年 Ha 等人提出了一个新隐私性定义[10],这个隐私性定义基于标签的输出副本与随机数的不可区分性。随后,Deursen 等人[11]指出了此定义的不完整性。Ma 等人在 2009 年对 Ha 模型[10]进行了推广(eHa 模型),认为隐私性定义应基于协议输出副本与随机数的不可区分性[3],同时证明了不可预测强隐私性要强于不可区分强隐私性,因此本文将使用此隐私性定义证明协议的安全性。

1　定义预备

1.1　数学定义

设 $A=(\cdots)$ 为伪随机算法,$y\leftarrow A(x_1,x_2,\cdots;cn)$ 表示以 $x_1,x_2,\cdots$ 和抛币随机数 cn 为输入,输出为 y;$y\leftarrow A^{O_1,\cdots,O_n}(x_1,x_2,\cdots)$ 表示在访问预言机 $O_1,\cdots,O_n$ 的情况下,以 $x_1,x_2,\cdots$ 为输入,输出为 y;若 S 表示一个集合,则 $s\in_R S$ 表示 s 在集合 S

收稿日期:2010 - 07 - 19。

作者简介:邓强东(1985 -),男,广东梅州人,硕士研究生,主要研究方向:密码学、网络安全;　王立斌(1972 -),男,广东龙门人,副教授,博士,主要研究方向:密码学、网络安全。

中均匀选取;若 $x_1, x_2, \cdots$ 是字符串,则 $x_1 \| x_2 \cdots$ 表示字符串的串联;如果 x 是一个字符串,则 $|x|$ 表示字符串的二进制比特长度;若 S 是一个集合,则 $|S|$ 表示集合的元素个数;$f \in_R \Gamma$ 表示从函数族 Γ 中随机选择一个函数 f;$\Pr[E]$ 表示事件 E 发生的概率,$\mathbf{N}$ 表示整数集,$\mathbf{R}$ 表示实数集。

定义 1　可忽略函数。

如果对于每一个 $c > 0$ 均存在一个数 $m \in \mathbf{N}$,对于所有的数 n,在 $n > m$ 时,使得 $F(n) < 1/n^c$ 都成立,则称函数 $F: N \mapsto \mathbf{R}$ 是可忽略的函数。

1.2　伪随机函数族

令 $l(k) = l_c + l_r + 1$ 和 $L(k) = l_{\mathrm{ID}}$ 为两个整数,其中 k 为安全参数。设 $F := (f_s)_{s \in S}$ 为带索引值的函数族,映射为 $\{0,1\}^{l(k)} \mapsto \{0,1\}^{L(k)}$。令 $\Gamma(l(k), L(k))$ 表示所有映射为 $\{0,1\}^{l(k)} \mapsto \{0,1\}^{L(k)}$ 的函数的函数集。给定对 $f_s \in F$ 和 $f \in \Gamma(l(k), L(k))$ 的预言询问,如果任意多项式时间的攻击者都无法区分这两个函数,则称函数族 F 是一个伪随机函数族。形式化描述如下。

定义 2　伪随机函数族。

函数族 $F := \langle f_s \mid s \in \{0,1\}^{k_s} \rangle$ 被认为是 $(l(k), L(k))$ 伪随机函数族,如果下述 3 个条件均成立:

1) $\forall k \in \mathbf{N}, \forall s \in_R \{0,1\}^{k_s}, f_s: \{0,1\}^{l(k)} \mapsto \{0,1\}^{L(k)}$;

2) $\forall k \in \mathbf{N}, \forall s \in \{0,1\}^{k_s}, f_s$ 多项式时间可计算;

3) 如果对于任意多项式时间的攻击者 A:

$$\left| \Pr\left[Adv^{f_s}(1^k) = 1 \mid s \in_R \{0,1\}^{k_s}\right] - \Pr\left[Adv^{f}(1^k) = 1 \mid f \leftarrow \Gamma(l(k, L(k)))\right] \right| \leqslant \varepsilon_{\mathrm{prf}}$$

其中 $\varepsilon_{\mathrm{prf}}$ 为可忽略量。

2　Molnar 协议

假定有一个多项式大小的标签集 $TS = (Tag_1, \cdots, Tag_l)$ 和一个读写器 R,则一个 RFID 系统定义为 $S = (TS, R, \mathrm{Initialize}, \pi)$。设标签 Tag_i 的密钥 $s_i \in_R \{0,1\}^{k_s}$,挑战信息 $c_i \in_R \{0,1\}^{l_c}$,标签 Tag_i 的应答信息为 (r_i, σ_i)。其中 $r_i \in_R \{0,1\}^{l_r}$,标签 $ID_i \in_R \{0,1\}^{l_{ID}}$。设 $F := (f_s)_{s \in S}$ 为伪随机函数族,映射为 $\{0,1\}^{l_c + l_r + 1} \mapsto \{0,1\}^{l_{ID}}$。协议的执行过程见图 1。

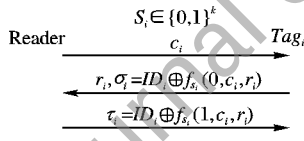

图 1　Molnar 协议

1) 初始化阶段。

① 初始化读写器 R。R 与每一个标签 Tag_i 共享一个密钥 s_i 和一个唯一的 ID_i,并且将 (ID_i, s_i) 存储在后台数据库 D. s. t 中,选取一个 $f_{s_i} \in F$ 与标签 Tag_i 共享;

② 初始化标签 Tag_i。Tag_i 存储了一个共享的密钥 s_i 和唯一的 ID_i,选取一个 $f_{s_i} \in F$ 与读写器 R 共享。

2) 协议 $\pi(R, Tag_i)$ 执行阶段。

① 首先读写器 R 发送一个挑战信息 c_i 给标签 Tag_i;

② 标签 Tag_i 收到挑战信息 c_i 后,随机选取 r_i,并且计算 $\sigma_i = ID_i \oplus f_{s_i}(0, c_i, r_i)$,然后将应答信息 (r_i, σ_i) 发送给读写器 R;

③ 读写器 R 在收到应答信息 (r_i, σ_i) 后,计算 $ID'_i = \sigma_i \oplus f_{s_i}(0, c_i, r_i)$,然后检查 (ID_i', s_i) 是否在后台数据库 D. s. t 中,并且输出最后一轮的消息 $\tau_i = ID_i' \oplus f_{s_i}(1, c_i, r_i)$ 给标签 Tag_i;

④ 标签收到最后一轮消息 τ_i 后,计算 $ID_i' = \tau_i \oplus f_{s_i}(1, c_i, r_i)$,标签检查 Tag_i 的 ID_i 是否等于所计算的 ID'_i。协议的此次会话由 $sid = c_i \| r_i \| \sigma_i \| \tau_i$ 标识。

3　安全模型和安全定义

3.1　安全模型

假定协议攻击者能完全控制通信信道,即攻击者能窃听、延迟、篡改协议传输的消息,通过定义预言机查询的方式形式化描述攻击者的能力。

1) $Send(u, m)$。向参与主体 U 发送消息 m,用来模拟被动和主动攻击。

2) $Reveal(Tag_i, s_i')$。用 s_i' 更新 Tag_i 的共享密钥和内部状态,并返回标签 Tag_i 的当前密钥 s_i。

3) $Test(Tag_i, c_i)$。如果 Tag_i 是新鲜的(即 Tag_i 执行协议过程中没有被执行 $Reveal$ 查询),则进行以下操作:在测试信息为 c_i 的情况下,进行一次随机抛币 $b(b \in \{0,1\})$,如果 $b = 1$,返回会话为 sid 的协议输出 $(c_i, r_i \| \sigma_i, \tau_i)$ 副本给攻击者;否则返回三元组 $(c_i, r_i \| R_1, R_2)$,其中 $R_1, R_2 \in_R \{0,1\}^{l_{\mathrm{ID}}}$。

上面定义的三种攻击者的能力能够用来模拟攻击者的大多数能力,例如窃听、延迟、重放协议传输的消息。根据协议的执行和询问内容的不同,攻击者允许进行 $Send(R, invoke)$, $Send(Tag_i, c)$, $Send(R, r \| \sigma)$ 和 $Send(Tag_i, \tau)$ 四种方式的预言询问。设攻击者进行 $Send(Tag_i, c)$, $Send(R, r \| \sigma)$, $Reveal(Tag_i, s_i')$ 和 $Send(Tag_i, \tau)$ 预言询问的次数分别不超过 q、s、u、v 次,且将预言机简记为 O_1、O_2、O_3、O_4。

3.2　不可预测的强隐私性

图 2 展示了强隐私性实验 $Exp_A^{\mathrm{unp}}(k, l, q, s, u, v)$(简记为 Exp_A^{unp})。攻击者 A 由算法 (A_1, A_2) 组成,运行在两个状态中。在了解阶段,算法 A_1 被要求仅选取一个挑战标签 T_c 和一个测试信息 $c_0 \in \{0,1\}^{l_c}$,并且也会输出一个状态信息 st 给算法 A_2。在实验过程中,攻击者 A 允许询问预言机 O_1、O_2、O_3 和 O_4 至多分别为 q、s、u、v 次(A_1 不允许对标签 T_c 进行 $Reveal$ 询问)。最后在猜测阶段,算法 A_2 允许访问除 T_c 外的所有所有标签,然后判断挑战信息对 $(r_0 \| \sigma^*, \tau^*)$ 是否为测试信息为 c_0 的协议 π_{sid} 的输出,其中 $sid = c_0 \| r_0 \| \sigma^* \| \tau^*$。

实验 $Exp_A^{\mathrm{unp}}(k, l, q, s, u, v)$:
1)初始化读写器 R 和标签集 TS,其中 $|TS| = l$, k 为安全系数;
2)$(T_c, c_0, st) \leftarrow A_1^{O_1, O_2, O_3, O_4}(R, TS)$(学习阶段);
3)设 $T' = TS - (T_c)$;
4)$b \in_R \{0,1\}$;
5)如果 $b=0$,则返回 $(c_0, r_0 \| \sigma^*, \tau^*)$,其中 $(\sigma^*, \tau^*) \in_R \{0,1\}^{l_{\mathrm{ID}}} \times \{0,1\}^{l_{\mathrm{ID}}}$,否则执行协议 $\pi_{sid}(R, T_c) \rightarrow (c_0, r_0 \| \sigma_0, \tau_0)$,返回 $(c_0, r_0 \| \sigma^*, \tau^*)$,其中 $(\sigma^*, \tau^*) = (\sigma_0, \tau_0)$, $sid = c_0 \| r_0 \| \sigma^* \| \tau^*$;
6)$b' \leftarrow A_2^{O_1, O_2, O_3, O_4}(R, T', st, r_0 \| \sigma^*, \tau^*)$(猜测阶段);
7)如果 $b = b'$,实验输出1,否则实验输出0。

图 2　不可预测的强隐私性实验

定义 3　猜测优势。

实验 $Exp_A^{\mathrm{unp}}(k, l, q, s, u, v)$ 攻击者 A 的优势定义为 $Adv_A^{\mathrm{unp}}(k, l, q, s, u, v) = \left| \Pr[Exp_A^{\mathrm{unp}}(k, l, q, s, u, v) = 1] - \frac{1}{2} \right|$。

定义 4　在实验 Exp_A^{unp} 中,如果攻击者 A 的优势 $Adv_A^{\mathrm{unp}}(k, l, q, s, u, v)$ 至少为 ζ,攻击者 A 的运行时间至多为 t,则称攻击者 $A(\zeta, t, q, s, u, v)$ -攻破了 RFID 系统 S。

定义 5　不可预测的强隐私性。

如果不存在攻击者 A 能够 (ζ, t, q, s, u, v) -攻破 RFID 系统 S,则称 RFID 系统 S 具有不可预测的强隐私性。

4　协议安全性分析

本章对 Molnar 协议的隐私性进行了分析与证明,其中证

明方法沿用 Bresson 等人基于 Game[4-5] 的方法。以下定理将协议的隐私性紧致归约到伪随机函数假设上，证明了此协议具有不可预测的强隐私性。

定理 1 假设 A 是一个针对 Molnar 协议的攻击者，其运行时间不超过 t，对预言机 O_1、O_2、O_3、O_4 的询问次数分别不超过 q、s、u 和 v，如果函数族 F 为伪随机函数族，映射为 $\{0,1\}^{k_s}\times\{0,1\}^{l_c+l_r+1}\mapsto\{0,1\}^{l_{ID}}$，则定义在其上的 RFID 系统 $S=(TS,R,\text{Initialize},\pi)$ 具有不可预测的强隐私性。攻击者的优势为：

$$Adv_A^{\text{unp}}(A)\leqslant\varepsilon_{\text{prf}}+\frac{s+q}{2^{l_{ID}-1}}+\frac{q^2}{2^{l_c}}+\frac{s^2}{2^{l_r}}$$

证明 通过定义一系列的 Game，以原始的攻击 Game G_0 开始，以 Game G_3 结束。利用 Shoup 引理[12] 确定 Game 之间可区分的概率上界。由于这些概率上界都是可忽略的值，所以相邻的 Game 之间难以区分，最终将协议的隐私性紧致归约到伪随机函数假设上。

对每个 Game G_i，事件 S_i 定义为攻击者 A 成功猜测 *Test* 查询中的 b，即 $b'=b$。

Game 定义如下。

1) Game G_0。这是在伪随机函数假设成立下的原始攻击 Game，是协议的真实执行。由定义(3)：

$$Adv_A^{\text{unp}}(A)=|2\Pr[S_0]-1| \tag{1}$$

2) Game G_1。G_1 按步骤①、②、③来模拟 *Send*、*Reveal*、*Test* 查询。显然，经过模拟后的 G_1 与 G_0 是不可区分的，即：

$$\Pr[S_1]=\Pr[S_0] \tag{2}$$

① 对读写器 *Send* 查询的模拟如下。

Rule $R1^{(1)}$。*Send*$(R,invoke)$ 查询按如下方式进行：

启动读写器 R 与标签 Tag_i 通信；

选取 $c_i\in\{0,1\}^{l_c}$；

返回 c_i。

Rule $R2^{(1)}$。*Send*$(R,r\|\sigma)$ 查询按如下方式进行：

计算 $ID=\sigma\oplus f_{s_i}(0,c_i,r)$；

查找(ID,s_i)是否在后台数据库 D. s. t 中；

计算 $\tau_i=ID\oplus f_{s_i}(1,c_i,r)$；

返回 τ_i。

② 对标签 *Send* 查询的模拟如下。

Rule $T1^{(1)}$。*Send*(Tag_i,c) 查询按如下方式进行：

选取 $r_i\in_R\{0,1\}^{l_r}$；

计算 $\sigma_i=ID_i\oplus f_{s_i}(0,c,r_i)$；

返回 $r_i\|\sigma_i$。

Rule $T2^{(1)}$。*Send*(Tag_i,τ) 查询按如下方式进行：

计算 $ID'_i=\tau\oplus f_{s_i}(1,c,r_i)$；

判断 ID'_i 是否等于 ID_i；

返回 1。

③*Reveal* 和 *Test* 查询的模拟如下。

Reveal(Tag_i,s'_i) 查询。返回 Tag_i 对应的共享密钥 s_i，并且用 s'_i 更新共享密钥和内部状态。

Test(Tag_c,c_c) 查询。对 Tag_c 没有进行过 *Reveal* 预言询问；在测试信息为 c_c 的情况下，进行一次随机抛币 b，如果 $b=1$，返回协议输出副本 $\pi(R,Tag_c)$；否则选取随机数 σ_c，$\tau_c\in_R\{0,1\}^{l_{ID}}$；最终返回协议副本$(c_c,r_c\|\sigma_c,\tau_c)$。

3) Game G_2。G_2 的模拟要避免随机选择的 c 和 r 存在碰撞，因此，在 G_2 中，每一个 c 和 r 是在随机空间中均匀分布的，根据生日悖论，在协议副本中出现碰撞的概率分别不超过 $q^2/2^{l_c+1}$ 和 $s^2/2^{l_r+1}$。

$$|\Pr[S_2]-\Pr[S_1]|\leqslant q^2/2^{l_c+1}+s^2/2^{l_r+1} \tag{3}$$

4) Game G_3。在 G_3 中，经过了学习阶段，攻击者 A 选中了其中的一个标签 Tag_c，并且挑选一个测试信息 c_c，进行 *Test*(Tag_c,c_c)。此刻选择一个函数$f\leftarrow\Gamma(l(k),L(k))$代替原来的伪随机函数$f_s$，其中$\Gamma(l(k),L(k))$为映射为$\{0,1\}^{l(k)}\mapsto\{0,1\}^{L(k)}$的函数集，$l(k)=l_c+l_r+1$，而$L(k)=l_{ID}$。

当攻击者 A 进行 *Test*(Tag_c,c_c) 预言询问时，模拟器随机的抛币 $b\in_R\{0,1\}$，抛币结果无论是 0 还是 1，都直接计算协议副本如下：

1) 取 $r_c\in_R\{0,1\}^{l_r}$，$\sigma^*=ID\oplus f(0,c_c,r_c)$，其中$f\leftarrow_R\Gamma(l(k),L(k))$；

2) 计算 $\tau^*=ID_c\oplus f(1,c_c,r_c)$；

3) 返回协议副本 $\pi(R,Tag_c)=(c_c,r_c\|\sigma^*,\tau^*)$。

让事件 X 表示 G_3 与 G_2 可区分；事件 X_1 表示当 *Test*(Tag_c,c_c) 时，G_2 的抛币 $b^{(2)}=1$；事件 X_2 表示当 *Test*(Tag_c,c_c) 时，G_2 的抛币 $b^{(2)}=0$；事件 M 表示 *Test* 查询后，返回的协议副本(σ^*,τ^*)与在 *Send* 查询后，返回的协议副本(σ,τ)冲突。当事件 M 发生时，可区分 G_3 与 G_2。

$$\Pr[X|X1]\leqslant(1/2)\times\varepsilon_{\text{prf}};$$

$$\Pr[X|X2]=(1/2)\times 0;$$

$$\Pr[M]=(s+q)/2^{l_{ID}};$$

$$\Pr[X]=\Pr[X|X1]+\Pr[X|X2]+\Pr[M]\leqslant(1/2)\times\varepsilon_{\text{prf}}+(s+q)/2^{l_{ID}}。$$

综上所述：

$$|\Pr[S_3]-\Pr[S_2]|=\Pr[X]\leqslant(1/2)\times\varepsilon_{\text{prf}}+(s+q)/2^{l_{ID}} \tag{4}$$

在 G_3 中，返回的协议副本同为与抛币无关的随机数，攻击者猜中硬币的概率为：

$$\Pr[S_3]=1/2 \tag{5}$$

综合式(2) ~ (5)，可得：

$$|\Pr[S_3]-\Pr[S_0]|\leqslant\frac{1}{2}\times\varepsilon_{\text{prf}}+\frac{s+q}{2^{l_{ID}}}+\frac{q^2}{2^{l_c+1}}+\frac{s^2}{2^{l_r+1}} \tag{6}$$

综合式(1) ~ (6)，可得：

$$Adv_A^{\text{unp}}(A)=2|\Pr[S_3]-\Pr[S_2]|\leqslant\varepsilon_{\text{prf}}+\frac{s+q}{2^{l_{ID}-1}}+\frac{q^2}{2^{l_c}}+\frac{s^2}{2^{l_r}}$$

所以定理 1 得证。

在伪随机函数假设下，Adv_A^{unp} 不超过一个可忽略的值，因此协议具有不可预测的强隐私性。

5 结语

本文利用 eHa 模型形式化描述协议参与者和攻击者的能力，在伪随机函数假设下，通过一系列彼此之间难以区分的 Game 模拟协议的执行，逐步限制攻击者的优势，将协议的隐私性紧致归约到伪随机函数假设上。证明了如果伪随机假设成立，则 Molnar 协议具有不可预测的强隐私性。

协议的证明形式化地描述了攻击者模型，严格地定义了协议的安全性，使用了基于 Game 的方法，从而紧致地得到满足安全定义的安全界。这种有效的证明技术为分析和解决 RFID 安全性问题提供了通用解决方法。

安全定义仍然是 RFID 系统隐私性保护的研究热点。Ma 等人证明了在不可预测的强隐私性定义下，最小安全假设为伪随机函数假设[3]。而不可预测的强隐私性虽然能够被证明比不可区分强隐私性更强，但是一些明显具有不可跟踪性的协议却无法满足此隐私性定义[11]。因此进一步改进安全定义从而减弱证明中的安全假设将是下一步工作的重点。

(下转第 804 页)

然后计算未被攻陷代理者的验证公钥：

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

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 比特长的消息 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 $rk_{A\to B}^{k,i} = (rsk_{A\to B}^{k,i}, rpk_{A\to B}^{k,i})$，构造一个部分重签名生成算法 ShareResign 的模拟器 $SIM_{\text{ShareResign}}$。$SIM_{\text{ShareResign}}$ 在 Z_p^* 选取 $t-1$ 个随机数 $r_1,\cdots,r_{t-1}$，代表 $t-1$ 个已被攻陷的代理者计算相应的部分重签名：

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

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

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

这里 $\lambda_{j,i}$ 是 Lagrange 插值多项式的系数。因此，$SIM_{\text{ShareResign}}$ 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 $n \geqslant 2t-1$，那么本文方案也是强壮的。

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 $t \leqslant n/2+1$ 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]// Eurocrypto'03: Proceedings of the 22nd International Conference on Theory and Applications of Cryptographic Techniques, LNCS 2656. Berlin: Springer-Verlag, 2003: 255 – 271.

[5] YANG XIAODONG, WANG CAIFEN. Threshold proxy re-signature schemes in the standard model [J]. Chinese Journal of Electronics, 2010, 19(2): 345 – 350.

（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-TAPIADOR 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，辛运帏. 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 overview 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.