基于 PUF 的开环 RFID 所有权转移协议

韦 民[1], 孙子文[1,2]

[1]江南大学物联网工程学院 无锡 中国 214122
[2]物联网技术应用教育部工程研究中心 无锡 中国 214122

摘要 本文主要针对在供应链的交接过程中, 标签在转移时的安全隐私和转移效率低的问题。为了针对低成本标签的安全与隐私问题, 采用物理不可克隆函数(Physical Unclonable Function, PUF)和随机数等作为加密机制; 为了抵御内部读写器攻击, 使用伪随机数随时更新; 采用 PUF 来保护标签的暴力攻击, 将 PUF 和随机数结合实现标签的匿名和不可被追踪性; 采用 Rabin 算法实现加密; 采用 Vaudenay 模型来证明所有权转移的安全与隐私性。仿真结果表明, 所有权转移时间降低, 加快所有权转移的速度, 提高供应链交接的效率。

关键词 物理不可克隆函数; Rabin 算法; 开环; 所有权转移
中图法分类号 TP391.45 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2019.07.02

Open - loop RFID ownership transfer protocol based on PUF

WEI Min[1], SUN Ziwen[1,2]

[1] Department of Internet of Things, Jiangnan University, Wuxi 214122, China
[2] Engineering Research Center of Internet of Things Technology Applications Ministry of Education, Wuxi 214122, China

Abstract This paper mainly aims at the security and privacy issues and the low efficiency of transfer in the process of handover in the supply chain. In order to solve the security and privacy problems of low cost tag, Physical Unclonable Function(PUF) and random number are used as the encryption mechanism. In order to resist internal reader attacks, pseudo-random numbers are used to update at any time. PUF is adopted to protect the violent attacks of tags, and the combination of PUF and random numbers can realize the anonymity and untraceability of tags. Rabin algorithm is used to encrypt. Vaudenay model is used to prove the security and privacy of ownership transfer. Simulation results show that the time of ownership transfer decreases, the speed of ownership transfer is accelerated, and the efficiency of supply chain transfer is improved.

Key words physical unclonable function; rabin algorithm; open loop; transfer of ownership

1 引言

标签所有权是指可以识别标签并控制与标签有关的所有信息的能力[1]。标签所有权转移意味着新所有者接管了标签的管理权。在分析射频识别(Radio Frequency Identification, RFID) 标签所有权转移协议时, 通常将后台服务器和读写器看作一个整体, 即后台服务器和读写器作为一个独立的通信实体, 在本文中统一称为读写器。RFID 所有权转移协议应满足以下特点: ①低成本, 满足 EPC Class-1 Generation-2 (EPC C1G2)标准; ②标签能够实现所有权转移; ③安全隐私保护。所有权转移协议具有以下安全与隐私权限: 当标签的所有权已经转移给新读写器时, 只有新读写器能够识别标签并且能够访问标签内的信息, 并且当前读写器不能再识别和控制标签; 标签所有权转移给新读写器后, 新读写器不应追溯标签与当前读写器之间的互动[2]。

RFID 所有权转移协议系统分为闭环与开环两种。闭环 RFID 系统定义为在所有权转移过程中标签在新读写器和当前读写器范围内的系统, 开环 RFID 系统被定义为在所有权转移过程中标签仅在新所有者范围内的系统[3]。

通讯作者: 孙子文, 博士, 教授, Email: sunziwen@jiangnan.edu.cn。
本课题得到国家自然科学基金(No.61373126)和中央高校基本科研业务费专项资金资助(No.JUSRP51510)资助。
收稿日期: 2018-06-25; 修改日期: 2018-10-20; 定稿日期: 2019-06-06

表 1　现有文献的方法

Table 1　Existing literature method

	方法	优点	缺点
Kulseng L 等人[4]	使用 PUF 和线性反馈移位寄存器、更新标签标识符(Identifier, ID)的所有权转移协议	首次将 PUF 使用进 RFID 标签中; 满足 EPC C1G2 标准; 可抵御 DOS 攻击	只是将 PUF 作为一个随机数在使用, 未充分发挥 PUF 的作用; 采用可信第三方(Trusted Third Party, TTP)机制, 实际生活中较难实现
Li Q S 等人[5]	使用 PUF 代替随机生成器, 提出了一种在开放环境下基于 PUF 的 RFID 所有权转移协议	满足 EPC C1G2; 采用 PUF 加密	与文献[4]一致, 只是将 PUF 作为一个随机生成器, 标签 ID 没有进行 PUF 加密保护, 因此 ID 存在被攻击获取的危险, 并进行位置跟踪攻击和拒绝服务攻击
Doss R 等人[6]	提出了基于二次剩余定理开环系统和闭环系统两种轻量级所有权转移协议	满足 EPC C1G2; 适用于大规模系统应用	存在内部读卡器恶意假冒攻击; 不满足前向不可跟踪性; 存在去同步化攻击
陈秀清等人[7]	提出了一个基于二次剩余定理的轻量级 RFID 所有权转移协议, 并使用改进的模型和定义形式化证明了协议的安全性和隐私性	将 Vaudenay 模型进行改进, 提出强前向不可追踪性	不满足 EPC C1G2 标准; 不能抵御暴力攻击
沈金伟等人[8]	提出了一种使用位运算的超轻量级 RFID 所有权转移协议, 并给出了基于 GNY 逻辑的协议安全性证明	较好的证明了所有权转移的安全性	GNY 逻辑不能证明所有权转移的隐私问题
王萍等人[14]	采用云服务器、伪随机函数和二次剩余定理加密, 提出一种所有权转移协议	采用云进行信息的存储及信息的传递; 移动性较强	不满足 EPC C1G2; 不能抵御暴力攻击; 采用的二次剩余定理方案不能抵御选择明文攻击

从表 1 中的已有研究来看, 当满足 EPC C1G2 标准时, 标签的安全隐私性降低, 且都不能抵御暴力攻击, 针对一些常见的攻击也不能很好抵御, 大多所有权转移都没有很好的针对隐私进行证明。因此, 在满足 EPC C1G2 标准的同时, 防御暴力、假冒、去同步等攻击, 改善加密算法, 更好地去证明协议的安全隐私性, 是本文面临的重大挑战。

本文研究了一个基于 PUF 的开环 RFID 所有权转移协议(Ownership Transfer protocol for PUF-based Open Loop RFID systems, OTPOR)。针对提出的挑战, OTPOR 使用 PUF、Rabin、异或等加密方案, 避免使用复杂的加密算法来满足 EPC C1G2 标准; 针对不同的攻击建立攻击防御模型; 利用 PUF 和改进的加密算法来加密信息; 使用改进的 Vaudenay 模型来证明 RFID 所有权转移协议的安全与隐私性。

2　RFID 所有权转移中攻击与防御策略

协议涉及 3 个参与方:①当前读写器(R_c), ②新读写器(R_n), ③标签(T)。RFID 所有权转移协议必须能够确保当前和新读写器的安全与隐私要求, 即当 RFID 标签所有权从当前读写器被转移给新读写器后, 只有新读写器能够询问标签, 而其他人(包括当前读写器)被阻止与标签进行通信且标签、新的和当前读写器的安全与隐私必须得到保护。

2.1　攻击模型

假设当前读写器、新读写器、标签之间通信信道是不安全的, 且当前读写器、新读写器、标签均可被攻击, 但服务器是安全的, 建立攻击模型如图 1 所示, 其中 PA_T、PA_R、PA_C 分别表示对标签、信道和读写器的不同强度的攻击。

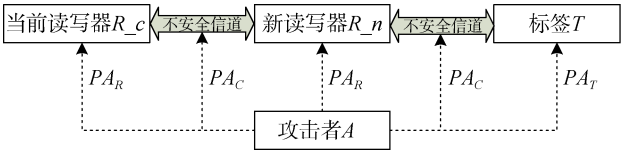

图 1　所有权转移时的攻击模型

Figure 1　Attack model of ownership transfer

Vaudenay 在 2007 年提出的攻击模型[10]对安全和隐私做了严格的定义, 之后, Vaudenay 模型及其改进的 Vaudenay 模型[7]被研究者用于 RFID 认证协议的安全与隐私证明。然而将 Vaudenay 模型用于 RFID 所有权转移协议的安全隐私证明的文献较少, 且(1)用于证明所有权转移的 Vaudenay 模型也没有描述清楚安全隐私问题, 同时 Vaudenay 模型中(2)攻击者错

过标签密钥更新阶段[7], 且(3)所提供的预言机只提供针对标签和信道的攻击。

针对 Vaudenay 模型存在的不足, 本文假设攻击者没有错过标签密钥更新阶段, 提供一个新的预言机来模拟针对读写器的攻击, 使用改进 Vaudenay 模型对强前向和后向不可追踪性证明。本文改进 Vaudenay 模型, 涉及的攻击者可访问的预言机及其功能描述如表 2 所示, 其中 $Observe(\bullet)$ 和 $Corrupt(RID_i)$ 预言机为新增预言机。

表 2 攻击者的预言机及其功能

Table 2 Function introduction of Attacker's each oracle

预言机	预言机的功能
$CreateTag(TID)$	创建一个具有唯一标识符 TID 的自由标签
$DrawTag(dist)\to vtag$	按照概率分配函数 $dist$ 随机选择标签, 并为标签分配临时标识符 $vtag$
$Free(vtag)$	释放标识符为 $vtag$ 的标签
$Launch()$	读写器发起一个新的所有权转移协议
$SendReader(m,RID_i,\pi)$	执行协议 π 的过程中, 给标识符为 RID_i 的读写器发送消息 m, 并输出读写器的响应
$SendTag(m,TID_i,\pi)$	在执行协议 π 的过程中, 给标识符为 TID_i 的标签发送消息 m, 并输出读写器的响应
$Observe(R,T)$	执行协议 π 的过程中, 窃听读写器 R 与标签 T 之间的交互信息
$Corrupt(RID_i)$	入侵标识符为 RID_i 的读写器, 返回读写器的内部信息
$Corrupt(vtag)$	入侵标识符为 $vtag$ 的标签, 返回标签的内部信息
$Result(\pi)$	完成协议 π 后, 若协议完成成功则输出 1, 否则输出 0

以下为针对信道、标签和读写器不同攻击的说明。

(1) 针对信道攻击

在任意攻击强度下, 攻击者都会调用 $Observe(R,T)$ 预言机窃听到读写器 R 与标签 T 之间的交互信息, 调用 $Observe(R\_c,R\_n)$ 预言机窃听到当前读写器 R_c 和新读写器 R_n 之间的交互信息。

(2) 针对标签的攻击

根据能否调用 $Result(\pi)$ 预言机, 可有两种调用类型: {Narrow, Wide}, Narrow 不能调用 $Result(\pi)$ 预言机, Wide 可以调用 $Result(\pi)$ 预言机, 本文只研究不能调用 $Result(\pi)$ 预言机的情况, 即 Narrow 等级; 根据攻击者调用 $Corrupt(\cdot)$ 预言机的能力, Vaudenay 模型[10]将攻击者的能力划分为四个能力等级: {Weak, Forward, Destructive, Strong}, 即弱攻击、前向攻击、破坏攻击、强攻击, 具体如下:

- Weak: 无法调用 $Corrupt(\cdot)$ 预言机, 但可以调用除 $Corrupt(\cdot)$ 之外的其他任意一个预言机。
- Forward: 调用 $Corrupt(\cdot)$ 预言机后, 只能调用 $Corrupt(\cdot)$ 预言机, 不能调用其他的预言机。
- Destructive: 调用 $Corrupt(\cdot)$ 预言机后, 由于标签、读写器遭受入侵攻击而损坏, 攻击者将无法访问任何预言机。
- Strong: 可以调用所有预言机。

根据攻击者调用 $Corrupt(\cdot)$ 预言机的能力, 针对标签的攻击有 4 种攻击强度 PA_T:

$$PA_T \in \{Narrow-Weak, Narrow-Forward, Narrow-Destructive, Narrow-Strong\} \quad (1)$$

各种攻击强度的详细描述如下:

- $PA_T = Narrow-Weak$, 攻击者可以调用其他预言机, 但无法调用 $Corrupt(\cdot)$ 预言机, 因此攻击者不能入侵到读写器、标签内部, 获取读写器、标签内部信息。
- $PA_T = Narrow-Forward$, 攻击者在调用 $Corrupt(\cdot)$ 预言机后, 还可以不停调用 $Corrupt(\cdot)$ 预言机, 达到使读写器、标签信息不停地泄露的目的。
- $PA_T = Narrow-Destructive$, 攻击者调用 $Corrupt(\cdot)$ 预言机后, 致使读写器、标签受到破坏, 攻击者不再调用其他任何预言机。
- $PA_T = Narrow-Strong$, 攻击者不停地调用任意的预言机来攻击读写器、标签。

(3) 针对读写器的攻击

同针对标签的攻击类似, 针对读写器的攻击亦有四种攻击强度 PA_R:

$$PA_R \in \{Narrow-Weak, Narrow-Forward, Narrow-Destructive, Narrow-Strong\}$$

后续内容将采用改进的 Vaudenay 模型用于证明

RFID 所有权转移协议的安全与隐私性。

2.2 防御模型

针对不同的攻击采用不同的防御方案。(1)针对信道攻击, 采用基于二次剩余定理的 Rabin 算法对传输信息进行加密; (2)针对读写器端的攻击, 采用 PUF 的激励响应对、Rabin 算法及伪随机数生成器来进行消息的确认与加密; (3)针对标签攻击中的持续调用 $Corrupt(vtag)$ 预言机导致标签持续地受到信息泄露的攻击, 采用具有不可破坏特性的 PUF 对标签的标识符和传输消息加密。所用的符号及其含义如表 3 所示。

表 3 协议中用的符号与含义

Table 3 Description of each notation in this protocol

符号	含义
T	标签
R_c / R_n	当前读写器、新读写器
p / q	大的素数且满足 $p \equiv 3(\mathrm{mod}\,4)$、$q \equiv 3(\mathrm{mod}\,4)$
n	正整数且 $n = p \cdot q$
$C_0 / C_1 / C_2 / C_3$	四个随机数
$TID / TID\_s / TID\_p$	标签 ID 号/异或后的伪 ID/经 PUF 加密后的 ID
$HRID\_c / HRID\_n$	当前/新读写器与随机数 Hash 加密后的 RID 值
h(・)	哈希函数
PRNG(・)	伪随机数生成器
K_{TID}	当前读写器与标签共享一个密钥串 $K_{TID}(K_{TID} = v_1 \| v_2 \| \cdots \| v_m)$, 其中 $v_p\left(p \in \{1,2,...,m\}\right)$ 为子密钥串
$R_p = \arg(v_p)$	表示将 $v_p\left(p \in \{1,2,...,m\}\right)$ 转变为与随机数相同的进位制的复制运算

2.2.1 协议模型

假设读写器与服务器之间的通信是安全的, 因此, 考虑标签在当前读写器和新读写器之间的所有权转移所设计模型如图 2 所示。

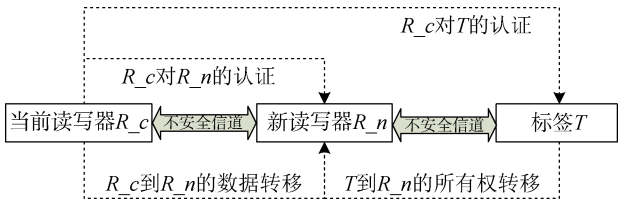

图 2 所有权转移协议模型

Figure 2 Model of Ownership Transfer Protocol

首先当前读写器对标签和新读写器进行认证, 认证通过后, 再将当前读写器关于标签的所有信息(密钥、TID 等)转移至新读写器, 从而完成标签 T 的所有权转移。

2.2.2 物理不可克隆函数的特性

PUF 以不可预知的方式将一组激励 $challenge$ 映射得到一组响应 $response$ [11]:

$$PF : challenge \to response \tag{1}$$

其中 $challenge$、$response$ 分别为不同位数的二进制数, $challenge$ 包含两部分: PUF 块号 Z 和激励 x, 即 $(Z,x) \in challenge$。

PUF 具有唯一性、随机性和不可破坏性。设任意的两个激励 $(Z,x) \in challenge$, $(Z',x') \in challenge$, 若 $PF(Z,x) = y$, $PF(Z',x') = y'$, 则 PUF 的特性可描述为

(1) 唯一性

对于同一块 PUF, 即 $Z = Z'$, 如果激励相同 $(x = x')$, 则响应相同 $(y = y')$ 的概率为 1; 对于不同块 PUF, 即 $Z \neq Z'$, 即使激励相同 $(x = x')$, 响应相同 $(y = y')$ 的概率为 0。用条件概率表示为

$$P(y = y' \mid Z \neq Z', x = x') = 1 \tag{2}$$

$$P(y = y' \mid Z \neq Z') = 0 \tag{3}$$

(2) 随机性

PUF 函数由于其行为类似随机生成器, 因而是不可预测的, 对于任意的响应 $y \in response$, 找到对应某块 PUF, 满足 $PF(Z,x) = y$ 的激励 $(Z,x) \in challenge$ 是不可实现的。用条件概率表示为

$$P\left(x = x' \mid \forall y \in response\right) = 0 \tag{4}$$

(3) 不可破坏性

若对含有 PUF 的设备进行任何物理攻击都将导致其 PUF 物理特性的破坏, 并且不能针对该特定设备正确评估 PUF 函数, 因此在任何概率多项式时间内, 攻击者在设备上执行物理攻击的成功率是可以忽略的。

可利用 PUF 的这些特性, 将其应用于保护标签的 ID 和传输的密钥, 使得标签不可追踪, 也使得密钥不可被破解。

在下文中假设一个标签仅有一块 PUF, 因此忽略 PUF 块数 Z, PUF 中的激励 challenge 只包含激励 x。

2.2.3 Rabin 算法

设 p 和 q 为私钥, 设为两个不同的素数, $n = p \cdot q$ 作为公钥, PT_1 为明文, CT 为密文。

加密方通过明文 PT_1 和公钥 n 产生密文 CT 的计

算如下,

$$CT = PT_1^2 \bmod n \tag{5}$$

解密方在已知密文 CT 和公钥 n 的前提下, 要想成功解密密文 CT 而求解出明文 PT_1, 还必须掌握私钥 p 和 q, 但直接从掌握的公钥 n 计算出 p 和 q 是一个数学难题, 即当 p 和 q 处于未知的状态时, 找到满足公式(5)的解 PT_1 在数学上是难以实现的。但解密方在已知密文 CT 的同时, 还掌握了组成公钥 n 的私钥 p、q, 则可通过中国剩余定理求解公式(5), 进而得到包括明文 PT_1 在内的四个解。

在转移协议中, 可利用 Rabin 算法中二次剩余定理的数学难题, 加密标签的标识符和共享密钥等, 达到加密传输消息的目的。

3 所有权转移协议的过程

本文设计了基于 PUF 的开环 RFID 系统的所有权转移协议, 它是由三个阶段组成, 即初始化阶段、认证阶段和所有权转移阶段。与大多数轻量级转移协议一致, 本协议假设标签与读写器和读写器与读写器之间的通信是不安全, 且采用异或和随机数生成器加密消息。此外, 本协议引入 Rabin 算法和 PUF, 来达到提高标签加密信息的安全与隐私性; 同时, 为防止读写器的假冒攻击, 使用当前读写器对新读写器和标签进行认证。

3.1 初始化阶段

对当前读写器 R_c、新读写器 R_n、标签 T 进行初始化, 产生各自加密后的标识符和密钥。

(1) 设 R_c 的标识符为 RID_c, 使用 Hash 函数将 RID_c 与伪随机数 r_i 加密, 产生加密后的标识符 $HRID\_c$:

$$HRID\_c = h(RID\_c \oplus r_i) \tag{6}$$

服务器生成共享密钥 S、密钥串 K_{TID}、随机数 C_1、S_1, 并将生成的信息发送给 R_c 与标签。

(2) 设 R_n 的标识符为 RID_n, 使用 Hash 函数将 RID_n 和伪随机数 r_j 加密, 产生加密后的标识符 $HRID\_n$:

$$HRID\_n = h(RID\_n \oplus r_j) \tag{7}$$

并将 $HRID\_n$ 发送至 R_c。

(3) 设 T 的标识符为 TID, 使用 PUF 将伪随机数 a 和 b 加密, 将加密后的响应值 $PF(a)$ 和 $PF(b)$ 与共享密钥 S 加密, 生成加密消息 C:

$$C = PF(a) \oplus PF(b) \oplus S \tag{8}$$

将加密消息 C 发送给 R_c, 之后删除 $PF(a)$、$PF(b)$ 和标签中的共享密钥 S。使用伪随机数 C_1 与标签的标识符 TID 生成 TID_s, 进一步使用 PUF 加密 TID_s, 产生加密后的值 TID_p:

$$TID\_s = TID \oplus C_1 \tag{9}$$

$$TID\_p = PF(TID\_s) \tag{10}$$

3.2 认证阶段

认证由当前读写器 R_c 发起对新读写器 R_n 和标签 T 的认证, 认证协议流程如图 3 所示, 具体步骤如下:

3.2.1 当前读写器发起认证

(1) 当前读写器发起并传输认证信息

R_c 产生随机数 C_0, 将 C_0 与所有权转移信号 OT 传输至 R_n。

(2) 新读写器计算并传输认证信息

R_n 计算认证信息:

$$A_1 = C_0 \oplus HRID\_n \tag{11}$$

认证信息 A_1 包含了新读写器加密后的标识符 $HRID\_n$, 然后将 A_1、C_0 和所有权转移信号 OT 发送至标签。

(3) 标签计算认证并传输信息

标签认证信息包括会话密钥 k 及会话信息 x'', R_p, F。

a) 生成标签与新读写器的会话密钥

计算第一步会话密钥:

$$k = PF(a) \oplus C_1 \oplus C_2 \tag{12}$$

在计算完成之后立即删除 $PF(a)$。

计算第二步会话密钥:

$$k = PF(b) \oplus k \oplus C \tag{13}$$

在计算完成之后立即删除 $PF(b)$。

最终的会话密钥 k 包含了随机数 a、b 经 PUF 函数加密后的 $PF(a)$、$PF(b)$ 值, C_1、C 为存储在标签的随机数、加密消息, C_2 为标签产生的伪随机数。这样通过两次 PUF 加密和两次删除可以保护标签的会话密钥 k。

b) 生成标签与新读写器的会话信息

获取新读写器标识符:

$$HRID\_n = A_1 \oplus C_0 \tag{14}$$

生成伪随机数 C_2, 并计算传输原码:

$$x = TID\_p \oplus C_2 \oplus C_0 \oplus S_1 \oplus v_p \tag{15}$$

传输原码包含了标签加密后的标识符 TID_p 及密钥串 K_{TID} 中第 p 个密钥 v_p。

依据 Rabin 算法加密传输原码 x 得会话信息 x':

$$x' = x^2 \bmod n \tag{16}$$

计算会话信息 R_p、F:

$$R_p = \arg(v_p) \tag{17}$$

$$F = C_2 \oplus HRID\_c \tag{18}$$

c) 标签传输认证信息

最后将标签的最终会话密钥 k 和认证信息 x'', R_p, F 发送至新读写器。

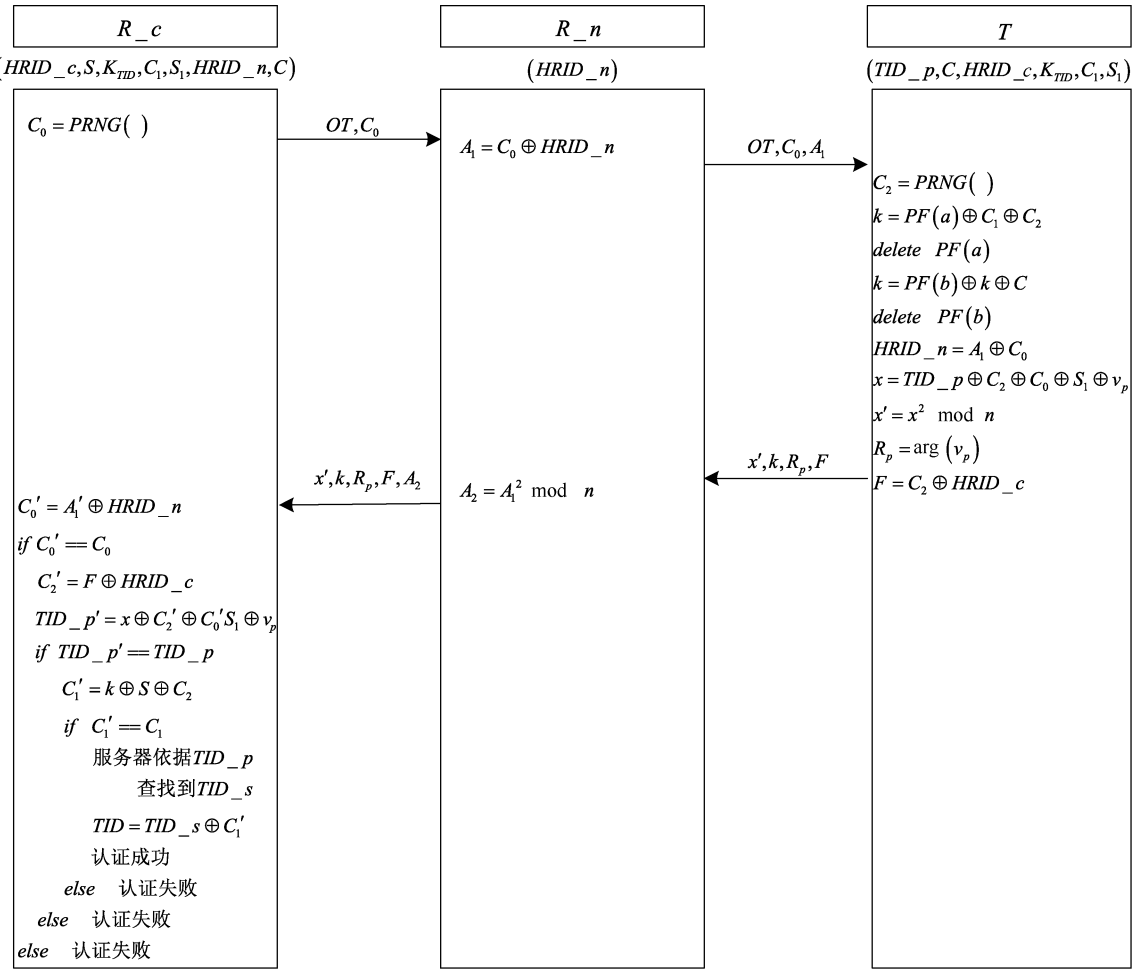

图 3 认证协议流程图

Figure 3 Flow chart of the authentication protocol

3.2.2 当前读写器接收认证信息

(1) 新读写器计算并传输认证信息

为了鉴定随机数 C_0 在传输过程中是否受到篡改, 计算确认消息:

$$A_2 = A_1^2 \bmod n \tag{19}$$

新读写器将消息 A_2, k, x', R_p, F 一起发送至当前读写器。

(2) 当前读写器接收认证信息并进行认证

a) 当前读写器对新读写器认证

将确认消息 A_2 利用存储的私钥 p、q 通过中国剩余定理求解出唯一解 A_1', 计算随机数 C_0':

$$C_0' = A_1' \oplus HRID\_n \tag{20}$$

依据 C_0、C_0' 进行认证, 认证原则为: 使用传输的值计算出的随机数 C_0', 与存储的随机数 C_0 相等, 确保随机数 C_0 未受到篡改。新读写器的认证规则为

$$\begin{cases} \text{如果} C_0 == C_0', \text{则} R\_n \text{认证成功} \\ \text{如果} C_0 \neq C_0', \text{则} R\_n \text{认证失败} \end{cases} \tag{21}$$

b) 当前读写器对标签认证

对标签的认证采用两步认证, 第一次认证是查看加密后的标识符是否被篡改, 在服务器中找到对应加密后标识符的 TID_s, 第二次认证是为了得到

标签的标识符。

计算随机数 C_2':

$$C_2' = F \oplus HRID\_c \tag{22}$$

将会话信息 x' 通过中国剩余定理求解出的唯一解 x，计算标签加密后的标识符 TID_p':

$$TID\_p' = x \oplus C_2' \oplus C_0' \oplus S_1 \oplus v_p \tag{23}$$

依据 TID_p、TID_p' 进行对标签的首次认证，认证原则为: 使用传输的值计算出加密后的标签标识符 TID_p'，必须与存储的标签标识符 TID_p 相等。标签首次认证规则为:

$$\begin{cases} \text{如果} TID\_p' == TID\_p, \ T\text{首次认证成功} \\ \text{如果} TID\_p' \neq TID\_p, \ T\text{首次认证失败} \end{cases} \tag{24}$$

计算随机数 C_1':

$$C_1' = k \oplus S \oplus C_2 \tag{25}$$

依据 C_1、C_1' 进行标签的最终认证，认证原则为: 使用传输的值计算出随机数 C_1'，必须与存储的随机数 C_1 相等。标签最终认证规则为:

$$\begin{cases} \text{如果} C_1 == C_1', \ T\text{最终认证成功} \\ \text{如果} C_1 \neq C_1', \ T\text{最终认证失败} \end{cases} \tag{26}$$

通过 TID_p 在服务器中搜索对应的 TID_s，并根据随机数 C_1' 计算出标签的唯一标识符 TID:

$$TID = TID\_s \oplus C_1' \tag{27}$$

并在服务器中查看是否与标签唯一标识符相等，若相等，表明当前读写器 R_c 对标签 T 认证成功，认证协议完成。

3.3 所有权转移阶段

所有权转移阶段由当前读写器 R_c 发起对标签的所有权从当前读写器 R_c 到新读写器 R_n 的转移，所有权转移流程如图 4 所示，具体步骤如下:

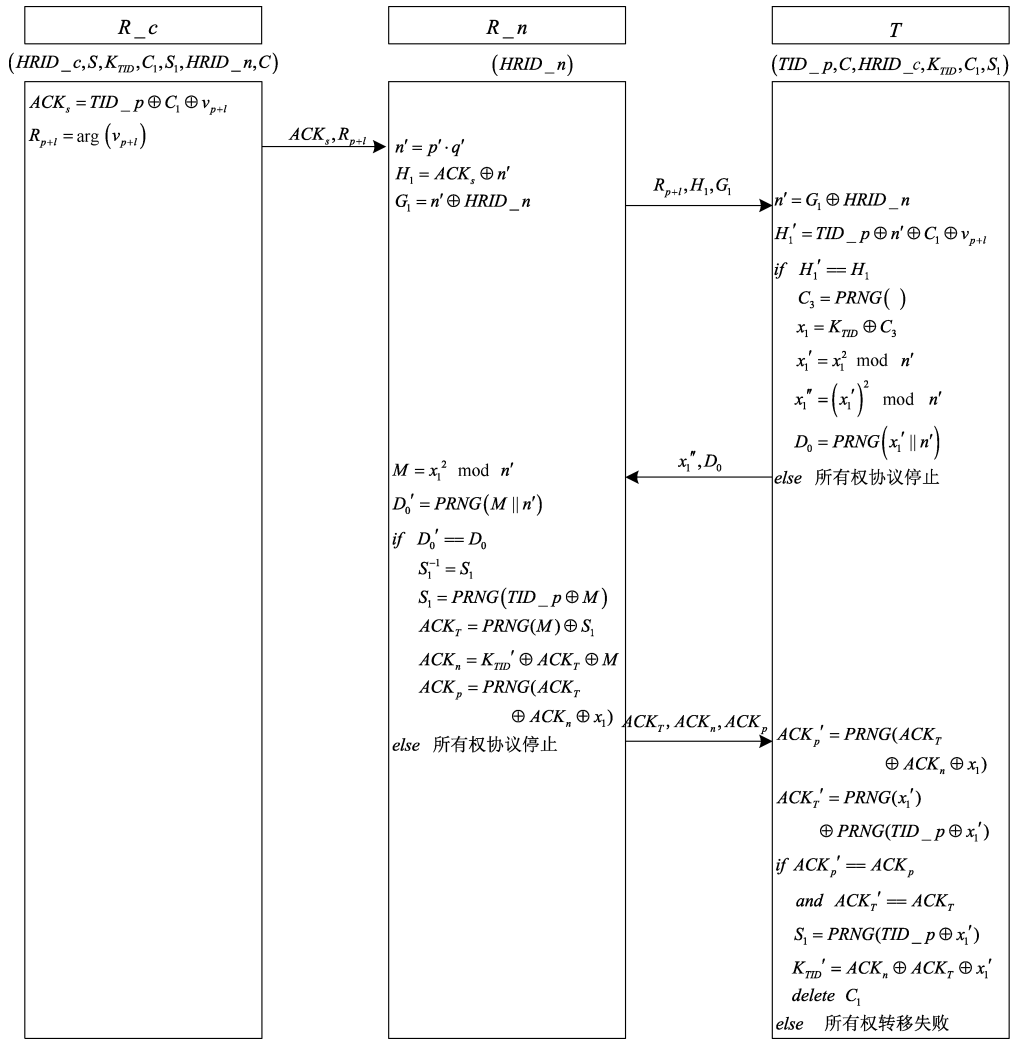

图 4 所有权转移流程图

Figure 4 Flow chart of ownership transfer

3.3.1 当前读写器发起转移

(1) 当前读写器发起并传输转移信息

当前读写器计算转移确认信息:

$$ACK_s = TID\_p \oplus C_1' \oplus v_{p+l} \tag{28}$$

转移确认消息 ACK_s 包括了标签加密后的标识符、随机数 C_1'、密钥串 K_{TID} 中第 $p+l$ 个子密钥 v_{p+l}, 转移确认消息将标签加密后的标识符 TID_p 和子密钥 v_{p+l} 加密发给新读写器, 使得新读写器获得与服务器搜索的接口。

计算会话消息:

$$R_{p+l} = \arg\left(v_{p+l} \right) \tag{29}$$

当前读写器将转移确认信息 ACK_s、会话消息 R_{p+l} 发送至新读写器。

(2) 新读写器传输信息

为了防止当前读写器假冒新读写器, 新读写器生成新的私钥 p'、q', 并计算新的公钥 n':

$$n' = p' \cdot q' \tag{30}$$

为了将公钥 n' 安全的传给标签, 新读写器计算标签已成功接收公钥 n' 的确认消息及传输加密公钥 n' 的传输消息:

$$H_1 = ACK_s \oplus n' \tag{31}$$

$$G_1 = n' \oplus HRID\_n \tag{32}$$

新读写器将会话消息 R_{p+l}、确认消息 H_1、传输消息 G_1 发送至标签。

(3) 标签计算确认并传输信息

计算公钥:

$$n' = G_1 \oplus HRID\_n \tag{33}$$

计算确认消息 H_1':

$$H_1' = TID\_p \oplus n' \oplus C_1 \oplus v_{p+l} \tag{34}$$

依据 H_1、H_1' 进行标签加密后标识符 TID_p 确认, 确认标签加密后标识符转移原则为: 使用传输的值计算得到的确认消息 H_1' 必须与传输的确认消息 H_1 相等。确认标签加密后标识符转移规则为:

$$\begin{cases} \text{如果} H_1 == H_1', \text{所有权转移继续} \\ \text{如果} H_1 \neq H_1', \text{所有权转移停止} \end{cases} \tag{35}$$

标签生成随机数 C_3, 计算传输原码:

$$x_1 = K_{TID} \oplus C_3 \tag{36}$$

为了保护随机数 C_3, 利用 Rabin 算法加密传输原码 x_1 得会话消息 x_1', 并使用 Rabin 算法加密 x_1' 得会话消息 x_1'':

$$x_1' = x_1^2 \bmod n' \tag{37}$$

$$x_1'' = \left(x_1' \right)^2 \bmod n' \tag{38}$$

计算传输消息:

$$D_0 = PRNG(x_1' \| n') \tag{39}$$

标签将会话消息 x_1''、传输消息 D_0 传递给新读写器。

3.3.2 新读写器接收转移信息

将会话信息 x_1'' 通过二次中国剩余定理求解出的唯一解 x_1, 计算会话消息:

$$M = x_1^2 \bmod n' \tag{40}$$

$$D_0' = PRNG(M \| n') \tag{41}$$

为了判断会话信息 x_1'' 在传输过程中是否收到篡改, 依据 D_0、D_0' 进行全局确认, 确认转移原则为: 使用传输的值计算出传输消息 D_0', 必须与传输的传输消息 D_0 相等。确认转移规则为:

$$\begin{cases} \text{如果} D_0 == D_0', \text{所有权转移继续} \\ \text{如果} D_0 \neq D_0', \text{所有权转移停止} \end{cases} \tag{42}$$

新读写器生成新密钥串 K_{TID}', 为了防止去同步化攻击, 将更新前的密钥保存; 为了防止假冒攻击, 更新密钥:

$$S_1^{-1} = S_1 \tag{43}$$

$$S_1 = PRNG(TID\_p \oplus M) \tag{44}$$

将更新后的密钥和密钥串传输给标签, 计算密钥及密钥串的确认消息:

$$ACK_T = PRNG(M) \oplus S_1 \tag{45}$$

$$ACK_n = K_{TID}' \oplus ACK_T \oplus M \tag{46}$$

$$ACK_p = PRNG(ACK_T \oplus ACK_n \oplus x_1) \tag{47}$$

将确认消息 ACK_T、ACK_n、ACK_p 发送至标签。

3.3.3 标签接收密钥更新消息

计算确认消息 ACK_p'、ACK_T':

$$ACK_p' = PRNG(ACK_T \oplus ACK_n \oplus x_1) \tag{48}$$

$$ACK_T' = PRNG(x_1') \oplus PRNG(TID\_p \oplus x_1') \tag{49}$$

为了确保标签接收到的密钥和密钥串未受到篡改, 依据确认消息 ACK_p、ACK_p' 和 ACK_T、ACK_T'

进行确认, 确认密钥转移原则为: 使用传输的值计算出确认消息 ACK_p'、ACK_T', 必须与传输的确认消息 ACK_p、ACK_T 相等。确认密钥转移规则为:

$$\begin{cases} \text{如果} ACK_p' == ACK_p \text{ and } ACK_T' == ACK_T, \\ \qquad\qquad \text{所有权转移继续} \\ \text{如果} ACK_p' \neq ACK_p \text{ or } ACK_T' \neq ACK_T, \\ \qquad\qquad \text{所有权转移停止} \end{cases} \tag{50}$$

计算更新后的共享密钥和密钥串:

$$S_1 = PRNG(TID\_p \oplus x_1') \tag{51}$$

$$K_{TID}' = ACK_n \oplus ACK_T \oplus x_1' \tag{52}$$

为了防止标签标识符 TID 的泄露, 删除随机数 C_1, 所有权转移协议结束。

4 协议的安全隐私性定义及其分析

使用 Vaudenay 模型并改进, 使其更好地应用于 RFID 所有权转移协议中, 来验证标签与读写器的安全与隐私性。

4.1 协议的安全隐私分析

定理 1、定理 2 和定理 3 证明了协议可抵御攻击者的去同步化攻击、假冒攻击等; 定理 4、定理 5 证明了协议满足强前向不可追踪性、后向不可追踪性。

4.1.1 协议的安全分析

定理 1. 当在 $PA_T = Narrow-Destructive$ 的攻击模型下, 即攻击者只能访问一次 Corrupt 预言机, 协议满足抵抗去同步化攻击。

证明.

攻击者通过阻止读写器与标签之间的传输或者通过修改确认消息 ACK_n 值来导致读写器与标签之间的共享密钥 K_{TID}' 不同步。

(1) 攻击者阻止读写器与标签之间的传输确认消息 ACK_n

由于标签未能接收到 ACK_n, 因此标签中的共享密钥串 K_{TID}' 未能更新, 标签下次所有权认证转移时使用的还是上次的共享密钥 K_{TID}, 但在本协议中, 因在读写器存放的上次的共享密钥还未删除, 因此, 依旧可以实现对标签的所有权认证转移。

(2) 攻击者修改确认消息 ACK_n

因为攻击者修改了确认消息 ACK_n 即 ACK_n', 所以 $ACK_n' \neq ACK_n$, 然而由公式(49)知 x_1' 使用的是标签中的值, 因此即使修改了 ACK_n 和 ACK_p 的值, 也不能通过标签的验证, 因此可抵御去同步攻击。

因此, 本协议可以抵御 $PA_T = Narrow-Destructive$ 攻击者的去同步攻击。

定理 2. 当在 $PA_R = Narrow-Strong$ 的攻击模型下, 协议满足抵抗内部读写器假冒攻击。

证明.

(1) 新读写器 R_n 假冒当前读写器 R_c

假设攻击者在第 i 次交互信息时攻击成功, 即攻击者会获取新读写器 R_n 发送而来的消息 $({}^ix'', {}^ik, {}^iR_p, {}^iF, {}^iA_2)$, 并发送给新读写器 R_n 消息 $({}^iHTID, {}^iR_{p+1}, {}^iACK_s)$。攻击者入侵当前读写器 R_c 可获得此时当前读写器 R_c 的内部信息 $({}^iK_{TID}, {}^ir_i, {}^ir_j, {}^iC, {}^iC_1)$, 若并通过当前读写器 R_c 窃听攻击, 会得到 ${}^iC_0$, 然而 ${}^iS, {}^ip, {}^iq$ 存放于服务器中, 认定其是安全的。因此若需要和标签认证, 则由公式(25)(27)可知

$$TID = {}^iTID\_s \oplus {}^ik \oplus {}^iC_2 \oplus {}^iS \tag{53}$$

由公式(53)知, 需要 ${}^iTID\_s$ 和 ${}^iS$, 而 ${}^iS$ 存放在服务器且未被盗取, 且在初始化时, 标签中的共享密钥 S 已被删除, ${}^iTID\_s$ 与 ${}^iTID\_p$ 在服务器中是对应的, 即使知晓 ${}^iTID\_p$ 也未知 ${}^iTID\_s$。因此计算出 TID 的概率为

$$\begin{aligned} P(TID) &= P({}^iTID\_s) \cap P({}^ik) \cap P({}^iC_2) \cap P({}^iS) \\ &= \frac{1}{2^{96}} \times 1 \times 1 \times \frac{1}{2^{96}} = \frac{1}{2^{192}} \approx 0 \ll \varepsilon \end{aligned} \tag{54}$$

因此 $Narrow-Strong$ 等级的新读写器 R_n 假冒 R_c 的概率近似为零。

(2) 当前读写器 R_c 假冒新读写器 R_n

假设攻击者在第 i 次交互信息时进行攻击, 有以下两种情况进行分析:

i. 攻击者使用 $Observe(R\_c, R\_n)$ 预言机获取当前读写器 R_c 发送给新读写器 R_n 的会话消息 $({}^iR_{p+1}, {}^iACK_s)$, 如果攻击者此时攻击成功, 表明新读写器 R_n 还没有参与会话消息 (H_1, G_1) 的生成和给标签发送会话消息 $({}^iR_{p+1}, {}^iG_1, {}^iH_1)$。当前读写器 R_c 利用 $Observe(R\_n, T)$ 预言机获取新读写器 R_n 与标签 T 之间的会话消息, 无法推算出新读写器的私钥 p'、q'。

ii. 攻击者使用 $Observe(R\_n,T)$ 预言机获取新读写器 R_n 接收到标签 T 会话消息 $\left({}^{i}x_1'',{}^{i}D_0\right)$, 如果攻击者此时攻击成功, 表明新读写器 R_n 还没有参与会话消息 $\left({}^{i}ACK_T,{}^{i}ACK_n,{}^{i}ACK_p\right)$ 的生成。若要假冒成功, 则需要计算确认消息 $\left({}^{i}ACK_T,{}^{i}ACK_n,{}^{i}ACK_p\right)$ 值, 由公式(48)、(49)、(51)知, 则需要知晓存储在新读写器 R_n 中的私钥 p、q, 但当前读写器 R_c 中并不存在。

因此 $Narrow-Strong$ 等级的当前读写器 R_c 假冒新读写器 R_n 的概率几乎为零。

因此, 协议可抵抗 $Narrow-Strong$ 等级的攻击者的内部读写器攻击。

定理 3. 当在 $PA_T = Narrow-Destructive$ 的攻击模型下, 协议满足抵御标签假冒攻击。

证明.

假设攻击者在第 i 次交互信息时攻击成功, 分两种情况:

(1) 在认证阶段, 攻击者会获取 R_n 发送而来的消息 $({}^{i}C_0,{}^{i}A_2)$, 并发送给 R_n 消息 $({}^{i}x_1'',{}^{i}k,{}^{i}R_p,{}^{i}F)$。

攻击者计算 ${}^{i}k$ 需要知晓 $PF(a)$和 $PF(b)$, 而 PUF 函数是依据电路在制造过程中工艺偏差, 使不同 PUF 函数产生的响应序列具有唯一性和不可复制性, 攻击者无法通过数学运算模拟 $PF(a)$和 $PF(b)$, 且攻击者进行物理入侵将对标签的 PUF 电路造成不可逆的破坏, 导致 PUF 电路失活, 使得 $PF\left(Z,x\right)' \neq PF\left(Z,x\right)$。因此攻击者对标签的入侵无法获得 ${}^{i}k$ 的全部参数, 攻击者无法成功计算 ${}^{i}k$, 且 ${}^{i}F$, ${}^{i}A_2$ 均有随机数生成, 因此在认证阶段满足抵御标签假冒攻击。

(2) 在所有权转移阶段, 攻击者想要获取 R_n 发送给标签的更新的密钥串 K_{TID}' 和更新的密钥 S_1'。

1) 想获取标签的更新的密钥串 K_{TID}'

由公式(36)可知, 若要求得 K_{TID}', 则:

$$K_{TID}' = x_1 \oplus C_3 \tag{55}$$

计算 ${}^{i}x_1$ 需要 ${}^{i}x_1''$ 和 n', 而攻击者无法获得 n' 对应的两个大素数 p' 和 q', 因而其不能获得 x_1; 此外, 攻击者获取 C_3, 而 C_3 是一个 96 位随机数, 在每次的会话中随机数都是不同的, 因此, 计算出 K_{TID}' 的概率为:

$$P\left(K_{TID}'\right) = \frac{1}{2^{96}} \times \frac{1}{2^{96}} = \frac{1}{2^{192}} < \varepsilon \tag{56}$$

2) 想获取标签的更新的密钥 S_1

有公式(44)(45)可知, 若要求得 ${}^{i}S_1$, 有两种方式:

①根据公式(44), 若要计算出 ${}^{i}S_1$, 需要知道 ${}^{i}PTID$、${}^{i}x_1'$, 因为 ${}^{i}x_1'$ 在传输过程中是未知的, 而 ${}^{i}PTID \oplus {}^{i}x_1'$ 作为伪随机数种子来生成随机数, 因此得到 ${}^{i}S_1'$ 的概率为:

$$P\left({}^{i}S_1\right) = \frac{1}{2^{96}} < \varepsilon \tag{57}$$

②根据公式(45), 若要计算出 ${}^{i}S_1$, 需要知道 ${}^{i}ACK_T$、${}^{i}x_1'$, ${}^{i}ACK_T$ 因是传输过程中可被窃取到, 因此得到 ${}^{i}S_1$ 的概率为:

$$P\left({}^{i}S_1\right) = 1 \times \frac{1}{2^{96}} = \frac{1}{2^{96}} < \varepsilon \tag{58}$$

因此在转移阶段满足抵御标签假冒攻击。

因此协议可抵御 Narrow-Destructive 等级的攻击者的标签假冒攻击。

4.1.2 协议的隐私分析

定理 4. 在 $Narrow-Strong$ 等级攻击者的攻击模型下, 协议满足强前向不可追踪性。

证明.

使用改进的 Vaudenay 模型的预言机对强前向不可追踪性的证明算法, 如图 5 所示。攻击者通过入侵和监听标签的第 i 次会话, 即使用 Corrupt(•)和 Observe(•)预言机, 得到标签第 i 次会话的内部信息 $\left(TID\_p,{}^{i}C,HRID\_c,{}^{i}K_{TID},C_1,S_1\right)$ 和会话记录, 见步骤 3～8, 且通过 Observe(•)预言机能监听到标签第 i+1 次的会话信息, 但不能得到密钥串 ${}^{i+1}K_{TID}'$, 见步骤 12～16。因此攻击者若要得到第 i+1 次标签与新读写器的密钥串 ${}^{i+1}K_{TID}'$, 通过公式(52)可知, 由步骤 16 中已知发送至标签中的确认消息 ACK_n、ACK_T, 还需知晓会话信息 ${}^{i+1}x_1'$, 则只有以下两种情况:

(1)通过步骤 15 中窃听到的 ${}^{i+1}x_1''$ 的值来计算会话信息 ${}^{i+1}x_1'$

计算会话信息 ${}^{i+1}x_1'$:

$$x_1'' = \left(x_1'\right)^2 \mod n' \tag{59}$$

即使攻击者知晓公钥 n', 也由于大素数的数学难题, 不能分解得到私钥 p',q', 从而也不能通过中国剩余定理来求得 ${}^{i+1}x_1'$。

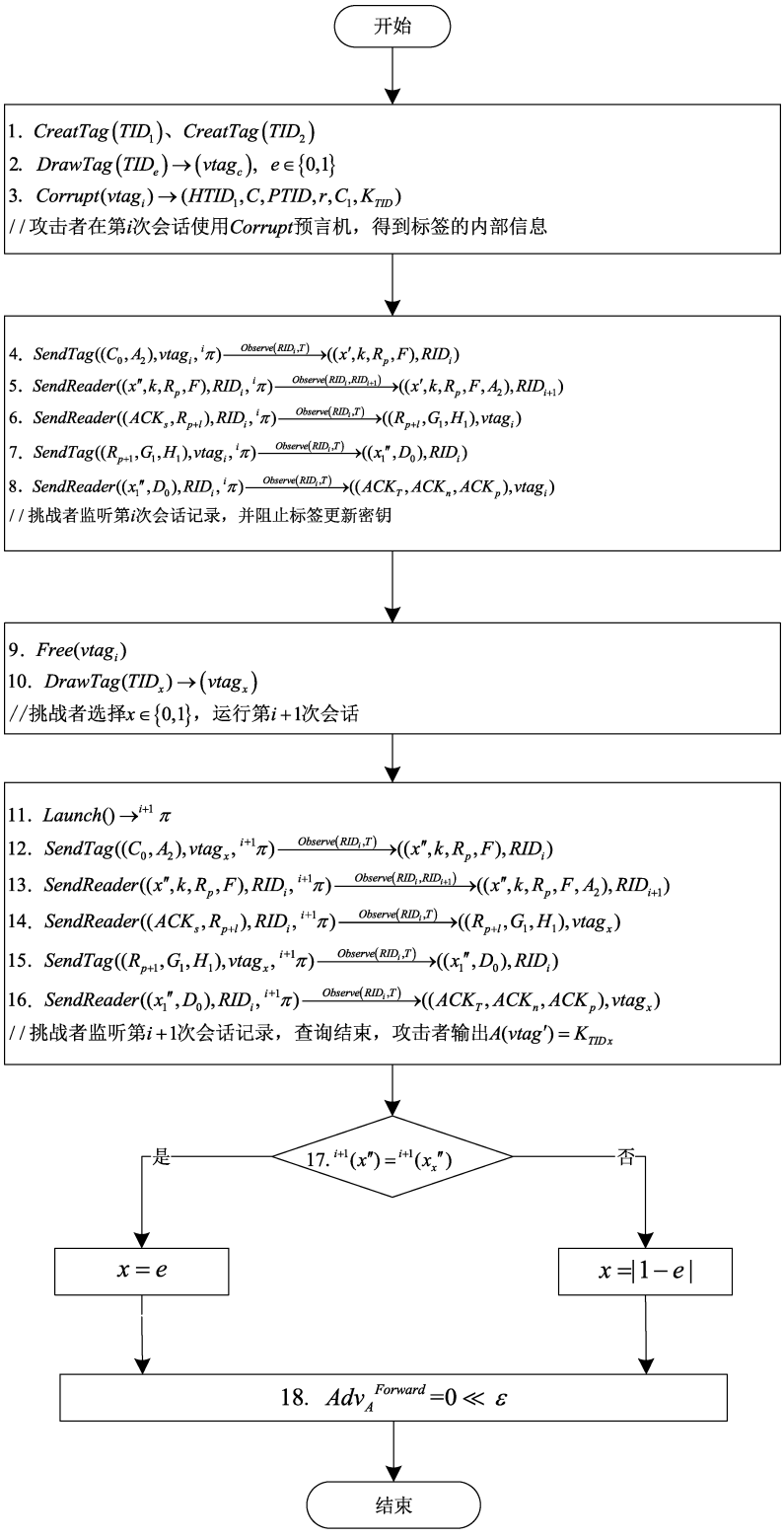

图 5　强前向不可追踪性证明

Figure 5　Proof of strong forward untraceability

(2) 直接使用公式(36) ${}^{i+1}x_1=K_{TID}\oplus C_3$ 求得 ${}^{i+1}x_1$ 来计算会话信息 ${}^{i+1}x_1'$

此时, 攻击者必须获取密钥串 K_{TID} 和随机数 C_3, 虽然 K_{TID} 可通过步骤 3 获取, 但 C_3 是一随机数, 在第 i 次与第 i+1 次值是不同的, 因此攻击者在已知第 i 次标签信息和第 i+1 次通信信息时, 不能求得 ${}^{i+1}x_1$。因此, $Narrow-Strong$ 等级的攻击者攻击时, 无法获得 ${}^{i+1}x_1'$, 攻击者强前向追踪的概率 $Adv_A^{Forward}\ll\varepsilon$, 因

此本协议满足强前向不可追踪性。

定理 5. 在 *Narrow – Strong* 等级攻击者的攻击模型下, 协议满足后向不可追踪性能。

证明.

使用改进的 Vaudenay 模型的预言机对后向不可追踪性的证明算法如图 6 所示。*Narrow – Strong* 等

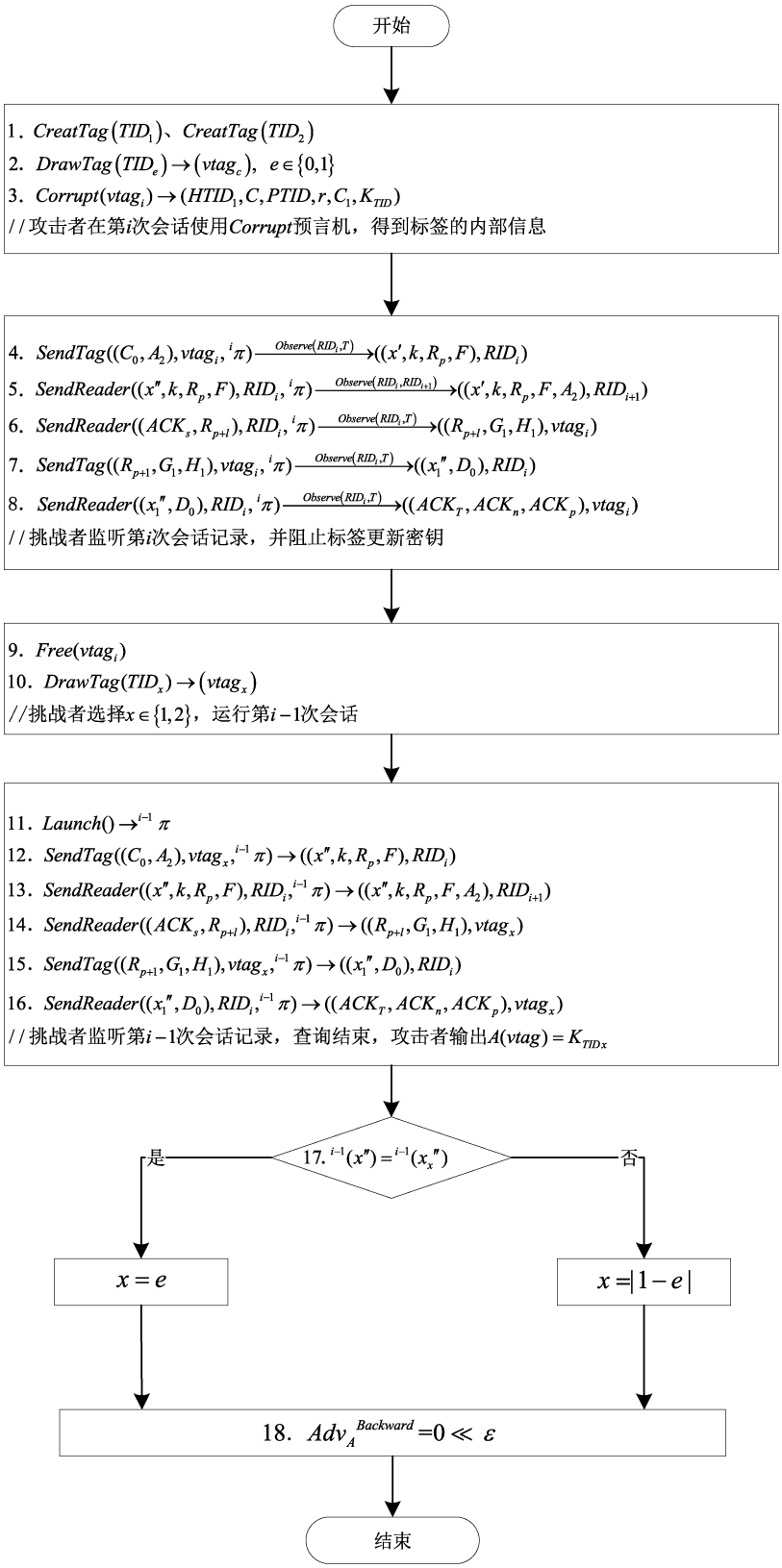

图 6　后向不可追踪性证明

Figure 6　Proof of backward untraceability

级的攻击者通过入侵和监听标签的第 i 次会话, 即使用 Corrupt(•)和 Observe(•)预言机, 得到标签第 i 次会话的内部信息 $\left(TID\_p,^{i}C,HRID\_c,^{i}K_{TID},C_1,S_1\right)$ 和会话记录, 见步骤 3～8。攻击者无法推断第 i–1 次标签密钥 $^{i-1}K_{TID}$, 且由步骤 12～16 可知, 第 i–1 次不能监听到消息的传递, 由公式(36)(38)可知, 无法推断第 i–1 次标签的传输原码 $^{i-1}x_1$ 及会话消息 $^{i-1}x_1''$, 因此无法对后向会话中的标签进行区分, 攻击者后向追踪的概率 $Adv_A^{Backward} \ll \varepsilon$, 协议满足后向不可追踪性。

4.2 协议性能比较

本文将改进的协议 OTPORM 与文献[6-7, 13-14]进行对比。

4.2.1 安全隐私保护比较

安全隐私对比如表 4 所示。文献[6-7, 13-14]均存在若标签被强行暴力破解, 可以获得标签的 ID, 可能被攻击或追踪。文献[13]密钥更新是标签先更新之后再 TTP 更新, 因此若在标签更新之后阻止标签更新, 则会现同步攻击; 文献[6]虽然满足前向不可追踪性, 但不满足强前向不可追踪性, 且存在着内部读写器假冒攻击的威胁; 文献[7,14]在标签端使用了 hash 函数来实现了标签的前后向不可追踪和各种安全性能, 但 hash 加密量大, 不适合低成本标签, 且不满足 EPC C1G2 标准。OTPORM 协议使用 PUF 将标签 ID 进行加密和保护随机数, 并使用 Mod 和伪随机数生成器来解决攻击者的假冒问题, 且适用于 EPC C1G2 标准。

表 4 协议安全隐私对比

Table 4 Protocol Security and Privacy Comparison

安全隐私	文献[6]	文献[7]	文献[13]	文献[14]	本协议
去同步攻击	×	√	×	√	√
读写器假冒攻击	×	√	√	√	√
标签假冒攻击	√	√	√	√	√
暴力攻击	×	×	×	×	√
强前向不可追踪	×	√	√	√	√
后向不可追踪	√	√	×	√	√
满足 EPCC1G2	√	×	√	×	√

注: √表示能抵御或满足, ×表示不能抵御或不满足

4.2.2 标签计算开销比较

OTPORM 协议将标签端的计算开销与文献[6-7, 13-14]进行对比, 如表 5 所示。其中, N1 表示标签存储密钥的数量, N2 表示标签加密函数的类别与数量, N3 表示伪随机数生成的个数, N4 表示标签信息交换的次数, 因异或运算量低, 可忽略不计, 因此未将异或加入标签计算开销中。

表 5 协议标签计算开销对比

Table 5 Comparison of calculation costs of tag

协议	N1	N2	N3	N4
文献[6]	4	1Hash+3Mod+4PRNG	3	7
文献[7]	4	5Hash+3Mod	3	5
文献[13]	4	8PRNG	5	2
文献[14]	4	2Hash+4Mod+5PRNG	5	5
本文协议	6	3Mod+4PRNG+3PUF	3	5

在文献[6-7]中, 均在标签端使用了 hash 函数, 虽然增强了标签的安全性, 但这是不满足 EPC C1G2 标准, 在 OTPORM 协议中增加了 PUF 电路, 因 PUF 电路相比较于 hash 电路, 电路的减少电路的消耗, 虽然相对于文献[13]来说提高了标签的成本, 但也提高了协议的安全与隐私性。

4.2.3 耗时对比

采用转移时间作为算法的耗时指标。所有权转移时间是指端到端的延迟时间, 即从当前读写去发出 OT 命令到标签完成所有权转移的时间, 即包括了读写器端、标签端、搜索服务器端的总时间。对 OTPORM 及文献[13]和文献[7]所有权转移时间进行了仿真, 仿真环境为 MATLAB。

不同协议的所有权转移时间对比如图 7 所示, 当标签数为 10000 个时, OTPORM 协议中某个标签平均搜索时间为 0.00449s, 所有标签的执行时间为 0.0037s, 读写器耗时为 21.70s, 而文献[13]所有的标签的执行时间为 0.0103s, 读写器耗时为 109.86s, 文

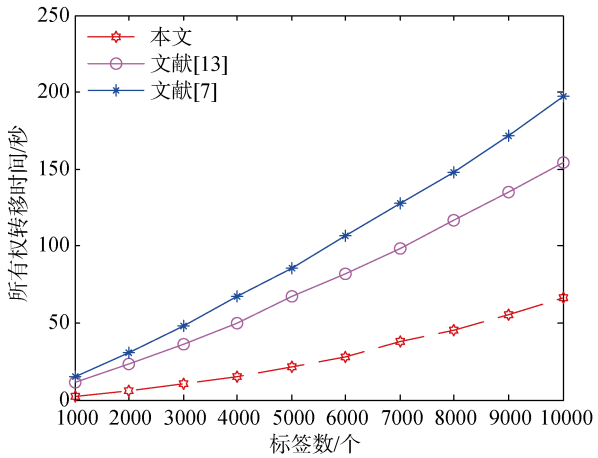

图 7 所有权转移时间对比

Figure 7 Comparison of ownership transfer time

献[7]的所有的标签的执行时间为 0.0032s, 读写器耗时为 152.4s, 因此相比较于文献[7, 13], OTPORM 协议的总时间降低。文献[13]由于采用了太多的伪随机数加密, 因此使得总时间增多, 文献[7]由于采用 hash 运算, 相比伪随机数加密, hash 加密的时间增多, 也同样增加了转移时间, 而文献[7, 13]与本文都是一个标签只需遍历服务器一次, 因此搜索服务器相同。由实验可知, OTPORM 协议在所有权转移时间上有较大优势。

5 总结

本文的基于 PUF 的开环 RFID 所有权转移 OTPORM 协议解决现有所有权转移协议中存在的内部读写器攻击、暴力攻击、强前向不可追踪性, 并使用 Vaudenay 模型来证明其的隐私性。与其他所有权转移协议相比较, OTPORM 协议具有较高的安全与隐私性, 且有着较好的开销。但如何将 PUF 更好的融入供应链环境中、提高更多标签运算和增强加密算法的安全级别是下一步研究的重点。

参考文献

[1] Munilla J, Burmester M, Peinado A, et al. “RFID Ownership Transfer with Positive Secrecy Capacity Channels,” *Sensors*, vol. 17, no. 1, pp. 53-61, 2016.

[2] Wu Weimin, Chen Chaoxiong, Lan Yijiang, et al. “Ownership transfer protocol based on Rabin encryption algorithm for RFID tags,” *Journal of Computer Applications*, vol. 34, no. 5, pp. 1531-1535, 2017.
(吴伟民, 陈超雄, 蓝炯江, 等. 基于 Rabin 加密算法的 RFID 标签所有权转移协议[J]. *计算机应用研究*, 2017, 34(5): 1531-1535.)

[3] Ray B, Abawajy J, Chowdhury M, et al. “Universal and secure object ownership transfer protocol for the Internet of Things,” *Future Generation Computer Systems*, vol. 78, pp. 838-849, 2017.

[4] Kulseng L, Yu Z, Wei Y, et al. “Lightweight mutual authentication and ownership transfer for RFID systems,” *INFOCOM*, 2010 Proceedings IEEE. IEEE, pp. 1-5, 2010.

[5] Li Q S, Xu X L, Chen Z. “PUF-Based RFID Ownership Transfer Protocol in an Open Environment,” International Conference on Parallel and Distributed Computing, *Applications and Technologies*(IEEE Computer Society), pp. 131-137, 2014.

[6] Doss R, Zhou W, Yu S. Secure RFID Tag Ownership Transfer Based on Quadratic Residues[J]. *IEEE Transactions on Information Forensics & Security*, vol. 8, no. 2, pp. 390-401, 2013.

[7] Chen Xiuqing, Cao Tianjie, Zhai Jingxuan. Provable Secure for the Lightweight RFID Ownership Transfer Protocol. *Journal of Electronics and Information Technology*, vol. 38, no. 8, pp. 2091-2098, 2016.
(陈秀清, 曹天杰, 翟靖轩. 可证明安全的轻量级 RFID 所有权转移协议[J]. *电子与信息学报*, 2016, 38(8): 2091-2098.)

[8] Shen Jinwei, Ling Jie. “Improved Ultra-lightweight Authentication of Ownership Transfer Protocol for RFID Tag,” *Computer Science*, vol. 41, no. 12, pp. 125-128(in Chinese), 2014.
(沈金伟, 凌捷. 一种改进的超轻量级 RFID 所有权转移协议[J]. *计算机科学*, 2014, 41(12):125-128.)

[9] Wang Yu. Security Authentication Study of Anti-cloning Tag[D]. Nanjing University of Posts and Telecommunications, 2014.
(王玉. 防克隆标签的安全认证研究[D]. 南京邮电大学, 2014.)

[10] Vaudenay S. “On Privacy Models for RFID,” Advances in Cryptology – *ASIACRYPT* 2007. Springer Berlin Heidelberg, 2007: 68-87.

[11] Kaul S D, Awasthi A K. “Privacy Model for Threshold RFID System Based on PUF,” *Wireless Personal Communications*, pp. 1-26, 2017.

[12] Edelev S, Taheri S, Hogrefe D. “A secure minimalist RFID authentication and an ownership transfer protocol compliant to EPC C1G2,” *IEEE International Conference on Rfid Technology and Applications*. IEEE, pp. 126-133, 2016.

[13] Sundaresan S, Doss R, Zhou W, et al. “Secure ownership transfer for multi-tag multi-owner passive RFID environment with individual-owner-privacy,” *Computer Communications*, vol. 55, no. C, pp. 112-124, 2015.

[14] Wang Ping, Zhou Zhiping. “An Improved RFID Ownership Transfer Protocol Based on Cloud,” *Netinfo Security*, vol. 8, pp. 60-68, 2017.
(王萍, 周治平. 一种基于云的 RFID 所有权转移协议的改进[J]. *信息网络安全*, 2017(8): 60-68.)

韦 民 于 2012 年在南京工程学院自动化(数控技术)专业获得学士学位。现在江南大学控制工程专业攻读硕士学位。研究领域为物理不可克隆函数、无线射频识别技术。研究兴趣包括: 射频识别安全协议等。Email: jiangnan_weimin@163.com

孙子文 于 2009 年在江南大学控制科学与工程专业获得博士学位。现任江南大学物联网工程学院教授。研究领域为模式识别与人工智能、无线传感网络理论与技术、信息安全。研究兴趣包括: 无线通信安全等。Email: sunziwen@jiangnan.edu.cn