文章编号:1671-6833(2023)02-0046-07

基于 PUF 的高安全性轻量级 RFID 三方认证协议

范文兵, 常正泰, 艾璐琳, 孔德涵

(郑州大学 电气与信息工程学院,河南 郑州 450001)

摘 要: 针对射频识别(RFID)三方认证协议存在的安全需求和资源开销难以折中的问题,提出一种基于 PUF 的高安全性轻量级 RFID 三方认证协议(PHL-RTAP)。PHL-RTAP 协议利用物理不可克隆函数(PUF)实现对标签身份的安全认证,保护标签免受物理克隆攻击,同时降低了标签开销,满足资源受限的 RFID 系统的需求;采用二次剩余算法实现对阅读器身份的安全认证,保护阅读器的数据隐私;引入随机数抵抗重放攻击,同时保证了阅读器与标签的匿名性和不可追踪性。PHL-RTAP 协议实现了服务器、阅读器和标签之间完整的三方认证,可以依据需求扩展 RFID 系统中阅读器和标签规模,使其适用于大规模标签的 RFID 系统。安全分析表明:PHL-RTAP 协议能够有效抵抗追踪、重放、物理克隆和去同步化等多种恶意攻击,使用 BAN 逻辑分析法和 AVISPA 工具证明了协议的安全性。与近期协议的对比分析显示:PHL-RTAP 协议弥补了同类 RFID 协议的安全缺陷,并且计算开销、通信开销和标签存储开销等资源开销都较低,在保证高安全性的同时实现了轻量级,适用于资源受限的 RFID 三方认证场景。

关键词: 射频识别; 物理不可克隆函数; 二次剩余; 三方认证; 形式化分析

中图分类号: TP309 **文献标志码**: A **doi**:10.13705/j.issn.1671-6833.2023.02.002

近年来,随着物联网技术的发展,射频识别(radio frequency identification, RFID)凭借其无物理接触认证[1]和快速识别等特性,被广泛应用于库存管理、供应链和目标追踪等方面。传统上,通常把阅读器和服务器认定为一个整体,然而,随着 RFID 产业的发展,这种 RFID 两方认证协议已不能满足应用场景的需求。新型的采用移动无线阅读器的 RFID 三方认证协议逐渐成为主流。由于移动阅读器工作在开放信道,攻击者可以轻松监听信道上传输的关键信息,从而威胁 RFID 系统的安全。因此,设计高安全性的轻量级 RFID 三方认证协议成为新形势下 RFID 产业亟待解决的问题。

针对 RFID 三方认证系统的安全问题,国内外学者已经展开大量研究。刘鹏等[2]提出基于哈希函数的移动 RFID 认证协议,该协议将主要计算开销集中到后台服务器。然而,后台服务器需要遍历搜索才能确认标签和阅读器的合法性,这极大降低了认证效率,不仅使协议容易受到拒绝服务攻击,还不利于协议的规模扩展。王国伟等[3]改进了上述问题,后台服务器只需遍历搜索阅读器,这在一定程度上降低了服务器搜索压力,但服务器搜索开销仍会随着阅读器数量的增加而大幅上升。

为了提高 RFID 系统的安全性,一些学者把经典的加密算法引入 RFID 认证协议。Farash 等[4]提出一种基于椭圆曲线加密技术的 RFID 认证协议。Xiao 等[5]提出一种基于云的 RFID 相互认证协议,使用哈希操作和对称算法以确保标签匿名性。上述重量级协议均采用高安全性的经典加密算法,不适合用于资源受限的 RFID 标签。

为了解决轻量级 RFID 标签无法负担经典加密算法的问题,Chien[6]提出基于循环移位等位流操作的 SASI 协议,然而,该协议容易受到跟踪攻击、代数攻击和去同步化攻击。Tian 等[7]提出基于比特置换的 RAPP 协议,但是该协议不能抵抗去同步化攻击。Chiou 等[8]提出基于二次剩余定理的三方认证协议,协议以明文形式传输标签伪标识符,攻击者可以阻止标签伪标识符更新来追踪标签位置。

攻击者可以通过物理探针等手段获取上述协议[2-8]中标签内部的关键信息,甚至可以克隆电子标签。为了解决这个问题,王利等[9]使用物理不可

收稿日期:2022-09-13;**修订日期**:2022-10-29

基金项目:河南省科技攻关项目(192102210086)

作者简介:范文兵(1969—),男,河南周口人,郑州大学教授,博士,主要从事信息安全、嵌入式系统与信息处理等研究,E-mail:iewbfan@zzu.edu.cn。

引用本文:范文兵,常正泰,艾璐琳,等. 基于 PUF 的高安全性轻量级 RFID 三方认证协议[J]. 郑州大学学报(工学版),2023,44(2):46-52. (FAN W B, CHANG Z T, AI L L, et al. High-security lightweight RFID triple authentication protocol based on PUF[J]. Journal of Zhengzhou University(Engineering Science), 2023, 44(2): 46-52.)

克隆函数(physical unclonable function,PUF)作为加密原语生成密钥。但是,该协议缺少对阅读器的合法性认证,没有实现完整的三方认证,另外标签端使用哈希函数对 ID 加密,增加了电子标签开销。此外,学者们[2-3,5,9]提出的认证协议容易受到针对阅读器的重放攻击,服务器无法确认这些数据来自合法阅读器还是攻击者,这危及了 RFID 系统的安全性。

针对上述问题,本文提出了一种基于 PUF 的高安全性轻量级 RFID 三方认证协议(PHL-RTAP)。PHL-RTAP 协议使用 PUF 和二次剩余算法保证标签和阅读器的安全性,并结合随机数实现了完整的 RFID 三方认证,同时降低了协议的成本开销,在安全需求和资源开销之间达到了折中的目的。

1　基于 PUF 的 RFID 三方认证协议

1.1　物理不可克隆函数

物理不可克隆函数(PUF)利用制造过程中产生的差异来唯一识别物理对象,攻击者不能对其进行物理或软件克隆,确保了其“不可克隆性”[10]。根据输入-输出对(激励-响应对,CRP)规模,可以把 PUF 分为强 PUF 和弱 PUF。

1.2　RFID 三方系统攻击模型

本文考虑的 RFID 三方系统攻击模型如图 1 所示,A_T 和 A_R 分别表示敌手对标签和阅读器发起的攻击,$A_{T\text{-}R}$ 和 $A_{R\text{-}D}$ 分别表示敌手对阅读器和标签之间以及阅读器和后台服务器之间信道发起的攻击。

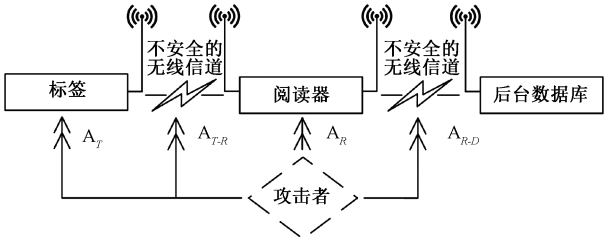

图 1　RFID 三方系统攻击模型

Figure 1　RFID triple system attack model

在本文的 RFID 系统攻击模型中,敌手可以在认证阶段监听、截获和重放通信链路上的信息流;敌手可以发起去同步化攻击和拒绝服务攻击;敌手可以发起位置追踪攻击[11];特别的,敌手可以对标签发起物理克隆攻击,以复制海量的“克隆标签”。

2　PHL-RTAP 协议

PHL-RTAP 协议由初始化阶段和认证阶段两部分组成。协议中所用符号如表 1 所示。对于 n 位向量 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$,$\mathrm{HD}(\boldsymbol{X},\boldsymbol{Y})$ 运算如下式:

$$\mathrm{HD}(\boldsymbol{X},\boldsymbol{Y})=\sum_{i=0}^{n-1}(\boldsymbol{X}[i]\oplus\boldsymbol{Y}[i])。\tag{1}$$

PHL-RTAP 协议采用文献[12]中 TVO-APUF 函数,该强 PUF 电路主要由 LFSR 和 APUF 两部分组成,在不影响 APUF 性能的前提下,可以提高底层 APUF 抵抗建模攻击的能力。此外,PHL-RTAP 协议中的标签端内部需要集成 PRNG 函数,PRNG 函数和 TVO-APUF 内部的 LFSR 函数具有共通性[13],因此,LFSR 可以与 PRNG 复用底层的硬件电路。

2.1　初始化阶段

初始化阶段完成后,标签 i 存储 TID^i 和 $SC_{l+1}{}^i$,阅读器 j 存储 RID^j、s_{SR} 和 m,后台服务器存储 TID^i、$SC_l{}^i$、$SR_l{}^i$、$SC_{l+1}{}^i$、$SR_{l+1}{}^i$、RID^j、s_{SR}、g、h。

设 y 和 y' 是两个正整数,若 $y^2\equiv y'\pmod m$,则称 y' 是 m 的二次剩余。其中,m 作为公钥存储在服务器,g 和 h 作为私钥存储在阅读器。服务器使用中国剩余定理(Chinese remainder theorem, CRT)反解 y' 时,会得到 4 个解。为了避免 y' 的非唯一解增加服务器计算开销,服务器使用 $(y^2)^2$ 代替上式的 y^2,即 $(y^2)^2\equiv y''\pmod m$,可以计算出唯一解[14]。

表 1　协议中的符号定义

Table 1　Symbol definition of the protocol

符号	含义
TID^i/RID^j	标签 i/阅读器 j 的身份标识符
$r/r_R/r_T$	服务器/阅读器/标签产生的随机数
s_{SR}	服务器与阅读器之间的共享密钥
g, h, m	两个大素数和两者的乘积
PRNG	伪随机数发生器
TVO-APUF^i	抗建模攻击的 PUF 运算[12]
$SC_l{}^i/SC_{l+1}{}^i$	$TVO\text{-}APUF^i$ 前/后一轮激励
$SR_l{}^i/SR_{l+1}{}^i$	$TVO\text{-}APUF^i$ 前/后一轮响应
⊕/mod/‖	异或运算/取余运算/连接运算
HD /τ	汉明距离运算/认证阈值

2.2　认证阶段

PHL-RTAP 协议认证阶段的具体步骤如下。

步骤 1　阅读器 j 向后台服务器发送一个请求 $Request$。

步骤 2　后台服务器收到请求认真消息后,产生一个随机数 r 发送给阅读器 j。

步骤 3　阅读器 j 收到 r 后,向通信范围内的标签广播 $Query$,并发送随机数 r。

步骤 4　标签 i 接收到 $Query$ 和 r 后,首先产生一个随机数 r_T,然后计算 $x=TID^i\oplus r$、$MT=SC_{l+1}{}^i\oplus r_T$,并从存储区取出 $SC_{l+1}{}^i$,接着生成:$R_l=\mathrm{TVO\text{-}APUF}^i(SC_{l+1}{}^i)$、$C_{l+1}{}^i=SC_{l+1}{}^i\oplus r\oplus r_T$、$R_{l+1}=\mathrm{TVO\text{-}}$

APUF^i($C_{l+1}{}^i$)。MT 通过 $SC_{l+1}{}^i$ 保护标签随机数 r_T、x 通过 r 保护标签 i 的 TID^i;输入 TVO-APUF^i 的激励 $SC_{l+1}{}^i$ 由服务器产生的 r 和标签产生的 r_T 共同决定其更新,这样无论攻击者假冒任何一方都无法完全控制 $SC_{l+1}{}^i$ 的更新。最后,标签 i 将 MT、x、R_l 和 R_{l+1} 发送给阅读器 j。

步骤5 阅读器 j 收到标签 i 发送的消息后,产生随机数 r_R,并计算 $y = RID^j \oplus r_R \oplus r$、$y'' = (y^2)^2 (\mathrm{mod}\ m)$、$MR = s_{SR} \oplus r_R$。$y$ 通过 r 和 r_R 实现阅读器 j 的动态不可追踪性,y'' 则进一步保护标识符 RID^j 的匿名性。最后,阅读器 j 把接收到的 MT、x、R_l、R_{l+1} 和 y''、MR 一并发送给后台服务器。

步骤6 后台服务器接收到阅读器 j 发送的消息后,首先,提取 y''、MR 以准备对阅读器 j 的认证;其次,根据存储的2个大素数 g 和 h,使用 CRT 反解 y'' 得到唯一的 y;再次,计算 $r_R = s_{SR} \oplus MR$、$RID^{j\prime} = y \oplus r_R \oplus r$,若在服务器的 RID 库中存在 $RID^j = RID^{j\prime}$,则阅读器 j 成功被服务器认证;最后,服务器计算针对阅读器 j 的确认消息:$ACK_R = \mathrm{PRNG}(RID^{j\prime} \oplus r_R)$。若 RID 库中不存在 $RID^j = RID^{j\prime}$,认证停止。

接下来,后台服务器提取 MT、x、R_l 和 R_{l+1} 以准备认证标签 i:首先,服务器使用 r 与消息 x 异或,得到 $TID^{i\prime}$,并在服务器的 TID 库中搜索 $TID^{i\prime}$,若无法查询出 $TID^{i\prime}$,则标签 i 的身份非法,反之,则取出该身份码对应的 $SC_{l+1}{}^i$ 和 $SR_{l+1}{}^i$;其次,服务器使用接收到的 R_l 与在 TID 库中取出的 $SR_{l+1}{}^i$ 进行计算:

$$\mathrm{HD}(R_l, SR_{l+1}{}^i) < \tau。 \tag{2}$$

若式(2)成立,则说明标签 i 的身份合法,即标签 i 成功被服务器认证,其中 τ 是服务器为标签内嵌 TVO-APUF 设置的认证阈值;其次,服务器使用存储在数据库的共享秘密信息 $SC_{l+1}{}^i$ 与消息 MT 异或,得到标签随机数 r_T;再次,服务器计算:$C_{l+1}{}^i = SC_{l+1}{}^i \oplus r \oplus r_T$,并计算针对标签 i 的确认消息:$ACK_T = \mathrm{PRNG}(C_{l+1}{}^i)$;最后,服务器把 ACK_R 和 ACK_T 发送给阅读器 j,以便阅读器 j 和标签 i 认证服务器的合法性。此外,服务器依次更新数据库中的秘密信息:$SC_l{}^i = SC_{l+1}{}^i$、$SR_l{}^i = SR_{l+1}{}^i$、$SC_{l+1}{}^i = C_{l+1}{}^i$、$SR_{l+1}{}^i = R_{l+1}$。

注意,如果式(2)不成立,则使用数据库中 $SR_l{}^i$ 替换式中的 $SR_{l+1}{}^i$。若替换后不等式仍不成立,则标签 i 的身份非法,认证停止;若替换后成立,则说明标签 i 遭受了去同步化攻击,为了恢复与标签 i 的同步性,在计算 $C_{l+1}{}^i$ 时需要将 $SC_{l+1}{}^i$ 替换为 $SC_l{}^i$,在更新时也需要停止对 $SC_l{}^i$ 和 $SR_l{}^i$ 的操作,仅更新 $SC_{l+1}{}^i$ 和 $SR_{l+1}{}^i$。

步骤7 阅读器 j 接收到服务器发送的 ACK_R 和 ACK_T 后,计算 $ACK_R{}' = \mathrm{PRNG}(RID^j \oplus r_R)$,若 $ACK_R{}'$ 与接收到的 ACK_R 不相等,则服务器的身份非法,停止认证;若两者相等,则服务器成功被阅读器 j 认证,阅读器 j 继续把 ACK_T 发送给标签 i。

步骤8 标签 i 接收到 ACK_T 后,计算 $ACK_T{}' = \mathrm{PRNG}(C_{l+1}{}^i)$,若 $ACK_T{}'$ 与接收到的 ACK_T 不相等,则服务器的身份非法,停止认证;若两者相等,则服务器成功被标签 i 认证,标签 i 继续更新存储区的 $SC_{l+1}{}^i$,即 $SC_{l+1}{}^i = C_{l+1}{}^i$。

3 协议安全性分析

3.1 非形式化安全分析

3.1.1 追踪攻击

标签 i 在每轮认证都使用自身产生的随机数 r 异或 TID^i。根据香农定理,如果在异或操作中有一项是随机的,那么使用简单的异或加密就能得到较高安全性。因此,攻击者无法通过监听和分析会话消息定位到 TID^i,也不可能推测出连续两轮认证中 x 之间的关联性,从而保证了标签匿名性。同理,阅读器 j 在每轮认证中也使用随机数 r_R、r 异或 RID^j。

(2)重放攻击。重放攻击适合于认证消息中没有注入新鲜因子(如引入时间戳或随机数)的协议。PHL-RTAP 协议的三方在每轮认证中都产生自己控制的随机数(r、r_R 和 r_T),所以攻击者重放上一轮认证消息无法通过三方中任意合法一方的认证。

(3)物理克隆攻击。攻击者希望在获得合法标签后,克隆该合法标签并批量生产非法的克隆标签,以达到欺骗服务器的目的。然而,由于标签内嵌 PUF 电路的天然物理不可克隆属性,攻击者根本无法制造出两个完全相同的 PUF 电路。

(4)去同步化攻击。攻击者通过阻止标签 i 和服务器之间动态共享秘密信息 $SC_{l+1}{}^i$ 的更新来使得双方失去同步性。但是,PHL-RTAP 协议中的服务器同时存储两轮秘密信息 $SC_l{}^i$ 和 $SC_{l+1}{}^i$,以及对应两轮响应 $SR_l{}^i$ 和 $SR_{l+1}{}^i$,即使服务器遭受了去同步攻击,也可以认证合法标签 i 的身份,并在下一轮认证中恢复标签 i 和服务器中 $SC_{l+1}{}^i$ 的一致性。

3.2 形式化安全分析

3.2.1 BAN 逻辑证明

本文涉及的主要推理法则包括接收消息法则 S_1、消息含义法则 H_1、新鲜性法则 F_1、随机值验证法则 N_1 和管辖权法则 R_1[15]。

$$S_1:\frac{P\lhd\{X,Y\}}{P\lhd X};\ H_1:\frac{P\mid\equiv P\overset{K}{\longleftrightarrow}Q,P\lhd\{X\}_K}{P\mid\equiv Q\mid\sim X};$$

$$F_1:\frac{P\mid\equiv\#(X)}{P\mid\equiv\#(X,Y)};\ N_1:\frac{P\mid\equiv\#(X),P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X};$$

$$R_1:\frac{P\mid\equiv Q\mid\Rightarrow X,P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}。$$

在 BAN 逻辑下 PHL-RTAP 协议的描述如下,其中 S、R 和 T 分别表示协议中的后台服务器、阅读器和标签。

(1) $M_1:R\rightarrow S:Request$;

(2) $M_2:S\rightarrow R:r$;

(3) $M_3:R\rightarrow T:Query,r$;

(4) $M_4:T\rightarrow R:x,MT,R_l,R_{l+1}$;

(5) $M_5:R\rightarrow S:x,MT,R_l,R_{l+1},y'',MR$;

(6) $M_6:S\rightarrow R:ACK_T,ACK_R$;

(7) $M_7:R\rightarrow T:ACK_T$。

在协议模型中,只需将用于认证的消息(M_5、M_6、M_7)展开形式化安全分析。为了便于 BAN 描述,将涉及共享动态秘密信息、标签 ID、随机数、二次剩余、PUF 运算的信息统一使用符号 K 加密表示,则 M_5、M_6 和 M_7 可以形式化为

$$M_5:S\lhd\{x,MT,R_l,R_{l+1},y'',MR\}_K;$$

$$M_6:R\lhd\{ACK_T,ACK_R\}_K;$$

$$M_7:T\lhd\{ACK_T\}_K。$$

PHL-RTAP 协议满足以下基本假设:

$$A_1:R\mid\equiv R\overset{K}{\longleftrightarrow}S;A_2:S\mid\equiv S\overset{K}{\longleftrightarrow}R;$$

$$A_3:S\mid\equiv S\overset{K}{\longleftrightarrow}T;A_4:T\mid\equiv T\overset{K}{\longleftrightarrow}S;$$

$$A_5:S\mid\equiv\#(r_T);A_6:T\mid\equiv\#(r_T);$$

$$A_7:R\mid\equiv\#(r_R);A_8:S\mid\equiv\#(r);$$

$$A_9:R\mid\equiv S\Rightarrow ACK_R;A_{10}:T\mid\equiv S\Rightarrow ACK_T;$$

$$A_{11}:S\mid\equiv T\Rightarrow R_l;A_{12}:S\mid\equiv R\Rightarrow RID^j。$$

PHL-RTAP 协议安全性证明的目标如下:

(1) Goal1:$S\mid\equiv R_l$;

(2) Goal2:$R\mid\equiv ACK_R$;

(3) Goal3:$T\mid\equiv ACK_T$;

(4) Goal4:$S\mid\equiv RID^j$。

证明　Goal1、Goal2、Goal3、Goal4:

由 $M_5:S\lhd\{x,MT,R_l,R_{l+1},y'',MR\}_K$,初始假设 $A_3:S\mid\equiv S\overset{K}{\longleftrightarrow}T$ 及推理法则 S_1、H_1,可得

$$S\mid\equiv T\mid\sim R_l。\tag{3}$$

由 $A_5:S\mid\equiv\#(r_T)$ 及推理法则 F_1,可得

$$S\mid\equiv\#(R_l)。\tag{4}$$

根据式(3)、式(4)及推理法则 N_1,可得

$$S\mid\equiv T\mid\equiv R_l。\tag{5}$$

根据式(5),$A_{11}:S\mid\equiv T\Rightarrow R_l$ 和法则 R_1,可得

$$S\mid\equiv R_l。\tag{6}$$

综上,安全目标 Goal1:$S\mid\equiv R_l$ 得证。

由 $M_6:R\lhd\{ACK_T,ACK_R\}_K$,初始假设 $A_1:R\mid\equiv R\overset{K}{\longleftrightarrow}S$ 及推理法则 S_1、H_1,可得

$$R\mid\equiv S\mid\sim ACK_R。\tag{7}$$

由 $A_7:R\mid\equiv\#(r_R)$ 及推理法则 F_1,可得

$$R\mid\equiv\#(ACK_R)。\tag{8}$$

根据式(7)、式(8)及推理法则 N_1,可得

$$R\mid\equiv S\mid\equiv ACK_R。\tag{9}$$

根据式(9),$A_9:R\mid\equiv S\Rightarrow ACK_R$ 及推理法则 R_1,可得

$$R\mid\equiv ACK_R。\tag{10}$$

综上,安全目标 Goal2:$R\mid\equiv ACK_R$ 得证。

由 $M_7:T\lhd\{ACK_T\}_K$,初始假设 $A_4:T\mid\equiv T\overset{K}{\longleftrightarrow}S$ 及推理法则 H_1,可得

$$T\mid\equiv S\mid\sim ACK_T。\tag{11}$$

由 $A_6:T\mid\equiv\#(r_T)$ 及推理法则 F_1 得出 $T\mid\equiv\#(C_{l+1})$,根据 $T\mid\equiv\#(C_{l+1})$ 及 F_1,可得

$$T\mid\equiv\#(ACK_T)。\tag{12}$$

根据式(11)、式(12)及推理法则 N_1,可得

$$T\mid\equiv S\mid\equiv ACK_T。\tag{13}$$

根据式(13),$A_{10}:T\mid\equiv S\Rightarrow ACK_T$ 和推理法则 R_1,可得

$$T\mid\equiv ACK_T。\tag{14}$$

综上,安全目标 Goal3:$T\mid\equiv ACK_T$ 得证。

由 $M_5:S\lhd\{x,MT,R_l,R_{l+1},y'',MR\}_K$,$y''=(y^2)^2(\mathrm{mod}\ m)$,$y=RID^j\oplus r_R\oplus r$ 及推理法则 S_1,可得

$$S\lhd\{RID^j\}_K。\tag{15}$$

根据式(15),初始假设 $A_2:S\mid\equiv S\overset{K}{\longleftrightarrow}R$ 及推理法则 S_1、H_1,可得

$$S\mid\equiv R\mid\sim RID^j。\tag{16}$$

由 $A_8:S\mid\equiv\#(r)$ 及推理法则 F_1,可得

$$S\mid\equiv\#(RID^j)。\tag{17}$$

根据式(16),式(17)及推理法则 N_1,可得

$$S\mid\equiv R\mid\equiv RID^j。\tag{18}$$

根据式(18),$A_{12}:S\mid\equiv R\Rightarrow RID^j$ 及推理法则 R_1,可得:

$$S\mid\equiv RID^j。\tag{19}$$

综上,安全目标 Goal4:$S\mid\equiv RID^j$ 得证。

3.2.2　AVISPA 工具验证

AVISPA[16]形式化安全验证工具可以评估 PHL-RTAP 协议的安全性。本文使用动态模型检查器(OFMC)后端对 PHL-RTAP 协议进行形式化安全

验证,由于 AVISPA 工具支持的运算类型有限,因此需要将 PHL-RTAP 协议中的一些复杂运算抽象为 AVISPA 工具支持的运算。PHL-RTAP 协议的抽象过程如下:将 PHL-RTAP 协议的 TVO-APUF^i 运算和 PRNG 运算抽象为 2 个不同的哈希运算;将步骤 5 中二次剩余算法加密的消息 y'' 抽象为使用共享密钥 Y 的加密形式,表示除掌握共享密钥 Y 的合法通信主体外,非法主体无法获得信息 RID^j;其他加密消息按照原协议加密形式描述。经过上述抽象化处理后,协议的最终形式与原形式的流程相似,适用于在 AVISPA 工具中描述和仿真分析。图 2 模拟了攻击者可能的攻击流程,图 3 的"SUMMARY"显示为"SAFE",这表明 PHL-RTAP 协议是安全的。

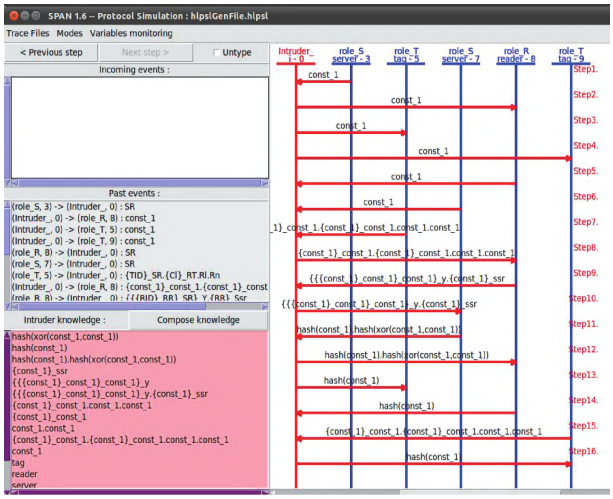

图 2 入侵者仿真结果

Figure 2 Intruder simulation result

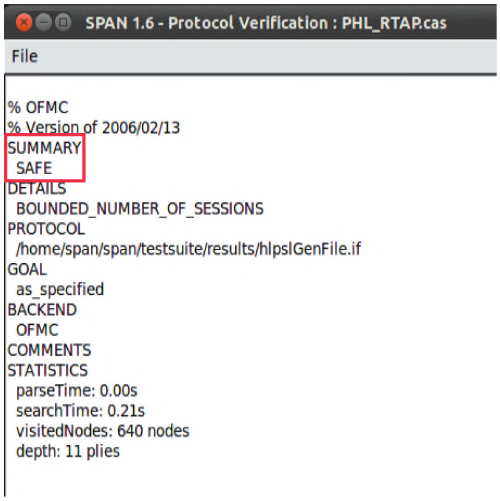

图 3 OFMC 验证结果

Figure 3 OFMC validation result

4 协议性能分析

4.1 安全性对比分析

将 PHL-RTAP 协议与现有文献的认证协议进行安全性对比,具体如表 2 所示。其中标注"是",表示该文献中的协议能够抵抗相应的攻击或实现三方认证,"否"表示不能抵抗相应攻击或没有实现完整的三方认证。

表 2 协议安全性对比

Table 2 Security comparison of protocols

安全属性	文献[3]	文献[8]	文献[9]	文献[17]	文献[18]	PHL-RTAP
追踪攻击	是	是	是	是	是	是
重放攻击	否	是	否	是	否	是
物理克隆攻击	否	否	是	否	是	是
伪造攻击	是	是	否	是	否	是
去同步化攻击	是	是	是	是	是	是
拒绝服务攻击	否	是	否	否	是	是
三方认证	是	是	否	否	是	是

文献[3]采用 Hash 加密机制,基于动态共享密钥实现了 RFID 协议,该协议无法抵抗物理克隆攻击。虽然文中声称可以抵抗重放攻击和拒绝服务攻击,但是如果攻击者重放步骤 3 的消息给后台数据库,数据库将通过对非法阅读器和非法标签的身份认证;此外,该协议只有在阅读器数量较少时可以防范拒绝服务攻击,但在拥有大量阅读器的庞大的 RFID 系统中,无法有效抵抗拒绝服务攻击。文献[8]使用二次剩余定理保护标签的关键信息,一旦遭受物理克隆攻击,攻击者可以获取该信息并复制大量与合法标签相同的"克隆标签"。文献[9]把 PUF 电路集成到标签来保证其物理不可克隆性,但是该协议缺少后台服务器和阅读器之间的相互认证,没有实现完整的三方认证过程,攻击者可以伪造成阅读器与合法服务器和合法标签进行通信交互,也可以发起针对服务器的重放攻击。文献[17]使用二次剩余,伪随机数生成器和超轻量级位流函数保护数据安全,但是该协议中的云服务器在认证阅读器和标签时,需要遍历计算阅读器和标签的身份信息,搜索开销过大,存在拒绝服务攻击的漏洞。此外,该协议无法抵抗针对标签的物理克隆攻击,并且缺少阅读器对服务器的身份认证。文献[18]提出一种采用 PUF 的轻量级 RFID 安全认证协议,该协议在标签端引入 PUF 电路以抵抗物理克隆攻击,然而,该协议没有充分利用 PUF 电路激励响应行为的不可预测性,只是采用简单的位重排运算实现阅读器对标签的认证,攻击者容易假冒标签欺骗合法阅读器。此外,一旦攻击者阻止标签端 T_i 的更新,就可以利用上一轮阅读器发送的消息,发起针对标签的重放攻击。本文的 PHL-RTAP 协议能够抵抗上述攻击,同时实现了完整的三方认证,因此,PHL-

RTAP 协议相比于近期文献[3,8,9,17-18]的协议具有更高的安全性。

4.2　性能对比分析

将 PHL-RTAP 协议与现有认证协议的开销进行对比，具体如表 3 所示。其中 x 表示异或，a 表示加法，pr 表示伪随机数运算，puf 表示 PUF 运算，r 表示循环移位，me 表示模幂运算，rme 表示乘法逆元运算，rn 表示生成随机数，t 表示提取时间戳，h 表示哈希运算，e 表示对称加解密操作，c 表示连接或去连接，per 表示位重排运算，m 表示模糊运算，pad 表示字符串填充或解填充运算。设标签存储和通信交互的相关消息长度是 L。

表 3　协议开销对比

Table 3　Cost comparison of protocols

协议开销	文献[3]	文献[8]	文献[9]	文献[17]	文献[18]	PHL-RTAP
标签计算开销	$1c+1x+3pr+1h+1rn$	$2x+2pr+2me$	$13x+3puf+2h+1rn$	$4x+1a+2r+3pr$	$3x+2per+1puf+1m+1pad$	$4x+2puf+1rn+1pr$
标签存储开销	$2L$	$4L$	$2L$	$2L$	$2L$	$2L$
阅读器计算开销	$2c+2pr+1h+1e+1rn$	$3x+3pr+1t+2me$	$1rn$	$13x+1a+5r+1t+5pr+3me+1rme$	$1t+2x+2pad+1e$	$4x+1rn+1me+1pr$
服务器搜索开销	$O(N)$	$O(1)$	$O(1)$	$O(N)$	$O(1)$	$O(1)$
通信开销	$11L$	$11L$	$12L$	$17L$	$13L$	$15L$

文献[3,9]的标签中均使用了高成本的哈希运算，不适合用于资源受限的 RFID 标签，并且文献[9]中阅读器的超低计算开销牺牲了安全性，使其容易受到伪造、重放、拒绝服务等恶意攻击。文献[17]虽然没有使用哈希运算，但其阅读器多次使用模幂运算，且其服务器的搜索开销为 $O(N)$，这不仅增加了服务器的计算搜索压力，也不利于认证协议中标签和阅读器的大规模扩展。文献[8]的标签使用了两次模幂运算，对标签计算能力要求较高，且增加了标签的存储开销。文献[18]的标签端仅使用了 PUF、位重排等轻量级运算，但在阅读器端使用高开销的对称密码算法解密消息，这给阅读器带来了较高的计算负担。PHL-RTAP 协议相较于文献[3,8-9]，标签计算开销最低，相较于文献[17-18]，阅读器计算开销降低，且服务器搜索开销是最低的复杂度 $O(1)$，标签存储开销也是最低的 $2L$，虽然其通信开销略高，但是协议中引入 PUF 电路抵抗物理克隆攻击，引入随机数抵抗重放攻击，因此 PHL-RTAP 协议通信开销的增长不可避免。

5　结论

本文提出了一种基于 PUF 的高安全性轻量级 RFID 三方认证协议，PHL-RTAP 协议引入了 PUF、二次剩余和随机数等运算，在满足低开销的前提下，有效抵抗追踪攻击、重放攻击、物理克隆攻击、去同步化攻击和伪造攻击等恶意攻击，实现了完整的 RFID 三方认证。此外，非形式化和形式化分析证明了 PHL-RTAP 协议的安全性，与近期 RFID 认证协议的对比表明，PHL-RTAP 协议在安全性和开销方面均有优势。因此，本文提出的 PHL-RTAP 协议在实现高安全性的同时，节省了系统的资源开销，适用于资源受限的 RFID 三方认证系统。

参考文献：

[1] 范文兵，李建华，禹士鹏，等. RFID 系统数据传输中 CRC 算法的分析与实现[J]. 郑州大学学报(工学版)，2010，31(2)：97-101.
FAN W B，LI J H，YU S P，et al. Analysis and implementation of CRC in RFID system[J]. Journal of Zhengzhou University (Engineering Science)，2010，31(2)：97-101.

[2] 刘鹏，张昌宏，欧庆于. 基于 Hash 函数的移动射频识别互认证安全协议设计[J]. 计算机应用，2013，33(5)：1350-1352.
LIU P，ZHANG C H，OU Q Y. Authentication protocol of mobile RFID based on Hash function[J]. Journal of Computer Applications，2013，33(5)：1350-1352.

[3] 王国伟，贾宗璞，彭维平. 基于动态共享密钥的移动 RFID 双向认证协议[J]. 电子学报，2017，45(3)：612-618.
WANG G W，JIA Z P，PENG W P. A mutual authentication protocol of mobile RFID based on dynamic shared-key[J]. Acta Electronica Sinica，2017，45(3)：612-618.

[4] FARASH M S，NAWAZ O，MAHMOOD K，et al. A provably secure RFID authentication protocol based on elliptic curve for healthcare environments[J]. Journal of Medical Systems，2016，40(7)：165-173.

[5] XIAO H N，ALSHEHRI A A，CHRISTIANSON B. A cloud-based RFID authentication protocol with insecure communication channels[C]//2016 IEEE Trustcom/BigDataSE/ISPA. Piscataway：IEEE，2016：332-339.

[6] CHIEN H Y. SASI：a new ultralightweight RFID authentication protocol providing strong authentication and strong

integrity[J]. IEEE Transactions on Dependable and Secure Computing, 2007, 4(4): 337-340.
[7] TIAN Y, CHEN G L, LI J H. A new ultralightweight RFID authentication protocol with permutation[J]. IEEE Communications Letters, 2012, 16(5): 702-705.
[8] CHIOU S Y, CHANG S Y. An enhanced authentication scheme in mobile RFID system[J]. Ad Hoc Networks, 2018, 71: 1-13.
[9] 王利, 李二霞, 纪宇晨, 等. 基于PUF的抗物理克隆RFID安全认证协议[J]. 信息网络安全, 2020, 20(8): 89-97.
WANG L, LI E X, JI Y C, et al. PUF-based anti-physical cloning RFID security authentication protocol[J]. Netinfo Security, 2020, 20(8): 89-97.
[10] 尹魏昕, 贾咏哲, 高艳松, 等. 物理不可克隆函数(PUF)研究综述[J]. 网络安全技术与应用, 2018(6): 41-42, 54.
YIN W X, JIA Y Z, GAO Y S, et al. Review of physical unclonable function (PUF)[J]. Network Security Technology & Application, 2018(6): 41-42, 54.
[11] 李永强, 刘兆伟. 基于区块链的车联网安全信息共享机制设计[J]. 郑州大学学报(工学版), 2022, 43(1): 103-110.
LI Y Q, LIU Z W. Blockchain-based secure data sharing mechanism design in the vehicular networks[J]. Journal of Zhengzhou University (Engineering Science), 2022, 43(1): 103-110.
[12] CHANG Z T, SHI S S, SONG B W, et al. Modeling attack resistant arbiter PUF with time-variant obfuscation scheme[C]//2021 31st International Conference on Field-Programmable Logic and Applications (FPL). Piscataway: IEEE, 2021: 60-63.
[13] 周楠楠. RFID系统中无源标签的伪随机数发生器[D]. 西安: 西安电子科技大学, 2015.
ZHOU N N. Pseudo random number generators in the passive tags of RFID system[D]. Xi'an: Xidian University, 2015.
[14] DOSS R, ZHOU W L, YU S. Secure RFID tag ownership transfer based on quadratic residues[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(2): 390-401.
[15] 杨世平. 安全协议及其BAN逻辑分析研究[D]. 贵阳: 贵州大学, 2007.
YANG S P. Security protocols and its BAN logic analysis[D]. Guiyang: Guizhou University, 2007.
[16] VIGANÒ L. Automated security protocol analysis with the AVISPA tool[J]. Electronic Notes in Theoretical Computer Science, 2006, 155: 61-86.
[17] FAN K, ZHU S S, ZHANG K, et al. A lightweight authentication scheme for cloud-based RFID healthcare systems[J]. IEEE Network, 2019, 33(2): 44-49.
[18] YE Q, SUN Z W. Lightweight RFID authentication protocol for cloud services using PUF encryption[C]//2021 33rd Chinese Control and Decision Conference (CCDC). Piscataway: IEEE, 2021: 5629-5634.

High-security Lightweight RFID Triple Authentication Protocol Based on PUF

FAN Wenbing, CHANG Zhengtai, AI Lulin, KONG Dehan

(School of Electrical and Information Engineering, Zhengzhou University, Zhengzhou 450001, China)

Abstract: To solve the difficult tradeoff between security requirements and resource cost in radio frequency identification (RFID) triple authentication protocol, a PUF-based high-security lightweight RFID triple authentication protocol (PHL-RTAP) was proposed. Physical unclonable function (PUF) was utilized to authenticate the tag identity for protecting the tag from physical cloning attacks and reducing the tag cost, meeting the demand of resource-constrained RFID system. The quadratic residual algorithm was adopted to secure the reader data privacy. Random numbers were introduced to resist replay attacks and ensure the anonymity and untraceability of tags and readers. The PHL-RTAP could realize a complete triple authentication between server, reader and tag, and expand the scale of readers and tags in RFID systems according to different requirements, so that it was suitable for large-scale tag RFID system. Security analysis showed that PHL-RTAP could effectively resist various malicious attacks such as tracking attacks, replay attacks, physical cloning attacks and desynchronization attacks. BAN logic analysis and AVISPA tool were used to verify the security of the protocol. Compared with recent protocols, PHL-RTAP could make up for the security defects of similar RFID protocols, and has low resource costs such as computing cost, tag storage cost, and communication cost. PHL-RTAP could achieve both high security and lightweight, and was suitable for resource-constrained RFID triple authentication scenarios.

Keywords: radio frequency identification; physical unclonable function; quadratic residue; triple authentication; formal analysis