



基于单向伪随机函数的移动 RFID 系统认证协议

简碧园^{1,2}, 刘道微¹

(1. 广州科技职业技术学院信息工程学院, 广东 广州 510550;

2. 华南理工大学计算机科学与工程学院, 广东 广州 510006)

摘要: 针对移动 RFID 系统认证中可能出现的成本、效率、安全问题, 设计了一种基于单向伪随机函数的移动 RFID 认证协议。协议在满足 Gen-2 标准的前提下, 综合采用位替换运算、异或运算和单向伪随机函数加密通信信息; 协议充分利用标签、读写器、后端数据库三方共享密钥和三方通信信息, 对信息进行加密传输和加密认证, 降低系统成本; 通过实现完整三方认证与密钥更新工作, 避免协议遭受假冒、去同步化等攻击行为。最后, 给出协议 GNY 理论逻辑证明以及安全、性能分析, 表明新协议的可行性与安全性。

关键词: 物联网; 移动 RFID; 单向伪随机函数; Gen-2 标准; 三方认证; GNY 逻辑

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2017187

Mobile RFID system authentication protocol based on one-way pseudo random function

JIAN Biyuan^{1,2}, LIU Daowei¹

1. School of Electronic and Computer Engineering,

Guangzhou Vocational College of Science and Technology, Guangzhou 510550, China

2. School of Computer Science and Engineering, South China University of Technology, Guangzhou 510006, China

Abstract: Aiming at the cost, efficiency and security of mobile RFID system authentication, a mobile RFID authentication protocol based on one-way pseudo random function was designed. The protocol reduced system cost by making full use of the three party of the shared key and communication information to encrypt transmission and authentication. Through the implementation of three party authentication and key update work, the agreement suffered counterfeit, desynchronization and other attacks was avoided. Finally, the logical proof of GNY and its security and performance analysis were given to show the feasibility and security of the new protocol.

Key words: internet of things, mobile RFID, one-way pseudo random function, the Gen-2 standard, three party authentication, GNY logic

收稿日期: 2017-01-05; 修回日期: 2017-06-06

基金项目: 广东省科技计划产学研合作项目 (No.2014B090908010); 广州市产学研协同创新重大专项产业技术研究专题项目 (No.201604010048); 广州市产学研协同创新重大专项产业技术研究专题项目 (No.201604016067); 广东省高等教育学会高职高专云计算与大数据专业委员会科研课题 (No.GDYJSKT16-16)

Foundation Items: Guangdong Province Science and Technology Plan (No.2014B090908010), Special Subject Research Project of Guangzhou University Industry Collaborative Innovation (No.201604010048), Special Subject Research Project of Guangzhou University Industry Collaborative Innovation (No.201604016067), Guangdong Institute of Higher Education Cloud Computing and Big Data Specialized Committee Research Topics (No.GDYJSKT16-16)

1 引言

近年来为实现智慧地球的目标,物联网迅速发展。作为物联网发展的排头兵,无线射频识别(radio frequency identification, RFID)技术成为了市场上最受关注的技术之一。它利用无线电信号无需接触识别目标并读写相关数据的特点,广泛应用于身份证件、门禁系统、供应链和车辆收费等领域^[1]。

射频识别系统主要分为3个部分:标签、读写器、后端数据库。传统意义上,读写器与后端数据库之间通过有线连接,一般视为安全的通信。但随着物联网和无线通信的紧密结合,移动支付、POS支付等业务的快速发展,移动RFID系统开始受到广泛的关注^[2]。在移动RFID系统中,读写器和后端数据库采用无线方式进行通信,具有移动性强、便捷等优点。但由于是无线连接,该链路下的通信存在安全隐患,容易受到假冒、重放等攻击,从而导致用户隐私的泄露^[3]。因此设计一种安全有效的移动RFID系统双向认证协议是很重要的。

2 相关研究

近年来,国内外学者对RFID系统认证协议的研究主要分为4个方向:基于重量级对称加密算法或非对称加密算法认证协议,如基于ECC椭圆曲线的RFID认证协议;基于散列函数、伪随机函数或物理不可克隆函数等单向函数的中量级RFID认证协议;基于二次剩余定理的轻量级认证协议;基于简单单位运算的超轻量级RFID认证协议。

单向函数与随机性理论是现代密码学的主要理论基础之一,几乎所有密码问题都需要“高质量的随机性”来实现。单向函数可以用来构造伪随机产生器(pseudo random generator, PRG)进而构成流密码(stream cipher)算法,或构造伪随

机函数(pseudo random function)^[4]。伪随机函数,其最初由Goldreich等人定义和构造,并在后续的研究中证明了伪随机函数在加密算法上的应用。2010年,Dodis和Pietrzak在标准模型下,构造出了抗信息泄露的伪随机函数。同年,Bellare和Cash基于标准模型和假设,设计出了抵抗相关密钥攻击的伪随机函数^[5]。

2008年,EPC Global(全球产品电子代码中心)推行EPC class1 Generation2(第1类第2代的产品电子代码)电子标签标准(简称Gen-2标准),Gen-2标准成为射频识别标签行业的标准。其约定标签内只有2500~5000门电路用于计算。而常用的散列函数(SHA-1和MD5需要1.5万~2万门电路)协议不适合Gen-2标准,因此国内外学者开始利用伪随机函数及一些简单单位运算来设计安全标准的协议^[6]。

在满足Gen-2标准的前提下,伪随机函数在移动RFID系统上的应用主要有:2011年,Yeh等人^[7]在协议中加入了随机数认证更新。在这之后,出现了很多基于随机函数的移动RFID认证协议^[8-10]。这些协议大都效率不高,标签成本增加,虽然保证了一定的安全性,但也存在安全隐患,如参考文献[10]并不能抵抗重放攻击,并且没有读写器对后端数据库的认证,不能抵抗假冒攻击。2015年,张琪等人^[11]提出了基于伪随机函数的移动射频识别认证协议,虽然满足Gen-2的标准,并具有一定的安全性。但是通过本文的研究发现该协议在实现后端数据库与读写器、标签认证之前,并没有标签和读写器的安全认证,没有完成其所描述的三方完整认证功能,所以存在假冒的安全漏洞。

其他满足Gen-2标准的移动RFID系统认证协议主要有:2013年,Doss等人^[12]基于二次剩余定理设计了隐私保护的移动RFID认证协议,该协议面向低成本标签的应用,但该协议后台数据库查询过程仍要执行多次匹配查询,认证效率较



低；此外，数据库接收到的消息不具备新鲜性，容易受到重放攻击。Wu 等人^[13]提出基于时间戳和标志位的移动 RFID 认证协议，该协议可有效抵御多种攻击行为，但该协议的密钥更新过程并非是不可逆的。攻击者能通过窃听与截获，在得到的历史信息中进行暴力破解，识别标签，因此该协议不能保证不可追踪性。

综上所述，现存移动 RFID 认证协议普遍存在以下缺点：不能满足 Gen-2 标准，不能适应移动 RFID 系统低成本轻量级的特点；不能完全满足标签、读写器、后端数据库的三方双向认证，存在安全漏洞；标签成本较高，认证效率较低，不能很好地适用于大规模的移动 RFID 系统。因此，本文设计了一种满足 Gen-2 标准的基于伪随机函数的移动 RFID 系统三方认证协议，在保证协议安全性的同时降低系统成本。

3 移动 RFID 认证协议设计

在本协议中，采用位替换运算^[14] $Sub(X, Y)$ 、异或和单向伪随机函数相结合的算法对协议信息进行加密传输，由于只采用简单位运算和轻量级伪随机函数，所以满足 Gen-2 标准，减少了标签和读写器端的计算量，降低了系统运算成本；同时本协议充分利用标签、读写器、后端数据库三方共享密钥信息和三方通信信息，依次将共享密钥和通信信息分成左、右两部分值进行加密传输和加密认证，同样降低读写器和标签成本；协议基于三方完整安全认证，避免协议遭受假冒、重放、去同步化等攻击行为，保证三方通信安全。

3.1 协议前提与符号说明

本文提出的协议与其他移动 RFID 系统认证协议类似做出如下假设：标签和读写器之间的通信信道是不安全的，攻击者可以进行窃听等攻击行为；读写器和后端数据库之间的通信信道也是不安全的，无线通信也可以被窃听。

本协议中出现的符号说明具体见表 1。

表 1 协议符号说明

符号	含义
T	标签
R	读写器
D	后端数据库
IDT	标签身份标识
IDR	读写器身份标识
key	标签、读写器、后端数据库共享密钥
key_L	三方共享密钥左半部分
key_R	三方共享密钥右半部分
key_{old}	上一轮三方共享密钥
R_1, R_2	随机数
A-G	三方通信数据
$Sub(X, Y)$	位替换运算
$g_{key}(X, Y)$	基于共享密钥的伪随机函数

其中，位替换运算采用指针的形式，从最高位开始遍历 X ，替换 Y ，它的实现比直接采用逻辑门效率更高，具体示例过程如图 1 所示以及参考文献[14]所述，设 $X=11100110$ ， $Y=10101101$ ， $Sub(X, Y)=11011110$ 。

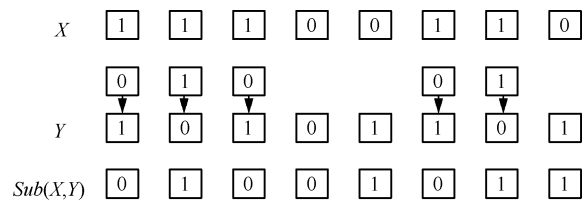


图 1 $Sub(X, Y)$ 位替换运算示例

3.2 协议具体认证过程

本协议总体分成初始化，读写器和标签相互认证，标签、读写器和后端数据库三方双向认证，密钥更新 4 个阶段，具体如下。

(1) 初始化阶段

标签存储自身的标识符 IDT 和三方共享密钥 key ；读写器存储自身标识符 IDR 和 key ；后端数据库存储 (IDT, IDR, key, key_{old})。

(2) 读写器和标签相互认证

图 2 给出了读写器和标签两端双向认证通信流程，具体过程如下。

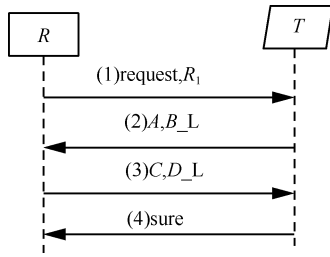


图2 标签和读写器两端双向认证

- 读写器产生随机数 R_1 ，并将请求认证指令 request 一起发送给标签。
- 标签收到请求指令后，利用自身存储的信息以及 R_1 ，计算生成 A 、 (B_L, B_R) ，且存储信息 B_R ，最后将 A 、 B_L 一起发送给读写器。

$$A = IDT \oplus Sub(key_L, key_R) \quad (1)$$

$$(B_L, B_R) = g_{key}(R_1 \oplus IDT \oplus key) \quad (2)$$

- 读写器接收到标签发送信息后，利用共享密钥 key ，计算获得标签唯一标识 IDT ，验证数据 B_L 。如果验证成功，标签认证通过，读写器计算生成 C 、 (D_L, D_R) ，存储信息 D_R ，最后将 C 、 D_L 一起发送给标签；如果验证失败，协议终止。

$$C = IDR \oplus Sub(key_L, key_R) \quad (3)$$

$$(D_L, D_R) = g_{key}(R_1 \oplus IDR \oplus key) \quad (4)$$

- 标签在收到 C 、 D_L 信息后，利用共享密钥 key ，计算获得读写器唯一标识信息 IDR ，验证数据 D_L ，如果验证成功，读写器认证通过，标签发送确认指令 $sure$ ，至此标签和读写器端双向认证完成；如果验证失败，协议终止。

(3) 后端数据库分别与读写器和标签双向认证
图3给出了标签、读写器和后端数据库三方双向认证通信流程。

- 读写器在收到标签端的确认消息后，将信息 B_L 、 D_L 、 R_1 转发给后端数据库，等待数据库的验证。

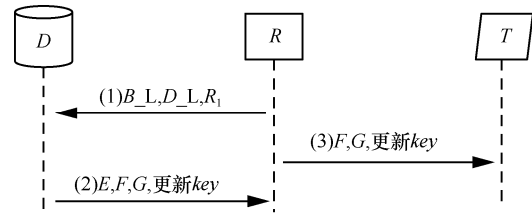


图3 标签、读写器和后端数据库三方双向认证

- 后端数据库在收到消息后，首先检索读写器唯一标识 IDR ，计算验证 D_L ，存储 D_R ，如果验证通过，读写器认证通过，数据库接着查询标签唯一标识 IDT ，计算验证 B_L ，存储 B_R ，如果验证通过，标签认证通过，如果 D_L 或 B_L 验证不相等，查找数据库中的 key_{old} ，重新计算 D_L 或 B_L ，相等后进行后续通信运算；但如果读写器或标签在两次计算中有一方认证未通过，协议终止。
- 数据库对读写器和标签认证通过后，数据库产生随机数 R_2 ，为共享密钥更新和计算消息 E 、 F 、 G 做准备。最后，将计算得到的 E 、 F 、 G 一起发送给读写器后，开始密钥更新。

$$E = D_R \oplus R_2, \quad F = B_R \oplus R_2 \quad (5)$$

$$G = Sub(key_L, key_R) \oplus R_2 \quad (6)$$

$$key_{old} = key, \quad key = g_{key}(IDT \oplus IDR \oplus R_2) \quad (7)$$

- 读写器收到数据库的回复消息后，根据 key ，计算得到 R_2 ，再利用存储的 D_R ，验证从数据库端收到的信息 E 。如果相等，验证成功，数据库和读写器端双向认证完成，更新密钥 key ，最后将消息 F 、 G 发送给标签；如果不相等，验证失败，协议终止。
- 标签在收到读写器端的消息后，根据 key ，计算得到 R_2 ，利用存储的 B_R ，验证从数据库收到的信息 F 。如果相等，验证成功，数据库和标签端双向认证完成，更新密钥



key; 如果不相等, 验证失败, 协议终止。

(4) 密钥更新阶段

已在上述阶段中有具体描述, 此处不做过多赘述。

最后, 图 4 给出了基于单向伪随机函数的移动 RFID 双向认证协议具体执行流程。

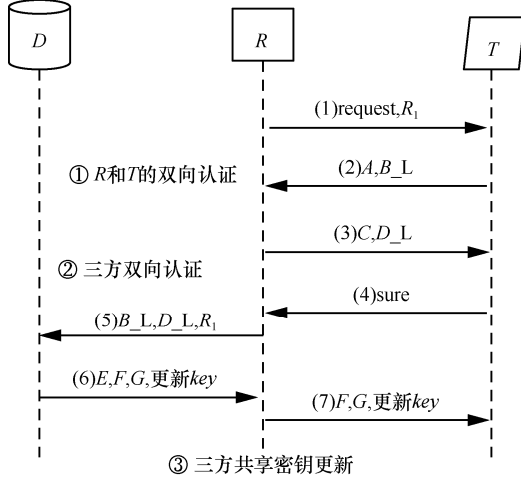


图 4 基于单向伪随机函数的移动 RFID 双向认证协议执行流程

4 协议 GNY 逻辑证明

本文利用 GNY 逻辑分析提出的协议, 根据协议的形式化描述及初始化假设, 由推理法则逐步得到协议目标^[15]。具体证明如下。

4.1 协议形式化描述

证明过程中, $g()$ 表示伪随机函数, g_{key1} 、 g_{key2} 分别表示 g_{key} 的左右两部分, 所以形式化描述本协议中的通信信息如下:

$$M_1 : T \triangleleft *R_1 \quad (8)$$

$$M_2 : R \triangleleft *[IDT], g_{key1}(R_1 \oplus IDT \oplus key) \quad (9)$$

$$M_3 : T \triangleleft *[IDR], g_{key1}(R_1 \oplus IDR \oplus key) \quad (10)$$

$$M_4 : D \triangleleft *R_1, g_{key1}(R_1 \oplus IDT \oplus key), g_{key1}(R_1 \oplus IDR \oplus key) \quad (11)$$

$$M_5 : R \triangleleft *[R_2], g_{key2}(R_1 \oplus IDT \oplus key), g_{key2}(R_1 \oplus IDR \oplus key) \quad (12)$$

$$M_6 : R \triangleleft *[R_2], g_{key2}(R_1 \oplus IDT \oplus key) \quad (13)$$

4.2 协议初始化假设

$$S_1 : T \in (IDT, key), g() \quad (14)$$

$$S_2 : R \in (IDR, key), g() \quad (15)$$

$$S_3 : D \in (IDT, IDR, key, key_{old}), g() \quad (16)$$

$$S_4 : T \in key, R \in key, D \in key \quad (17)$$

$$S_5 : R \in R_1 \quad (18)$$

$$S_6 : D \in R_2 \quad (19)$$

$$S_7 : T \models \varphi(R_1 \oplus IDT \oplus key) \quad (20)$$

$$S_8 : R \models \varphi(R_1 \oplus IDR \oplus key) \quad (21)$$

$$S_9 : D \models \varphi(R_1 \oplus IDT \oplus key), \varphi(R_1 \oplus IDR \oplus key) \quad (22)$$

4.3 协议目标

(1) R 对 T 的认证

$$G_1 : R \models T \sim \# g_{key1}(R_1 \oplus IDT \oplus key) \quad (23)$$

(2) T 对 R 的认证

$$G_2 : T \models R \sim \# g_{key1}(R_1 \oplus IDR \oplus key) \quad (24)$$

(3) D 对 R 的认证

$$G_3 : D \models R \sim \# g_{key1}(R_1 \oplus IDR \oplus key) \quad (25)$$

(4) D 对 T 的认证

$$G_4 : D \models T \sim \# g_{key1}(R_1 \oplus IDT \oplus key) \quad (26)$$

(5) R 对 D 的认证

$$G_5 : R \models D \sim \# g_{key2}(R_1 \oplus IDR \oplus key) \quad (27)$$

(6) T 对 D 的认证

$$G_6 : T \models D \sim \# g_{key2}(R_1 \oplus IDT \oplus key) \quad (28)$$

4.4 协议推理证明

由信息 M_2 , 可以得到:

$$R \triangleleft g_{key1}(R_1 \oplus IDT \oplus key) \quad (29)$$

即:

$$R \triangleleft [R_1 \oplus IDT \oplus key]_{key1} \quad (30)$$

根据初始化假设 S_2 , 可以得到:

$$R \in key1 \quad (31)$$

根据初始化假设 S_1 和 S_2 , 可以得到:

$$R \models R \xleftarrow{key1} T \quad (32)$$

再根据初始化假设 S_8 , 可以得到:

$$R \models \varphi(R_1 \oplus IDT \oplus key) \quad (33)$$

接着由初始化假设 S_8 和信息 M_2 , 可以得到:

$$R \models \#(R_1 \oplus IDT \oplus key) \quad (34)$$

再根据新鲜性规则 F_1 , 可以得到:

$$R \models \#((R_1 \oplus IDT \oplus key), key1) \quad (35)$$

$$F_1: \frac{P \models \#X}{P \models \#(X, Y), P \models \#F(X)} \quad (36)$$

接着由式 (30) ~ 式 (33)、式 (35) 以及消息解释规则 I_1 , 可以得到:

$$R \models T \mid \sim \{R_1 \oplus IDT \oplus key\}_{key1} \quad (37)$$

$$R \models T \mid \sim g_{key1}(R_1 \oplus IDT \oplus key) \quad (38)$$

$$I_1: \frac{P \triangleleft^*(X)_K, P \in K, P \models P \xleftarrow{K} Q, P \models \varphi(X), P \models \#(X, K)}{P \models Q \mid \sim X, P \models Q \mid \sim (X)_K, P \models Q \in K} \quad (39)$$

最后根据式 (38) 和信息 M_2 , 可以得到:

$$R \models T \mid \sim \#g_{key1}(R_1 \oplus IDT \oplus key) \quad (40)$$

所以目标 G_1 证明成功。同理可证其他 5 个目标, 这里不再赘述。

5 协议安全性分析

本协议主要的安全基础在于标签、读写器和后端数据库的三方认证过程。在满足后端数据库对标签和读写器的双向认证之前, 加入读写器与标签的预认证, 确保协议信息在开始的标签和读

写器无线链路中, 可以安全传输; 并利用单向伪随机函数的不可逆性, 有效地抵抗攻击者的暴力破解。

本协议利用三方共享密钥信息串联起标签、读写器和数据库的三方认证过程, 因为共享密钥都是通过位替换运算、异或运算加密传送; 并引入随机数保证信息新鲜性, 所以协议可有效抵抗假冒攻击。

本协议在每次认证的过程中通过读写器和后端数据库产生的随机数 R_1 、 R_2 的随机不可预测性与伪随机函数的单向性, 可有效地抵抗攻击者的窃听、重放攻击。

本协议中无论是标签与读写器还是数据库与读写器之间传送的信息, 每次认证通信的信息都在不断变化 (随机数 R_1 、 R_2), 不可关联, 所以本协议可以抵抗攻击者多次截获相同的信息以确定标签或读写器的跟踪行为。

本协议在数据库初始化阶段, 加入了上一轮共享密钥的信息, 为了抵抗去同步化攻击。通过, 引入随机数 R_2 来更新共享密钥 key , 使每次认证中伪随机函数的计算因子不确定性增大, 保证了协议的安全性。

综上所述, 表 2 给出了本文协议和其他移动 RFID 协议的安全性比较, 其中 $\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$

6 协议性能分析

本节主要从标签和读写器的计算量、存储量和通信量 3 个方面对本协议进行性能分析, 见

表 2 协议的安全性比较

攻击类型	参考文献[7]	参考文献[10]	参考文献[11]	参考文献[12]	本文协议
暴力破解攻击	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$
假冒攻击	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$
窃听重放攻击	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$
跟踪行为	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$
去同步化攻击	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$	$\sqrt{}表示可以抵抗此种攻击行为, \times表示不能抵抗此种攻击行为。$



表 3、表 4。

表 3 协议标签端性能比较

协议	计算量	存储空间	通信量
参考文献[7]	$4H() + 3m + 2g()$	$3I$	$2L$
参考文献[10]	$5g()$	$3I$	L
参考文献[11]	$4XOR + 2g()$	$3I$	L
参考文献[12]	$4m + 3g()$	$3I$	$5L$
本文协议	$8XOR + sub + 3g()$	$2I$	$2L$

表 4 协议读写器端性能比较

协议	计算量	存储空间	通信量
参考文献[7]	$g()$	$2I$	$3L$
参考文献[10]	$2g()$	I	$3L$
参考文献[11]	$2XOR + 3g()$	$2I$	$3L$
参考文献[12]	$H() + 2g() + 4m$	$3I$	$5L$
本文协议	$8XOR + sub + 3g()$	$2I$	$2L$

6.1 标签端

标签计算量：本协议的标签只包含两种简单单位运算（位替换运算和异或运算）以及轻量级伪随机函数运算，并且对读写器和数据库的认证也是通过之前计算产生的存储数据以及异或提取运算，满足 Gen-2 标准低成本要求。

标签存储量：本协议在初始化阶段，标签只存储了标签唯一标识信息 IDT 和共享密钥 key 。

标签通信量：本协议标签端的传输信息主要有认证信息 A 、 B_L 和认证通过确认信息。

表 3 中， $H()$ 表示散列运算， XOR 表示异或运算， m 表示模平方运算， sub 表示位替换运算，标识、共享密钥的长度都是 I ，通信量的单位为 L 。

6.2 读写器端

读写器计算量：同标签端基本类似，不再赘述。

读写器存储量：在初始化阶段，读写器只存储唯一标识 IDR 和共享密钥 key 。

读写器通信量：本协议读写器端的传输信息主要有认证请求信息、认证信息 C 、 D_L 和中间传送信息 F 、 G 。

通过表 3、表 4 可以看出，本文协议与其他协议相比，无论是标签还是读写器在存储空间和通信量方面，都继续保持较低的成本，并没有因为加入了读写器和标签的预认证，构成完整三方认证而使成本增加；计算量方面，因为协议为保证完整三方认证，所以标签和读写器两端计算量稍有增加，但与对比协议相比，也并无较大差距，符合 Gen-2 标准。

7 结束语

本文设计的基于单向伪随机函数的移动 RFID 系统认证协议，在满足 Gen-2 标准的前提下，协议实现三方完整安全认证过程，以防止恶意攻击，有效地保证了协议的安全性、稳定性；利用简单单位运算与轻量级伪随机函数相结合的方式，实现了协议的加密、解密过程，有效地减少标签和读写器端的计算开销；同时，利用三方共享密钥信息以及通信计算信息，有效地减少标签和读写器成本。最后，基于本文协议给出了经典 GNY 理论逻辑证明和安全、效率分析，证明了本文协议在面向移动、开放的环境中可实现其预期的安全、低成本目标。但该协议在实际应用中是否能满足大规模的应用还有待下一步实验性研究。

参考文献：

- [1] 张平, 李建武, 冯志勇, 等. 认知无线网络基础理论与关键技术研究[J]. 电信科学, 2014, 30(2): 1-13.
ZHANG P, LI J W, FENG Z Y, et al. Research on basic theory and key technology of cognitive radio network[J]. Telecommunications Science, 2014, 30(2): 1-13.
- [2] 方箭, 王坦, 黄标. 高频段宽带无线通信前瞻[J]. 电信科学, 2014, 30(3): 109-113.
FANG J, WANG T, HUANG B. Outlook of broadband wireless communications at high frequency bands[J]. Telecommunications Science, 2014, 30(3): 109-113.
- [3] 冯剑, 王平阳, 王琳, 等. 基于能量获取的无线通信系统研究[J]. 电信科学, 2015, 31(2): 124-131.
FENG J, WANG P Y, WANG L, et al. Research on energy harvesting communication system[J]. Telecommunications Science, 2015, 31(2): 124-131.

- [4] 郁昱, 李祥学. 基于单向函数的伪随机产生器与通用单向哈希函数[J]. 西安邮电大学学报, 2016, 21(2): 1-9.
YU Y, LI X X. One-way function based pseudorandom generator and universal one-way hash function[J]. Journal of Xi'an University of Posts and Telecommunications, 2016, 21(2): 1-9.
- [5] 徐津, 温巧燕. 消息认证码的理论研究[D]. 北京: 北京邮电大学, 2015.
XU J, WEN Q Y. Theoretical research on message authentication codes[D]. Beijing: Beijing University of Posts and Telecommunications, 2015.
- [6] EPC global. EPC "radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz-960 MHz version 1.2.0[EB/OL]. (2013-03-10)[2017-01-05]. <http://www.gs1.org/gsm/ kc/ epc- global/uhfcl92/uhfcl92-1-2-0-standard-20080511.pdf>.
- [7] YE H T C, WU C H, TSENG Y M. Improvement of the RFID authentication scheme based on quadratic residues[J]. Computer Communications, 2011, 34(3): 337-341.
- [8] CHANG P. A location-privacy-protected RFID authentication scheme[C]//The 2011 IEEE International Conference on Communications, August 1-3, 2011, Chengdu, China. New Jersey: IEEE Press, 2011: 1-4.
- [9] ZHOU J. A quadratic residue-based lightweight RFID mutual authentication protocol with constant-time identification[J]. Journal of Communications, 2015, 10(2).
- [10] NIU B, ZHU X, CHI H, et al. Privacy and authentication protocol for mobile RFID systems[J]. Wireless Personal Communications, 2014, 77(3): 1-19.
- [11] 张琪, 梁向前, 位书敏. 基于伪随机函数的移动射频识别认证协议[J]. 计算机应用, 2015, 35(4): 977-980.
ZHANG Q, LIANG X Q, WEI S M. Authentication protocol based on pseudo-random function for mobile radio frequency identification[J]. Journal of Computer Applications, 2015, 35(4): 977-980.
- [12] 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.
- [13] WU X Q, ZHANG M, YANG X L. Time-stamp based mutual authentication protocol for mobile RFID system[C]//Wireless and Optical Communication Conference(WOCC), May 16-18, 2013, Chongqing, China. New Jersey: IEEE Press, 2013: 702-706.
- [14] 杜宗印, 章国安, 袁红林. 基于位替换运算的RFID双向认证协议[J]. 电视技术, 2013, 37(19): 134-137.
DU Z Y, ZHANG G A, YUAN H L. Bits substitution based on RFID mutual authentication protocol[J]. Video Engineering, 2013, 37 (19): 134-137
- [15] 侯峻峰, 黄连生. 安全协议形式化验证方法和安全协议设计研究[D]. 北京: 清华大学, 2004.
HOU J F, HUANG L S. Research on formal verification and design of security protocols[D]. Beijing: Tsinghua University, 2004.

[作者简介]



简碧园 (1983-), 男, 广州科技职业技术学院信息工程学院教研室主任、讲师, 主要研究方向为计算机网络技术、云计算技术、信息安全。



刘道微 (1989-), 男, 广州科技职业技术学院信息工程学院硕士生, 主要研究方向为信息安全、RFID 系统所有权转移协议、RFID 系统双向认证协议及 RFID 系统密钥无线生成算法。