



一种基于二次剩余的改进的 RFID 认证协议

刘直良

(黄淮学院信息工程学院, 河南 驻马店 463000)

摘要: 针对现有基于二次剩余的无线射频识别 (RFID) 认证协议在安全和成本方面的漏洞与不足, 设计了一种基于二次剩余的改进的 RFID 双向认证协议。改进的协议在基础二次剩余算法框架下, 混入随机数加密, 使消息在数据库认证识别时更为高效快速; 引入超轻量级位替换运算和异或运算加密通信信息, 降低系统计算成本; 加入数据库端随机数查重校验机制, 避免协议遭受去同步化和拒绝服务等攻击行为; 最后, 给出协议的 GNY 逻辑证明, 表明改进协议的可行性。通过分析协议安全性和性能, 表明改进协议具有较高安全性和较低成本。

关键词: 二次剩余; 无线射频识别; 高效; 双向认证; 超轻量级; 查重校验; GNY 逻辑

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018042

An improved RFID authentication protocol based on quadratic residue

LIU Zhiliang

School of Electronic and Computer Engineering, Huanghuai University, Zhumadian 463000, China

Abstract: In view of the existing radio frequency identification(RFID) authentication protocol based on quadratic residue in the security and cost aspects of the loopholes and deficiencies, an improved RFID bidirectional authentication protocol based on the quadratic residue was designed. The improved protocol was mixed with random number encryption under the framework of the quadratic residue, which makes the message certification and identification more efficient and fast in database authentication and identification; the ultra-lightweight bit replacement operations and XOR encryption communication information was introduced, which reduces the cost of system computing; in database, the random number checking mechanism was added to avoid attacks such as agreement to be synchronized and denial of service attacks; finally, the GNY logical proof of the protocol was given, which shows the feasibility of the improved protocol. The protocol security and performance analysis indicate that the improved protocol has higher security and lower cost.

Key words: quadratic residue, radio frequency identification, efficient, bidirectional authentication, ultra-light weight, checking, GNY logic

收稿日期: 2017-10-09; 修回日期: 2018-01-10

基金项目: 河南省重点科技攻关项目 (No.152102210227)

Foundation Item: Key Science and Technology Projects in Henan Province of China (No.152102210227)

1 引言

无线射频识别 (radio frequency identification, RFID) 是一种通过无线电信号识别目标并读写相关数据的技术。近年来为逐步实现智慧城市、智慧地球的目标, 需要以完整且安全的物联网技术为基础。因此, 作为物联网发展的先行者, 无线射频识别技术成为市场上最受关注的技术之一。它广泛应用于汽车收费、身份证件、门禁控制和生产控制等领域^[1]。但是, 一方面由于 RFID 系统本身具有无线通信的特点, 容易遭受信号干扰、恶意攻击等安全性问题; 另一方面由于系统硬件资源成本和计算能力的限制。因此想要设计出安全性高、低成本的 RFID 认证协议也是极具研究性的课题^[2]。

2 相关工作

2.1 二次剩余理论概述

若 a 、 m 互质 (记为 $(a, m)=1$), m 整除 $b^2 - a$ (记为 $b^2 \equiv a \pmod{m}$) 有解, 则称 a 为模 m 的二次剩余 (或平方剩余)。

本文二次剩余加密、解密算法操作具体如下^[3,4]: 因为 m 是一个非常大的数, 对其进行因数分解是不可能的, 可以保证加密数据的安全性; 又因为 m 是一个复合数, 在通信双方知道 m 的因数分解下 (n 个素数的乘积), 可以分解 $b^2 \equiv a \pmod{m}$, 通过求解每一个分解方程, 而得到 k 个 b 的值, 再根据提供的已知数据, 解密唯一值。具体加密解密过程如下所述。

(1) 密钥产生: 随机选择两个大素数 p 、 q , $p \equiv q \equiv 3 \pmod{4}$, 即这两个素数形式为 $4k+3$, 计算 $m = p * q$, 以 m 作为公钥, p 、 q 作为私钥。

(2) 加密: $a \equiv b^2 \pmod{m}$, 返回 a 。

(3) 解密: 根据 p 、 q 、 a 解密 b , 其中 C 是中国剩余定理, 具体如下:

$$x_1 = a^{(p+1)/4} \pmod{p}, \quad x_2 = -(a^{(p+1)/4}) \pmod{p}$$

$$x_3 = a^{(q+1)/4} \pmod{q}, \quad x_4 = -(a^{(q+1)/4}) \pmod{q}$$

$$b_1 = C(x_1, x_3, p, q), \quad b_2 = C(x_1, x_4, p, q)$$

$$b_3 = C(x_2, x_3, p, q), \quad b_4 = C(x_2, x_4, p, q)$$

返回 b_1 、 b_2 、 b_3 、 b_4 , 解密后有 4 个不同的解密结果, 所以在应用中, 通常还需要后续计算解密, 确定唯一解。比如, 可在 b 中加入某些冗余信息, 如随机数、身份 ID 等, 以便验证者可以快速有效地提取密文^[5]。

2.2 相关协议综述

近年来, 国内外很多学者在 RFID 认证协议方面做出了大量工作, 研究主要分为 3 个方向, 见表 1。

表 1 协议分类

协议分类	具体举例
重量级	基于 ECC 椭圆曲线密码编码 ^[6] 等
轻量级	单向函数 ^[7,8] 物理不克隆函数 ^[9] 、二次剩余等
超轻量级	仅基于简单单位运算 ^[10] , 如异或、移位等

其中为了设计出高效安全的 RFID 认证协议, 基于二次剩余理论的研究成果也尤为突出, 主要列举如下。2008 年, Chen 等人^[11]提出了一种基于二次剩余的认证协议, 此协议有较好的安全性, 但标签要进行公钥加解密运算及多次散列运算, 时间复杂度大、计算成本较高。2011 年, Yeh 等人^[12]在其提出的协议中完整证明了参考文献^[11]不能提供位置隐私并且不能抵抗重放攻击。之后, 轩秀巍等人^[3]提出了一种基于二次剩余的增强型 RFID 认证协议, 在该协议中进一步证明了参考文献^[12]容易受读写器假冒攻击和拒绝服务攻击, 并在此基础上提出了一种改进的更简单安全的认证协议。但是通过本文的研究发现, 参考文献^[3]并不能抵抗去同步化攻击和拒绝服务攻击, 具体证明将在第 2.3 节详解。2013 年, Doss 等人^[4]根据二次剩余定理提出了一种新的可隐私保护的移动 RFID 认证协议, 该协议遵循 EPC Gen-2 标准^[13] (EPC class1 Generation2, 电子标签标准), 系统



复杂度低, 适合低成本标签的应用, 但由于协议过程中后端数据库识别标签仍要进行多次计算查询, 所以协议认证效率较低; 另外, 当后端数据库收到读写器发送的消息后并没有对消息的新鲜性进行验证, 攻击者可以进行重放攻击, 以达到破坏或窃取秘密信息的目的。2015 年, Zhou^[14]提出了一种基于二次剩余的定时 RFID 认证协议, 在不使用计算代价昂贵的散列函数情况下, 实现在恒定时间内的识别认证。但此做法需要在后台数据库中标记每一个标签的有效认证时间, 这必然会在查询后台数据时增加对比时耗, 认证效率不高, 且认证过程稍显烦琐, 对于通常实际应用中使用的无源标签来说, 计算量较大。2016 年, 周治平等^[15]提出了一种更具实用性的基于二次剩余的移动 RFID 认证协议, 该协议增加了时间戳生成器, 提高系统安全性。

本文综合前人研究提出了一种改进的基于二次剩余的可抵抗去同步化攻击、拒绝服务攻击等多种常见攻击的 RFID 认证协议, 且协议在数据库端的认证效率上要优于现有方案。

2.3 具体协议不足

参考文献[15]提出的更具实用性的基于二次剩余的移动 RFID 认证协议, 包括 Doss 协议的初始化和双向认证阶段, 新增加了时间戳生成器, 提高系统安全性, 但是该协议仍然在标签端延续使用散列函数进行加密运算, 标签端成本略高, 与此对应的数据库也仍要进行多次散列运算进行匹配查询, 认证效率略低。而参考文献[3]在以下情况下不能抵抗去同步化攻击^[16]以及拒绝服务攻击。

2.3.1 去同步化攻击

攻击者假冒标签, 通过截获、重放窃听到的消息, 就可以通过数据库的身份验证, 以获取数据库的信任, 进行后续过程。最终因标签与数据库两边的共享密钥更新不同步, 协议失效。具体

攻击过程如下。

(1) 第一轮通信

正确标签和读写器开始进行通信认证, 当攻击者窃听通信消息 $\langle x, R, M, h(x), h(r), s \rangle$, 并截获数据库将要发送给标签端的验证消息 $\langle \text{Ack} \rangle$ 。此时, 数据库 key 更新成功, 而正常标签因为没有收到消息 $\langle \text{Ack} \rangle$ 而没有同时更新 key, 这时数据库和标签两端数据分别为:

D: $\text{key} = \text{PRNG}(\text{key}), \text{key_old} = \text{key};$

T: $\text{key} = \text{key}$

(2) 第二轮通信

攻击者假冒正确标签与数据库进行通信认证, 当读写器发送完消息 $\langle s, \text{request} \rangle$ 时, 攻击者重放上一轮窃听得到的 $\langle x, R, M, h(x), h(r), s \rangle$ 给数据库, 因为随机数对协议秘密信息的无关性, 使得数据库仅根据提供的随机数进行秘密信息提取的工作。因此数据库认证假冒标签成功, 更新 key, 这时攻击者对原标签重放上一轮截获到的 $\langle \text{Ack} \rangle$, 原标签认证成功, 更新 key, 这时数据库和标签两端数据分别为:

D: $\text{key} = \text{PRNG}(\text{PRNG}(\text{key})) \text{key_old} = \text{key};$

T: $\text{key} = \text{PRNG}(\text{key})$

至此攻击者成功的对参考文献[3]进行了共享密钥去同步化攻击, 由于标签和数据库后端共享密钥 key 没有同步更新, 这样在进行新一轮通信时, 标签就不能被数据库识别。最终, 认证失败, 攻击成功。

2.3.2 拒绝服务攻击

攻击者窃听正常通信过程, 记录消息 $\langle x, R, M, h(x), h(r), s \rangle$, 在标签下一次与读写器通信之前, 如果攻击者不断地向原服务器重放消息 $\langle x, R, M, h(x), h(r), s \rangle$, 由于此时原数据库只根据提供数据进行解密计算, 并没有新鲜性验证, 所以数据库对攻击者认证成功, 并不断计算 $\langle \text{Ack} \rangle$ 的值, 这不仅消耗通信资源, 使得其他正常的读写器无法与新数据库完成通信, 还可能因为通信请求频繁



进行后续计算得到 Ack, 并将 Ack 回复给读写器后更新共享密钥 key, 若不成立, 说明验证失败, 协议终止。

$$ID = p \oplus a \oplus b_i, \text{ Ack} = ID \oplus \text{Sub}(b, \text{key_R})$$

$$\text{key} = \text{PRNG}(\text{key}), \text{key_old} = \text{key}$$

(5) 读写器收到 Ack 消息后, 将之转发给标签。

(6) 标签收到 Ack 消息后, 验证 $\text{Ack}' = ? \text{Ack}$ 。若成立, 标签更新其密钥 key, 若不成立, 标签验证后端数据库失败 (也即验证读写器失败), 协议终止。

图2为本文提出的一种基于二次剩余的RFID认证协议过程。

4 改进协议形式化证明

本文以 GNY 逻辑证明^[18,19]为依据对改进协议进行形式化证明。证明如下:

(1) 形式化模型, 模型中标签为 T , 读写器为 R , 用 GNY 逻辑化形式语言来描述本协议中的消息。

$$M1: T \triangleleft *a$$

$$M2: R \triangleleft *F_1[b], *F_2[b]$$

$$M3: T \triangleleft *F_3[b]$$

(2) 初始化假设, 设 P1、P2 表示标签、读写器的拥有; P3、P4 表示标签、读写器对数据新鲜性的信任; P5、P6 表示标签和读写器对密钥的信任; P7、P8 表示标签和读写器相信各自的信息是

可识别的。

$$P1: T \in (ID, \text{key}), P2: R \in (ID, \text{key}, \text{Temp})$$

$$P3: T \models \#(ID, \text{key}, b), P4: R \models \#(ID, \text{key}, a)$$

$$P5: T \models R \xleftarrow{\text{key}} T, P6: R \models T \xleftarrow{\text{key}} R$$

$$P7: T \models \phi(b), P8: R \models \phi(a)$$

(3) 安全目标, 本协议的安全目标有 4 个, 即读写器对标签的认证识别; 标签对读写器拥有双方共享密钥 key 的信任; 读写器对标签拥有双方共享密钥 key 的信任; 标签对读写器的认证识别。

$$D1: R \models T \sim \#F_1(b), D2: T \models R \in \text{key}$$

$$D3: R \models T \in \text{key}, D4: T \models R \sim \#F_2(a)$$

(4) 证明过程, 当标签收到消息 M2 时, 由假设 P4, 得 $R \models \#(\text{key})$, 根据新鲜性规则 F1:

$$\frac{P \models \#(X)}{P \models \#(X, Y), P \models \#(F(X))} \text{ 可得 } R \models \#(b, \text{key}); \text{ 由已}$$

知假设 P2、P6, 得 $R \in (\text{key})$ 、 $R \models R \xleftarrow{\text{key}} T$; 认证成功 $R \triangleleft *(b)_{\text{key}}$, $R \models \phi(b)$, 根据消息解析规则 I1:

$$\frac{P \triangleleft *(X)_K, P \in K, P \models P \xleftarrow{K} Q, P \models \phi(X), P \models \#(X, K)}{P \models Q \sim X, P \models Q \sim (X)_K, P \models Q \in K} \text{ 得到}$$

$$R \models T \sim \#F_1(b), \text{ 目标 D1 得证, 目标 D4 同理。}$$

当标签收到消息 M3 后, 如果验证消息成功, 即有: $T \models \phi(b)$; 由初始化假设 P1、P3 可知: $T \in (\text{key})$ 、 $T \models \#(\text{key})$ 、再根据新鲜性规则 F7:

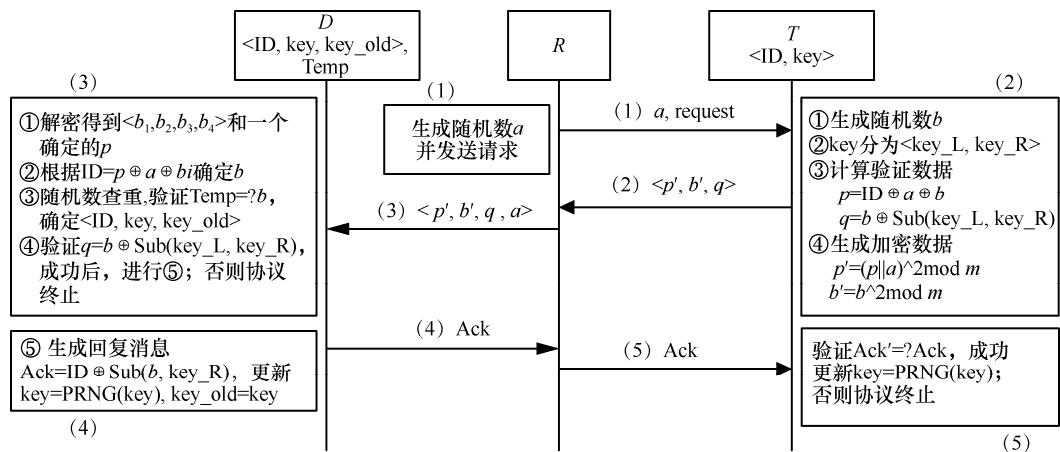


图2 一种改进的基于二次剩余的RFID认证协议过程

$$\frac{P|\equiv\phi(X), P|\equiv\#(K), P\in K}{P|\equiv\#(X)_K, P|\equiv\#(X)_K^{-1}}$$

可以得到 $T|\equiv\#(b)_{\text{key}}$, 所以 $T|\equiv\#(b)$; 再根据新鲜性规则 F1, 得到: $T|\equiv\#(b, \text{key})$; 最后根据消息 M3, 假设 P1、P5 以及消息解析规则 I1, 得到 $T|\equiv R \in \text{key}$, 预期目标 D2 实现, 目标 D3 同理。

5 改进协议安全性分析

5.1 去同步化攻击

当攻击者企图用第 2.3.1 节中描述的去同步化攻击方式, 使数据库与标签两端的共享密钥信息不一致时, 攻击会失败。因为, 本协议在保留上一轮共享密钥的前提下, 数据库端加入标签随机数查重机制, 当第一次重放 $\langle p', b', q \rangle$ 时, 数据库即检测出 $\text{Temp}=b$, 协议就会终止, 并不会造成两方密钥不一致的问题, 所以, 新协议可以抵抗去同步化攻击。

5.2 拒绝服务攻击

当攻击者企图以第 2 节描述的不断重复 $\langle p', b', q, a \rangle$ 信息, 以完成资源消耗, 系统崩溃地拒绝服务攻击时, 攻击将会失败。因为, 在本协议中使用随机数查重机制, 记录上一轮认证过程中数据库从标签端得到的随机数。因为随机数发生器产生数据的信息性和短期不可重复性, 当攻击者第一次重放数据时, 数据库解密得到随机数 b , 验证得到 $\text{Temp}=b$, 即是上一轮所用随机数和当前所用随机数相同, 于是系统判定异常, 协议终止, 也就不会继续发生由于频繁交互通信所造成的秘密信息泄露等严重问题。所以, 新协议可以抵抗拒绝服务攻击。

5.3 假冒攻击

一方面, 攻击者在不知道标签标识 ID 和标签随机数 b 的前提下假冒标签, 将无法计算出正确的二次剩余加密信息 $p' = (p \parallel a)^2 \bmod m$ 和 $b' = b^2 \bmod m$, 即使将这些信息发送给数据库求解出的 p 和 b 也是不真实的, 无论在验证 $\text{ID} = p \oplus a \oplus b_i$ 还是在验证 $q = b \oplus \text{Sub}(\text{key_L}, \text{key_R})$ 的过程中, 都无法与

数据库中的标签信息进行匹配, 故数据库认证失败, 协议终止; 另一方面, 攻击者在不知道二次剩余解密私钥 p 、 q 信息的前提下假冒数据库, 将无法解密得到标签秘密信息 ID 和 key , 从而无法计算出正确的确认消息 Ack , 所以标签认证失败, 协议终止。因此, 新协议可以抵抗假冒攻击。

5.4 重放攻击

本协议利用读写器和标签的双随机数机制和随机数查重验证机制来抵抗攻击者进行的重放攻击。当攻击者截获来自标签的消息 $\langle p', b', q \rangle$ 假冒标签, 并在下一轮重放时, 因为在数据库端加入对上一轮随机数 b 的查重检测, 所以当发现 $\text{Temp}=b$ 时, 协议终止, 攻击者重放攻击失败; 当攻击者截获来自数据库的回复信息, 以假冒数据库并在下一轮重放 Ack 时, 因为标签端会在新一轮认证中产生新的随机数 b 而此时标签端的随机数 b 和重放 Ack 中的 b 并不一致, 所以认证失败, 协议终止。因此新的协议可以抵抗重放攻击。

5.5 标签匿名性

在本协议全部通信过程中标签的标识 ID 并没有明文传输, 而是通过二次剩余加密处理; 并且, 攻击者在没有私钥 x 、 y 的前提下仅通过窃听得到的 $\langle p', b', q, a, \text{Ack} \rangle$ 消息中并不能获得标签 ID, 所以本协议标签端具有匿名性。

5.6 跟踪攻击

本协议中, 虽然标签 ID 不变, 但是每次通信过程中 $\langle p', b', q, \text{Ack} \rangle$ 均是由随机数 a 、 b 经过组合计算而得到, 具有新鲜性和不确定性, 攻击者无法仅通过上述窃听得到的消息对协议进行跟踪攻击。

5.7 前向安全

在本协议中, 通过二次剩余理论和位替换与异或超轻量级运算加密数据, 在保证数据具有一定安全性的前提下, 引入了标签随机数组合运算, 具有不可预测性和协议无关性, 即使标签信息发生泄露, 攻击者仍然不能根据标签现有信息



表3 协议的安全性比较

攻击类型	参考文献[3]协议	参考文献[4]协议	参考文献[14]协议	参考文献[15]协议	本协议
去同步化攻击	×	√	O	√	√
拒绝服务攻击	×	√	O	√	√
假冒攻击	√	×	√	√	√
重放攻击	×	×	√	×	√
标签匿名性	√	√	√	√	√
跟踪攻击	√	√	√	√	√
前向安全	√	O	O	O	√

推测标签以前的行为,因此协议具有前向安全性。

综上所述,针对以上攻击类型,表3给出了本协议和其他相关RFID协议的安全性比较。

表3中,“√”表示可以抵抗这种攻击行为,“×”表示不能抵抗这种攻击行为,“O”表示不确定。

6 改进协议性能分析

本节主要从标签的计算量、存储量和通信量3个方面对本协议进行性能分析,见表4。

表4 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[3]协议	2E+4H+2P	3I	L
参考文献[4]协议	4E+3P	3I	L
参考文献[14]协议	3E+2P+4X	3I	2L
参考文献[15]协议	2E+3P	3I	L
本文协议	2E+3X+S+2P	2I	L

标签计算量:本协议标签端包含二次剩余基础算法和随机数生成器之外摒弃成本较高的散列运算,仅使用两种简单单位运算(位替换位和异或运算),降低标签成本。

标签存储量:初始阶段,标签只存储了标签唯一标识信息ID和与数据库之间的共享密钥key。

标签通信量:每一轮认证过程中,标签端只传送一次 $\langle p', b', q \rangle$ 信息。

表4中,E表示二次剩余计算,H表示散列运算,X表示异或运算,P表示随机数计算,S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。

通过表4可以看出,本文协议与其他对比协议在综合考虑标签通信量和存储空间占用量的情况下,有明显优势。在存储量方面因为标签充分利用已有信息(共享密钥),将共享密钥分成左右两部分进行加密计算,减少了其他信息的引入,故本协议最优。计算量方面,因为协议引入超轻量级位运算并减少了随机数生成次数,所以同样降低标签计算成本,具有明显优势。综上所述,本协议具有更好的性能。

7 结束语

本文分析并总结了现有RFID认证协议的分类与特点,并通过分析一些二次剩余理论协议的安全漏洞与性能缺陷,设计了一种改进的基于二次剩余的超轻量级RFID安全认证协议。改进协议具有如下特点:在基础二次剩余算法中加入随机数混合加密运算,实现更高效认证;摒弃常用的散列算法,引入超轻量级位运算,降低成本;设计数据库随机数校验机制,避免协议遭受一些恶意攻击。下一步会对所提出协议进行进一步的实验仿真。

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]. Telecommu-

- nications Science, 2014, 30(2): 1-13.
- [2] 李荣荣, 寇建涛, 董刚, 等. 面向智慧园区的 RFID 系统信息安全认证方案[J]. 电信科学, 2016, 32(2): 164-169.
LI R R, KOU J T, DONG G, et al. A security authentication scheme in RFID system for smart park[J]. Telecommunications Science, 2016, 32(2): 164-169.
- [3] 轩秀巍, 滕建辅, 自煜. 基于二次剩余的增强型 RFID 认证协议[J]. 计算机工程, 2012, 38(3): 123-125.
XUAN X W, XI J F, ZI Y. Enhanced RFID authentication protocol based on quadratic residue[J]. Computer Engineering, 2012, 38(3): 123-125.
- [4] 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.
- [5] 高利军. 无线射频识别系统安全认证协议研究[D]. 天津: 天津大学, 2015: 70-71.
GAO L J. Research on security authentication protocol for radio frequency identification system[D]. Tianjin: Tianjin University, 2015: 70-71.
- [6] VAIDYA B, MAKRAKIS D, MOUFTAH H T. Authentication mechanism for mobile RFID based smart grid network[C]//Electrical and Computer Engineering(CECE), May 4-7, 2014, Toronto, ON, Canada. Piscataway: IEEE Press, 2014: 1-6.
- [7] 裴小强, 卫宏儒. 基于 Hash 链的 RFID 安全双向认证协议[J]. 计算机应用, 2014, 34(S1): 47-49.
PEI X Q, WEI H R. RFID mutual security authentication protocol based on Hash-chain[J]. Journal of Computer Applications, 2014, 34(S1): 47-49.
- [8] NIU B, ZHU X, CHI H, et al. Privacy and authentication protocol for mobile RFID systems[J]. Wireless Personal Communications, 2014, 77(3): 1713-1731.
- [9] 寇红召, 张紫楠, 马骏. 基于物理不可隆函数的 RFID 双向认证[J]. 计算机工程, 2013, 39(6): 142-145.
KOU H Z, ZHANG Z N, MA J. RFID bi-directional authentication based on physical immovable function[J]. Computer Engineering, 2013, 39(6): 142-145.
- [10] 王超. 超轻量级 RFID 认证协议研究与实现[D]. 南京: 南京航空航天大学, 2014.
WANG C. Research and implementation of super lightweight RFID authentication protocol[D]. Nanjing: Nanjing University of Aeronautics & Astronautics, 2014.
- [11] CHEN Y L, CHOU J S, SUN H M. A novel mutual authentication scheme based on quadratic residues for RFID systems[J]. Computer Networks, 2008, 52(12): 2373-2380.
- [12] YEH 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.
- [13] IMPLIED E OR, THIS T, IS D, et al. Specification for RFID air interface EPC "radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860MHz-960MHz [EB]. 2013.
- [14] ZHOU J. A quadratic residue-based lightweight RFID mutual authentication protocol with constant-time identification[J]. Journal of Communications, 2015, 10(2): 117-123.
- [15] 周治平, 张惠根. 一种更具实用性的移动 RFID 认证协议[J]. 传感技术学报, 2016, 29(2): 271-277.
ZHOU Z P, ZHANG H G. A more practical mobile RFID authentication protocol[J]. Chinese Journal of Sensors and Actuators, 2016, 29(2): 271-277.
- [16] 马巧梅. 基于 HMAC 的轻量级 RFID 认证协议[J]. 微处理机, 2015, 5(4): 27-31.
MA Q M. A HMAC-based RFID lightweight authentication protocol[J]. Microprocessors, 2015, 5(4): 27-31.
- [17] 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.
- [18] 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 method and security protocol design for security protocol[D]. Beijing: Tsinghua University, 2004.
- [19] 王崇霞, 高美真, 刘倩, 等. 混合云联合身份认证与密钥协商协议设计[J]. 电信科学, 2014, 30(4): 95-99, 108.
WANG C X, GAO M Z, LIU Q, et al. Design of united identity authentication and key agreement protocol for hybrid cloud [J]. Telecommunications Science, 2014, 30(4): 95-99, 108.

[作者简介]



刘直良 (1982-), 男, 黄淮学院信息工程学院讲师, 主要研究方向为网络与通信。