计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2021,30(12):345−349 [doi: 10.15888/j.cnki.csa.008185]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

轻量级的射频识别系统认证协议①

谢海宝[1], 郝伟伟[1], 吕　磊[2]

[1](河南省市场监督管理局 信息中心, 郑州 450008)
[2](河南工业大学 信息科学与工程学院, 郑州 450008)
通讯作者: 谢海宝, E-mail: xihaba81@163.com

摘　要: 射频识别系统中电子标签与读卡器之间基于无线方式交互数据, 因无线方式固有的开放性, 使得二者间交互数据易被第三方人员获取, 为确保数据安全性, 文中设计一种轻量级的认证协议. 文中选取轻量级的伪随机函数作为数据加密算法, 能够使得射频识别系统整体计算量降低, 且同时确保交互数据的安全性; 伪随机函数可以对任意输入长度参数进行运算, 使其输出结果长度相同. 通过安全角度、计算量角度、门电路角度综合分析文中协议, 表明协议具备较高安全需求的同时, 整体计算量优于其他对比协议.

关键词: 射频识别系统; 无线通信链路; 开放性; 轻量级; 伪随机函数

引用格式: 谢海宝,郝伟伟,吕磊.轻量级的射频识别系统认证协议.计算机系统应用,2021,30(12):345–349. http://www.c-s-a.org.cn/1003-3254/8185.html

Lightweight Authentication Protocol for RFID System

XIE Hai-Bao[1], HAO Wei-Wei[1], LYU Lei[2]

[1](Information Center, Administration for Market Regulation Bureau, Henan Province, Zhengzhou 450008, China)
[2](College of Information Science and Technology, Henan University of Technology, Zhengzhou 450008, China)

Abstract: In a Radio-Frequency IDentification (RFID) system, the interaction data between an RFID tag and the reader is in a wireless communication mode. Due to the inherent openness of the mode, the interaction data can be easily obtained by a third party. For the sake of data security, a lightweight authentication protocol is designed in this study. A lightweight pseudo-random function is selected as the data encryption algorithm, which can reduce the overall calculation amount of the RFID system and ensure the security of the interaction data. Meanwhile, it can operate on an input parameter of any length and give an output of a fixed length. A comprehensive analysis of the protocol from the perspectives of security, calculation amount, and gate circuit shows that the protocol has high security requirements and the overall calculation amount is also less than those of other protocols in comparison.

Key words: RFID system; wireless communication link; openness; lightweight; pseudo-random function

射频识别技术虽出现在上个世纪上半时期, 但真正得到大范围推广却是在本世纪; 该技术是一种不需要与特定商品相接触, 就可以读出该特定商品中存放数据的技术[1,2]. 一个完整的射频识别系统具备成本低、较容易部署、使用寿命长等优势, 使得射频识别技术现在多个领域中应用, 比如: 门禁系统、地铁卡系统、校园卡系统等[3,4].

比较经典的射频识别系统一般至少包含后台数据库、电子标签、读卡器 3 个实体设备[5−7]. 后台数据库主要用来存放系统应用过程中产生的数据, 具备强大

① 基金项目: 国家自然科学基金 (61705060)
Foundation item: National Natural Science Foundation of China (61705060)
收稿时间: 2021-02-07; 修改时间: 2021-03-05; 采用时间: 2021-03-16

的计算和搜索查找能力, 同时也具备较大的存储空间; 电子标签一般主要在用户手上, 用于存放用户的一些个人隐私信息, 比如: 用户标识、用户金额等, 电子标签计算能力有限、存储空间同样也有限; 读卡器一般主要固定在某个地方, 用于读取电子标签中信息, 再将读取的信息发送给后台数据库, 很多时候读卡器并不真正的参与运算.

在上述经典的射频识别系统中, 电子标签与读卡器之间无线方式交互数据, 极其容易被第三方窃听, 导致用户隐私信息泄露, 研究人员一般认为不可靠、不安全; 读卡器与后台数据库之间绝大多数基于有线方式交互信息, 第三方获取数据并不是很容易, 一般可认定为安全、可靠, 并可将二者看成一个系统或整体对待[8,9]. 文中为能够保证电子标签与后台数据库二者间数据交互安全, 提出一个采用伪随机函数实现加密的轻量级认证协议.

1 相关工作

文献 [10] 中利用散列函数设计一个认证协议, 对协议分析, 可以提供一些安全需求, 但因数据加密过程中部分数据第三方可以获取, 使得协议无法抵抗第三方穷举分析.

文献 [11] 中设计一个超轻量级的协议, 虽能够极大程度上降低系统计算量, 但依据现有的研究结果表明, 超轻量级的协议绝大多数都是基于按位运算实现, 而简单的按位运算是无法提供绝对的安全性, 因此文献 [11] 中协议安全性级别有待商榷.

文献 [12] 中利用经典的哈希函数设计一个认证协议. 协议设计过程中充分考虑到各种常见类型的攻击, 因此该协议具备良好的安全需求. 但电子标签一端将会多次用到哈希函数进行运算, 将会使得系统整体计算量增加, 低沉本受限制的电子标签无法大规模推广.

文献 [13] 中基于物理不可克隆技术设计一个认证协议. 物理不可克隆技术使得协议可以抵抗假冒攻击等, 但对协议分析, 表明协议最后一个步骤并没有完成电子标签对读卡器的验证, 使得协议存在安全缺陷.

文献 [14] 中结合 Universal 哈希函数给出一个协议. Universal 哈希函数与经典的哈希函数之间存在些许不同, 但整体工作原理相差并不大. 因具备的单向性, 是第三方难以假冒或重放; 却无法在低成本电子标签系统中推广使用.

文献 [15] 中采用 RRAM 物理不可克隆技术设计一个认证协议. 协议设计过程中, 部分消息加密时未混入随机数, 使得部分消息前后多次认证过程中消息计算数值相同, 给了第三方破解机会.

对近些年经典协议进行分析, 指出大多数协议存在或多或少缺陷不足, 文中基于伪随机函数设计一个轻量级的认证协议.

2 双向认证协议设计

(1) 协议中部分符号解释

READER: 由读卡器和后台数据库构成的整体

TAG: 电子标签

ID_T: TAG 的假名身份标识

ID_{T_new}: TAG 当前的假名身份标识

ID_{T_old}: TAG 上次的假名身份标识

ID_{T_L}: TAG 真实身份标识前面一半

ID_{T_R}: TAG 真实身份标识后面一半

KEY: TAG 与 READER 二者间共享秘密值

KEY_{new}: TAG 与 READER 二者间当前共享秘密值

KEY_{old}: TAG 与 READER 二者间上次共享秘密值

$f(x,y)$: 伪随机函数

x: TAG 生成的随机数

y: READER 生成的随机数

$\oplus$: 按位异或运算

&: 按位与运算

(2) 认证协议步骤

可以结合图 1 中的流程, 将文中协议步骤描述如下:

①READER 向 TAG 发送一个认证请求指令,READER 与 TAG 之间将开启认证.

② TAG 接到消息, TAG 先生成随机数, 在依次计算得到消息$M1 = x \oplus ID_{T_L}$、$M2 = f(x, ID_{T\_R})$, 待消息计算完毕, TAG 将向 READER 发送 $M1$、$M2$、ID_T.

③ READER 接到消息, 先在数据库中查找是否有数据与接到的 ID_T 相同.

若未找到, 则协议停止.

若找到, 则协议可继续. READER 将对接到的 $M1$ 进行变形, 并将变形之后结果带入消息 $M2$ 中可得到$M2' = f(x', ID_{T_R}) = f(M1 \oplus ID_{T_L}, ID_{T_R})$, 然后对比 $M2$、$M2'$ 值是否相等.

若不相等, 则协议停止.

若相等, 则可表明 TAG 通过 READER 验证, 协议再次继续. READER 将生成随机数, 并依次计算得到消息

$M3 = y \oplus ID_{T\_R}$, $M4 = f(x,y)$, 最后将 $M3$, $M4$ 发送给 TAG.

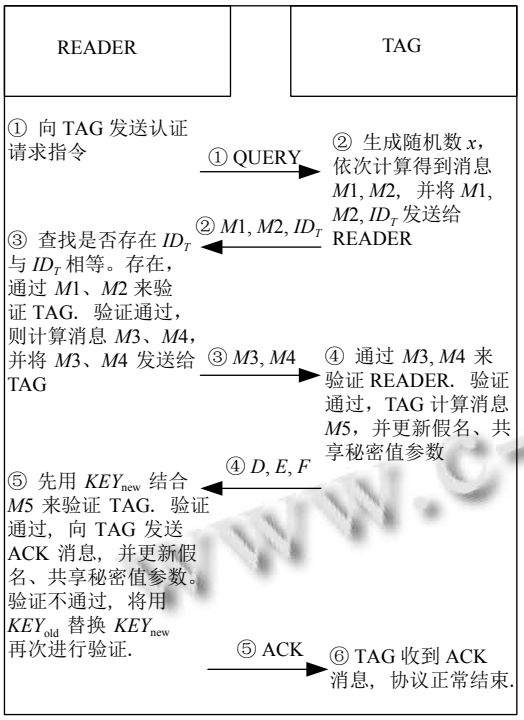

图 1 协议流程图

④ TAG 接到消息后, TAG 会发起对 READER 的验证, 具体验证过程如下:

TAG 将先对接到的消息 $M3$ 进行变形处理, 并将变形处理结果带入消息 $M4$ 中可得到 $M4' = f(x,y') = f(x, M3 \oplus ID_{T\_R})$, 接着比较 $M4$、$M4'$二者是否相等.

若不相等, 协议停止.

若相等, 可表明 READER 通过 TAG 的验证, 协议继续. TAG 将计算消息 $M5 = f(x \oplus KEY, y \,\&\, KEY)$, 并将 $M5$ 发送给 READER. 待 TAG 发送消息 $M5$ 之后, TAG 一端将进行共享秘密值、TAG 假名身份标识更新操作 $ID_T = f(y, ID_T)$、$KEY = f(x, KEY)$.

⑤ READER 接到消息后, 先用当前 READER 与 TAG 间共享秘密值 KEY_{new} 来验证 TAG, 具体过程见下:

READER 利用存放的 KEY_{new}、之前计算所得 x、自己生成 y 计算得到消息 $M5' = f(x \oplus KEY_{new}, y \,\&\, KEY_{new})$, 接着比较计算得到 $M5'$ 与接到消息 $M5$ 大小关系.

两者关系不等, READER 将再次用上次二者间共享秘密值验证 TAG, 即用 KEY_{old} 替换 KEY_{new} 再次进行计算可得到 $M5'' = f(x \oplus KEY_{old}, y \,\&\, KEY_{old})$, 然后再次对比 $M5$ 与 $M5''$ 大小. 还是不等, 协议停止; 此时等, READER 验证 TAG 通过, 协议继续执行, READER 向 TAG 发送 ACK 确定消息, 同时 READER 端进行信息更新 $ID_{T\_old} = ID_{T\_new}$, $ID_{T\_new} = f(y, ID_T)$, $KEY_{new} = f(x, KEY_{old})$.

两者关系等, READER 验证 TAG 通过, 协议继续执行, READER 向 TAG 发送 ACK 确定消息, 同时 READER 端进行信息更新 $ID_{T\_old} = ID_{T\_new}$, $ID_{T\_new} = f(y, ID_T)$, $KEY_{old} = KEY_{new}$, $KEY_{new} = f(x, KEY_{new})$.

⑥ TAG 接到消息, 确定接到消息为 ACK, 则表明 TAG 与 READER 间双向认证完成, 协议可正常结束.

3 安全性分析

(1) 双向认证

双向认证是协议要具备的最基本的安全需求. 文中协议具备该安全需求, 具体的分析见下:

在第③步中, READER 将先通过 TAG 假名参数验证 TAG 真实性, 接着将再次结合消息 $M1$、$M2$ 对 TAG 进行验证, 只有两次都验证通过, READER 才会继续执行协议.

在第④步中, TAG 将结合消息 $M3$、$M4$ 对 READER 进行验证, 验证通过, TAG 将才会进行后续操作.

在第⑤步中, READER 将先用 KEY_{new} 来验证 TAG 真假; 验证不通过时, READER 将再次用 KEY_{old} 来验证 TAG 真伪. 前后两次验证通过, 协议才继续.

基于上述分析, 文中协议可提供双向认证安全需求.

(2) 假冒攻击

从理论上来讲, 第三方既可以假冒成 READER, 也可以假冒成 TAG. 鉴于文中篇幅有限, 这里仅选取第三方假冒成 READER 来分析.

比如: READER 假冒成合法读卡器向合法 TAG 发送认证请求指令, 开始认证协议. 经过一段时候后, 第三方可以收到合法 TAG 发送来的消息 $M1$、$M2$, 第三方试图通过对接到的消息 $M1$、$M2$ 进行分析从而破解出隐私信息, 然后在计算正确消息 $M3$、$M4$, 但第三方无法成功. 无法成功的主要原因有: 第三方不知晓 TAG 真实身份标识, 使得第三方无法通过消息 $M1$、$M2$ 破解分析出合法 TAG 生成的随机数 x, 第三方在不知道随机数 x 的情况下, 第三方只能随机选择一个数冒充为随机数 x, 可想而知, 第三方就无法计算出正确的消息 $M3$、$M4$. 当合法 TAG 接到第三方发送来的消息

$M3$、$M4$ 时, 只需要进行简单计算, 合法 TAG 即可识别出第三方是假冒的, 协议停止.

基于上述分析, 文中协议可提供抵抗假冒攻击安全需求.

(3) 重放攻击

第三方可以窃听当前会话过程, 获悉当前会话过程中所有消息, 待下轮会话时, 第三方可以重放窃听的消息, 以企图通过合法实体验证, 进而获取更多隐私信息. 但文中协议中, 第三方只能以失败而告终, 具体原因如下: 文中协议设计过程中, 每个消息加密之时, 都引入随机数, 或引入 READER 生成的随机数, 或引入 TAG 生成的随机数, 或同时引入 READER、TAG 生成的随机数, 这样操作之后, 将使得每轮消息计算值处于变动之中. 即: 第三方人员在重放上轮窃听消息时, 本轮认证中用到的消息值早已发生变更, 第三方重放消息失败, 协议停止, 第三方未获取任何隐私信息.

基于上述分析, 文中协议可提供抵抗重放攻击安全需求.

(4) 异步攻击

文中协议在 READER 一端将会存放 READER 与 TAG 间之前认证过程中用到的共享秘密值, 这样就可以抵抗第三方发起的异步攻击. 具体原因分析如下: 当 READER 用当前共享秘密值发起对 TAG 验证时, 验证通过, 就直接进行后续操作; 如果没有验证验证, 则 READER 将会调出上一轮认证过程中用到的共享秘密值, 将用上轮认证过程中用到的共享秘密值替换当前共享秘密值再次发起对 TAG 的验证. 如果本次验证还是失败, 则 READER 将再次调出上上次认证用到的共享秘密值, 以此方式可以实现抵抗第三方发起的异步攻击.

基于上述分析, 文中协议可提供抵抗异步攻击安全需求.

(5) 穷举攻击

第三方可能对窃听获悉的消息采用穷举的方式穷尽出所有其可能值, 进而获取隐私信息. 但文中协议可是第三方无法穷举成功, 这里选择消息 $M1$、$M2$ 为例进行详细分析:

第三方可以对消息 $M1$ 进行变形处理, 并将变形处理结果带入消息 $M2$ 中可得到$M2' = f(M1 \oplus ID_{T_L}, ID_{T_R})$. 在变形之后所得到消息 $M2$ 中, 第三方仍有两个参量ID_{T_L}、ID_{T_R}不知晓, 因此第三方就无法采用穷举方式穷尽所有可能值, 第三方只能以失败而告终.

基于上述分析, 文中协议可提供抵抗穷举攻击安全需求.

(6) 前向安全

第三方想通过窃听获悉的消息逆推出上轮认证用到的部分隐私信息, 以此来获悉更多用户隐私信息. 但文中协议中, 第三方无法从窃听获悉的消息中分析或逆推出上轮会话中用户隐私信息, 具体原因分析如下: 文中协议设计过程中, 每个认证消息均不是明文方式发送, 而是采用伪随机函数加密之后再发送, 这使得第三方窃听获悉的数据是密文; 第三方在不知晓关键参数情况下, 是无法分析或逆推出之前认证中用户隐私信息; 同时所有消息加密过程中都有随机数的加入, 这样使得前后每次消息值不同, 并且随机数具备互异性、无法预测性, 更加增加了第三方破解分析难度.

基于上述分析, 文中协议可提供前向安全需求.

4 性能分析

从文中前面章节有关经典射频识别系统组成描述可以知晓, READER 整体计算能力强、存储空间大; 相反, TAG 计算能力薄弱、存储空间有限, 故本章节仅选取 TAG 作为性能分析对象. 将文中协议与其他近些年提出的经典协议进行性能方面分析, 结果见表 1 所示.

表 1 不同协议之间性能分析对比

对比类型	计算量	通信量
文献[13]	5 Ta+6 Tb+1 Tc	7 L+3 bit
文献[14]	3 Ta+4 Td+2 Tc	8 L+1 bit
文献[15]	2 Ta+7 Tb+1 Tc	5 L+1 bit
文中协议	2 Ta+5 Te+1 Tc	6 L+2 bit

对表 1 中出现的符号所表示的意思解释见下面: Ta 符号代表的意思为按位运算的计算量 (此处按位运算可包含按位异或运算、按位与运算等); Tb 符号代表的意思为物理不可克隆函数的计算量; Tc 符号代表的意思为随机数发生器产生随机数的计算量; Td 符号代表的意思为哈希函数的计算量; Te 符号代表的意思为伪随机函数的计算量.

文中协议整个过程中 TAG 一端仅只生成一个随机数, 故会有 1 Tc 计算量. 在步骤 (2) 中, TAG 在计算消息 $M1$ 时第 1 次用到 Ta 计算量, 在计算消息 $M2$ 时第 1 次用到 Te 计算量; 在步骤 (4) 中, TAG 在对消息 M3 变形处理时会第 2 次用到 Ta 计算量, 在计算消息

$M4'$时会第 2 次用到 Te 计算量, 在计算消息 $M5$ 时会第 3 次用到 Te 计算量, 在更新 TAG 假名身份标识、共享秘密值时分别第 4 次、第 5 次用到 Te 计算量.

基于上述分析, 文中协议在 TAG 一端总体计算量为 2 Ta+5 Te+1 Tc.

文中协议一个完整会话包含的会话消息有 $M1$、$M2$、ID_T、$M3$、$M4$、$M5$、ACK、认证请求指令 QUERY, 其中消息 $M1$、$M2$、ID_T、$M3$、$M4$、$M5$ 每个长度都是 L 位, ACK、认证请求指令 QUERY 长度都是 1 个比特即可. 故文中协议通信量大小为 6 L+2 bit.

通过本节及第 3 节分析, 可发现文中协议不仅可以弥补其他经典协议中安全不足, 同时在计算量方面优于其他协议, 具有推广使用价值.

5 结论与展望

文中先介绍射频识别技术在运用过程中出现的安全隐患, 在分析近些年经典的认证协议存在的问题, 最后设计出一个轻量级的认证协议. 文中设计协议在兼顾计算量的同时, 也考虑安全性, 故选择轻量级的伪随机函数作为消息加密算法; 为能够应对假冒、重放等攻击, 协议在消息加密中全部混入随机数, 可保持消息新鲜性; 为能够抵抗第三方发起的异步攻击, 协议在 READER 一端存放若干轮之前认证用到的共享秘密值. 结合安全性、计算量等角度分析文中协议及近些年其他经典协议可发现, 文中协议可弥补其他协议安全不足之处, 同时可保证计算量、门电路总个数未增加.

参考文献

1 Xie R, Jian BY, Liu DW. An improved ownership transfer for RFID protocol. International Journal of Network Security, 2018, 20(1): 149–156.

2 刘道微, 凌捷, 杨昕. 一种改进的满足后向隐私的 RFID 认证协议. 计算机科学, 2016, 43(8): 128–130, 158. [doi: 10.11896/j.issn.1002-137X.2016.08.027]

3 Tang D, Wang YQ, Yang HP. Array erasure codes with preset fault tolerance capability. International Journal of Network Security, 2018, 20(1): 193–200.

4 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. 计算机应用研究, 2017, 34(5): 1531–1535. [doi: 10.3969/j.issn.1001-3695.2017.05.057]

5 Zuo C. Defense of computer network viruses based on data mining technology. International Journal of Network Security, 2018, 20(4): 805–810.

6 史志才, 王益涵, 张晓梅, 等. 一种具有隐私保护与前向安全的 RFID 组证明协议. 计算机工程, 2020, 46(1): 108–113.

7 段艳萍. 轻量级 RFID 群组标签生成协议. 控制工程, 2020, 27(4): 751–757.

8 石乐义, 贾聪, 宫剑, 等. 基于共享秘密的伪随机散列函数 RFID 双向认证协议. 电子与信息学报, 2016, 38(2): 361–366.

9 Veena K, Meena K. Identification of cyber criminal by analyzing users profile. International Journal of Network Security, 2018, 20(4): 738–745.

10 郭奕旻, 李顺东, 陈振华, 等. 一种轻量级隐私保护的 RFID 群组证明协议. 电子学报, 2015, 43(2): 289–292. [doi: 10.3969/j.issn.0372-2112.2015.02.013]

11 黄可可, 刘亚丽, 殷新春. 基于位重排变换的超轻量级 RFID 双向认证协议. 计算机应用, 2019, 39(1): 118–125. [doi: 10.11772/j.issn.1001-9081.2018071738]

12 王萍, 周治平, 李静. 无后端数据库的 RFID 安全认证协议的改进方案. 计算机科学与探索, 2018, 12(7): 1117–1125. [doi: 10.3778/j.issn.1673-9418.1705011]

13 Feng T, Guo JQ. A new access control system based on CP-ABE in named data networking. International Journal of Network Security, 2018, 20(4): 710–720.

14 Xie R, Ling J, Liu DW. Wireless key generation algorithm for RFID system based on bit operation. International Journal of Network Security, 2018, 20(5): 938–950.

15 Tang F, Huang D. A BLS signature scheme from multilinear maps. International Journal of Network Security, 2020, 22(5): 728–735.