文章编号：1007-757X(2022)09-0052-04

适用于低成本 RFID 系统的双向认证算法

卢爱芬

（广州科技职业技术大学，信息工程学院，广东，广州 510550）

摘　要：在运用射频识别系统过程中，电子标签与读卡器间采用无线信道方式进行数据交换。无线信道固有的开放性使得数据交换过程时易被攻击者窃听，存在一定的安全隐患。为了解决该安全隐患问题，设计一个双向认证算法，用于保护电子标签与读卡器间数据交换安全性。算法为适用于低成本 RFID 系统，采用变形反比例函数对传送信息进行加密，变形反比例函数实现时巧妙结合加密参数自身汉明权重值，在减少信息引入的同时，亦可增加算法安全性能。文章从安全性及性能分析等多角度与已知算法进行比较，文中提出的算法具备较高的安全性能及低成本计算量特征。

关键词：物联网；射频识别技术；变形反比例函数；双向认证

中图分类号：TP393　　文献标志码：A

Mutual Authentication Algorithm for Low-cost RFID System

LU Aifen

(School of Information Engineering, Guangzhou University of Science and Technology, Guangzhou 510550, China)

Abstract: In the application of RFID systems, the data exchange between the tag and the reader is based on the wireless channel. The inherent openness of the wireless channel makes the data exchange process easy to be eavesdropped by attackers, and there is a certain security risk. In order to solve the problem, this paper designs a mutual authentication algorithm to protect the data between the tag and the reader exchange security. In order to be suitable for low-cost RFID system, the algorithm uses the deformable inverse proportion function to encrypt the transmitted information. When the deformable inverse proportion function is implemented, it skillfully combines the Hamming weight value of the encryption parameter itself, which can reduce the introduction of information and increase the security performance of the algorithm. The algorithm is compared from the perspectives of formal logic analysis, security analysis and performance analysis. The algorithm proposed has the characteristics of rigorous logic reasoning, high security performance and low cost of computation.

Key words: Internet of Things; radio frequency identification (RFID) technology; deformable inverse proportional function; bi-directional authentication

0　引言

射频识别系统一般包含电子标签、读写器、后台服务器三者。其中，电子标签因体积小、方便携带、易部署、成本不高、使用时间长等众多优势，使射频识别技术在很多领域中得到应用[1-3]。常见的电子标签一般有 2 种类型：一种是自身携带电源，可主动发起认证；另一种是自身并没有携带电源，无法主动发起认证，只能被动式响应读写器信息。现有的射频识别系统中，大多数用的电子标签还是属于无电源类型的[4-6]。

射频识别系统中经典的通信模型是读写器与后台服务器间有线链路实现交互，一般认为安全可靠；读写器与电子标签间采用无线链路，因无线链路自身具备的开放性，使得消息易被攻击者监听获取，存在安全隐患[7-8]。在早期的射频识别系统认证算法中，较多时候会采用经典的密码加密算法对所要发送信息进行加密，但现有的电子标签因低成本因素，使得电子标签计算能力受到严格限制，无法采用经典加密算法[9-10]。

文献[11]中采用简单的异或运算、与运算实现信息加密，但协议无法抵抗攻击者发起的物理攻击，攻击者物理攻击成功后，可对标签发起假冒攻击。文献[12]中采用物理不可克隆函数对信息加密，算法虽具备一定安全性，但因读写器端未存放前后轮会话共享密钥，使得协议无法抗去同步化攻击。文献[13]中采用经典的 HASH 函数实现信息加密，文献[14]中算法对文献[13]中算法进行了详细安全性分析，指出文献[13]中算法无法提供会话实体间双向认证缺陷，同时算法还无法抗攻击者发起的假冒攻击安全缺陷。

针对现有大多数双向认证算法或存在安全隐患或存在计算量大无法适用低成本 RFID 系统等不足，文中在结合众多协议基础之上，设计一个采用变形反比例函数实现加密的

基金项目：广东省教育部产学研合作专项基金项目(2008B090500266)

作者简介：卢爱芬(1975－)，女，硕士，讲师，研究方向为信息安全、计算机网络体系结构、软件工程。

双向认证算法。

1　双向认证算法

本小节首先介绍算法中涉及的符号含义，然后给出文中算法加密用的变形反比例函数具体定义，最后给出算法。

1.1　算法符号含义

R 表示读写器；

T 表示电子标签；

ID_L 表示电子标签标识符左边一半；

ID_R 表示电子标签标识符右边一半；

ID 表示电子标签标识符；

K 表示电子标签与读写器间共享秘密值；

K_{new} 表示电子标签与读写器间当前共享秘密值；

K_{old} 表示电子标签与读写器间上轮共享秘密值；

$Gf(x,y)$ 表示变形反比例函数；

a 表示电子标签产生的随机数；

b 表示读写器产生的随机数；

& 表示按位与运算；

⊕ 表示按位异或运算。

1.2　变形反比例函数

变形反比例函数按照如下方式定义：约定 x、y 都是长度为 L 位的二进制串；$\mathrm{hm}(x)$、$\mathrm{hm}(y)$ 分别表示二进制串 x、y 的汉明重量值；变形反比例函数一般形式如 $y=m/x+n$。当 $\mathrm{hm}(x)>\mathrm{hm}(y)$ 时，取 $\mathrm{hm}(y)$ 的值作为上述一般形式中 m 的值，取 $\mathrm{hm}(x)$ 的值作为上述一般形式中 n 的值，同时对参数 y 进行反比例函数加密计算。当 $\mathrm{hm}(x)\leqslant\mathrm{hm}(y)$ 时，取 $\mathrm{hm}(y)$ 的值作为上述一般形式中 n 的值，取 $\mathrm{hm}(x)$ 的值作为上述一般形式中 m 的值，同时对参数 x 进行反比例函数加密计算。为便于文中有关变形反比例函数描述，文中统一用符号 $Gf(x,y)$ 表示。

即如下：

$$Gf(x,y)=\begin{cases}\dfrac{\mathrm{hm}(y)}{y}+\mathrm{hm}(x)(\mathrm{hm}(x)>\mathrm{hm}(y))\\ \dfrac{\mathrm{hm}(x)}{x}+\mathrm{hm}(y)(\mathrm{hm}(x)\leqslant\mathrm{hm}(y))\end{cases}\tag{1}$$

1.3　算法步骤描述

与文献[15]一样，做出如下约定：读写器与数据库间采用有线方式交互消息，安全可靠，故将二者看成一个整体。文中算法在认证之前有一个初始化过程，初始化过程完成，R 端储存信息有 ID_L、ID_R、K，T 端储存信息有 ID_L、ID_R、K。具体流程如图 1 所示。

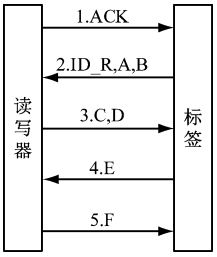

图 1　双向认证算法

结合图 1 可将文中基于变形反比例函数的双向认证算法具体步骤描述如下。

步骤 1　R 向 T 发送 ACK 认证请求命令，开始认证过程。

步骤 2　T 产生随机数 a，计算得到消息 $A=a\oplus$ ID_L、消息 $B=Gf(a,$ID_L$)$，并将 ID_R、A、B 发送给 R。

步骤 3　R 将依据收到的 ID_R 在数据库中查找是否存在该数据。未找到，则算法停止。找到，R 可将与 ID_R 相关联的信息全部取出来。先对 A 进行变形 $A\oplus$ ID_L 可得到随机数 a'，然后计算得到 $B'=Gf(a',$ID_L$)$，接着对比 B' 与 B 的关系。

B 与 B' 不等，算法终止；如果相等，说明 T 通过 R 的验证。R 开始产生一个随机数 b，计算得到消息 $C=a\oplus b$、消息 $D=Gf(a,b)$，并将 C、D 发送给 T。

步骤 4　T 将对 C 进行变形处理 $C\oplus a$ 可得到随机数 b'，计算得到 $D'=Gf(a,b')$，然后对比 D' 与 D 的值。

D 与 D' 不等，算法终止；如果相等，说明 T 对 R 的验证完成。T 计算得到消息 $E=Gf(a\oplus D,b)$，并将 E 发送给 R。

步骤 5　R 计算得到 E'，对比 E' 与 E 的大小关系。

E 与 E' 不等，算法终止；如果相等，说明 R 完成对 T 的验证。R 计算得到消息 $F=Gf(a\&b,K)$，开始更新信息，信息更新完成后，将 F 发送给 R。

当 $*=$old 时，$K_{new}=Gf(a,b\oplus K\mathrm{old})$。

当 $*=$new 时，$K_{old}=K_{new}$、$K_{new}=Gf(a,b\oplus K_{new})$。

步骤 6　T 收到信息后，T 计算得到 F'，并比较 F' 与收到 F 的大小。

F 与 F' 不等，算法终止。如果相等，表明 R 通过 T 的验证。T 开始更新信息 $K=Gf(a,b\oplus K)$。T 信息更新完成后，则双向认证完成。

2　算法安全性分析

双向认证。通信实体间能够对彼此的真伪进行验证是算法最基本的安全需求。文中算法 R 与 T 间的双向认证都分 2 次进行，在步骤 3 中，R 通过 A、B 完成第一次对 T 的认证；在步骤 5 中，R 再次通过 E 完成第二次对 T 的认证。在步骤 4 中，T 则是通过 C、D 第一次完成对 R 的认证；在步骤 6 中，T 将再次通过 F 完成第二次对 R 的认证。基于上述，文中算法可以实现通信实体间的双向认证。

假冒攻击。当攻击者假冒成 R 时，攻击者可以接收到合法 T 发送来的消息 ID_R、A、B，但因攻击者不知晓 ID_L 值，攻击者无法从消息 A、B 中破解出有用的隐私信息，使得攻击者计算的消息 C、D 值并不是正确的值；当 T 收到攻击者发送来的 C、D 消息时，T 只需要进行简单的计算，即可识别出消息来源是攻击者伪造的。当攻击者假冒成 T 时，攻击者会随机选择数据进行消息 A、B 的计算；当 R 收到攻击者发送来的消息时，R 对 A、B 进行简单验证，即可辨别出消息发送方是攻击者伪造。基于上述，算法可以抵抗假冒攻击。

重放攻击。攻击者窃听当前会话过程，可以获取当前会话过程中所有消息，在下一轮会话过程中重放当前窃听所得消息，以企图通过某会话实体验证，从而达到破解隐私信息目的。文中算法采用信息加密过程中混入随机数方法来解

决攻击者发起的重放攻击，当攻击者重放上轮消息时，本轮消息加密过程中用到的随机数已发生变更，使得攻击者重放的消息无法通过验证。鉴于随机数由随机数发生器随机产生，具有无法预测性，因此攻击者无法预测下轮会话用到的随机数。基于上述，文中算法可抵抗重放攻击。

追踪攻击。文中算法所有消息都是加密之后在发送，攻击者获取的消息都是密文，无法直接破解出有用信息。信息加密通过混入随机数方式，使得前后两轮会话同一个会话实体计算所得消息值也是不同的，这样攻击者就无法从获取的消息中分析出电子标签的位置，无法实施追踪攻击。基于上述，文中算法可抵抗追踪攻击。

异步攻击。文中算法在 R 一端存放有当前会话、上轮会话过程中 R 与 T 间的共享秘密值，以此来抵抗异步攻击。具体在算法步骤 5 中，R 会先用 K_{new} 来发起对 T 的验证，验证通过，可直接进行后续操作；若验证失败，则 R 会再次用 K_{old} 来发起对 T 的验证。当且仅当，前后两次对 T 的验证都失败，算法才会终止。基于上述，文中算法可抵抗异步攻击。

后向安全。攻击者想要从获取的当前会话消息中分析部分隐私信息，然后用此信息再来逆推出上轮会话中部分隐私信息，该种攻击方式称为后向安全攻击。文中协议在信息加密时候引入随机数，使得前后消息值不同；加之随机数具有随机性、前后无关联性、互异性等特征，使得攻击者无法从当前获取消息逆推出上轮消息加密用到隐私信息。基于上述，文中算法具备后向安全性。

将本文算法与其他算法之间进行安全性对比分析结果如表 1 所示。在表 1 中，✓表示能够抵抗该种类型攻击，×表示无法抵抗该种类型攻击。

表 1　不同算法间安全性对比

攻击类型	文献[11]	文献[12]	文献[13]	文献[14]	本文算法
双向认证	✓	✓	×	✓	✓
假冒攻击	×	✓	×	×	✓
重放攻击	✓	✓	✓	✓	✓
追踪攻击	✓	✓	✓	✓	✓
异步攻击	✓	×	✓	✓	✓
后向安全	✓	✓	✓	✓	✓

3　算法性能分析

本文选择电子标签作为性能分析对象，选择电子标签为对象的因素有：电子标签满足低成本要求，使得电子标签计算能力及存储空间严重受到制约。从电子标签一端的计算量及存储量角度出发，将本文算法与其他算法进行性能比较，分析结果如表 2 所示。

对表 2 中出现的符号所表示的含义解释如下：AND 符号表示按位与运算、OXR 符号表示按位异或运算、PUF 符号表示物理不可克隆函数、HASH 符号表示哈希函数、Gf 符号表示变形反比例函数、L 符号表示会话消息长度。

在上述不同的运算算法中，不同的算法自身具备的计算量大小不同，其中AND、XOR、Gf三种运算都是基于按位运算实现，因此三者都属于超轻量级的运算；而 PUF、HASH 两种运算则是属于轻量级的运算。基于上述，本文算法与文献[11]中算法在电子标签一端的计算量应是大致相当；本文算法在电子标签一端的计算量要优于文献[12-14]中电子标签一端的计算量。

表 2　不同算法间性能对比

对比文献	计算量	存储量/L
文献[11]	AND、OXR	5
文献[12]	PUF	5
文献[13]	HASH	4
文献[14]	HASH	3
文中算法	Gf	3

从电子标签一端的存储量角度分析，本文算法电子标签一端需要存放的信息有：ID、K、a，因此存储量大小为 3L。与其他算法相比较，要少于其他算法电子标签一端存储开销。

综合表 2 中计算量、存储量角度分析，文中算法虽与文献[11]中电子标签一端计算量相当，但存储量角度有减少，且文中算法可以弥补文献[11]中算法存在的安全不足；文中算法计算量要少于文献[12-14]中电子标签计算量，具备推广优势，同时文中算法可以弥补上述文献中算法存在的安全漏洞。

4　总结

本文给出一个基于变形反比例函数实现的双向认证算法。算法采用变形反比例函数实现对信息加密，根据变形反比例函数定义可得，算法计算量能够达到超轻量级别；同时变形反比例函数充分利用加密参数自身汉明重量参数，能够减少参量的引入，从而可降低存储量。文中最后从多个角度对文中算法进行了详细的安全分析，表明文中算法可抵抗重放攻击、异步攻击、假冒攻击等常见类型的攻击，具备较高的安全性能；性能对比角度，表明文中算法具备低计算量特征，能够在现有低成本 RFID 系统中推广使用。

参考文献

[1] XU Y W, WU C. Further Characterization of H Vectorial Functions[J]. International Journal of Network Security, 2017, 19(6): 899-903.

[2] MAFARJA M M, MIRJALILI S. Hybrid Whale Optimization Algorithm with Simulated Annealing for Feature Selection [J]. Neurocomputing, 2017, 260: 302-312.

[3] 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[J]. 计算机工程，2020，46(1)：108-113.

[4] XIE R, LING J, LIU D W. Wireless Key Generation Algorithm for RFID System Based on Bit Operation [J]. International Journal of Network Security, 2018, 20(5): 938-949.

[5] GAO X Z, WANG X, OVASKA S J, et al. A Hybrid Optimization Method of Harmony Search and Opposition Based Learning[J]. Engineering Optimization, 2012, 44(8): 895-914.
[6] TANG F, HUANG D. A BLS Signature Scheme from Multilinear Maps[J]. International Journal of Network Security, 2020, 22(5): 728-735.
[7] DE SIQUEIRA E C, SOUZA M J F, DE SOUZA S R. A Multi-objective Variable Neighborhood Search Algorithm for Solving the Hybrid Flow Shop Problem [J]. Electronic Notes in Discrete Mathematics, 2018, 66: 87-94.
[8] WANG Y L, SHEN J J, HWANG M S. A Survey of Reversible Data Hiding for VQ-Compressed Images [J]. International Journal of Network Security, 2018, 20(1): 1-8.
[9] 刘道微，凌捷，杨昕. 一种改进的满足后向隐私的 RFID 认证协议[J]. 计算机科学, 2016, 43(8): 128-130.
[10] NI S, XIE M B, QIAN Q. Clustering Based K-anonymity Algorithm for Privacy Preservation[J]. Int. J. Netw. Secur., 2017, 19(6): 1062-1071.
[11] FAN K, JIANG W, LI H, et al. Lightweight RFID Protocol for Medical Privacy Protection in IoT[J]. IEEE Transactions on Industrial Informatics, 2018, 14(4): 1656-1665.
[12] KAUL S D, AWASTHI A K. Privacy Model for Threshold RFID System Based on PUF[J]. Wireless Personal Communications, 2017, 95(3): 2803-2828.
[13] 汪杰，汪学明. 改进的轻量级移动 RFID 双向认证协议[J]. 计算机工程与设计, 2018, 39(4): 912-917.
[14] 刘卓华，黄彩娟，所辉. 改进的抗假冒攻击的移动 RFID 双向认证协议[J]. 计算机应用与软件, 2020, 37(6): 309-315.
[15] TANG D, WANG Y Q, YANG H P. Array Erasure Codes with Preset Fault Tolerance Capability[J]. International Journal of Network Security, 2018, 20(1): 193-200.

（收稿日期：2021-01-05）

（上接第 40 页）

统中的本局手持设备下发任务，主要包括线路名称和线路代码 2 个字段。任务接收成功后，地理信息采集系统可将线路名称和线路代码自动加至系统内部的线路选择列表中，并且地理信息采集系统可根据终端数据进行批量选择，在任务下发后，结合城市道路交通安全设施的实际情况，由城市道路交通安全设施管理者自主进行发布[10]。

5 总结

本文针对城市道路交通安全设施地理信息采集应用场景的不同需求进行了详细分析，为了满足不同层次的需求，针对地理信息采集系统进行设计研究，以此为城市道路交通安全设施提供重要运行数据，并在系统内存储大量地理信息。城市道路交通安全设施的稳定性至关重要，今后应加强对城市道路交通安全设施的维护工作，对于地理信息采集系统的关键问题应及时解决，提升地理信息采集系统外业工作的易用性，将地理信息采集系统贴近于实际生产中，广泛应用于城市道路交通安全设施的维护中。

参考文献

[1] 李龙斌，王鹏. 大数据在测绘地理信息中的应用探析[J]. 世界有色金属, 2019(22): 231.
[2] 张迎春. 计算机技术在地理信息领域的应用[J]. 智能建筑与智慧城市, 2020(6): 96-97.
[3] 温世林. 大数据在测绘地理信息方面的应用[J]. 中国管理信息化, 2021, 24(4): 190-192.
[4] 岳军红，王涛，任英桥，等. 基于 WebGIS 的地理信息系统开发应用[J]. 微型电脑应用, 2018, 34(12): 40-42.
[5] 骆京铭. 城市智能交通管理系统设计与实现[J]. 自动化技术与应用, 2019, 38(6): 171-175.
[6] 袁广升，薛守钰，陈永，等. 基于 STM32 的 GPS 信息采集与传输系统设计[J]. 汽车实用技术, 2016(1): 86-89.
[7] 杨莹，佟夏辉. 测绘地理信息统计数据质量控制分析[J]. 科技创新与应用, 2021(6): 188-190.
[8] 马佐霖. 网络地理信息系统中空间矢量数据自动采集方法[J]. 电子设计工程, 2019, 27(11): 79-82.
[9] 刘文，刘海波. 大数据和云计算在矿山测绘地理信息中的应用及其标准化探讨[J]. 世界有色金属, 2019(20): 261.
[10] 宋莎. 大数据在测绘地理信息中的应用研究[J]. 城市建设理论研究(电子版), 2019(27): 54-55.

（收稿日期：2021-07-12）