



一种基于字合成运算的射频识别双向认证协议

占善华^{1,2}, 黄少荣¹

(1. 广东司法警官职业学院信息管理系, 广东 广州 510006;

2. 广东工业大学计算机学院, 广东 广州 510006)

摘要: RFID 系统由标签、读写器、后台数据库 3 部分组成, 其中标签与读写器之间通过无线信道进行信息传输, 存在易被攻击者截获通信信息的风险。提出一种基于字合成运算的射频识别双向认证协议。所提协议运用二次剩余定理对信息进行加密, 增大破解难度; 每轮通信加密过程中, 随机数的添加使得前后通信消息均不一致, 致使攻击者无法发起追踪攻击行为。消息加密过程中, 同时采用字合成运算方法, 能够有效减少 RFID 系统总的计算量; 后台数据库端引入随机数校验机制, 使系统能够有效抵抗异步攻击等攻击。安全性分析表明, 基于字合成运算的射频识别双向认证协议具备较高的安全性; 性能分析表明, 协议具备轻量级计算量的标准。

关键词: 射频识别; 随机数; 字合成运算; 二次剩余定理

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018300

A bidirectional authentication protocol for RFID based on Syn

ZHAN Shanhua^{1,2}, HUANG Shaorong¹

1. Department of Information Management, Guangdong Justice Police Vocational College, Guangzhou 510006, China

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

Abstract: The RFID system is made up of three parts: tags, readers and databases. The information between tags and readers are transmitted through wireless channel, which is easy to be intercepted by attackers. A two-way authentication protocol based on word Synthesis operation was proposed. The two remainder theorem was used to encrypt communication messages by the proposed protocol, the difficulty of cracking was increased; In the process of each round of communication encryption, a random number was added to make the communication messages inconsistent, so that the tracking attacks could not be initiated by attackers. In the communication message encryption, the word synthesis algorithms was adopted at the same time, the total calculation of the system could be effectively reduced. A random checking mechanism was introduced at the database, enabling a synchronous attack and other attacks to be effectively resisted by the system. Security analysis shows that the protocol has high security, and performance analysis shows that the protocol has the standard of lightweight computation.

Key words: RFID, random number, Syn, quadratic residual theorem

收稿日期: 2018-03-12; 修回日期: 2018-09-28

基金项目: 国家自然科学基金资助项目 (No.61672171, No.61772141); 广东省教育厅重大科研项目 (No.2016KZDXM052); 广东司法警官职业学院第三届院级课题 (No.2017YB007)

Foundation Items: The National Natural Science Foundation of China (No.61672171, No.61772141), Natural Science and Technology Major Project of Educational Commission of Guangdong Province (No.2016KZDXM052), The Third Academy-Level Scientific Research Project of Guangdong Justice Police Vocational College (No.2017YB007)



1 引言

无线射频识别 (radio frequency identification, RFID) 是一种通过无线电信号自动识别目标标签且同时读写相关数据的技术^[1]。因标签成本较低、部署容易等优点, 无线射频识别技术已经广泛应用在如汽车收费等各个领域^[2-3]。标签与读写器之间不是采用有线方式通信, 而是采用无线方式, 故易被攻击者攻击, 从而截获传输的数据信息, 因此存在一定的安全隐患, 需要为其设计双向认证协议以保证信息的安全可靠传输^[4-5]。

近年来, 国内外许多专家学者提出了不少的认证协议^[6-11], Chen 等^[12]提出一种基于二次剩余定理的认证协议, 因需要进行多次 Hash 计算, 认证协议的整体计算量较大。Yeh 等^[13]指出 Chen 等在参考文献^[12]中所提协议存在一定安全隐患, 该协议不能抵抗攻击者的重放攻击。轩秀巍等人^[14]提出一种基于二次剩余定理的增强型认证协议, 所提协议不能抵抗攻击者的去同步化攻击。Doss 等^[15]提出了一种基于二次剩余定理的可隐私保护的移动认证协议, 所提协议因数据库在校验标签真伪过程中需进行多次计算及查询, 协议效率偏低。Zhou 等^[16]提出了一种基于二次剩余的定时双向认证协议, 所提协议存在以下缺陷: 需在数据库端存放所有标签的有效认证时间, 从而数据库端在查询过程中需花费较多时间, 协议效率较低。张惠根等人^[17]提出了一种基于二次剩余定理的更具实用性的移动认证协议, 该协议在认证过程中增加了时间戳生成器, 在一定程度上提高了系统安全性, 但同时也增加了成本。

在总结众多参考文献基础之上, 本文提出一种安全的基于字合成运算的双向认证协议。协议基于二次剩余定理及按位运算进行加密, 确保加密信息的安全性。在加密过程中, 由于随机数的

加入, 能够加大破解的难度。

2 协议描述

2.1 符号说明

本文协议有关假设与参考文献^[18]一致, 具体见参考文献^[18]。

双向认证协议开始之前, 标签端存放信息 (K , ID , n), 读写器端存放信息 (K_i , ID_i , n)。

字合成运算是指由 P 的前 $(L-M)$ 位与 Q 的后 M 位组合形成新的 L 位数组, 其中 M 的设定为: $M = \text{Hw}(Q)$, $\text{Hw}(Q)$ 表示为 Q 的汉明重量, 字合成运算用符号 $\text{Syn}(Q, P)$ 表示。有关字合成运算可参考文献^[19]。

取长度 $L=12$, 设 $P=001010100111$, $Q=110011001001$, 设定 $M = \text{Hw}(Q) = 7$, 则根据上述字合成运算的定义可以得到 $\text{Syn}(P, Q) = 100100100101$, 具体运算过程如图 1 所示。

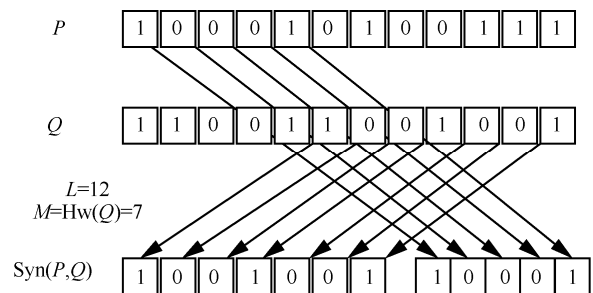


图 1 字合成运算的运算过程

符号说明见表 1。

2.2 协议过程

双向认证协议过程如图 2 所示。

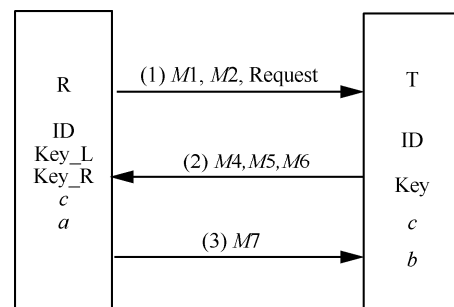


图 2 双向认证协议过程

表1 符号说明

符号	含义
R	读写器
T	标签
ID _{<i>i</i>}	标号为 <i>i</i> 的标签的标识符
Key	标签与读写器之间当前的共享密钥
Key _{new}	标签与读写器之间更新后的共享密钥
Key _{old}	标签与读写器之间上一轮的共享密钥
Key _L	Key的左半部分
Key _R	Key的右半部分
<i>N</i>	标签上一轮产生的随机数
<i>a</i>	读写器产生的随机数
<i>b</i>	标签本轮产生的随机数
<i>c</i>	两个大素数之积
⊕	异或运算
	按位串联符
Syn(·)	字合成运算

变量解释见表2。

表2 变量解释

变量	解释
<i>M1</i>	$a \oplus \text{Key}_L$
<i>M2</i>	$a \oplus \text{Key}_R$
<i>M3</i>	$\text{ID} \oplus a \oplus b$
<i>M4</i>	$b \oplus \text{Syn}(\text{Key}_L, \text{Key}_R)$
<i>M5</i>	$(M3 a)^2 \bmod c$
<i>M6</i>	$b^2 \bmod c$
<i>M7</i>	$\text{ID} \oplus \text{Syn}(b, \text{Key}_R)$

具体步骤如下。

(1) 读写器产生一个随机数, 然后计算 *M1*、*M2*; 并将 (*M1*、*M2*、Request) 传送给标签。

(2) 标签验证 $M1 \oplus \text{Key}_L$ 与 $M2 \oplus \text{Key}_R$ 是否相等。如果不相等, 说明读写器是假的, 协议立刻终止; 反之, 标签生成一个随机数, 然后计算 *M3*~*M6* (有关二次剩余定理知识可参考文献[20]); 最后将 (*M4*~*M6*) 传送给读写器。

(3) 读写器结合二次剩余定理对 *b* 进行解密, 可得到 *b1*、*b2*、*b3*、*b4*; 通过 *M4*、*Key_L*、*Key_R*

确定 *b1*~*b4* 中有关 *b* 的取值; 通过 *M5*、*c*、*a* 以及二次剩余定理对 *M3* 进行解密, 可得到 *M3₁*~*M3₄*; 通过 *ID*、*a*、*b* 可以计算得到一个 *M3'*。

比对并判断 *M3'* 与上述 *M3₁*~*M3₄* 是否有相等的值。若没有, 表明解密失败, 说明标签是伪造的, 协议立刻终止; 反之, 对比解密得到的 *b* 是否与 *N* 的值相等。若相等, 协议立刻终止; 反之, 令 $N=b$, 读写器搜索 <*ID*、*Key*、*Key_{old}*> 的组合, 再计算 *M7*, 并更新共享密钥 (即 $\text{Key}_{\text{old}}=K$, $\text{Key}_{\text{new}}=\text{PRNG}(K)$), 最后将 *M7* 传送给标签。

(4) 标签计算得到一个 *M7'*; 对比 *M7'* 与接收的 *M7* 是否相等。如果不相等, 协议立刻终止; 反之, 更新共享密钥 (即 $\text{Key}_{\text{old}}=K$, $\text{Key}_{\text{new}}=\text{PRNG}(K)$)。

3 协议安全性分析

3.1 去同步化攻击

异步攻击也称为去同步化攻击, 是指读写器与标签在认证的过程中, 由于攻击者的干扰, 读写器与标签之间的认证信息不同步, 从而导致标签与读写器之间的认证失败。为了抵抗异步攻击, 双向认证协议在读写器端不仅保存本轮认证所需要的信息, 同时也保存上轮认证过程中涉及的信息。当攻击者使得标签与读写器之间本轮认证需要的信息不同步的时候, 读写器也可以调用存放的上轮认证信息进行认证, 从而可以抵抗异步攻击。

3.2 拒绝服务攻击

攻击者想获得当前标签的密钥 *Key_L*、*Key_R* 的值, 则攻击者必须要获得上次的密钥来解密以前的认证信息。获取方法有两种: 一种方法是破解用位运算加密的密文, 因为标签在每次认证成功后, 都会通过位运算来更新新的密钥 *Key_L*、*Key_R* 的值; 另一种方法是, 通过上一轮的信息集合来获得上次的密钥, 但是标签每次



认证中计算用到的随机数 a 、 b 都是不同的。因此攻击者无法从认证过程的信息中获得密钥 Key_L 、 Key_R 的值, 故改进的双向认证协议能够抵抗拒绝服务攻击。

3.3 假冒攻击

当攻击者伪装成合法的读写器的时候, 攻击者因不知道 ID 、 Key_L 、 Key_R 等隐私信息, 因此攻击者无法计算出正确的 $M4 \sim M6$ 的值。在协议认证的第三步中, 标签通过验证 $M4$ 的正确性, 能够发现读写器是攻击者伪造的, 协议立刻终止, 从而能够抵抗假冒攻击。

当攻击者伪装成合法标签的时候, 攻击者因不知道 ID 、 Key_L 、 Key_R 等隐私信息, 因此攻击者无法在认证协议的第四步中计算出正确的随机数 a 、 b 的值, 从而导致传输给读写器的 $M6$ 的值也是错误的。读写器在认证协议的第四步中, 通过验证 $M6$ 的正确性, 能够发现标签是攻击者伪造的, 协议立刻终止, 从而能够抵抗假冒攻击。

3.4 重放攻击

改进的协议中, 读写器在认证过程中会产生两个随机数 a 、 b , 并且 $M4$ 、 $M5$ 、 $M6$ 的计算过程中都与 a 、 b 相关联, 使得攻击者无法通过重放信息获得隐私。当攻击者重放信息时, 读写器这端将会产生两个新的随机数, 从而可以确保 $M4$ 、 $M5$ 、 $M6$ 消息的新鲜性, 因此重放攻击失败。

3.5 暴力破解攻击

改进的协议中, 通信信息都是采用密文传输, 同时传输的信息中, 对于攻击者而言, 有两个以上的隐私信息是攻击者不知晓的, 在这种情况下, 攻击者是无法用暴力破解的手段来获取隐私密钥等信息的。比如: 在 $M1 = a \oplus \text{Key_L}$ 中, 对于攻击者来说, 只能获得传输的 $M1$ 的值, 但是 $M1$ 中的两个值都是无法知晓的, 同时随着随机数 a 的变化, $M1$ 的值每次也都是不一样的, 更加增大了攻击者的攻击难度。因此协议可以抵抗暴力破解攻击。

4 BAN 逻辑证明

(1) 协议的理想化模型

消息① $R \rightarrow T: M1, M2;$

消息② $T \rightarrow R: M4, M5, M6;$

消息③ $R \rightarrow T: M7。$

(2) 协议的初始假设

协议的初始假设见表 3。

表 3 协议的初始假设

协议	假设
P_1	$R \models R \stackrel{\text{KEY}}{\leftrightarrow} T$
P_2	$T \models R \stackrel{\text{KEY}}{\leftrightarrow} T$
P_3	$R \models R \stackrel{\text{ID}}{\leftrightarrow} T$
P_4	$T \models R \stackrel{\text{ID}}{\leftrightarrow} T$
P_5	$R \models \#(a)$
P_6	$T \models \#(a)$
P_7	$R \models \#(b)$
P_8	$T \models \#(b)$
P_9	$R \models T \Rightarrow M4$
P_{10}	$R \models T \Rightarrow M5$
P_{11}	$R \models T \Rightarrow M6$
P_{12}	$T \models R \Rightarrow M1$
P_{13}	$T \models R \Rightarrow M2$
P_{14}	$T \models R \Rightarrow M7$

(3) 协议的安全目标

协议的安全目标见表 4。

表 4 协议的安全目标

协议	目标
G_1	$T \models M1$
G_2	$T \models M2$
G_3	$T \models M7$
G_4	$R \models M4$
G_5	$R \models M5$
G_6	$R \models M6$

(4) 协议的分析推理

由协议的理想化模型中的消息①得 $T \triangleleft \{M1\}$ (T 曾经收到消息 $M1$)，并且由初始假设 P_2 及消息含义法则 $\frac{P \models P \leftrightarrow Q, P \triangleleft \{X\}_K}{P \models Q \sim X}$ (若主体 P 相信主体 P 和 Q 的共享密钥 K ，且 P 曾经收到用 K 加密的密文 X ，则 P 相信主体 Q 发送过来的消息 X)，得到 $T \models R \sim M1$ 。

由假设 P_6 及消息新鲜性法则 $\oplus$ (如果一个消息的一部分是新鲜的，则整个消息也是新鲜的)，得到 $T \models \#(M1)$ 。

由已经推导出来的 $T \models R \sim M1$ 、 $T \models \#(M1)$ 及随机数验证法则 $\oplus$ ，得到 $T \models R \models M1$ 。

由 $T \models R \models M1$ 、初始化假设 P_{12} 以及管辖法则 $\frac{P \models Q \Rightarrow X, P \models Q \models X}{P \models X}$ ，可得 $T \models M1$ 。因此，

目标 G_1 得证。

运用上述条件和法则，同理可证得 $G_2 \sim G_6$ 。此处不再赘述。

5 协议性能分析

对于表 5 中的符号，给出如下解释说明： p_1 代表二次剩余定理运算的计算量大小， p_2 代表散列函数运算的计算量大小， p_3 代表按位进行异或运算的计算量大小， p_4 代表产生随机数运算的计算量大小， p_5 代表字合成运算的运算量大小。令标签的标识符 ID、共享密钥 Key、两个大素数乘积 c 长度均为 l 。

表 5 性能比较

协议	计算量	存储空间	通信量
参考文献[13]	$2p_1 + 4p_2 + p_4$	$3l$	$7l$
参考文献[14]	$4p_1 + 3p_4$	$3l$	$8l$
参考文献[15]	$3p_1 + 4p_3 + 2p_4$	$3l$	$5l$
参考文献[16]	$2p_1 + 3p_4$	$3l$	$7l$
本文协议	$2p_1 + 3p_3 + 2p_4 + p_5$	$3l$	$6l$

$p_1 \sim p_5$ 操作的计算量大小从大到小为： p_2 、 p_1 、 p_4 、 p_5 、 p_3 。 p_5 、 p_3 操作都是属于超轻量级的按位运算，因此 p_5 、 p_3 操作次数对系统的整体运算总量影响可忽略不计。

双向认证协议中标签一端存的信息有：标签的标识符 ID、共享密钥 Key、两个大素数乘积 c ，因此标签一端的存放量空间大小为 $3l$ 。一个完整的认证过程，通信信息有： $M1$ 、 $M2$ 、 $M4$ 、 $M5$ 、 $M6$ 、 $M7$ ，可知协议的通信量大小为 $6l$ 。

本文双向认证协议与其他协议进行标签一端的存储量大小、协议的通信量大小对比时，本文协议与其他协议相当；在标签一端的计算量大小方面，引入字合成运算进行加密，能够有效减少总的运算量，使得双向认证协议在标签一端的计算量方面存在一定的优势，并弥补了参考文献[13-16]中协议的不足之处。

6 结束语

RFID 系统中，标签与读写器之间通过无线方式进行通信，易被攻击者截获信息，为确保通信消息的安全性，本文提出一种轻量级的利用字合成运算及二次剩余定理进行加密的双向认证协议。该协议采用字合成运算及二次剩余定理方法对传输信息进行加密，增大破解难度；通信消息加密过程中，由于随机数的混合，使得前后通信消息值不可能一样，进一步增大破解的难度，提升安全性；读写器一端采用随机数校验机制，能够有效抵抗异步攻击等攻击方式。对协议进行安全性分析，表明协议具备较高的安全性。

参考文献：

- [1] 赵明慧, 张磊, 元晋. 基于区块链的社会物联网可信服务管理框架[J]. 电信科学, 2017, 33(10): 19-25.
ZHAO M H, ZHANG L, QI J. A framework of trusted services management based on block chain in social internet of things [J]. Telecommunications Science, 2017, 33(10): 19-25.
- [2] 章谦骝, 章坚武. 基于云安全技术的智慧政务云解决方案[J]. 电信科学, 2017, 33(3): 107-111.

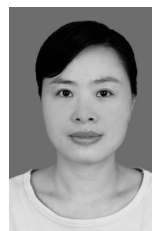


- ZHANG Q H, ZHANG J W. Solution for smart government cloud based on cloud security technology[J]. Telecommunications Science, 2017, 33(3): 107-111.
- [3] 吴震东, 潘树诚, 章坚武. 基于 CNN 的连续语音说话人声纹识别[J]. 电信科学, 2017, 33(3): 59-66.
- WU Z D, PAN S C, ZHANG J W. Continuous speech speaker recognition based on CNN[J]. Telecommunications Science, 2017, 33(3): 59-66.
- [4] 裴华东, 涂莹, 丁麒. 基于标签库系统的电力企业客户画像构建与信用评估及电费风险防控应用[J]. 电信科学, 2017, 33(Z1): 206-213.
- QIU H D, XU Y, DING Q. Customer portrait construction and credit evaluation of electric power enterprise based on tag library system and the application of electricity bill risk prevention and control[J]. Telecommunications Science, 2017, 33(Z1): 206-213.
- [5] ALOMAIR B, CUELLAR J, POOVENDRAN R. Scalable RFID systems: a privacy-preserving protocol with constant time identification[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(8): 1-10.
- [6] 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.
- LIU D W, LING J, YANG X. Improved RFID authentication protocol with backward privacy[J]. Computer Science, 2016, 43(8): 128-130.
- [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. 基于物理不可克隆函数的 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 mutual authentication based on physical unclonable 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 ultra-lightweight RFID authentication protocol[D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2014.
- [11] 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.
- [12] 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.
- [13] 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.
- [14] 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.
- [15] 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.
- [16] ZHOU J. A quadratic residue-based lightweight RFID mutual authentication protocol with constant-time identification[J]. Journal of Communications, 2015, 10(2): 117-123.
- [17] 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.
- [18] XIE R, JIAN B Y, LIU D W. An improved ownership transfer for RFID protocol[J]. International Journal of Network Security, 2018, 20(1): 149-156.
- [19] MAMUN M S I, MIYAJI A, RAHMAN M S. A secure and private RFID authentication protocol under SLPN problem[C]//6th International Conference on Network and System Security, November 21-23, 2012, Fujian, China. Berlin: Springer, 2012: 476-489.
- [20] GODOR G, IMRE S. Hash-based mutual authentication protocol for low-cost RFID systems[C]//18th EUNICE Conference on Information and Communications Technologies, August 11-12, 2012, Wuhan, China. Berlin: Springer, 2012: 76-87.

[作者简介]



占善华 (1987-), 男, 广东司法警官职业学院信息管理系讲师, 广东工业大学计算机学院博士生, 主要研究方向为人工智能、机器学习、信息安全。



黄少荣 (1976-), 女, 广东司法警官职业学院信息管理系教授, 主要研究方向为计算智能。