



研究与开发

基于伪随机函数的 RFID 系统双向认证协议

邓文雯¹, 孙成明², 秦培亮¹

(1. 苏州农业职业技术学院智慧农业学院, 江苏 苏州 215008;

2. 扬州大学信息工程学院, 江苏 扬州 225127)

摘要: 移动 RFID 系统中, 读写器与后台数据库之间不再通过有线方式通信, 而采用无线方式通信, 但也存在一定的安全隐患问题。为确保通信数据的安全, 提出一种基于伪随机函数的移动 RFID 双向认证协议。协议确保标签、读写器、后台数据库三方均进行认证, 从而保障通信的安全性; 采用字合成等位运算, 在一定程度上能够减少总的计算量; 三方认证, 使得移动 RFID 系统具备更为广泛的运用价值。安全性及性能分析表明, 所提协议具有较高的安全性及较低的成本。

关键词: 射频识别; 伪随机函数; 字合成运算; 移动系统; 三方认证

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018229

A bidirectional authentication protocol for mobile RFID system based on PRF

DENG Wenwen¹, SUN Chengming², QIN Peiliang¹

1. College of Wisdom Agriculture, Suzhou Polytechnic Institute of Agriculture, Suzhou 215008, China

2. School of Electronic and Computer Engineering, Yangzhou University, Yangzhou 225127, China

Abstract: In mobile RFID system, the reader and the database no longer communicate through the wired way, but communicate wirelessly, so there are also some potential safety issues. In order to ensure the safety of communication data, a mobile RFID bidirectional authentication protocol based on pseudo-random function was proposed. The protocol ensured the tripartite entities: the tag, the reader and the database, was authenticated each other, and thereby ensured the security of communication. The use of word synthesis operation to a certain extent, could be used to reduce the total amount of computation. The mobile RFID systems have more extensive using value by tripartite authentication; security analysis and performance analysis show that the proposed protocol has higher security and lower costs.

Key words: RFID, pseudo random function, word synthesis operation, mobile system, tripartite authentication

收稿日期: 2017-12-07; 修回日期: 2018-08-07

通信作者: 邓文雯, dw_83@126.com

基金项目: 江苏省农业三新工程项目 (No.SXGC[2016]300)

Foundation Item: Jiangsu Province-Level Project on Renewal of Agricultural Products, Technologies and Production Model (No.SXGC[2016]300)

1 引言

RFID 技术是一种利用无线电信号且不需要接触识别目标标签,同时读写目标标签内部相关数据的技术^[1]。标签、读写器、后台数据库三者组成了现有的绝大多数 RFID 系统,其中因标签具备体积小、便于携带、使用寿命长、容易安装部署等众多优点,RFID 系统已经广泛运用于身份证件、交通运输、车辆收费等各行各业中^[2-3]。

传统的 RFID 系统中,读写器与后台数据库之间通过有线方式进行通信,绝大多数的研究认定两者之间通信安全可靠,因此常常将两者作为一个整体来研究。但伴随着社会的发展及人们生活需求的提高,例如移动支付等业务的出现及快速发展,使得传统的 RFID 系统并不能较好地适用于这些应用中,为满足需求,移动 RFID 系统的出现完美地解决了上述问题^[4-5]。在移动 RFID 系统中,读写器与后台数据库之间不再通过网线传输信息,而是采用无线方式进行通信。无线通信方式存在一定的安全隐患,易被攻击者攻击,因此众多适用于传统 RFID 系统的认证协议不再适用于移动 RFID 系统。为适应移动 RFID 系统的快速发展,众多专家学者开始关注移动 RFID 系统的认证协议,并已设计出一些适用于移动 RFID 系统的认证协议^[6-7]。

近年来,国内外许多专家学者提出了不少认证协议,按照协议的计算量对其进行分类,大致可分为以下 3 种:重量级认证协议,如基于 ECC 椭圆曲线;轻量级认证协议,如基于 hash 函数、伪随机函数、PUF、二次剩余定理;超轻量级认证协议,仅基于按位运算,如异或运算。基于上述描述可得知,设计认证协议用到的方法很多,每种方法都有自身的优势及不足之处,运用其优势,可设计出安全的满足需求的协议。重量级认证协议因其具有较大的计算量及较高的安全性,主要应用于一些特定场合,比如保密性或安全性要求很高的军事基地等

场合,因此应用范围不广;超轻量级认证协议基于按位运算设计所得,在参考文献[8]中已指出:因按位运算自身运算的特征,使得基于按位运算设计的认证协议不可能完全安全,存在一定的安全隐患。综合比对之后,虽轻量级认证协议计算量高于超轻量级认证协议,但安全性高于超轻量级认证协议,故轻量级认证协议现仍受到专家学者的青睐。现有的设备产生伪随机函数难度不大且需要的设备成本不高,使得基于伪随机函数设计的认证协议具备一定的安全性^[9-13]。因此本文采用伪随机函数方法来设计轻量级认证协议。

为进一步提高协议的安全性、降低协议的计算量,在总结上述文献基础之上,本文提出一种基于伪随机函数的移动 RFID 系统双向认证协议。所提协议采用伪随机函数及字合成运算对传输信息进行加密,能够有效地减少系统总的计算量;三方均相互认证,从而确保通信实体各方的身份无误;安全性分析表明,所提协议能够有效抵抗假冒攻击、重放攻击等攻击方式。

2 移动 RFID 认证协议

2.1 符号说明

本文协议与其他此类移动 RFID 系统认证协议一样,做出如下假设:

- (1) 标签与读写器之间采用无线方式进行通信,该通信方式不安全,易被攻击者攻击;
- (2) 后台数据库与读写器之间采用无线方式进行通信,该通信方式不安全,易被攻击者攻击;
- (3) 协议认证开始之前,存放在标签、读写器、后台数据库中的信息均安全,且攻击者无法获取;
- (4) 后台数据库具备大量查询及计算的能力;
- (5) 协议认证开始之前,标签一端存放如下信息: (ID_t, K) , 读写器一端存放信息 (ID_r, K) , 后台数据库一端存放信息 (ID_r, ID_t, K, K_{old}) 。



字合成运算是指由 X 的前 $(L-M)$ 位与 Y 的后 M 位组合而形成新的 L 位数组, 其中 M 的设定为: $M = \text{Hw}(Y)$, $\text{Hw}(Y)$ 表示 Y 的汉明重量, 字合成运算用符号 $\text{Syn}(X, Y)$ 表示。有关字合成运算更多规定, 见参考文献[14]。

取长度 $L=12$, 设 $X=010010111101$, $Y=100001011100$, 设定 $M = \text{Hw}(Y) = 7$, 则根据上述字合成运算的定义可以得到 $\text{Syn}(X, Y) = 101110001001$, 具体运算过程如图 1 所示。在实际运用过程中, $M = \text{Hw}(Y)$ 的设定对外保密, 只有通信实体之间才知晓, 从而增大攻击者的破解难度。

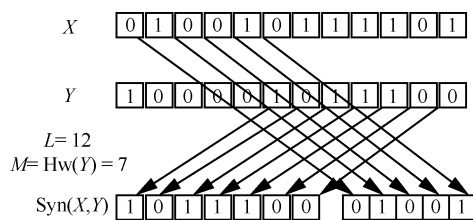


图 1 字合成运算过程

表 1 中给出了本文协议相关符号的说明。

表 1 符号说明

符号	含义
T	标签
R	读写器
DB	后台数据库
ID _t	标签的标识符
ID _r	读写器的标识符
ID _{t_L}	标签的标识符左半部分
ID _{t_R}	标签的标识符右半部分
ID _{r_L}	读写器的标识符左半部分
ID _{r_R}	读写器的标识符右半部分
K	标签、读写器、后台数据库三方共享密钥
K _L	三方共享密钥的左半部分
K _R	三方共享密钥的右半部分
K _{old}	上一轮三方共享密钥
K _{new}	更新后的三方共享密钥
x	读写器产生的随机数
y	后台数据库产生的随机数
⊕	异或运算
&	与运算
Syn(X, Y)	字合成运算

2.2 协议认证过程

图 2 中出现的变量解释见表 2。

表 2 变量解释

变量	解释
M1	$x \oplus K_L$
M2	$x \oplus K_R$
M3	$\text{ID}_{t_R} \oplus \text{Syn}(x \& K_L, K_R)$
M4	$f_K(x \oplus \text{ID}_{t_R} \& K)$
M5	$\text{ID}_{r_R} \oplus \text{Syn}(x \& K_R, K_L)$
M6	$f_K(x \oplus \text{ID}_{r_R} \& K)$
M7	$K \oplus y \oplus \text{ID}_{r_R}$
M8	$K \oplus y \oplus \text{ID}_{t_R}$
M9	$\text{Syn}(K, x) \& y$
M10	$\text{Syn}(M9 \oplus x, M9 \& x) \oplus K$
K _{new}	$f_K(x \oplus y \& K)$

本文协议认证过程如图 2 所示, 具体介绍如下。

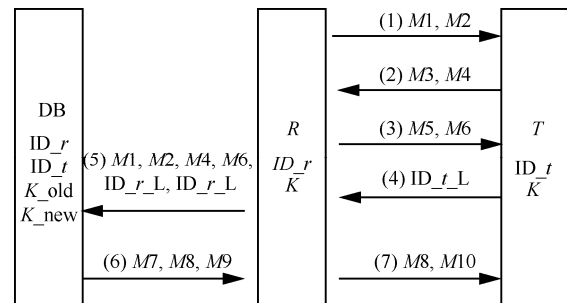


图 2 移动 RFID 认证协议

步骤 1 读写器产生一个随机数, 记为 x ; 然后计算 $M1$ 、 $M2$; 最后将 $\langle M1, M2 \rangle$ 一并发送给标签。

步骤 2 标签在接收到读写器发送来的信息后, 进行如下操作:

(1) 计算 $M1 \oplus K_L$ 、 $M2 \oplus K_R$, 比对 $M1 \oplus K_L$ 与 $M2 \oplus K_R$ 是否相等;

(2) 若不相等, 说明读写器是伪造的, 协议立刻终止; 反之, 说明通过步骤 (1) 中计算可得到正确的随机数 x , 然后进行步骤 (3);

(3) 利用 ID_{t_R} 、 x 、 K_L 、 K_R 、 K 计算得到 $M3$ 、 $M4$, 最后将 $\langle M3, M4 \rangle$ 一并发送给读写器。

步骤 3 读写器在接收到标签发送来的信息后, 进行如下操作:

(1) 通过计算 $M3 \oplus \text{Syn}(x \& K_L, K_R)$, 可得到 ID_t_R ;

(2) 读写器自身利用 ID_t_R, x, K 计算可得到一个 $M4'$, 然后比对 $M4'$ 与 $M4$ 的值是否相等;

(3) 若两者的值不相等, 说明标签是伪造的, 协议立刻终止; 反之, 说明通过步骤 (1) 中计算可以得到正确的 ID_t_R , 然后进行步骤 (4);

(4) 利用 ID_r_R, x, K_L, K_R, K 计算得到 $M5, M6$, 最后将 $\langle M5, M6 \rangle$ 一并传送给标签。

步骤 4 标签在接收到读写器发送来的信息后, 进行如下操作:

(1) 通过计算 $M5 \oplus \text{Syn}(x \& K_R, K_L)$, 可得到 ID_r_R ;

(2) 标签自身利用 ID_r_R, x, K 计算可得到一个 $M6'$, 然后比对 $M6'$ 与 $M6$ 的值是否相等;

(3) 若两者值不相等, 说明读写器是伪造的, 协议立刻终止; 反之, 说明通过步骤 (1) 中计算可以得到正确的 ID_r_R , 然后进行步骤 (4);

(4) 标签将自身的 ID_t_L 发送给读写器。到此, 标签与读写器两者之间双向认证完成。

步骤 5 读写器在接收到标签发送来的信息后, 读写器将 $\langle M1, M2, M4, M6, ID_t_L, ID_r_L \rangle$ 一并传送给后台数据库。

步骤 6 后台数据库在接收到读写器发送来的信息后, 后台数据库先实现对读写器的认证, 对读写器认证通过之后, 再对标签进行认证, 只有在两者均通过认证的前提下, 后台数据库才会进行后续密钥更新等相关操作。

后台数据库对读写器的认证, 操作如下:

(1) 后台数据库查找是否存在 ID_r_L , 若不存在, 协议终止; 反之, 进行步骤 (2);

(2) 找到与 ID_r_L 相对应的 $\langle K_L, K_R, ID_t_R, ID_r_R \rangle$, 然后计算 $M1 \oplus K_L, M2 \oplus K_R$, 接着比对 $M1 \oplus K_L$ 与 $M2 \oplus K_R$ 是否相等;

(3) 若不相等, 说明读写器是伪造的, 协议立刻终止; 反之, 说明通过步骤 (2) 中计算可得到正确的随机数 x , 然后进行步骤 (4);

(4) 后台数据库自身利用 ID_r_R, x, K 计算可得到一个 $M6''$, 然后比对 $M6''$ 与 $M6$ 的值是否相等;

(5) 若两者值不相等, 则用 K_{old} 代替 K 再次进行计算, 如果值仍然不相等, 说明读写器是伪造的, 协议立刻终止; 反之, 表明读写器通过后台数据库的认证, 接下来将进行后台数据库对标签的认证。

后台数据库对标签的认证, 操作如下:

(1) 后台数据库查找是否存在 ID_t_L , 若不存在, 协议终止; 反之, 进行步骤 (2);

(2) 找到与 ID_t_L 相对应的 $\langle K_L, K_R, ID_t_R, ID_r_R \rangle$, 后台数据库自身利用 ID_t_R, x, K 计算可得到一个 $M4''$, 然后比对 $M4''$ 与 $M4$ 的值是否相等;

(3) 若不相等, 则用 K_{old} 代替 K 再次进行计算, 如果值仍然不相等, 说明标签是伪造的, 协议立刻终止; 反之, 说明标签通过后台数据库的认证。

在后台数据库对标签、读写器均认证通过后, 进行如下操作:

(1) 后台数据库产生一个随机数, 记为 y ;

(2) 后台数据库利用 ID_r_R, ID_t_R, y, x, K 计算得到 $M7, M8, M9$;

(3) 后台数据库开始进行密钥更新, 即: $K_{old} = K, K_{new} = f_K(x \oplus y \& K)$;

(4) 后台数据库将 $\langle M7, M8, M9 \rangle$ 一并传送给读写器。

步骤 7 读写器在接收到后台数据库发送来的信息后, 进行如下操作:

(1) 读写器通过计算 $M7 \oplus K \oplus ID_r_R$, 可得到随机数 y ;

(2) 读写器利用 y, x, K 计算可得到一个 $M9'$,



然后比对 $M9'$ 与 $M9$ 的值是否相等;

(3) 若不相等, 说明后台数据库是伪造的, 协议立刻终止; 反之, 说明通过步骤 (1) 中计算可得到正确的随机数 y , 然后进行步骤 (4);

(4) 读写器利用 $M9$ 、 x 、 K 计算得到 $M10$;

(5) 读写器一端开始进行密钥更新操作, 即: $K_{old}=K$, $K_{new}=f_K(x \oplus y \& K)$, 最后将 $\langle M8, M10 \rangle$ 一并传送给标签。

步骤 8 标签在接收到读写器发送来的信息后, 进行如下操作:

(1) 标签通过计算 $M8 \oplus K \oplus ID_{t_R}$, 可得到随机数 y ;

(2) 标签利用 y 、 x 、 K 计算可得到一个 $M10'$, 然后比对 $M10'$ 与 $M10$ 的值是否相等;

(3) 若不相等, 说明后台数据库及读写器均是伪造的, 协议立刻终止; 反之, 说明通过步骤 (1) 中计算可得到正确的随机数 y , 然后进行步骤 (4);

(4) 标签一端开始进行密钥更新操作, 即: $K_{old}=K$, $K_{new}=f_K(x \oplus y \& K)$ 。至此, 标签、读写器、后台数据库三方之间相互认证结束, 可进行安全通信。

3 协议安全性分析

(1) 假冒攻击

在移动 RFID 系统中, 攻击者可伪装成标签、读写器、后台数据库三方中的任意一方, 下面将分别进行分析。

当攻击者伪装成标签时: 攻击者因不知晓 K 、 ID_t 等信息, 因此攻击者无法计算出正确的 $M3$ 、 $M4$ 的值。在协议的步骤 3 中, 读写器经过计算便可以得知: 接收到的 $M3$ 、 $M4$ 是错误的, 从而判断出标签是伪造的, 协议即可终止, 攻击者伪装成标签并未获取有效的隐私信息。同时在协议的步骤 6 中, 后台数据库也会对标签进行认证, 综上可得该情况下的假冒攻击失败。

当攻击者伪装成读写器时: 攻击者给标签发

送信息, 但攻击者不知晓 K_L 、 K_R , 因此攻击者无法计算出正确的 $M1$ 、 $M2$ 的值, 当标签接收到读写器发送来的信息后, 在协议中的步骤 2 中, 标签通过计算就可以判断出读写器是伪造的, 协议立刻终止, 攻击者假冒攻击失败。攻击者给后台数据库发送消息时, 因缺少正确的 x 、 K 等信息, 没有办法计算出正确的 $M6$ 的值, 因此在协议的步骤 6 中, 后台数据库通过计算 $M6$ 的值, 就可以判断出读写器是伪造的, 协议终止, 攻击者假冒攻击失败。综上可得该情况下, 攻击者假冒读写器失败。

当攻击者伪装成后台数据库时: 攻击者缺少 x 、 K 、 ID_r 、 ID_t 等信息, 因此攻击者就无法计算出正确的 $M7$ 、 $M8$ 、 $M9$ 的值, 攻击者只能讲错误的数值传送给读写器。在协议的步骤 7 中, 读写器进行计算, 可以验证出 $M7$ 、 $M9$ 是错误的, 从而识别出后台数据库是伪造的, 协议终止, 攻击者未获取有用隐私信息, 攻击失败。综上可得该情况下, 攻击者假冒后台数据库失败。

(2) 重放攻击

攻击者企图通过重放某个信息, 获取标签中的隐私信息, 但攻击者无法如愿以偿。读写器产生的随机数 x , 后台数据库产生的随机数 y , 可以保证传输信息的新鲜性。因为协议中所有信息在加密过程中均与 x 或与 y 或与 x 、 y 相关, 即: 信息在加密过程中, 有 x 或 y 参与的计算, 从而使得每轮认证过程中消息均不一样。随机数由随机数产生器产生, 随机数的产生具备不重复性及无法预测性, 因此攻击者无法通过当前获取的信息, 推测出下轮认证所用到的信息具体值, 从而使攻击者重放攻击失败。

(3) 暴力破解攻击

攻击者通过监听协议一个完整的通信过程, 可以获取 $M1$ 、 $M2$ 、 $M3$ 、 $M4$ 、 $M5$ 、 $M6$ 、 $M7$ 、 $M8$ 、 $M9$ 、 $M10$ 所有消息, 攻击者企图通过穷举的方法对上面所获取的消息进行穷举, 暴力地破解

出标签的隐私信息,但攻击者最终还是以失败告终。因为传送的所有消息中,都至少保证有两个参数,对于攻击者来说,攻击者是无法知晓的,此处以 $M3$ 为例进行具体分析。

$M3$ 的计算式为 $M3 = ID_t_R \oplus \text{Syn}(x \& K_L, K_R)$,在其计算中,攻击者不知道 ID_t_R 、 x 、 K_L 、 K_R 的值;虽然攻击者通过监听可以获取 ID_t_L 的值,但 ID_t_R 与 ID_t_L 之间并无任何关系,两者之间无法相互推出;同时字合成运算中用到的 M 的设定,攻击者亦是不知晓的。因此,基于上述,在计算式 $M3$ 中,攻击者不知道任何一个参数的正确的值,因此攻击者无法通过穷举的方法暴力破解出标签端的隐私信息。综上可得,协议可以抵抗攻击者的暴力破解攻击。

(4) 追踪攻击

攻击者企图通过 $M3$ 、 $M4$ 的值,分析出有用的信息,从而对标签发起追踪攻击,但攻击者无法成功。在协议中,不管是 $M3$ 消息,还是 $M4$ 消息,在加密过程中,均用到随机数 x ,因随机数自身每次产生不同的值,故消息 $M3$ 、 $M4$ 每次的计算结果是不相同的,且前后两次的值无任何关系,攻击者无法由当前 $M3$ 或 $M4$ 的信息推导出上轮或下次认证过程中的 $M3$ 或 $M4$ 的值,从而使得攻击者发起的追踪攻击失败。基于上述分析,攻击者无法追踪到标签的位置,因此协议可以抵抗攻击者的追踪攻击。

(5) 去同步化攻击

去同步化攻击是指攻击者通过某种手段,使得标签、读写器、后台数据库三者之间的共享密钥不再同步。

在本文协议步骤 2 中,标签验证读写器通过后,才会进行后续计算;在步骤 3 中,读写器在验证标签通过后,才会进行后续计算;在步骤 4 中,标签将会再次对读写器进行验证;在步骤 6 中,后台数据库将会对读写器、标签一一进行认证;在步骤 7 中,读写器实现对后台数据库的验

证;在步骤 8 中,标签实现对后台数据库及读写器的认证。基于上述分析可以看出,协议中每步骤均在验证通过后,才会进行后面的操作;同时后台数据库一端不仅存放当前的共享密钥 K ,而且还保留有上轮认证过程中用到的共享密钥 K_old ,能够更进一步地抵抗攻击者的去同步化攻击,因此协议可以抵抗攻击者的去同步化攻击。

4 BAN 逻辑证明

本文采用 BAN 逻辑对文章中所提的认证协议进行形式化证明,证明过程中做出如下规定:读写器用 R 符号表示,标签用 T 符号表示,后台数据库用 DB 符号表示,证明过程如下所示。

(1) 协议的理想化模型

消息① $R \rightarrow T: M1, M2$;

消息② $T \rightarrow R: M3, M4$;

消息③ $R \rightarrow T: M5, M6$;

消息④ $T \rightarrow R: ID_t_L$;

消息⑤ $R \rightarrow DB: M1, M2, M4, M6, ID_t_L, ID_r_L$;

消息⑥ $DB \rightarrow R: M7, M8, M9$;

消息⑦ $R \rightarrow T: M8, M10$ 。

(2) 协议的初始假设

$P_1: R \models R \overset{K}{\leftrightarrow} T$,表示读写器相信读写器与标签之间的共享密钥 K 。

$P_2: T \models T \overset{K}{\leftrightarrow} R$,表示标签相信读写器与标签之间的共享密钥 K 。

$P_3: T \models \#(x)$,标签相信随机数 x 的新鲜性。

$P_4: T \models \#(y)$,标签相信随机数 y 的新鲜性。

$P_5: T \models R \Rightarrow M2$,标签相信读写器对消息 $M2$ 的管辖权。

$P_6: T \models R \Rightarrow M5$,标签相信读写器对消息 $M5$ 的管辖权。

$P_7: T \models R \Rightarrow M6$,标签相信读写器对消息 $M6$ 的管辖权。

$P_8: T \models R \Rightarrow M10$,标签相信读写器对消息



M_{10} 的管辖权。

P_9 : $T \models DB \Rightarrow M_8$, 标签相信后台数据库对消息 M_8 的管辖权。

(3) 协议的安全目标

G_1 : $T \models M_5$, 标签相信消息 M_5 。

G_2 : $T \models M_2$, 标签相信消息 M_2 。

G_3 : $T \models M_1$, 标签相信消息 M_1 。

G_4 : $T \models M_6$, 标签相信消息 M_6 。

G_5 : $T \models M_8$, 标签相信消息 M_8 。

G_6 : $T \models M_{10}$, 标签相信消息 M_{10} 。

(4) 协议的分析推理

由协议的理想化模型中的消息③得 $T \triangleleft \{M_5\}$ (T 曾经收到消息 M_5), 并且由初始假设

P_2 及消息含义法则 $\frac{P \stackrel{K}{\models} P \leftrightarrow Q, P \triangleleft \{X\}_K}{P \models Q \sim X}$ (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 $T \models R \sim M_5$ 。

由假设 P_3 及消息新鲜性法则 $\frac{P \models \#(X)}{P \models \#(X, Y)}$ (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 $T \models \#(M_5)$ 。

由已经推导出来的 $T \models R \sim M_5$ 、 $T \models \#(M_5)$

及随机数验证法则 $\frac{P \models \#(X), P \models Q \sim X}{P \models Q \models X}$, 得到

$T \models R \models M_5$ 。

由 $T \models R \models M_5$ 、初始化假设 P_6 以及管辖法则 $\frac{P \models Q \Rightarrow X, P \models Q \models X}{P \models X}$, 可得 $T \models M_5$ 。因此,

目标 G_1 得证。

运用上述条件和法则, 同理可证得 G_2 至 G_6 。此处不再赘述。

5 协议性能分析

移动 RFID 系统有标签、读写器、后台数据库 3 部分, 其中读写器、后台数据库具备一

定的计算能力及一定容量的存储空间; 标签相对于前两者而言, 计算能力、存储空间大小都远不及前两者。正因为如此, 设计协议过程中, 较少考虑读写器、后台数据库的计算量及存储空间, 主要侧重目标于标签一端。故本文性能分析中选取标签一端的计算量、存储空间作为重点研究对象进行比较分析, 分析结果见表 3。

表 3 性能比较

协议	计算量	存储空间
参考文献[8]协议	4 ph1+3 ph2+2 ph3	3l
参考文献[9]协议	2 ph1+2 ph3+4 ph4	5l
参考文献[10]协议	4 ph2+3 ph3+3 ph4	4l
本文协议	3 ph3+15 ph4+3 ph5	2l

对表 3 中的符号说明如下: ph1 表示 hash 函数的计算量; ph2 表示模运算的计算量; ph3 表示伪随机函数的计算量; ph4 表示位运算的计算量 (异或运算、与运算均属于按位运算, 因位运算属于超轻量级的计算, 计算量非常小, 因此可将异或运算的计算量、与运算的计算量看成等量的计算量, 用一个相同的符号表示); ph5 表示字合成运算的计算量。约定共享密钥 K 、标签的标识符 ID_t 的长度均为 l 。

因本文协议中, 标签一端事先需要存放的信息有: 共享密钥 K 、标签的标识符 ID_t , 因此标签一端的存储空间大小为 $2l$ 即可满足需求。在 ph1、ph2、ph3、ph4、ph5 中, 计算量由大到小依次排列的顺序是: ph1、ph2、ph3、ph5、ph4。其中 ph4 属于超轻量级的计算, 相对于 ph1、ph2 来说, ph4 的计算量要远远少于 ph1、ph2 的计算量, 因此 ph4 的操作次数多几次, 对整体的计算量影响几乎可忽略。ph5 是采用移位的方式进行的计算, 计算量也不大, 且小于 ph1、ph2、ph3 的计算量。从表 3 中分析可得出, 本文所提协议具备轻量级协议的计算量。

6 结束语

针对传统 RFID 系统无法满足移动支付等移动业务的不足,文中提出一种适用于移动的无线射频识别系统认证协议。所提协议能够解决读写器与后台数据库之间认证的问题。标签、读写器、后台数据库三方进行通信过程中,采用先验证后通信的机制,只有在验证通过前提下,才可进行后续通信,从而保障传输信息的安全性。摒弃采用 hash 加密的方案,利用伪随机函数及字合成运算对传输信息进行加密,从而减少协议的整体计算量。消息加密过程中随机数的引入,能够保证消息的新鲜性,同时增大攻击者的破解难度;安全性及性能分析表明,协议具备较高的安全保障及较低的成本。下一步研究方向:考虑协议在实际生活中是否能满足大规模的应用,将是接下来要进一步完善的工作。

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] MUNILLA J, BURMESTER M, PEINADO A, et al. RFID ownership transfer with positive secrecy capacity channels[J]. Sensors, 2017, 17 (1): 53-70.
- [3] CHIOU S Y, KO W T, LU E H. A secure ECC-based mobile RFID mutual authentication protocol and its application[J]. International Journal of Network Security, 2018, 20(2): 396-402.
- [4] BURMESTER M, MUNILLA J, ORTIZ A, et al. An RFID-based smart structure for the supply chain: resilient scanning proofs and ownership transfer with positive secrecy capacity channels[J]. Sensors, 2017, 17(7): 1562-1581.
- [5] LI X D, ZHOU C L, XU N. A secure and efficient image encryption algorithm based on DNA coding and spatiotemporal chaos[J]. International Journal of Network Security, 2018, 20(1): 110-120.
- [6] 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.
- [7] 周恒, 畅志贤, 杨武军, 等. 一种 5G 网络切片的编排算法[J]. 电信科学, 2017, 33(8): 130-137.
ZHOU H, CHANG Z X, YANG W J, et al. An orchestration algorithm of 5G network slicing [J]. Telecommunications Science, 2017, 33(8): 130-137.
- [8] ZHOU J. A quadratic residue-based lightweight RFID mutual authentication protocol with constant-time identification[J]. Journal of Communications, 2015, 10(2).
- [9] QIAN Q, JIA Y L, ZHANG R. A lightweight RFID security protocol based on elliptic curve cryptography[J]. International Journal of Network Security, 2016, 18(2): 354-361.
- [10] NOUREDDINE C, FOUJIL C, CAYREL P L, et al. Improved RFID authentication protocol based on randomized McEliece cryptosystem[J]. International Journal of Network Security, 2015, 17(4): 413-422.
- [11] 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.
- [12] 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.
- [13] 庞晓丹, 李薇薇, 孙茜, 等. LTE 无线网络虚拟化中切片调度策略[J]. 电信科学, 2017, 33(2): 66-72.
PANG X D, LI W W, SUN Q, et al. Slice scheduling strategy in LTE wireless network virtualization[J]. Telecommunications Science, 2017, 33(2): 66-72.
- [14] TIAN Y, CHEN G L, LI J H. A new ultra-lightweight RFID authentication protocol with permutation[J]. IEEE Communications Letters, 2012, 16(5): 702-705.

[作者简介]



邓文雯(1983—),女,苏州农业职业技术学院智慧农业学院讲师,主要研究方向为计算机应用技术、物联网技术。

孙成明(1973—),男,博士,扬州大学信息工程学院教授、硕士生导师,主要研究方向为作物系统模拟与图像识别、作物精准栽培与农业信息技术、气候变化与碳源汇机理及其估算。

秦培亮(1981—),男,苏州农业职业技术学院智慧农业学院副教授,主要研究方向为复合传动及机械设计制造。