软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(12):3215−3222 [doi: 10.13328/j.cnki.jos.004832]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

RFID 快速隐私保护认证协议*

翟 黎[1,2]

[1](信息安全国家重点实验室(中国科学院 信息工程研究所),北京 100093)

[2](中国科学院大学,北京 100190)

通讯作者: 翟黎, E-mail: zhaili@iie.ac.cn

摘 要: 基于对称密码体系的 RFID 隐私保护认证协议的构造是学术界和工业界研究的热点问题.具有完整性隐私保护协议的效率不够高效,需要对系统中所有的标签进行穷尽搜索,难以应用于物联网海量终端的环境.给出了一种高效的 RFID 隐私保护认证协议的构造方法.构造的协议采用了单比特输出的伪随机函数,将协议的认证过程分解为多个步骤,与传统的基于对称密码体系的 RFID 认证协议相比,构造的协议显著提高了读写器对标签的搜索效率.构造的协议具有隐私性,并且计算开销小,读写器端对标签的搜索效率高,能够很好地应用于海量终端的物联网环境.

关键词: RFID;认证协议;隐私保护;伪随机函数;物联网

中图法分类号: TP309

中文引用格式: 翟黎. RFID 快速隐私保护认证协议.软件学报,2015,26(12):3215−3222. http://www.jos.org.cn/1000-9825/4832.htm

英文引用格式: Zhai L. Fast privacy preserving RFID authentication protocol. Ruan Jian Xue Bao/Journal of Software, 2015, 26(12):3215−3222 (in Chinese). http://www.jos.org.cn/1000-9825/4832.htm

Fast Privacy Preserving RFID Authentication Protocol

ZHAI Li[1,2]

[1](State Key Laboratory of Information Security (Institute of Information Engineering, the Chinese Academy of Sciences), Beijing 100093, China)

[2](University of Chinese Academy of Sciences, Beijing 100190, China)

Abstract: Privacy-preserving RFID authentication protocols based on symmetric-key cryptography technology have increasingly become popular. However, current RFID authentication protocols are inefficient due to the requirement of full search for all the RFID tags in the systems. In this paper, a new efficient method is proposed to construct highly effective privacy preserving RFID protocols. Based on pseudorandom functions with single output bit, this protocol can significantly improve the performance of tag searching process. Moreover, the protocol satisfies anonymity, authenticity, and efficiency requirements in the large-scale systems.

Key words: radio frequency identification; authentication protocol; privacy preservation; pseudorandom function; Internet of Things

RFID(radio frequency identification)是一种无线识别技术,能够自动地识别物体或者人.RFID 系统由标签、读写器和后端数据库这 3 大部分构成.标签通常附着在货物上,读写器通过无线射频信号与标签进行通信,后端数据库则包含了标签的密钥及货物的相关信息.标签通常是无源的,需要读写器提供的能量来工作,计算能力有限.标签通常只能执行一些简单的运算,例如 Hash 函数和对称密码函数.读写器则具有强大的计算能力,能够执行复杂的密码学函数.

* 基金项目: 国家高技术研究发展计划(863)(2013AA014002)
Foundation item: National High-tech R&D Program of China (863 Program) (2013AA014002)
收稿时间: 2014-04-08; 定稿时间: 2015-03-06

RFID 系统通常需要实现两种需求:识别和隐私保护.识别最简单的方法是通过广播一个标识符,但是明文广播标识符会失去隐私性,敌手很容易通过这个标识符进行追踪.在一个低成本的 RFID 标签上,能够使用的电路门数大约是 2 000 门.通常,一个对称密码算法所需要的电路门数在 3 000 门以上.对于 AES 算法,所需要的电路门数在 10 000 门以上[1].基于成本的考虑,RFID 标签中所使用的算法主要都是对称密码算法.

采用对称密码体系的 RFID 认证协议存在一个矛盾:一方面,为了保证标签的匿名性,不能以明文的方式发送标识符;另一方面,标签和读写器需要共享密钥.所以在一组标签中,读写器很难找到与标签共享的密钥.因此,采用对称密码体系的协议通常采用穷举搜索的方法来确定标签的密钥,即:将所有的合法密钥进行逐一查找,如果找到能够正确解密标签消息的密钥,则认证成功;如果没有找到,则认证失败.该方法的计算复杂度是线性的 $O(n)$,其中,n 是系统中标签的数量.

为了提高读写器对标签的认证效率,Molnar 和 Wagner 提出了一种基于树的 RFID 认证协议[4],该协议的识别效率可以达到 $O(\log n)$.基于树的 RFID 提高了认证效率,但标签之间存在大量的相同密钥,这会导致协议容易受到俘获攻击.有学者指出[5]:当敌手俘获系统中少量的标签时,敌手就能够根据这些标签中共享的密钥,以很高的概率来区分协议中剩下的标签.这对于系统的隐私性来说是一种极大的破坏.并且,系统的分支因子越小(树状结构的分支数),标签能够抵抗这种俘获攻击的能力就越差.所以,基于树的协议牺牲了安全性,在系统的安全性和识别效率之间做了折衷.事实上,有学者证明了:能够提供完整隐私保护协议的认证复杂度的下界是 $O(n)$,也就是任何低于这个复杂度的协议都不能提供完整的隐私保护功能[6,7],敌手总能以不可忽略的概率来区分系统中的标签.

本文第 1 节介绍基于单比特输出伪随机函数的 RFID 认证协议框架.第 2 节对协议的效率进行分析.第 3 节给出两个具体的伪随机函数、实例化协议,并与现有的协议的效率进行比较.第 4 节总结全文.

1 高效的 RFID 认证协议

本节描述利用单比特输出的伪随机函数来构造具有隐私保护的 RFID 认证协议.在协议中,读写器和标签发送的消息中没有暴露与标签身份相关的信息,保证了协议的隐私性.并且,标签之间没有任何公共的秘密信息,即使系统中某个标签被敌手截获,也不影响系统中其他的标签,因此可以很好地抵抗俘获攻击.本文的协议采用了单个比特输出的伪随机函数,在对标签进行识别时,读写器能够快速的排除错误标签,从而加速标签的搜索效率.

在本文中使用的一些符号定义如下:

- n,系统中标签的数量;
- ID_k,第 k 个标签的标识符;
- f,单比特输出的伪随机函数;
- m,安全参数 m 为一个整数;
- G,长度为 m 二进制串的集合;
- ε,单比特的随机噪声,服从参数为 η 的伯努利分布.

在本文中,假定读写器和标签之间是不安全的信道,读写器和数据库之间则是采用安全的信道.因此,我们只考虑读写器和标签之间的安全问题,不考虑读写器和数据库的安全问题.并且,单比特的伪随机函数可以分为确定型和概率型两种,这两种函数分别对应了两类协议:确定型协议和概率型协议.下面分别介绍这两种情况.

1.1 使用确定型函数的认证协议

我们来描述一下确定型协议的执行过程.

- 初始化

在系统中存在 n 个标签 $ID_1,\ldots,ID_n$,后端数据库记录这 n 个标签的 ID 和标签的密钥.读写器和标签之间共享一个单比特输出的确定型伪随机函数 f 和 s 个子密钥.图 1 给出了确定型协议的执行过程.

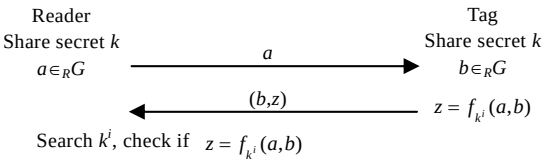

Fig.1 Deterministic authentication protocol

图 1 确定型协议

- 执行过程

标签和读写器之间共享 s 个子密钥 k^i,协议总共执行 s 轮,每一轮使用一个不同的子密钥.如果每一轮的结果都是标签被读写器接受,则认证成功;反之失败.协议的第 i 轮的执行步骤如下:

1) 读写器向标签发送一个随机的消息 a,$a\in_R G$;
2) 标签向读写器发送消息 b,$b\in_R G$,标签计算 $z = f_{k^i}(a,b)$,标签发送(b,z)给读写器;
3) 读写器接收标签发送过来的消息(b,z),读写器在数据库中穷搜当前候选标签的密钥 k^i(在第 1 轮时,所有的标签都是候选标签),并验证 $f_{k^i}(a,b) = z$:如果相同,则将密钥 k^i 和密钥对应的 ID 保留在候选标签中;反之,则将该密钥对应的 ID 排除在候选 ID 之外.

在 s 轮协议都执行完毕后,如果候选标签中还剩一个标签,该标签即为合法的标签,协议认证成功;如果还剩余多个标签,则说明标签的输出发生了碰撞,协议认证失败;如果候选标签的个数为 0,认证失败,标签是不合法的标签.容易看出:对于正确的标签,在没有敌手或者外界的干扰下,总能认证成功;但是对于不正确的标签,也有一定的概率通过验证.假设函数 f 是均匀的,错误的标签通过某一轮的概率为 2^{-1},通过全部 s 轮的概率为 2^{-s}.协议的误识率(false accept rate,简称 FAR)和拒识率(false reject rate,简称 FRR)分别为

$$P_{FAR}=2^{-s} \text{ and } P_{FRR}=0.$$

而对于候选标签有多个的情况,假定系统中标签个数为 n,除掉一个正确的标签,剩下的 $n-1$ 个标签发生通过验证的概率为

$$P_{collision}=(n-1)2^{-s}.$$

不难看出:对于不同的 n,只要选取足够大的 s,协议发生碰撞的概率是极小的.图 2 演示了协议中标签的查找过程,系统中的标签 ID_3 在某一轮没有通过验证,排除在候选标签之外.

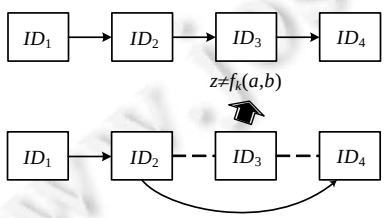

Fig.2 Process of searching tags

图 2 标签的查找过程

1.2 使用概率型函数的认证协议

概率型协议和确定型协议的执行步骤相似,不同之处在于,标签给读写器的应答中会引入一定的噪声.概率型协议的优点有:

- 首先,在密码学理论中,有一大类基于机器学习理论的伪随机函数,例如 LPN 函数[8]、NLHB 函数[9]、LWE 函数[10]等等.这类函数的特点是:通常,软硬件实现的复杂度较低,并且学术界对于其函数性质研究的比较充分,而概率型协议能够很好地应用这一大类函数;

- 其次,概率型协议中,读写器对于标签的应答并不要求完全一致,允许有一定的误差存在,只要总的误差不超过限定的范围即可.在实际的环境中,信号在传输过程中有各种各样的干扰,通常的解决办法是引入纠错码或消息重传一类的机制来保证信号的正确性.而概率型协议本身就具有一定的容错性,对于协议的实现者来说,能够降低实现的成本和复杂性.

但是概率型协议的缺点在于:在对标签的密钥的搜索过程中,由于有噪声的存在,读写器不能很快的定位正确的密钥,相比较于确定型协议,需要更多的操作才能找到正确的密钥.

设概率型协议总共执行 s 轮,如果某个标签被拒绝的次数大于上限 c,则认证失败,该标签被认为是一个非法标签.协议的具体执行过程如下:

1) 读写器向标签发送一个随机的消息 $a,a\in_R G$;
2) 标签向读写器发送消息 $b,b\in_R G$,标签计算 $z=f_{k^i}(a,b)\oplus\varepsilon$, ε是一个随机的单比特噪声,并且服从参数为η的伯努利分布,标签发送(b,z)给读写器;
3) 读写器接收标签发送过来的消息(b,z),读写器在数据库中穷搜当前的候选密钥 k^i,并验证 $f_{k^i}(a,b)=z$:如果相同,则将密钥 k^i和密钥对应的ID保留,作为候选标签,并且错误计数不变;反之,则将该密钥对应标签的错误计数加 1.如果错误计数小于上限 c,则继续保留该标签在候选集合中;如果超过上限 c,则将该标签从候选集合中排除.

在 s 轮协议都执行完毕后,标签的候选集合中还剩余一个标签,则认证成功;如果还剩余多个标签,则说明标签的输出发生了碰撞,协议认证失败,但是发生这种情况的概率极小,是可忽略不计的;如果候选标签的个数为 0,则认证失败,标签是不合法的标签.图 3 演示了概率型协议的执行过程.

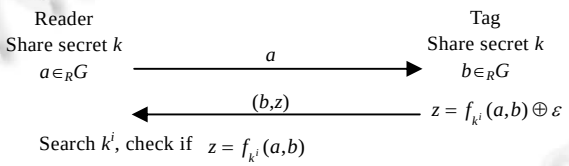

Fig.3 Probabilistic authentication protocol

图 3 概率型协议

容易看出:即使对于合法的标签,读写器也有一定的概率会对标签认证失败.并且,失败的概率与噪声参数η有关,当η越大时,读写器对合法标签的识别概率会越低.协议拒识率与η,s,c 有如下的关系:

$$P_{FRR}=\sum_{j=0}^{s-c-1}\binom{s}{j}(1-\eta)^j\eta^{s-j} \tag{1}$$

错误的标签被读写器接受的概率(误识率)为

$$P_{FAR}=\sum_{j=0}^{c}\binom{s}{j}2^{-s} \tag{2}$$

2 协议的分析

在本节,我们将对上一节提出的协议进行效率分析.对于确定型的协议,读写器识别单个标签平均需要计算两次确定型伪随机函数 f;对于概率型的协议,读写器需要计算 $2c$ 次概率型伪随机函数 f,其中,c 是概率型协议中的容错次数.

- 确定型函数 f

假定函数 f 的输出是均匀分布的,可以推导出读写器识别单个标签平均所需要的次数是 2.

先计算读写器从候选集合中排除单个标签所需的次数.读写器根据后端数据库查找到标签 i 的密钥 k_i,读写器计算 $z_i=f_{k_i}(a,b)$. 读写器验证 $z=z'$:如果相等,读写器将标签保留到候选集合中;反之,则排除该标签,继续对下

一个 ID 进行查找.

容易看出:对于一个合法的标签密钥,该密钥能够通过全部的 s 轮的检验.对于一个错误的或者不合法的密钥,该密钥每次能够通过检验的概率为 1/2,这样的密钥在第 i 轮正好被淘汰的概率为(前 i–1 轮通过检验,第 i 轮失败的概率):

$$p_i=\frac{1}{2^{i-1}}\times\frac{1}{2}=\frac{1}{2^i}.$$

我们记某个错误的标签被排除掉所需的次数为 X_i,根据期望的定义,X_i 的期望为

$$E(X_i)=\sum_{i=1}^{\infty}i\times p_i=\sum_{i=1}^{\infty}i\times\frac{1}{2^i}=2.$$

我们记读写器排除所有错误标签的次数为 X.根据期望的线性性,读写器排除所有错误标签的期望次数为

$$E(X)=E\left(\sum_{i=1}^{n}X_i\right)=\sum_{i=1}^{n}E(X_i)=2n.$$

- 概率型函数 f

在概率型的协议中,函数的输出引入了一个噪音 ε.按照协议的规则,读写器对标签总共验证 s 次,如果某个标签验证失败的次数大于等于 c 次,则该标签被认为是一个非法标签;如果标签验证失败的次数小于 c 次,则该标签为一个合法标签.

为了分析需要,我们引入下面这些符号:令事件 Γ_i 表示某个错误标签在正好在第 i 轮被读写器拒绝;令事件 Ψ_i^j 表示某个错误标签通过了读写器的前 i 轮验证,并在这过程中 j 次验证失败;令事件 Λ_i 表示某个错误标签在第 i 轮验证中失败.

对于一个均匀的伪随机函数发生器,错误的标签每次验证成功或者失败的概率都是 1/2.在总共 i 次验证中,有 j 次验证失败,一共有 $\binom{i}{j}$ 种可能,每种情况发生的概率是 $\left(\frac{1}{2}\right)^{i-j}\left(\frac{1}{2}\right)^j$.事件 Ψ_i^j 发生的概率为

$$\Pr[\Psi_i^j]=\binom{i}{j}\left(\frac{1}{2}\right)^{i-j}\left(\frac{1}{2}\right)^j.$$

事件 Γ_i 发生,表示某个错误标签正好在第 i 轮被淘汰.也就是说,错误标签通过了前 i–1 次验证,其中出现了 c–1 次错误,并且在第 i 次也是验证错误,即 $\Gamma_i=\Psi_{i-1}^{c-1}\wedge\Lambda_i$. 其中,$\Lambda_i$ 表示第 i 轮验证失败.标签正好在第 i 轮被淘汰的概率为

$$\Pr[\Gamma_i]=\Pr[\Psi_{i-1}^{c-1}\wedge\Lambda_i]=\Pr[\Psi_{i-1}^{c-1}]\Pr[\Lambda_i]=\binom{i-1}{c-1}\left(\frac{1}{2}\right)^{(i-1)-(c-1)}\left(\frac{1}{2}\right)^{c-1}\left(\frac{1}{2}\right)=\binom{i-1}{c-1}\left(\frac{1}{2}\right)^i.$$

记单个错误标签被排除掉所需的次数为 X_i,X_i 的期望为

$$E(X_i)=\sum_{i=1}^{\infty}i\times\Pr[\Gamma_i]=\sum_{i=1}^{\infty}i\times\binom{i-1}{c-1}\left(\frac{1}{2}\right)^i=\sum_{i=1}^{\infty}c\times\binom{i}{c}\left(\frac{1}{2}\right)^i.$$

引理 1. 对于任意的正整数 c,有如下的等式成立:

$$\sum_{i=1}^{\infty}\binom{i}{c}\left(\frac{1}{2}\right)^i=2.$$

证明:不难验证,当 c 为任意的正整数时,该级数都是收敛的.下面用数学归纳法来证明该级数的值恒等于 2.

1) 当 c=1 时,直接进行计算:

$$\sum_{i=1}^{\infty}\binom{i}{c}\left(\frac{1}{2}\right)^i=\sum_{i=1}^{\infty}\frac{i}{2^i}=2;$$

2) 假设 c=k 时成立,则当 c=k+1 时:

$$\sum_{i=1}^{\infty}\binom{i}{k+1}\left(\frac{1}{2}\right)^i=\sum_{i=1}^{\infty}\left[\binom{i-1}{k+1}+\binom{i-1}{k}\right]\left(\frac{1}{2}\right)^i=\frac{1}{2}\sum_{i=1}^{\infty}\binom{i-1}{k+1}\left(\frac{1}{2}\right)^{i-1}+\frac{1}{2}\sum_{i=1}^{\infty}\binom{i-1}{k}\left(\frac{1}{2}\right)^{i-1}=\frac{1}{2}\sum_{i=1}^{\infty}\binom{i}{k+1}\left(\frac{1}{2}\right)^i+1 \quad (3)$$

其中,公式(3)中的第 2 步是由著名的二项式系数的恒等式得到的.根据上面的等式,移项,我们可以导出:

$$\sum_{i=1}^{\infty}\binom{i}{k+1}\left(\frac{1}{2}\right)^i=2.$$

即:当 $c=k+1$ 时,该级数的和也等于 2. □

根据上面的引理,当 c 为正整数时,有:

$$E(X_i)=c\sum_{i=1}^{\infty}\binom{i}{c}\left(\frac{1}{2}\right)^i=2c.$$

记读写器排除所有错误标签的次数为 X.根据期望的线性性,读写器排除所有错误标签的期望次数为

$$E(X)=E\left(\sum_{i=1}^{N}X_i\right)=\sum_{i=1}^{N}E(X_i)=2cN.$$

即,读写器排除整个系统中的错误标签所需要的计算 f 函数的总次数为 $2cN$.

3 协议的实例化

本文在前面给出了快速认证协议的框架,并对该框架下的协议运行效率进行了分析.在本节中,将确定型协议和概率型协议实例化,给出两个具体的协议.

- 确定型协议

协议中的确定型函数 f 实例化为

$$f_k(a,b)=H((a\|b)\times k \bmod 2^m-1),$$

其中,m 为正整数,且 2^m-1 为一个素数;×为普通的整数乘法;a,b 都是长度不超过 $m/2$ 的串;$H(x)$表示 x 的二进制表示的各个比特的异或和,记 x 的各个二进制表示为 $x_1,x_2,\ldots,x_m$,则 $H(x)=\oplus_{i=1}^{m}x_i$.

模乘函数是流密码的设计中常用的一类函数,并且在一些 RFID 协议[11]里也用到了这一类函数.假定选定的函数 f 是伪随机的.根据上面的效率分析,我们的协议识别某个合法标签平均需要计算 $2n$ 次 f 函数,即,计算 $2n$ 次模乘运算.而对于一个使用对称密钥算法的认证协议来说,需要计算 n 次完整的加密函数.

笔者在一台运行 Linux 的主频为 2.6GHz 的台式上执行了 10 亿次 127 比特的模乘运算,耗时 3.5s,所以执行一次 127 比特的乘法需要 8 个 CPU 时钟周期.平均每个标签需要执行两次乘法,这样所需的时钟周期是 16 个.在理想情况下,线性搜索对于单个标签的计算代价也至少为 1 个 CPU 时钟周期.可以看出,该协议的效率是非常高的.

- 概率型协议

我们将协议中概率型函数 f 实例化为

$$f_k(a,b)=\langle a\|b,k\rangle\oplus\varepsilon.$$

函数$\langle x,y\rangle\oplus\varepsilon$是著名的 *LPN* 函数,其中,$x,y$ 是两个二元域上的向量,||表示对两个向量进行连接,$\langle x,y\rangle$表示向量的点乘运算,ε是一个遵循伯努利分布的噪声,⊕表示二元域的加法运算.f 函数可以等价为

$$f_k(a,b)=\langle a\|b,k\rangle\oplus\eta=\langle a,k_1\rangle\oplus\langle b,k_2\rangle\oplus\eta.$$

k_1 和 k_2 分别表示 k 的前后两段.经过实例化之后,该协议等价于一个匿名化后的 HB#协议[12].Katz 等人[13]给出了一个 *LPN* 函数的伪随机性质,任何多项式时间算法都不能区分 *LPN* 函数和一个随机函数,否则,该算法能够求解 LPN 问题.因此,我们这里的实例化是合理的.

假定协议的总轮数 s=321,协议的容错次数 c=71,噪声参数η=1/8.根据选取的参数和公式(1)计算,合法的标签被敌手拒绝的概率 $P_{FAR}<2^{-6}$.又由公式(2)可知:该组参数下,非法的标签被读写器接受的概率为 $P_{FAR}<2^{-80}$,也就是协议的安全性满足 80 比特.根据我们前面的分析,读写器排除一个错误标签平均需要执行的 f 函数的次数为 $2c$=142.即,读写器排除一个标签需要执行 142 次点乘运算.对于我们熟悉的 X86 处理器,执行一次二元域上的点

乘运算只需要 1 个时钟周期,所以需要的时钟周期为 142.并且二元域上的点乘运算操作简单,更适合于硬件实现,效率还可以进一步提高.

表 1 中给出了协议的效率比较.Hummingbird 和 WG-8 是针对资源受限环境设计的两个轻量级密码算法,文献[14]给出了这两种算法所需的时钟周期数,基于这两种算法的搜索单个标签所需的时钟周期为 2 056 和 1 564.文献[15]给出了 OSK 协议、PFP 协议和 SFP 协议所需的时钟周期数.本文中,确定型协议搜索单个标签所需的时钟周期数为 16,概率型协议所需的时钟周期数为 142.

Table 1 Performance comparisons

表 1 效率比较

协议	时钟周期数
OSK	2 548
Hummingbird	2 056
WG-8	1 564
PFP	264
SFP	208
概率型协议(模乘)	16
概率型协议(点乘)	142

4 结束语

本文构造了一类基于单比特输出的伪随机函数的 RFID 认证协议,该协议改进了密钥搜索的效率,在现有的基于对称密钥的隐私保护认证协议中,本文中的协议效率是最优的.本文将伪随机函数分为确定型和概率型两类,并分别进行了讨论.使用确定性函数的标签搜索次数少,但是函数的执行效率略低;而使用概率型函数的协议标签搜索次数多,但是函数本身的执行效率高.伪随机函数 f 的选取是协议设计的关键,在本文中选择了模乘函数和 *LPN* 函数,而寻找效率更高的函数,是一个值得进一步研究的问题.

References:

[1] Feldhofer M, Dominikus S, Wolkerstorfer J. Strong authentication for RFID systems using the AES. In: Joye M, Quisquater, eds. Proc. of the Cryptographic Hardware and Embedded Systems (CHES 2004). LNCS 3156, Berlin: Springer-Verlag, 2004. 357−370. [doi: 10.1007/978-3-540-28632-5_26]

[2] Juels A. RFID security and privacy: A research survey. IEEE Journal on Selected Areas in Communications, 2006,24(2):381−394. [doi: 10.1109/JSAC.2005.861395]

[3] Zhou YB, Feng DG. Design and analysis of cryptographic protocols for RFID. Chinese Journal of Computers, 2006,29(4):581−589 (in Chinese with English abstract).

[4] Molnar D, Wagner D. Privacy and security in library RFID: Issues, practices, and architectures. In: Proc. of the 11th ACM Conf. on Computer and Communications Security. ACM Press, 2004. 210−219. [doi: 10.1145/1030083.1030112]

[5] Avoine G, Dysli E, Oechslin P. Reducing time complexity in RFID systems. In: Preneel B, Tavares S, eds. Proc. of the Selected Areas in Cryptography. LNCS 3897, Berlin: Springer-Verlag, 2006. 291−306. [doi: 10.1007/11693383_20]

[6] Damgård I, Pedersen MØ. RFID security: Tradeoffs between security and efficiency. In: Malkin T, ed. Proc. of the Topics in Cryptology—CT-RSA 2008. LNCS 4964, Berlin: Springer-Verlag, 2008. 318−332. [doi: 10.1007/978-3-540-79263-5_20]

[7] Vaudenay S. On privacy models for RFID. In: Kurosawa K, ed. Proc. of the Advances in Cryptology—ASIACRYPT 2007. LNCS 4833, Berlin: Springer-Verlag, 2007. 68−87. [doi: 10.1007/978-3-540-76900-2_5]

[8] Blum A, Kalai A, Wasserman H. Noise-Tolerant learning, the parity problem, and the statistical query model. Journal of the ACM, 2003,50(4):506−519. [doi: 10.1145/792538.792543]

[9] Madhavan M, Thangaraj A, Sankarasubramanian Y, Viswanathan K. NLHB: A non-linear Hopper-Blum protocol. In: Proc. of the 2010 IEEE Int'l Symp. on Information Theory Proceedings. IEEE, 2010. 2498−2502. [doi: 10.1109/ISIT.2010.5513440]

[10] Regev O. On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM, 2009,56(6):34. [doi: 10.1145/1568318.1568324]

[11] Alomair B, Lazos L, Poovendran R. Securing low-cost RFID systems: An unconditionally secure approach. Journal of Computer Security, 2011,19(2):229−257. [doi: 10.3233/JCS-2010-0406]

[12] Gilbert H, Robshaw MJ, Seurin Y. HB#: Increasing the security and efficiency of HB+. In: Smart N, ed. Proc. of the Advances in Cryptology—EUROCRYPT 2008. LNCS 4965, Berlin: Springer-Verlag, 2008. 361−378. [doi: 10.1007/978-3-540-78967-3_21]

[13] Katz J, Shin JS, Smith A. Parallel and concurrent security of the HB and HB+ protocols. Journal of Cryptology, 2010,23(3): 402−421. [doi: 10.1007/s00145-010-9061-2]

[14] Fan X, Mandal K, Gong G. Wg-8: A lightweight stream cipher for resource-constrained smart devices. In Singh K, Awasthi AK, eds. Proc. of the Quality, Reliability, Security and Robustness in Heterogeneous Networks. LNICST 115, Berlin: Springer-Verlag, 2013. 617−632. [doi: 10.1007/978-3-642-37949-9_54]

[15] Ma CS. Low cost RFID authentication protocol with forward privacy. Chinese Journal of Computers, 2011,34(8):1387−1398 (in Chinese with English abstract).

附中文参考文献:

[3] 周永彬,冯登国.RFID 安全协议的设计与分析.计算机学报,2006,29(4):581−589.

[15] 马昌社.前向隐私安全的低成本 RFID 认证协议.计算机学报,2011,34(8):1387−1398.

翟黎(1985－),男,湖北武汉人,博士生,主要研究领域为 RFID 认证协议,隐私保护,轻量级对称加密算法.