一种能抵抗拒绝服务攻击的 RFID 安全认证协议

胡 炜, 李永忠, 李正洁
(江苏科技大学 计算机科学与工程学院, 江苏 镇江 212003)

摘 要: 在分析现有一些 RFID 认证协议的基础上,采用流密码加密和密钥动态更新的方法设计了一种能抵抗拒绝服务攻击的 RFID 安全认证协议。对该协议的安全性和性能进行了分析,结果表明协议能够有效防止拒绝服务攻击、隐私攻击、窃听攻击、重传攻击,同时解决了 RFID 的隐私问题。

关键词: 射频识别; 安全协议; 拒绝服务; 相互认证
中图分类号: TN915.08;TP309 **文献标志码**: A **文章编号**: 1001-3695(2012)02-0676-03
doi:10.3969/j.issn.1001-3695.2012.02.073

New defending RFID authentication protocol against DoS attacks

HU Wei, LI Yong-zhong, LI Zheng-jie
(*College of Computer Science & Engineering, Jiangsu University of Science & Technology, Zhenjiang Jiangsu* 212003, *China*)

Abstract: By analyzing some existing RFID authentication protocols, this paper proposed a new mutual authentication protocol, which was based on the use of symmetric encryption and dynamic update key to prevent the denial-of-service attack. Then discussed the security and performance of this protocol. The result shows that this protocol has provided good security for RFID system, and can defeat location privacy attack, relay attack, eavesdropping attack, denial-of-service attack, and solve problems of RFID security privacy.

Key words: RFID; security protocol; denial-of-service(DoS) attack; mutual authentication

射频识别(radio frequency identification,RFID)是一种通过射频信号传输信息来识别和控制被标志物品的技术,它由阅读器(reader)、RFID 标签(tag)和对标签存储信息进行处理的后台数据库系统(back-end database)三大部分组成。其中,后台数据库系统和阅读器通过安全信道进行通信,阅读器与标签之间通过射频信号(不安全信道)互相通信,如图 1 所示。后端数据库是计算和存储能力强大,同时包含所有 Tag 的信息的数据库系统。随着 RFID 的大面积应用,隐私与安全的问题变得日益严重。由于是一种开放型的无线环境,周围隐蔽的攻击者可以获取到电子标签上的信息,从而造成个人的敏感信息如金钱、药物等的泄露,而且可能暴露用户的位置隐私,使得用户被跟踪。另外,现在很多的防盗或监控安全系统都采用了 RFID 技术,在这种系统里,后台服务器可能遭受拒绝服务器(DoS)攻击。例如,攻击者可以通过一些射频信号装置短时间内向阅读器端发送大量数据信号,导致 RFID 系统被大量信号淹没,使的 RFID 系统失去预警和处理数据的能力,处于停滞状态[1]。由于标签和阅读器的通信公开,信道不是安全的,所以针对它们的攻击有很多种,如伪造克隆 RFID 标签和阅读器、嗅探(窃听攻击)、跟踪标签、物理攻击、重放攻击、窜改数据等。因此,在 RFID 应用时,必须仔细分析存在的安全威胁,采取适当的安全措施。一种有效的措施是设计 RFID 安全认证协议,它只允许被认证的对象(标签、阅读器、后台服务器)访问相关数据。考虑到成本问题,本文提出的认证协议只用到了流密码加密和随机化函数,分析表明,它能抵抗拒绝服务(DoS)攻击。

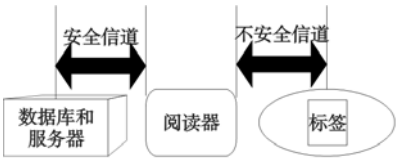

图1 RFID系统组成

1 RFID 系统现有的安全协议的简要介绍

由于 RFID 芯片是低成本芯片,它们的计算能力有限,如遵循 EPCglobal Class-1 Gen-2 RFID 规范的标签,通信频段在 800 ~ 960 MHz,仅支持单片机 16bit 的伪随机数生成器(pseudo-random number generator,PRNG)和循环冗余码(cyclic redundancy code,CRC)的计算[2]。所以有很多的密码算法在 RFID 标签上都无法使用。当前实现 RFID 安全机制所采用的方法大致可分为物理方法(如扼杀标签、阻止标签)和采用密码算法的方法两种类型。物理方法通常采用在售出商品时毁坏或是移除标签来实现对标签信息保护(扼杀标签的方法),或通过增设一个屏蔽装置对标签实施屏蔽,使得标签无法接收到外界的电磁波(阻止标签方法)[3,4]。但通过扼杀标签的物理方案对 RFID 实施安全保护,会使得标签无法重用。通过对标签增设屏蔽装置的物理方法也会给 RFID 系统带来不便和增加投入。因此,更多 RFID 的安全建议是采用密码算法设计安全认证协议以抵抗 RFID 的安全威胁问题,如 Hash-Lock 协议、随机化 Hash-Lock 协议、Hash 链协议、基于杂凑的 ID 变化协议、David 的数字图书馆 RFID 协议、分布式 RFID 询问—响应认证协议、LCAP 协议等[5~7]。

收稿日期: 2011-06-03; **修回日期**: 2011-07-17

作者简介:胡炜(1986-),男,硕士研究生,主要研究方向为网络与信息安全(h2uw3ei@163.com);李永忠(1961-),男,教授,硕导,主要研究方向为网络安全、计算机应用、藏文信息处理;李正洁(1987-),女,硕士研究生,主要研究方向为网络与信息安全.

在 Hash-Lock 协议中[3],数据库和标签共享密钥 k,询问后的标签发送通过哈希函数加密后的 $ID_k = hash(k)$,数据库通过哈希数据库内的每个标签的密钥来匹配 ID_k。但是在此协议中,由于每次标签发送的 ID_k 是固定不变的,这样很容易遭受跟踪攻击。随机化 Hash-Lock 协议在标签内引入伪随机数发生器解决了该问题,但是该协议的缺点是不能够抵抗重放攻击和伪造标签的攻击。后来文献[8]提出的 hash 链协议对随机化 Hash-Lock 协议作了改进。此外还有 Dimitriou 提出的协议[9],该协议同样采用 hash 技术来提供隐私保护,且实现了标签与阅读器的双向认证,在认证后标签才改变它的计数器值和相应的输出值。但该协议还是存在认证期间的标签输出静态值导致容易被跟踪,且还会引起数据不同步的问题[7]。文献[10]中提出了 O-FRAP(optimistic forward secure RFID authentication protocol)认证协议,该协议的密钥在认证后被更新,保证前向安全,不容易被跟踪。但其缺点是为了保证后台数据库与标签的数据同步,每次查询都要利用整个数据库的每条记录作计算和匹配,这样会使攻击者通过伪造的标签与阅读器通信,浪费后台服务器的资源,造成服务器可能遭受拒绝服务攻击,导致 RFID 系统崩溃。

综上所述,目前 RFID 系统还缺乏一个实用的低成本的安全的隐私保护认证协议。现在很多的 RFID 系统都应用于安全领域,RFID 标签会与后台服务器频繁通信,一旦攻击者伪造标签对服务器发起 DoS 攻击,使 RFID 系统崩溃,会给使用安全系统的用户带来很大损失。而现阶段提出的很多协议都很难抵抗这种攻击,本文的目的就是设计一个安全协议解决这一问题。

2　本文 RFID 安全认证协议

2.1　设计目标

本文的 RFID 安全协议设计需要考虑以下几点:

a)标签信息以密文传输,保护内容隐私。

b)标签发出的信息具有随机性,即每次的通信应随机化,保证不被跟踪。

c)减少计算的复杂度为标签节省空间,降低成本。

d)实现标签与服务器(或阅读器)的双向认证。

e)能够解决数据库数据与标签数据之间的不同步问题。

f)能够抵抗拒绝服务攻击。

2.2　初始化

针对以上协议的不足和 RFID 标签低成本的特点,本文采用了流密码加密和伪随机生成函数(PRNG)设计了一个安全认证协议。本文所用的符号如表 1 所示。每个标签和服务器都保持两个密钥。一个是公共密钥 k_c,该密钥用于在查询数据库之前判断标签和阅读器的合法性,是固定不变的,而且所有合法标签都相同。另一个是私有的密钥 k_t,每个标签的密钥 k_t 都是唯一的,这个密钥在认证的过程中动态更新。本文的流加密算法开始时在标签、阅读器和服务器上都持有一个密钥流产生器,密钥 k_c 和 k_t 只是作为产生器的密钥源,由产生器产生密钥流,再通过异或运算加密二进制明文。每个密钥流产生器都是采用相同算法。PRNG( )函数是单向的伪随机函数,即是不可逆的。

后台数据库 D 中为每一个保持一个数组(k_c(ID),ID,k_t),在标签中存储一组数据(ID,k_t,k_c),其中 k_t 和 k_c 存储在标签的保护区内,服务器只存储 k_c。

表 1　符号说明

R	阅读器	k_c	S 与 T 的固定密钥
T	RFID 标签	k_t	S 与每个 T_i 标签都共享的密钥
S	后台服务器	r_t	T 产生的随机数
D	S 的数据库	r_s	S 产生的随机数
ID	射频标签的标志值	r_r	R 产生的随机数
PRNG( )	伪随机函数(单向函数)	D. query( )	数据库的查询过程
k( )	以 k 为密钥的加密函数	D. update( )	数据库中更新密钥的过程
⊕	异或函数	‖	连接操作符

2.3　协议流程

如图 2 所示,整个认证过程分 10 个步骤,所有的加密操作都采用流密码加密,协议的步骤如下:

a)在电子标签 T 进入到阅读器 R 的通信范围之内时,阅读器发送一个询问信号 Query 给电子标签。

b)收到信号的标签产生一个与 ID 位数相同的随机数 r_t,然后把这个随机数 r_t 发送给阅读器。

c)阅读器收到数据后,产生自己的随机数 r_r,并与随机数 r_t 一起通过安全的信道发送给后台服务器 S。

d)服务器将 r_r 与 r_t 连接:$b = r_r \| r_t$,使用公共密钥 k_c 加密 b:$c = k_c(b)$,并把 c 传回阅读器。

e)阅读器把自己的随机数 r_r 和 c 一起发送给标签 T。

f)标签收到后,将收到的 r_r' 和 r_t 作连接,再使用公共密钥 k_c 加密:$c' = k_c(r_r' \| r_t)$,然后判断 c 是否相等 c',如果不相等则认为阅读器不合法;否则,计算一个 k_c(ID),它表示对 ID 用公共密钥 k_c 加密,再与 r_t 异或:$a = k_c(ID) \oplus r_t$,这是为了使每次传输的数据都有变化,防止被追踪。然后再将 a 与 $r_r' \| r_t$ 连接,用公共密钥 k_c 加密:$m = k_c(a \| r_r' \| r_t)$,用标签自己唯一的密钥 k_t 加密 r_t:$d = k_t(r_t)$,把 a、d、m 三个数据发给阅读器。最后更新自己的密钥 k_t:$k_t' = PRNG(k_t)$,它表示用原先的密钥做种子随机生成新密钥。

g)阅读器把收到的 a 与 $r_r \| r_t$ 连接,再用公共密钥 k_c 加密:$m' = k_c(a \| r_r \| r_t)$,比较收到的 m 与 m',如果不相等则认为是遭受到了攻击,认为标签不合法,停止认证过程;否则,阅读器会把收到的 a、d 传给后台服务器。

h)服务器将收到的 a 与 r_t 异或得到 $n = a \oplus r_t$,即为 k_c(ID),再用 n 作为索引在数据库里查找标签 T 的记录,在记录里找到标签对应的 ID 和密钥 k_t:(ID ,k_t)←D. query(n)。

(a)用密钥 k_t,加密 r_t:$d' = k_t(r_t)$。通过判断 d 是否等于 d',来对标签的合法性进行验证,如果相等,则认为标签是合法的,认证通过,执行 b);如果不等,就先执行 b),然后再重新执行 a)。为了防止标签遭受阻塞攻击引起数据不同步。

(b)用与标签相同的方法更新密钥 k_t:$k_t'' = PRNG(k_t)$。

(c)再用 k_t'' 更新数据库记录:D. update(k_t'')。

(d)生成一个随机数 r_s,用 k_t'' 加密:$h = k_t(r_s)$,把 h 和 r_s 发给阅读器。

i)阅读器将 h 和 r_s 转发给标签。

j)标签收到后,用它更新后的密钥 k_t' 加密 r_s:$h' = k_t(r_s)$,比较 h' 和 h,如果相等,标签就认为阅读器和后台服务器合法,认证通过。到此,整个认证过程结束。

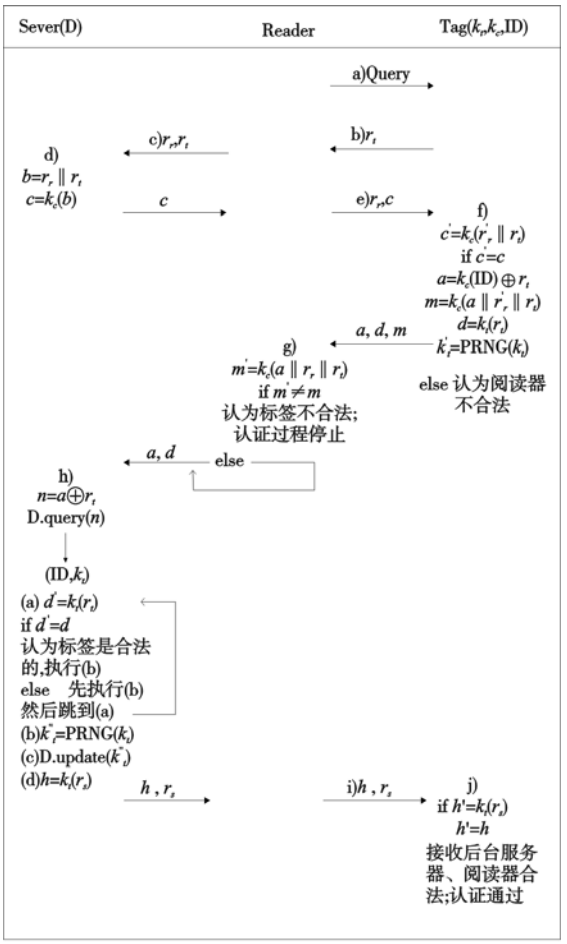

图2 本文RFID安全认证协议示意图

3 安全性与工作性能分析

3.1 安全性分析

表2将该协议与文献[3,8~10]中提出的协议进行了以下安全性方面的对比分析。

a)隐私保护(抵抗嗅探)。上述协议利用加密的方法使信息交换过程中的数据具有不可读性,保证了数据不被中间人恶意窃听。在本协议中,ID是通过加密传输的,窃听者在不知道密钥 k_e 的情况下是得不到ID的,而且必须知道密钥 k_t 才能通过认证。

b)重放攻击。因为在传输的过程中携带了一定数量的随机数,保证了每次来回传输的数据都有变化;而且对随机数进行加密,然后进行比较验证,当中任何一步出错都会导致整个通信的结束,因此非法用户不可能实施重放攻击。

c)前向安全性。如果一个非法用户破坏了一个标签,拥有它现在保存的大部分数据,那么它就可以追踪该标签以前的会话,这就是前向攻击。在本协议中,每次认证都会用PRNG函数随机化更新密钥,而且PRNG函数是单向函数,即使保存在标签的密钥 k_t 泄露了,攻击者也推导不出旧密钥的 k_t,所以保证了前向安全性。

d)数据一致性(数据同步)。非法用户可以阻断协议中步骤f)发起的通信会话,这样就导致服务器更新了密钥 k_t,而标签没有更新其存储的密钥 k_t,服务器和标签会失去同步。本协议未使用在数据库和标签中存储两个密钥(新、旧密钥),而是在服务器端重复使用PRNG函数更新密钥 k_t 来认证标签,防止数据不同步。

e)位置跟踪[11]。通过使用对称流密码加密系统,使得密文之间的相关度较低[12],而且每次认证过程的每个会话都有随机数参与,每次的会话都会随随机数变化而变化,非法用户既不能将窃听到的信息与某个标签以前的应答信息相联系,也不能将某个标签的应答信息与其他标签的应答信息区分开,因此非法用户要跟踪标签的位置是非常困难的。

f)拒绝服务式攻击(DoS)。在阅读器和每个标签上都保存了一个公共密钥 k_e。服务器发出查询命令后用密钥 k_e 加密随机数 r_r 与 r_t,并发送给标签。标签可以先计算判别阅读器和服务器的合法性,然后通过标签再用密钥 k_e 加密自己的 a、r_r 与 r_t,并发送给阅读器。阅读器在计算之后判断标签的合法性,如果标签不合法,阅读器就不会把数据传给服务器,防止了伪造的标签对后台服务器发起的拒绝服务式攻击。

g)伪造服务器与标签的攻击。由于本协议的ID在传送中都用密钥 k_e 加密了,非法用户很难通过窃听得到,从而不能计算 a 和 m,进而不能假冒服务器与标签。虽然非法用户通过某种途径可以得到一个标签的密钥 k_e,那么协议将会暴露其他标签的ID,但是验证标签和服务器的过程都需要密钥 k_t,不断更新的密钥 k_t 是很难得到的,所以本协议可以有效防止伪造服务器与标签的攻击。

表2 RFID认证协议的安全性对比

协议	相互认证	窃听	重放攻击	位置追踪	信息泄露	前向攻击	同步性	拒绝服务攻击
文献[3]	×	√	×	×	√	×	√	×
文献[8]	×	√	×	×	√	×	×	×
文献[9]	×	√	×	√	√	√	×	×
文献[10]	√	√	√	√	√	√	√	×
本文	√	√	√	√	√	√	√	√

3.2 性能分析

本协议还具有工作效率高的特点。在整个认证过程中只需简单的异或操作,避免了由于使用hash锁算法而造成速度与资源的额外开销,过程简单实用。由于流密码的工作特性特别适合于硬件实现且速度快,因此能够应用在RFID这种资源极其有限的系统上。同时实现了标签与阅读器的双向认证。没有像文献[10]那样在数据库和标签中保持两个密钥 k_t(新密钥和旧密钥),只存储一个密钥,这样虽然浪费了一点计算资源,但是为RFID标签节省了存储空间。为了对性能作进一步分析,比较了本文方案与其他方案所运用的函数及基本操作,结果如表3所示。可以看出本文的协议方案在各种函数的计算开销上处于中间水平,并没有降低协议的执行性能。

表3 函数及基本操作的比较

协议	哈希函数或者加密函数次数		异或函数次数		随机函数(PRNG)次数	
	标签	服务器	标签	服务器	标签	服务器
文献[3]	2	2	0	0	0	0
文献[8]	3	5	3	3	1	2
文献[9]	2	3	1	1	0	2
文献[10]	6	5	1	1	1	1
本文	5	4	1	1	1	1

4 结束语

本文设计了新的RFID相互认证协议,该 (下转第682页)

于当前主流的差分隐私保护方法。因此,在相同隐私保护级别下,如果数据发布者更关注数据发布结果准确率,本文提出的方法就优于传统的差分隐私保护方法。

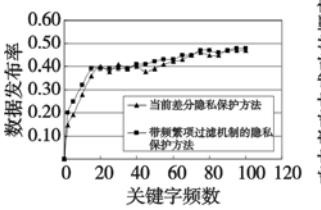

图2　数据发布率比较

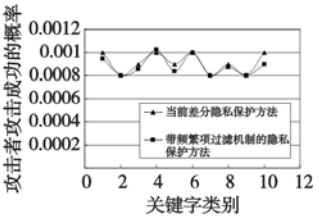

图3　隐私保护级别比较

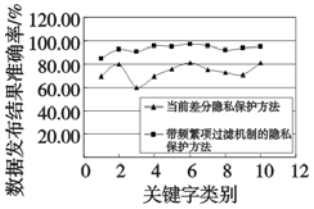

图4　数据发布结果准确率比较

4　结束语

本文就现有差分隐私保护算法由于对数据隐私保护过度而导致数据发布准确性降低这一问题进行了深入研究,分析了差分隐私保护方法隐私保护过度根本原因,提出了一种带频繁项过滤机制的隐私保护新方法,并通过理论和实验验证证明了带频繁项过滤机制的隐私保护方法达到了差分隐私保护级别,可以有效克服差分隐私方法对数据保护过度这一问题。虽然带频繁项过滤机制的隐私保护方法的数据发布率略低于传统的差分隐私保护方法,但前者的数据发布准确性比后者有很大程度上的提高。因此,在数据发布者更关注数据发布结果准确率情况下,本文的方法优于传统的差分隐私保护方法。

在未来的工作中,将在降低对数据发布率影响的情况下,进一步提高数据发布准确性,并将进一步探索如何提高数据发布率。

参考文献:

[1] VERYKIOS V S, BERTINO E, FOVINO I N. State of the art in privacy preserving data mining[J]. ACM SIGMOD Record, 2004, 33(1): 50-57.

[2] 阚莹莹,曹天杰.一种增强的隐私保护 K-匿名方法——(α,L)多样化 K-匿名[J].计算机工程与应用,2010,46(21):148-151.

[3] 周水庚,李丰,陶宇飞,等.面向数据库应用的隐私保护研究综述[J].计算机学报, 2009,32(5):848-858.

[4] 任静涵,张保稳,陈晓桦.隐私保护数据挖掘研究进展[J].信息安全与通信保密,2008,27(8):2823-2827.

[5] DWORK C. Differential privacy: a survey of results[C]//Proc of the 5th Annual Conference on Theory and Applications of Models of Computation. 2008: 1-19.

[6] DWORK C, SMITH A. Differential privacy for statistics: what we know and what we want to learn[J]. Journal of Privacy and Confidentiality, 2009, 2(1): 135-154.

[7] LIU Tan-tan, WANG Fan, ZHU Jie-dan, *et al*. Differential analysis on deep Web data sources[C]//Proc of the 2010 IEEE International Conference on Data Mining Workshops. 2010: 33-40.

[8] ZHANG Ning, LI Ming. Distributed data mining with differential privacy [J]. ACM SIGMOD Record, 2010, 15(1): 493-502.

[9] 刘彩虹,刘强,李爱平.基于向量内积的非频繁项挖掘算法研究[J].计算机工程与科学,2011,33(2):92-96.

[10] 鲍钰,黄国兴.基于 Web 日志的隐私保护关联规则挖掘方法[J].计算机科学, 2009,38(8):220-223.

[11] 雷红艳,邹汉斌.限制隐私泄露的隐私保护聚类算法[J].计算机工程与设计,2010,31(7):1444-1446.

[12] KOROLVA A, KENTHAPADI K, MISHRA N, *et al*. A releasing search queries and clicks privately[C]//Proc of International World Wide Web Conference Committee. 2009: 171-180.

(上接第 678 页)协议具有成本低、效率高、安全性和隐私性好等优点。对应用此安全协议的可行性进行了分析研究,其能够解决隐私、重放、前向安全性、同步性、不可分辨性与位置跟踪、拒绝服务式攻击等安全问题。但是协议中使用的流密码加密,本文并没有给出具体算法,这需要考虑具体的硬件设计,现有的算法有 A5、f9 等[13]。设计一个合适的密码算法是今后的研究方向。

参考文献:

[1] LAURIE A. Practical attacks against RFID[J]. Network Security, 2007(9): 4-7.

[2] YUKIYASU T, TERUO S, TOMOYASU S, *et al*. Cryptanalysis of DES implemented on computers with cache[C]//Proc of the 5th International Workshop on Cryptographic Hardware and Embedded Systems. [S.l.]: Springer-Verlag, 2003: 62-76.

[3] SARMA S, WEIS S, ENGELS D. RFID systems, security and privacy implications, MIT-AUTOID-WH-014[R]. [S.l.]: Auto-ID Center, MIT, 2002.

[4] JUELS A, RIVEST R L, SZYDLO M. The blocker tag: selective blocking of RFID tags for consumer privacy[C]//Proc of ACM Conference on Computer and Communications Security. 2003: 103-111.

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

[6] GARFINKEL S L, JUELS A, PAPPU R. RFID privacy: an overview of problems and proposed solutions[J]. IEEE Security & Privacy Magazine, 2005, 3(3): 34-44.

[7] JUELS A. RFID security and privacy: a research survey[J]. IEEE Journal on Selected Areas in Communications, 2004, 24(2): 381-394.

[8] KIRN H S, OH J H, CHOI J Y. Analysis of the RFID security protocol for secure smart home network[C]//Proc of International Conference on Hybrid Information Technology. 2006: 356-363.

[9] DIMITRIOU T. A light weight RFID protocol to protect against traceability and cloning attacks[C]//Proc of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks. 2005: 137-145.

[10] LE T V, BURNMESTER M, De MEDEIROS B. Universally composable and forward secure RFID authentication and authenticated key exchange[C]//Proc of the 2nd ACM Symposium on Information, Computer and Communications Security. 2007: 242-252.

[11] 王信,薛小平,张思东.RFID 系统数据安全研究[J].信息技术与信息化,2006(1):51-53.

[12] 杨波.现代密码学[M].2 版.北京:清华大学出版社,2007.

[13] MENEZES A J, Van OORSCHOT P C, VANSTONE S A. Handbook of applied cryptography[M]. Boca Raton: CRC Press, 1997.