文章编号:1674－2869(2019)05－0504－07

基于循环组的RFID安全认证协议

张腾达[1],董　辉[*2]
1. 安徽新闻出版职业技术学院,安徽　合肥　230601;
2. 亳州职业技术学院,安徽　亳州　236800

摘　要:针对射频识别(RFID)系统存在的信息隐私和安全问题,分析典型的RFID安全认证协议及其劣势,提出了基于循环组的RFID系统相互认证协议。该协议不在标签侧执行伪随机函数,而是执行简单的异或和取模运算,并基于匿名集和信息泄漏度量标签受攻击时分析系统的隐私性能和安全级别。与常见认证协议相比,所提出的协议具备运算效率高、内存需求低等优势。性能分析和仿真实验表明,该协议能够抵抗重放、异步和中间人等典型攻击,与其它认证协议相比具有更强的安全性和更好的隐私保护能力,并能满足RFID标签低成本的要求。

关键词:射频识别;循环组;安全隐私;认证协议
中图分类号:TP393.08　　**文献标识码**:A　　**doi**:10.3969/j.issn.1674-2869.2019.05.018

Security Mutual Authentication Protocol of Radio-Frequency Identification Based on Cyclic Group

ZHANG Tengda[1], *DONG Hui*[*2]
1. Anhui Vocational College of Press and Publishing, Hefei 230601, China;
2. Vocational and Technical College, Bouzhou 236800, China

Abstract: Aiming at the problems of privacy and security in radio-frequency identification (RFID) system, we analyzed the typical RFID security and privacy authentication protocol and their disadvantages, and then proposed a mutual authentication protocol based on the cyclic group for RFID system. Rather than execute the pseudo-random function on the tag side, our protocol is based on simple module and exclusive OR operations. Additionally, it measures the privacy protection ability and security level based on the anonymous set and information leakage. Compared with existing authentication protocol, the proposed protocol has the advantages of high computational efficiency and lower memory requirements. Results of simulation experiments show that our protocol has good performance insecurity and privacy protection. It can handle many typical attacks effectively, such as replay, asynchronous and man-in-the-middle, etc. Furthermore, it can satisfy the low-cost requirement of RFID tags.

Keywords: radio-frequency identification (RFID); cyclic group; security and privacy; authentication protocol

射频识别(Radio-Frequency Identification, RFID)技术是物联网(Internet of Things, IoT)的核心技术之一,在农业、交通、制造及军事等各领域都有广泛的应用[1]。RFID系统由阅读器、标签及服务器实体组成。服务器存储有关标签的所有信息,并通过安全信道与阅读器连接。通常阅读器

收稿日期:2019-07-02
基金项目:安徽省高校自然科学研究重点项目(KJ2018A0887,KJ2016A493);安徽省亳州市产业创新团队项目(亳组[2015]20号-2)。
作者简介:张腾达,硕士。E-mail:Ztengda1983@163.com
***通讯作者**:董　辉,硕士,教授。E-mail:181588266@qq.com
引文格式:张腾达,董辉. 基于循环组的RFID安全认证协议[J]. 武汉工程大学学报,2019,41(5):504-510.

的使用者是可信的，而阅读器和标签之间的信息交互是通过天线耦合来完成的，传输信道具有开放性，使得传输的数据信息极易被截获和破解，攻击者通过对阅读器或标签进行读写操作，来阻止或破坏两者之间正常通信。另外因标签只具备有限的计算和存储能力，使得攻击者容易对标签跟踪、获取隐私等，造成RFID系统面临信息泄漏、安全等多种威胁[2]，因此如何提高RFID认证协议的安全性和隐私保护是射频识别技术研究的热点之一。本文设计了一种基于循环组、取模（Mod）和异或运算（ExclusiveOR，XOR）的RFID系统安全认证协议，在不增加成本的前提下，提高RFID系统的信息隐私性能及安全级别。

1　相关工作

1.1　现状分析

为了增强RFID系统的安全性和隐私保护并降低计算复杂度，国内外研究人员提出了许多RFID系统相互认证方案。文献[3]提出了RFID群组认证协议，该方案不具备不可追踪性，且无法抵抗交错攻击；文献[4]提出了改进的RFID群组认证协议，但对标签的计算能力要求较高；文献[5]基于传统密码学设计了RFID认证协议，具有良好的安全性，但不适于标签的低计算能力；文献[6]提出了一种基于哈希（Hash）函数的MH认证协议，实现了RFID协议安全性与效率的平衡，但M-Hash函数所需的门电路较为复杂，成本较高；文献[7]设计了基于串空间模型方法的认证协议，具有较高的安全性，但增大了空间开销；文献[8]基于单向伪随机函数的移动RFID系统认证协议，但该协议并不适合大规模的RFID系统；文献[9]提出了一种基于改进的伪随机函数的RFID双向认证协议，但同样存在计算力要求较高的问题；文献[10]设计了基于组对称密钥的匿名安全认证，具有较好的隐私级别和安全性，但标签侧空间开销较高；文献[11]提出了一种基于Hash函数和云计算的轻量级RFID群组标签认证协议，但协议复杂度大、硬件实现较难。

针对上述协议存在的隐私泄漏和安全威胁，本文提出了基于循环组的RFID相互认证协议。该协议只通过简单的取摸和异或运算，不执行随机数函数，减小标签端计算量，实现读写器和标签之间的认证，同时可有效降低标签的硬件成本，提高运算速度。通过性能分析和仿真实验，该协议可有效抵抗追溯攻击、重放攻击、去同步攻击、中间人攻击、伪造攻击等。

1.2　基本概念

假设G是一个非空集合，运算符$*$把G中任意两个元素组合成一个新的元素。如G遵守集合运算定律，则集合G与运算符$*$一起是一个组，G中的元素总数用$|G|$表示。设H是G组的一个子集，则称H是G的一个子组。

定义1循环组：若存在元素$a\in G$，使得$G=<a>=\{a^n\ |n\in Z\}$成立，则G称为循环组，元素a称为循环组G的生成器。

循环组的特征约定

1）假设$G=<a>$是n阶循环组。如果$\mathrm{Gcd}(k,n)=1$（Gcd为最大公约数运算符），则$G=<a^k>$。

2）循环组的每个子组都是循环的。

3）假设$G=<a>$是n阶循环组，则G的任何子组的顺序都是n的约数。

4）对于n的每个正约数k，组G恰好具有由$<a^{n/k}>$表示的阶数为k的一个子组。

1.3　RFID系统模型

在该系统模型中，由于阅读器和服务器之间的通信信道彼此信任，为简单起见，可把阅读器和服务器组合成一个实体看作阅读器[12]。

本文基于循环组的特征，在此构建了RFID系统模型。选择n阶循环组$G=<a>$并找到它的一些子组$H_i=<a_i>(i=1,2,\cdots,f,f<n)$，根据循环组的第4个特征，这里$a_i=a^{n/k}$，如果$a_i$和$a_j$分别是$G$的两个不同子组$H_i$和$H_j$的生成器，显然$a_i$和$a_j$是$G$中不同的元素。在系统里如果$H_p$是最高阶子组（$|H_p|=P$）并且$H_{p-1}$是系统中第二高阶子组（$|H_{p-1}|=Q$），则可以仅利用$H_p$的$Q$个元素来分配标签，使得$i$的值在两个子组中是相同的，$i$是在服务器查找表中的索引参数。

服务器查找表是标签在服务器数据库中的一个索引表，如表1所示。表中对于$H_j=<a_j>$的每一个元素a_j^i，分配了一个对应的标签T_{ji}，并以i作为标签T_{ji}在表中的索引。两个临时参数$m_{ji_{\mathrm{old}}}$和$m_{ji_{\mathrm{new}}}$与标签T_{ji}相关联，将唯一标识号ID_{ji}和密钥K_{ji}存储也到标签T_{ji}存储器内，最初$m_{ji_{\mathrm{old}}}=0$和$m_{ji_{\mathrm{new}}}$为随机值。对于与H_j中的元素a_j^i相关联的每个标签T_{ji}，在H_j中存储a_j^i的逆元素，即$(a_j^i)^{-1}$。另外，在标签的内存中，生成一个机数m_{R_4}，m_{R_4}的初值与$m_{ji_{\mathrm{new}}}$相同。

1.4　攻击者模型

对于RFID系统，攻击者主要通过窃听、拦截

表1 RFID服务器查找表

Tab.1 RFID server look-up table

子组	索引值	标签	存储数据
$H_1=<a_1>$	i_1	T_{1i1}	$[ID_{1i1},K_{1i1},R_{1i1old},R_{1i1new}]$
	i_2	T_{1i2}	$[ID_{1i2},K_{1i2},R_{1i2old},R_{1i2new}]$
	…	…	…
	$i_{\|H1\|-1}$	$T_{1i\|H1\|-1}$	$[ID_{1i\|H1\|-1},K_{1i\|H1\|-1},R_{1i(\|H1\|-1)old},R_{1i(\|H1\|-1)new}]$
…	…	…	…
$H_m=<a_m>$	i_1	T_{mi1}	$[ID_{mi1},K_{mi1},R_{mi1old},R_{mi1new}]$
	i_2	T_{mi2}	$[ID_{mi2},K_{mi2},R_{mi2old},R_{mi2new}]$
	…	…	…
	$i_{\|Hml-1}$	$T_{mi\|Hml-1}$	$[ID_{mi\|Hml-1},K_{mi\|H1l-1},R_{mi(\|Hml-1)old},R_{mi(\|Hml-1)new}]$

或篡改阅读器与标签之间的传输的消息实现攻击[3]。根据文献[3]攻击者模型加以改进，设计了符合本文实验要求的攻击者模型。攻击模型如下：

1）SendTag(Msg,T_{ji})→Msg_1：攻击者可以向标签T_{ji}发送消息Msg，标签T_{ji}以消息Msg_1响应。

2）SendReader(Msg,R)→Msg_2：攻击者向给阅读器R发送消息Msg，R回复消息Msg_2。

3）DrawTags(S)查询

攻击者可以使用此查询随时从系统S访问一组标签。

4）Corrupt(T_{ji})查询

攻击者通过此查询能够访问标签存储器中的数据。

在模型中，攻击者分别对攻击对象R和T来利用SendTag和SendReader操作执行查询运算，一次能够向至少(N-2)个标签发送Corrupt查询指令，其中N是DrawTags查询获得的标签总数。

2 基于循环组的RFID认证协议

2.1 符号约定

为了便于描述，下面给出协议中所用到的标识符及含义说明，如表2所示。

表2 协议中的符号及含义

Tab.2 Symbols and meanings in proposed protocols

标识符	含义	标识符	含义
$G=<a>$	有限循环组，a为其生成器元素	$H_j=<a_j>$	G的子组，a_j为其生成器元素
K_{ji}	与子组H_j的第i个标签T_{ji}的密钥	$(a_j^i)^{-1}$	子组H_j中的a_j^i的逆元素
$m_{nm}:n=1,2,3,\cdots$	由阅读器生成的临时数据	$\otimes$	异或运算(XOR)符
Mod	取模运算符	ID_{ji}	标签T_{ji}的唯一标识号
$\alpha,\beta,\gamma,\delta,\xi,\eta$	为阅读器或标签侧计算结果内容		

2.2 协议原理

协议初始阶段，阅读器中存储生成的循环组G和密钥K，标签中持有标签ID及密钥K，另外还有两个临时参数$m_{R_{old}}$和$m_{R_{new}}$，$m_{R_{old}}$初值为0，$m_{R_{new}}$初值为随机数。本文提出的协议如图1所示。

协议的具体过程描述如下：

①Hello

标签进入阅读器的阅读范围后，阅读器向标签发送信号“Hello”，发起验证，开启认证过程。

② $Mg_1:T_{ki}\rightarrow R:\{i,\alpha\}$

标签T_{ki}计算$\alpha=(a_k^i)^{-1}\otimes m_{R_4}$，并生成请求消息$Mg_1=\{i,\alpha\}$，标签将$Mg_1$发送给阅读器R。

③ $Mg_2:R\rightarrow T_{ki}:\{\beta,\gamma\}$

阅读器R收到标签的请求消息Mg_1后，根据表1阅读器，使用i作为索引对所有子组执行以下步骤，直到找到正确的标签。

计算H_k中a_k^i的逆元素$(a_k^i)^{-1}$，其中a_k是子组H_k的发生器；

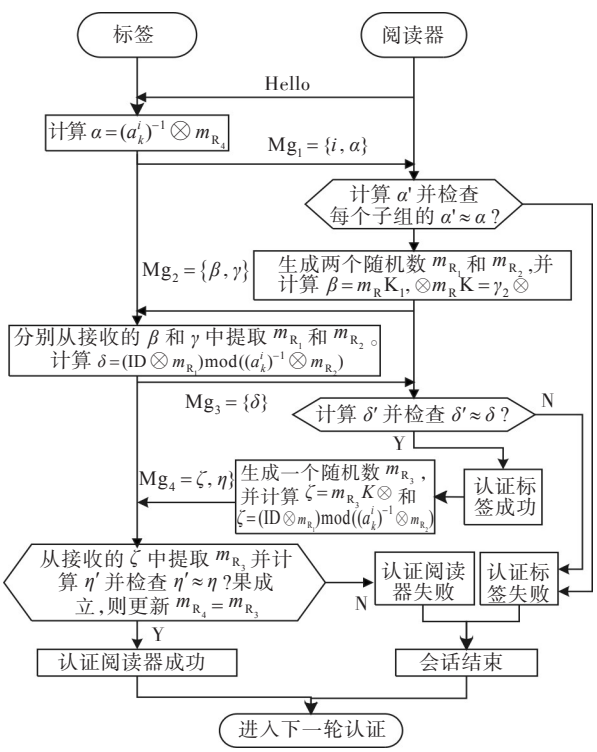

图1 相互认证协议流程

Fig. 1 Flowchart of mutual authentication protocol

阅读器计算 $\alpha'=(a_k^i)^{-1}\otimes(m_{R_{old}}/m_{R_{new}})$，并检查 α' 是否等于接收到的 α，如果相等，它在子组 H_k 内得到正确的标签 T_{ki}，否则，则阅读器终止协议，认证失败；

阅读器生成2个随机数 m_{R_1} 和 m_{R_2}，并计算 $\beta=m_{R_1}\otimes K_{ki}$ 及 $\gamma=m_{R_2}\otimes K_{ki}$，其中 K_{ki} 是标签 T_{ki} 的密钥。阅读器生成消息 $Mg_2=\{\beta,\gamma\}$ 并将其发送到标签。

④ $Mg_3:T_{ki}\rightarrow R:\{\delta\}$

在接收到阅读器发送消息 Mg_2 时，标签 T_{ki} 利用其密钥 K_{ki} 分别从 β 和 γ 中提取出 m_{R_1} 和 m_{R_2}，并计算 $\delta=(ID_{ki}\otimes m_{R_1})\bmod((a_k^i)^{-1}\otimes m_{R_2})$，生成消息 $Mg_3=\{\delta\}$ 发送给阅读器。

⑤ $Mg_4:R\rightarrow T_{ki}:\{\zeta,\eta\}$

阅读器收到消息 Mg_3 之后，计算 $\delta'=(ID_{ki}\otimes m_{R_1})\bmod((a_k^i)^{-1}\otimes m_{R_2})$，并检查 δ' 是否等于接收的 δ，如成立，则阅读器认证标签 T_{ki} 成功，阅读器生成随机数 m_{R_3}，并设置 $m_{kiold}=m_{kinew}$，且 $m_{kinew}=m_{R_3}$，同时，还计算 $\zeta=m_{R_3}\otimes K_{ki}$ 和 $\eta=(ID_{ki}\otimes m_{R_3})\bmod((a_k^i)^{-1}\otimes m_{R_1})$，生成消息 $Mg_4=\{\zeta,\eta\}$ 并发送到标签 T_{ki}。否则终止会话，本轮认证结束，等待进入下一轮认证。

⑥验证结束

在接收到消息 Mg_4 时，标签 T_{ki} 从 ζ 中提取 m_{R_3} 并计算 $\eta'=(ID_{ki}\otimes m_{R_3})\bmod((a_k^i)^{-1}\otimes m_{R_1})$。标签检查 η' 是否等于接收的 η。如果是，则标签认证阅读器成功，并更新 $m_{R_4}=m_{R_3}$，否则认证失败，本轮会话终止，进入下一轮认证过程。

3　隐私与安全分析

3.1　隐私分析

3.1.1　隐私及隐私实验模型　根据文献[13]，RFID系统隐私可用式(1)表示：

$$P[E_{A,S}^{pr}(k,n,r,s,t)\ \text{Succeeds in Guessing}\ b]\leqslant\frac{1}{2}+\frac{1}{\text{poly}(k)}\tag{1}$$

其中 $E_{A,S}^{pr}[k,n,r,s,t]$ 实验模型，A表示攻击者，S表示RFID系统，r，s 和 t 分别表示攻击者利用SendTag和SendReader的能力、表示计算步骤、计算标识，b 为估算位，$\text{poly}(k)$ 是安全参数 k 的函数，n 是标签数。

实验中攻击者的主要目标是在计算和交互限制中识别两个不同的标签，如果攻击者没有明显的优势，则认为RFID认证协议是安全的。攻击过程分为以下3个阶段：

初始阶段：攻击者A与系统S交互，在不超过其界限的情况下查询系统标签数据库并对其进行分析。

攻击阶段：A从数据库获得的标签集合中任意选择两个未损坏的标签。并随机选择其中的一个，攻击者获取并分析该标签上的数据。

估算阶段：A输出估算位 b。如果估算成功，则应 $b=1$，否则 $b=0$。

如果 $b=1$，实验模型 E 是成功的。

3.1.2　隐私级别的度量　当一些标签被泄露时，所有标签都被分区，隐私权度量标准是使用不相交的标签分区进行观察，使得攻击者不能区分属于同一分区的标签，但可以区别属于不同分区的标签[14]。$|P_i|$ 表示分区 P_i 的大小，N 为标签数，$|P_i|/N$ 是随机选择的标签属于分区 P_i 的概率。本文根据匿名集和数据泄漏分析所提出的方案的隐私级别。

1)基于匿名集的隐私级别

基于匿名集的隐私级别 ρ 被表征为用标签总数N标准化的平均匿名集大小[11]，如式(2)所示：

$$\rho=\frac{1}{N^2}\sum_i|P_i|^2\tag{2}$$

协议中攻击者无法区分两个标签是否属于同一个子组，因此，如果 D 是整个系统中受攻击标签的总数，分为 D 个匿名集，另一个是未受攻击标签匿名集个数($N-D$)，每个匿名集的大小为皆为1。结合等式(2)，所提协议实现的隐私级别可表示为：

$$\rho=\frac{1}{N^2}[D+(N-D)^2]\tag{3}$$

2)基于信息泄漏的隐私级别

如果攻击者将具有 N 个标签的系统划分为 k 个不相交集，则信息泄漏 Π 可以表示为式(4)：

$$\Pi=\sum_{i=1}^{k}\frac{|P_i|}{N}\log_2\left(\frac{N}{|P_i|}\right)\tag{4}$$

在所提出的协议中，根据上文分区集，结合等式(4)，信息泄漏 Π 可以表示为式(5)：

$$\Pi=\frac{1}{N}\log_2 N+\frac{N-D}{N}\log_2\left(\frac{N}{N-D}\right)\tag{5}$$

3.1.3　隐私分析

定理1　所提出的协议具有隐私安全性。

证明假设提出的协议不能保护RFID系统信

息隐私。则攻击者赢得实验的成功概率是不可忽视的。攻击者A的隐私攻击过程分为如下3个阶段：

初始阶段：攻击者A通过查询操作获取一组标签。

A通过DrawTag查询发送信息到标签T_i，在不超出其计算范围的情况下分析标签数据。A可以使用Corrupt查询来处理最多$n-2$个标签。执行步骤如下

$$T_i \leftarrow \mathrm{DrawTag}(S)$$

$$\left\{i,\left(a_k^k\right)^{-1},K,ID,R\right\} \leftarrow \mathrm{Corrupt}(T_i)$$

攻击阶段：攻击者A从DrawTags查询获得的标签中任选两个未损坏的标签，例如T_i和T_j，作为攻击标签，令$b \in \{i,j\}$。随机选择其中的T_b并分析在其上运行SendTag查询。执行步骤如下：

$$Mg_1 = \{i,\alpha\} \leftarrow \mathrm{SendTag}(\mathrm{init},T_b)$$

$$Mg_2 = \{\beta,\gamma\} \leftarrow \mathrm{SendReader}(Mg_1,R)$$

$$Mg_3 = \{i,\delta\} \leftarrow \mathrm{SendTag}(Mg_2,T_b)$$

$$Mg_4 = \{\zeta,\eta\} \leftarrow \mathrm{SendReader}(Mg_3,R)$$

估算阶段：攻击者输出相应标签的估算位b'。如果$b'=b$，攻击者会赢得实验。但这种情况只有当攻击者知道存储在T_b的内存及其母群G中的所有秘钥时才有可能，显然这是不可能的，上述假设是错误的。因此，所提出的协议保护了RFID系统的隐私。

3.1.4 不可追溯分析

定理2 所提出的协议对于攻击者具有不可追溯性。

证明：假设所提议的协议是可追溯的，即攻击者可以随时追踪标签，这意味着攻击者能够区分任意两个标签。攻击者对标签的追溯同样可分为如下3个阶段，初始阶段：攻击者对RFID系统S使用DrawTags查询访问标签。对标签和阅读器，分别执行SendTag和SendReader查询，以获得并分析阅读器和标签之间传输的信息。本阶段执行步骤如下：

$$T_i \leftarrow \mathrm{DrawTag}(S)$$

$$Mg_1 = \{i,\alpha\} \leftarrow \mathrm{SendTag}(\mathrm{init},T_i)$$

$$Mg_2 = \{\beta,\gamma\} \leftarrow \mathrm{SendReader}(Mg_1,R)$$

$$Mg_3 = \{i,\delta\} \leftarrow \mathrm{SendTag}(Mg_2,T_i)$$

$$Mg_4 = \{\zeta,\eta\} \leftarrow \mathrm{SendReader}(Mg_3,R)$$

攻击阶段：攻击者选择两个未损坏的标签T_i和T_j，并向他们发送Corrupt查询。A随机选择T_b：$b \in \{i,j\}$。攻击者将对查询到标签T_b进行评估。

$$Mg_1{*} = \{i,\alpha\} \leftarrow \mathrm{SendTag}(\mathrm{init},T_b)$$

$$Mg_2{*} = \{\beta,\gamma\} \leftarrow \mathrm{SendReader}(Mg_1{*},R)$$

$$Mg_3{*} = \{i,\delta\} \leftarrow \mathrm{SendTag}(Mg_2{*},T_b)$$

$$Mg_4{*} = \{\zeta,\eta\} \leftarrow \mathrm{SendReader}(Mg_3{*},R)$$

$$\left\{i,\left(a_k^i\right)^{-1},K,ID,R\right\} \leftarrow \mathrm{Corrupt}(T_i)$$

估算阶段：A输出估算位b'。

如果$b'=b$，攻击者将赢得比赛，但只有在$P_r[Mg_1{*}=Mg_1]=1$的情况下才有可能，而且由于消息Mg_1取决于标签的随机数m_{R_4}，m_{R_4}它在每次认证过程中都是不同的，显然上式难以成立。因此，上述假设是错误的，即攻击者无法追踪标签。

3.2 安全分析

3.2.1 抵抗重放攻击 重放攻击的攻击者可以窃听无线信道，捕获并分析在阅读器和标签之间先前所传输的消息[15]。在所提出的方案中，攻击者伪造消息作为有效标签/读取器是不可行的，因为每次发送的消息在每次认证会话中都会生成新的随机数，这是攻击者无法提前获得的，这是因为随机的异或运算（XOR）具有攻击者无法获知的密钥K，所以即使不法分子截取到之前的应答消息，也无法通过重放应答消息，最终使得攻击者的所有重播消息都是非法消息。因此，基于上述的分析，本协议方案可以成功阻止重放攻击。

3.2.2 抵抗中间人攻击 因为在次认证过程中，发送的消息中使用新的随机数，从发送的消息中估算或计算这些值的概率可以忽略不计，而攻击者在不知道密钥、唯一标识号和循环组数据的情况下拦截任何传输的消息是不可信的。因此攻击者无法在阅读器和标签之间充当中间人，所以本文协议可以有效的抵抗中间人攻击。

3.2.3 抵抗去同步攻击 对于每个标签，服务器在其数据库中存储两个对应的随机数$m_{R_{old}}$和$m_{R_{new}}$，服务器会在成功进行身份验证会话后更新这些值，而攻击者获得认证前未更新的随机数的值是无用的，因此攻击者不可能使认证过程失去同步。

3.2.4 防范伪造攻击 本文协议采用了阅读器和标签之间按流程相互认证的方法，认证信息在接收时对发送方的身份进行认证后再进行计算。由于密钥信息具有机密性且在每次认证后又随机化，使得攻击者即使获得阅读器或标签的标识或认证前的密钥也是不可信的，无法伪造标签或阅读器，不能实现攻击者与阅读器或标签的相互认证，因此协议可以防范阅读器或标签伪造攻击。

4　性能分析及仿真实验

4.1　性能分析

本文提出的协议方案在标签计算、服务器计算和存储方面的效率，如表3所示。协议方案的搜索复杂度是$O(\gamma)$，仅执行取摸和异或运算，与文献[4]的搜素复杂度相当，但与文献[10]相比本文所设计安全认证协议相比具一定的的优势。假设协议中使用的所有参数都是L比特位长，本协议在标签侧保留4个数据项信息，因此存储成本是$4L$比特。另外，本协议不在标签侧使用任何随机数生成器函数，而是在阅读器侧运行伪随机数生成的随机数，与文献[4]和文献[10]进行比较，减少了标签的计算量，本协议计算过程标签存储空间开销较小，较好的节省轻量级标签的制造成本。

表3　计算成本和性能比较

Tab. 3　Comparison of cost and performance of computation

协议	实体	文献[4]协议	文献[10]协议	本文协议
对称加密/解密	T	2	2	×
	R	2	3	√
所需存储空间	T	$(5*2^l)L$	$(z+2^l)L$	$4L$
搜索复杂度	R	$O(\gamma)$	$O(\gamma+\lvert\pi\rvert)$	$O(\gamma)$
相互认证		√	×	√

注：T为标签；R为阅读器；γ为系统中的组总数；$|\pi|$为与标签的ID、相关联的密钥数；z为每个标签分配的标识符数

4.2　仿真实验

在仿真实验中，RFID系统设定N=1 024个标签，标签被随机分成64组，选择从0到512个受攻击标签数的范围。在所提出的方案中，不必在每个组中采用相同数量的标签。对系统中D个受攻击的标签运行100次模拟。根基公式(3)和公式(5)，在实验中，在每次模拟运行中，从所有标签组中随机选择受攻击标签，分别就基于匿名集RFID系统隐私级别和基于信息泄漏的RFID系统隐私级别，对文献[4]和文献[10]及本文所设计的认证方案进行MATLAB仿真实验与计算，仿真结果如图2所示。图2(a)的仿真结果表明，该方案实现的隐私级别比文献[4]和文献[10]的协议均有所提高，经计算分别提高了51.5%和98.2%。当D变为512时，根据图2(b)所示的仿真结果，所提出的协议比文献[4]和文献[10]的方案泄露的信息均有降低，有计算得知分别减少了30.5%和50.6%。因此当标签被攻击时，所提出的方案在隐私级别和信息泄漏方面比其他协议有更优秀的表现。

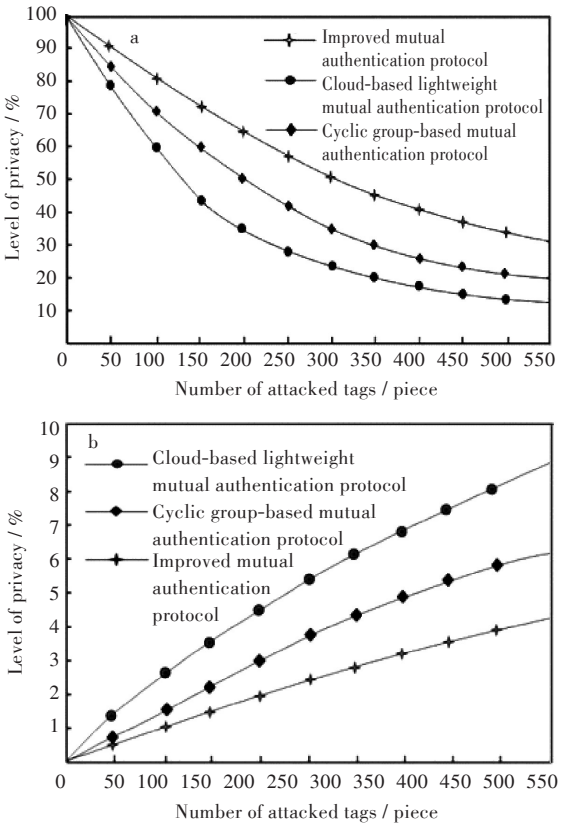

图2　RFID系统隐私级别：(a)基于匿名集，(b)基于信息泄漏

Fig. 2　Levels of privacy of RFID system：(a)based on anonymous set，(b)based on information leakage

5　结　语

本文在研究常见RFID系统认证协议的基础上，提出了一种基于循环组的RFID系统安全认证协议方案，并详细分析在RFID系统受到典型攻击的情形下，所提出的协议在信息隐私和安全方面的性能表现。该协议的最大特点是基于标签侧的取摸(Mod)和按位XOR运算，使用非常少的资源来存储数据和执行运算，协议的算法复杂度较小，执行效率较高。性能分析和仿真实验结果表明，当RFID系统部分标签受到攻击时，所提出的协议具有较高的隐私性能和安全级别，而且有着成本低优势。今后的研究重点是如何把所提出的协议应用在RFID实际系统中，为RFID的安全与应用提供更好的保障。

参考文献

[1]　王利恒，王祥力，陈荡，等. 无线射频识别装置的设计[J]. 武汉工程大学学报，2015，35(1)：65-70.

[2]　周世杰，张文清，罗嘉庆. 射频识别(RFID)隐私保护技术综述[J]. 软件学报，2015(4)：960-976.

[3] HERMAS J, PTEETERS R, PRENEEL B. Proper RFID privacy: model and protocols[J]. IEEE Transactions on Mobile Computing, 2014, 13(12): 2888-2902.
[4] 孙达志,朱泽光. 改进的RFID群组证明协议[J]. 计算机工程与设计,2017(8):2076-2080.
[5] SHI Z C, CHEN J W, CHEN S S, et al. A lightweight RFID authentication protocol with confidentiality and anonymity [C]//Procofthe 2nd IEEE Advanced Information Technology, Electronic andAutomation Control Conference. Piscataway, New Jersey: IEEE Press, 2017: 1631-1634.
[6] 张兴,李畅,韩冬,等. 基于Hash轻量级RFID安全认证协议[J]. 计算机工程与设计,2018(5):1269-1275.
[7] 李翠,石林. 基于射频识别的安全认证协议设计[J]. 计算机工程,2016(3):172-176.
[8] 简碧园,刘道微. 基于单向伪随机函数的移动RFID系统认证协议[J]. 电信科学, 2017(6):138-145.
[9] 李希元,孙超,郑薇. 基于伪随机函数的RFID双向认证协议[J]. 计算机工程与应用, 2018(17):67-70.
[10] RAHMA N F, HOQUE M E, AHAMED S I. Anonpri: a secure anonymous private authentication protocol for RFIDsystems[J]. Information Sciences, 2017(379): 195-210.
[11] 李璐璐,董庆宽,陈萌萌. 基于云的轻量级RFID群组标签认证协议[J]. 计算机科学,2019(1):182-189.
[12] 李立娟. 低成本RFID空中接口安全协议研究与设计[D].北京:北京邮电大学,2010.
[13] 张海鹏,程雨,何健,等. 一种安全高效的电子标签群组认证方案[J].电子科技,2018,31(3):65-69.
[14] JUELS A, WEIS S A. Defining strong privacy for RFID [J]. ACM Transactions Information and System Security, 2009, 13(1): 1-23.
[15] 博雅,刘年义,杨亚涛,等. 基于椭圆曲线密码的无线射频识别双向认证协议[J]. 计算机工程,2017,(1): 196-200.

本文编辑:陈小平

☆

(上接第503页)

参考文献

[1] 康同曦. 线性回归与逻辑回归的比较分析[J]. 福建质量管理, 2018(21):205.
[2] 郭文锋,樊超,郭新东. 基于二元逻辑回归模型的MOOC退课预测[J]. 计算机时代, 2017(12):50-53.
[3] 盛逸凡,李远耀,徐勇,等. 基于有效降雨强度和逻辑回归的降雨型滑坡预测模型[J]. 水文地质工程地质, 2019,46(01):156-162+172.
[4] 刘黎志,邓介一,吴云韬. 基于HBase的多分类逻辑回归算法研究[J]. 计算机应用研究, 2018,35(10): 3007-3010.
[5] 雷大江,杜萌,李智星,等. 稀疏多元逻辑回归问题优化算法研究[J]. 重庆邮电大学学报(自然科学版), 2019,31(3):354-366.
[6] 李权,曾涛,覃虎,等. 基于多元逻辑回归的兰坪县崩塌滑坡敏感性评价[J]. 测绘与空间地理信息, 2015, 38(12):36-39,43.
[7] 谭雪敏,吴远峰,袁正午,等. 拉格朗日多项式逻辑回归分类算法并行计算优化[J]. 遥感信息, 2016,31 (1):96-101.
[8] 吾雨森. 面向GPU集群领域的关键算法研究和实现[D]. 杭州:杭州电子科技大学, 2017.
[9] 李辉,王建文,叶明雯. 基于Hadoop的海量气象水文数据并发处理模型[J]. 计算机应用, 2018,38(增刊2):187-191.
[10] 马莹,赵辉,崔岩. 基于Hadoop平台的改进KNN分类算法并行化处理[J]. 长春工业大学学报, 2018, 39(5):484-489.
[11] 张海涛. 基于Hadoop的大数据计算之研究[J]. 电子测试, 2019(4):119-120.
[12] 冯祥,张媛媛. 基于Hadoop的MapReduce运行流程研究[J]. 福建电脑, 2018,34(12):118,173.
[13] 应毅,刘亚军. MapReduce并行计算技术发展综述[J]. 计算机系统应用, 2014(4):1-6,11.
[14] 杭州杨帆科技有限公司. 一种云计算环境下基于MapReduce的分布式并行文本聚类方法:中国, CN201710286671.2[P]. 2017-07-21.
[15] 李楠,于孟渤,贾珍珍,等. 基于改进MapReduce模型的BP神经网络并行化研究[J]. 通信技术,2018, 51(4):799-804.
[16] HILBE J M. 实用逻辑斯谛回归方法[M]. 程晓亮,杨艳秋,译. 北京:机械工业出版社,2019:13-49.

本文编辑:陈小平