# 基于交叉位运算的超轻量级RFID认证协议

杜宗印 章国安 袁红林
(南通大学电子信息学院 南通 226019)

**摘 要** 针对射频识别系统存在的安全隐患、标签成本较高等问题,提出了一种基于交叉位运算的超轻量级RFID认证协议(CURAP),并基于BAN逻辑形式化分析方法,证明了该协议的正确性与安全性。CURAP定义了交叉位运算,包含异或及左循环移位运算,且协议运行中,数据更新运算只在读写器中进行,而标签从传输消息中进行简单的异或运算提取即可。安全分析与性能评估表明,CURAP不但具有较强的双向认证性,能够抵抗多种攻击,而且可以有效降低标签的计算需求、存储空间,适用于低成本的RFID系统。

**关键词** 射频识别,认证协议,BAN逻辑,超轻量级,交叉
**中图法分类号** TP309 **文献标识码** A

## Crossover Based Ultra-lightweight RFID Authentication Protocol

DU Zong-yin ZHANG Guo-an YUAN Hong-lin
(School of Electronics and Information, Nantong University, Nantong 226019, China)

**Abstract** Aiming at the security hole of RFID system and tag's cost, we proposed a crossover based ultra-lightweight RFID authentication protocol(CURAP), and proved the correctness and security of this protocol with BAN logic formal analysis method. CURAP defines crossover operation involving bitwise XOR and left rotation. And data updating operation only is occurred in the reader, then the tag makes simple bitwise XOR extraction from transmission message. Security analysis and performance evaluation show that CURAP not only provides strong mutual authentication, resists various attacks, but also can lessen the computation requirement and storage space on tags, fit for low-cost RFID system.

**Keywords** RFID, Authentication protocol, BAN logic, Ultra-lightweight, Crossover

## 1 引言

RFID(Radio Frequency Identification,射频识别)是一种自动识别人或物的非接触式技术,具有工作距离长、适用恶劣环境、多目标同时识别等优点,在现实生活中有着广泛的应用。RFID系统包含后端数据库、读写器及标签3部分,基本模型如图1所示。其中标签一般直接附在物体上,受到计算能力、存储空间等问题的限制,并且标签与读写器之间通过无线不安全信道通信,面临着噪声、障碍物等多种安全隐患。因此,提高安全性、降低成本是RFID认证协议设计与应用的主要要求。

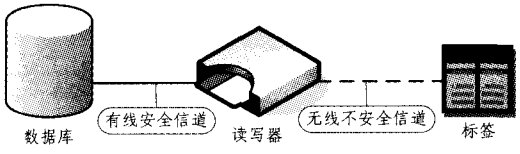



图1 RFID系统的基本模型

Peris-Lopez 2006年提出的认证协议LMAP[1]只包含异或(XOR)、按位与(AND)、按位或(OR)及模二加(+)运算,有效降低了标签的成本,引起了人们的关注。文献[2]将这些只包括简单位运算的认证协议称为超轻量级认证协议。但后来发现LMAP并不能抵抗主动及被动攻击[3];文献[4]对其进行了改进,提出只包含异或及模二加运算的LAMP+,它的计算需求更小,安全性也有所提高;而文献[5]对其进行分析发现它仍存在跟踪等攻击。

2007年,超轻量级认证协议SASI[2]因引入了左循环移位运算$Rot(X,Y)$——将$X$循环左移$wt(Y)$位,$wt(Y)$为$Y$的汉明重量,而提高了协议加密算法的复杂程度,增强了认证性和安全性。但文献[6]提出由于该协议频繁使用按位OR、AND运算,使输出结果具有极大的偏重性,从而导致标签的隐私性不强,且易受跟踪攻击。文献[7]在SASI协议的基础上引入了$MIXBIXS$函数,不再使用AND、OR运算,提出了Gossamer协议,但最终发现由于其初始状态读写器中只包含当前标签信息,而存在拒绝服务攻击[8]。

为了更好地提高RFID系统的安全性,降低RFID标签的成本,本文根据遗传算法的相关知识[9],首先定义了交叉位运算$Cro(X,Y)$,结合XOR、$Rot(X,Y)$运算提出了一种基于交叉位运算的超轻量级RFID认证协议(CURAP),并对该协议进行了BAN逻辑形式化证明及安全分析与性能评估。如图

到稿日期:2013-01-20 返修日期:2013-06-07 本文受国家自然科学基金项目(61071086),交通运输部科技项目(2012-319-813-270)资助。
杜宗印(1988—),男,硕士生,主要研究方向为安全认证协议,E-mail:duzongyin0720@163.com;章国安(1965—),男,博士,教授,主要研究方向为无线通信网络、认知无线Mesh网络,E-mail:gzhang@ntu.edu.cn(通信作者);袁红林(1971—)男,博士,副教授,主要研究方向为无线信号识别技术。

1 所示，RFID 系统中后端数据库与读写器之间为有线安全信道，本文以下叙述中将它们看成协议一方，统称为读写器 $R$，而标签为另一方 $T$。

## 2 所提协议 CURAP

### 2.1 交叉位运算

我们首先对交叉位运算进行定义：设 $X$、$Y$ 是两个具有 $L$ 位的二进制数组（$L$ 为偶数），$X=x_1x_2x_3\cdots x_L$，$Y=y_1y_2y_3\cdots y_L$，$x_i,y_i\in\{0,1\}$，$i=1,2,\cdots L$，那么交叉位运算 $Cro(X,Y)$ 是由 $X$ 的奇数位与 $Y$ 的偶数位相互交叉，而形成 $L$ 位新数组，即 $Cro(X,Y)=y_2x_1y_4x_3y_6x_5\cdots y_Lx_{L-1}$。该运算可在标签中有效实现：设指针 $p_X$、$p_Y$ 分别指向数组 $X$、$Y$，然后将其分别遍历 $X$、$Y$，当 $p_X$ 指向 $X$ 的奇数位时，则把此位上数字按顺序赋予第三个数组的偶数位，当 $p_Y$ 指向 $Y$ 的偶数位时，则把其位上数字按顺序赋予第三个数组的奇数位，所得第三个数组即为 $Cro(X,Y)$。

为了更好地说明该定义，我们这里取 $L=16$，设 $X=1010011100101100$，$Y=0110010110011101$，则 $Cro(X,Y)=1101101100111110$。$Cro(X,Y)$ 详细运算过程如图 2 所示。

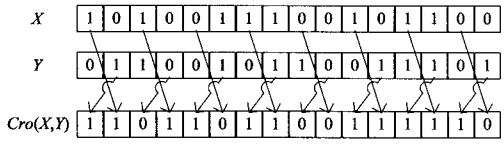



图 2 $Cro(X,Y)$运算过程

### 2.2 CURAP 通信流程

本文所提协议 CURAP 初始状态要求每个标签与读写器预先共享标签真实身份 $ID$、当前会话的认证密钥 $K_1$、$K_2$ 及标签的临时身份标识 $TID$，即 $\{ID, TID^{new}, K_1^{new}, K_2^{new}\}$，且读写器中需保留协议前一轮会话信息 $\{TID^{old}, K_1^{old}, K_2^{old}\}$、含有伪随机数发生器。下面给出协议中经常用到的符号：

$ID$：标签真实身份标识。

$TID$：标签临时身份标识（*temporary identity*）。

$K_i$：标签认证密钥，$i=1,2$。

$N_i$：随机数，$i=1,2$。

$A\sim G$：读写器与标签之间的交互信息。

$\oplus$：按位异或（XOR）运算。

$Rot(X,Y)$：左循环移位运算，将 $X$ 循环左移 $wt(Y)$ 位，$wt(Y)$ 为 $Y$ 的汉明重量。

$Cro(X,Y)$：交叉位运算，如图 2 所示。

CURAP 通信流程包含标签识别、双向认证、更新 3 个阶段，如图 3 所示。

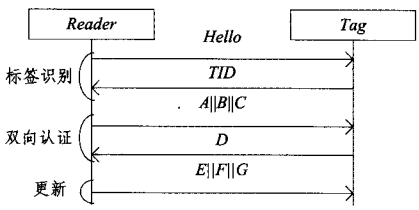



图 3 协议通信流程

标签识别阶段：读写器向标签发送请求信号“Hello”，初始化协议；标签收到请求信号后，返回 $TID$ 给读写器，读写器在后端数据库中搜索与之相同的 $TID$，若搜到，则检索出与之相匹配的密钥 $K_1$、$K_2$，进入双向认证阶段，否则读写器重新发送请求信号。

双向认证阶段：读写器搜到相同的 $TID$ 后，生成两个随机数 $N_1$、$N_2$，并利用相匹配的密钥 $K_i$ 计算 $A=Cro(K_1,K_2)\oplus N_1$、$B=Rot(K_1,K_2)\oplus N_2$、$C=Cro(N_2,K_1)\oplus Cro(Rot(N_1,N_2),K_2)$，并发送信息 $A\|B\|C$ 至标签；标签收到 $A\|B\|C$ 后，提取 $N_1$、$N_2$，$N_1=A\oplus Cro(K_1,K_2)$、$N_2=B\oplus Rot(K_1,K_2)$，并与自身存储的密钥 $K_1$、$K_2$ 共同计算 $C'=Cro(N_2,K_1)\oplus Cro(Rot(N_1,N_2),K_2)$，若 $C'$ 与 $C$ 不相等，则标签认证读写器失败，协议终止，若 $C'$ 与 $C$ 相等，则认证读写器成功，标签计算 $D=Rot(N_1,N_2)\oplus Cro(N_1\oplus N_2,K_1\oplus K_2)$，并将之返回给读写器。

读写器接收到信息 $D$ 后，利用自身存储的数据计算 $D'=Rot(N_1,N_2)\oplus Cro(N_1\oplus N_2,K_1\oplus K_2)$，并验证 $D'$ 是否等于 $D$，若两者相等，则读写器成功认证标签，双向认证完成，进入更新阶段，否则，认证标签失败，协议终止。

更新阶段：读写器与标签完成双向认证，即读写器验证 $D'=D$ 后，读写器内部更新标签假名及密钥，即：$TID^{new}=Cro(N_1,K_1\oplus K_2)\oplus Rot(N_2,N_1)$、$K_1^{new}=Cro(K_1,N_2)\oplus K_2$、$K_2^{new}=Cro(K_2,N_1\oplus N_2)$、$TID^{old}=TID$、$K_1^{old}=K_1$、$K_2^{old}=K_2$，然后，读写器利用更新后的数据及 $N_1$、$N_2$ 计算 $E=TID^{new}\oplus N_1\oplus N_2$、$F=K_1^{new}\oplus N_1$、$G=K_2^{new}\oplus N_2$，并发送 $E\|F\|G$ 至标签；标签收到 $E\|F\|G$ 后，提取 $TID^{new}=E\oplus N_1\oplus N_2$、$K_1^{new}=F\oplus N_1$、$K_2^{new}=G\oplus N_2$，并同时丢弃原来使用的数据。

## 3 协议的 BAN 逻辑形式化分析

BAN 逻辑是由 Burrows、Abadi 和 Needham 于 1989 年提出的基于信念的模态逻辑，其语法、推理法则及推理步骤在文献[10]中作了详细描述。BAN 逻辑对协议进行形式化分析，即根据协议的理想化模型及初始化假设，由逻辑的推理法则逐步推导出协议预期的安全目标。本协议的 BAN 逻辑形式化分析如下。

协议的理想化模型：

消息① $R\rightarrow T: Hello$

消息② $T\rightarrow R: TID$

消息③ $R\rightarrow T: \{A,B,C\}$，$A$、$B$、$C$ 是包含随机数 $N_i$ 并用密钥 $K_i$ 加密后的密文。

消息④ $T\rightarrow R: \{D\}$，$D$ 是包含随机数 $N_i$ 并用密钥 $K_i$ 加密后的密文。

消息⑤ $R\rightarrow T: \{E,F,G\}$

初始假设：

$P_1: R|\equiv R\overset{K_i}{\leftrightarrow}T$，$R$ 相信 $R$ 和 $T$ 的共享密钥 $K_i$。

$P_2: T|\equiv R\overset{K_i}{\leftrightarrow}T$，$T$ 相信 $R$ 和 $T$ 的共享密钥 $K_i$。

$P_3: R|\equiv R\overset{TID}{\rightleftharpoons}T$，$R$ 相信 $R$ 和 $T$ 的共享秘密信息 $TID$。

$P_4: T|\equiv R\overset{TID}{\rightleftharpoons}T$，$T$ 相信 $R$ 和 $T$ 的共享秘密信息 $TID$。

$P_5: R|\equiv \#(N_i)$，$R$ 相信随机数 $N_i$ 的新鲜性。

$P_6: T|\equiv \#(N_i)$，$T$ 相信随机数 $N_i$ 的新鲜性。

$P_7$：$T|\equiv R|\Rightarrow C$，$T$ 相信 $R$ 对 $C$ 的管辖权。

$P_8$：$R|\equiv T|\Rightarrow D$，$R$ 相信 $T$ 对 $D$ 的管辖权。

安全目标：

$G_1$：$R|\equiv D$，$R$ 相信 $D$。

$G_2$：$T|\equiv C$，$T$ 相信 $C$。

分析推理：

由消息④得 $R\triangleleft\{D\}$（$R$ 曾接收到消息 $D$）及初始假设 $P_1$ 及消息含义法则 $\frac{P|\equiv P\overset{K}{\leftrightarrow}Q,P\triangleleft\{X\}_K}{P|\equiv Q|\sim X}$（若主体 $P$ 相信主体 $P$ 和 $Q$ 的共享密钥 $K$，且 $P$ 曾接收到用 $K$ 加密的密文 $X$，则 $P$ 相信主体 $Q$ 发送过消息 $X$），得 $R|\equiv T|\sim D$。

由初始假设 $P_5$ 及消息新鲜性法则 $\frac{P|\equiv\#(X)}{P|\equiv\#(X,Y)}$（如果一个消息一部分是新鲜的，则整个消息也是新鲜的），得 $R|\equiv\#(D)$。

由已推导出的 $R|\equiv T|\sim D$、$R|\equiv\#(D)$ 及随机数验证法则 $\frac{P|\equiv\#(X),P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$ 得 $R|\equiv T|\equiv D$。

由 $R|\equiv T|\equiv D$、初始假设 $P_8$ 及管辖法则 $\frac{P|\equiv Q|\Rightarrow X,P|\equiv Q|\equiv X}{P|\equiv X}$ 可得 $R|\equiv D$。

同理，由消息③、初始假设 $P_2$ 及消息含义法则 $\frac{P|\equiv P\overset{K}{\leftrightarrow}Q,P\triangleleft\{X\}_K}{P|\equiv Q|\sim X}$、接收法则 $\frac{P\triangleleft(X,Y)}{P\triangleleft X}$ 得 $T|\equiv R|\sim C$。由初始假设 $P_6$ 及消息新鲜性法则 $\frac{P|\equiv\#(X)}{P|\equiv\#(X,Y)}$ 得 $T|\equiv\#(C)$。再由随机数验证法则 $\frac{P|\equiv\#(X),P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$ 得 $T|\equiv R|\equiv C$。最后由初始假设 $P_7$ 及管辖法则 $\frac{P|\equiv Q|\Rightarrow X,P|\equiv Q|\equiv X}{P|\equiv X}$ 可得 $T|\equiv C$。

## 4 安全分析与性能评估

### 4.1 安全分析

(1)双向认证。本协议能够安全实现读写器与标签身份的双向认证，是因为协议运行中读写器与标签各自产生了认证信息 $C$ 和 $D$，且只有合法的读写器与标签才能用正确的密钥 $K_i$ 和随机数 $N_i$ 计算出一致的认证数据 $C'$ 和 $D'$。

(2)数据完整性。读写器在双向认证阶段产生的传输消息 $C$ 也能够保证数据的完整性，如果攻击者试图通过改变消息 $A$、$B$ 来模仿随机数 $N_1$、$N_2$，则计算 $C$ 并传给标签时，标签能够识别此时 $C$ 是无效的，因为 $C=Cro(N_2,K_1)\oplus Cro(Rot(N_1,N_2),K_2)$，攻击者若对 $N_1$、$N_2$ 的猜测产生丝毫的错误，都很有可能导致计算出不一致的 $C$。

(3)标签匿名性和不可跟踪性。协议整个运行过程中使用的是标签的临时身份 $TID$，而不像文献[4]使用了标签真正 $ID$，攻击者不可能从截获的传输信息中提取出标签身份，故该协议具有标签匿名性；同时，攻击者截取标签传输消息 $TID$、$D$，对其进行位置跟踪。由于协议运行结束时，标签都会更新 $TID$ 与密钥 $K_i$，而且每次会话中都会产生新的随机数 $N_i$，$D$ 随之改变，故攻击者对它们跟踪是毫无意义的，因此该协议同时具有不可跟踪性。

(4)抵抗假冒攻击。攻击者可能假冒标签（读写器）截获认证信息 $C(D)$，假装成功认证读写器（标签），但由于协议会话每次都会产生新的随机数 $N_i$ 及更新共享密钥 $K_i$，故攻击者不能计算出一致的消息 $D(C)$，使其本身被读写器（标签）成功认证。

(5)抵抗重传攻击。该协议运行结束时，合法读写器与标签的共享密钥 $K_i$ 及共享秘密 $TID$ 都会进行更新，并且每次会话使用的随机数 $N_i$ 都不同，即使攻击者截取前一次交互信息 $C$、$D$，在以后会话中进行重放，也不会通过认证。

(6)抵抗拒绝服务攻击。协议运行更新阶段时，读写器内有两组信息 $\{TID^{new},K_1^{new},K_2^{new}\}$ 及 $\{TID^{old},K_1^{old},K_2^{old}\}$，而当读写器发送至标签的 $E\|F\|G$ 被攻击者截获时，标签内数据更新失败，即标签内此时存储 $\{TID^{old},K_1^{old},K_2^{old}\}$。读写器再次向标签发送请求信号，合法标签返回 $TID^{old}$，而读写器仍能在后端数据库中搜索到相同的数据，协议同样能够正常运行。故该协议能够抵抗 Gossamer 协议所存在的拒绝服务攻击。

(7)抵抗暴露攻击。该协议运行时，所有密文均不会暴露给攻击者。协议运行中，攻击者可能通过某种手段获得 $Cro(K_1,K_2)$，进而可以提取出 $K_1/K_2$ 的奇位/偶位，但并不能得到完整的 $K_1/K_2$；攻击者还可能试图通过截获消息 $E\|F\|G$ 提取相应更新后的密文信息，但 $E\|F\|G$ 的计算都有随机数 $N_i$ 的参与，使攻击者不能成功破解。

### 4.2 性能评估

我们主要从标签的计算需求、存储空间和通信量 3 方面对本协议进行性能评估。

计算需求：该协议只包含 3 种简单位运算，它们都可以在标签中有效地实现；并且该协议更新阶段中，数据更新运算只在读写器中进行，标签只按位异或做了简单的提取运算，使标签内的计算量得到了有效降低。

存储空间：该协议运行时，标签只包含了其真实 $ID$ 及当前协议会话信息 $\{TID^{new}、K_1^{new}、K_2^{new}\}$，若协议运行中各信息长度设为 $L=128$ 位，标签所需存储空间共为 $4L=512$ 位。

通信量：该协议运行中共传输了请求信息“Hello”及读写器与标签的交互信息 $A-G$，而标签的传输消息只有 $TID$ 和认证消息 $D$，若同样设各传输消息长度为 $L=128$ 位，标签的总通信量为 $2L=256$ 位。

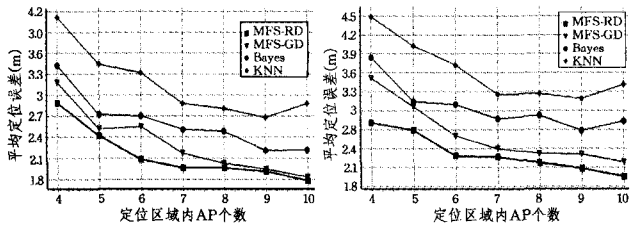
为进一步地说明本文提出协议 CURAP 的性能，将它与其它几种超轻量级认证协议进行了对比，如表 1 所列。

表 1 超轻量级 RFID 认证协议性能比较

| 协议 | 计算需求 | 存储空间 | 通信量 |
|---|---|---|---|
| LMAP | ∧∨⊕+ | 768 | 256 |
| SASI | ∧∨⊕+Rot | 896 | 256 |
| Gorssamer | ⊕+RotMixBits | 896 | 256 |
| CURAP | ⊕ RotCro | 512 | 256 |

**结束语** 本文针对 RFID 系统现阶段存在的安全和成本问题，提出了一种超轻量级安全认证协议 CURAP，并用 BAN 逻辑形式化证明了其可行性。该协议包含异或、左循环移位及交叉 3 种位运算，且与其他协议不同的是，该协议更新阶段，只有读写器进行数据更新运算，标签内部只做简单的异或提取运算。安全分析表明，该协议具有较强的双向认证及数据完整性，可以抵抗假冒、重传、拒绝服务及暴露等多种攻击；性能评估表明，该协议较以往协议成本更低，可有效降低标签的计算需求、存储空间及通信量。

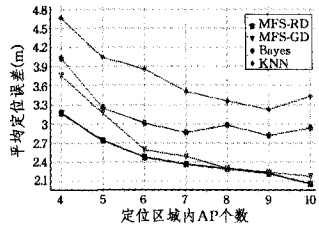
（下转第 42 页）



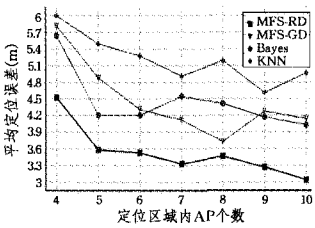

(a) d=2m



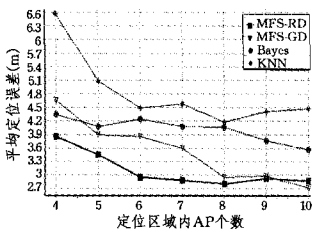

(b) d1=4m,d2=2m




(c)d1=4m,d2=4m




(d)d=4m




(e)d=6m

图 5　各个算法在不同参考点间距条件下，平均定位误差随着 AP 个数的变化情况

**结束语**　本文针对室内 RSS 信号的时变随机特性降低定位精度的问题，将重叠度引入到指纹相似度的判别计算中，并根据各 AP 在匹配定位中的不同作用，对各个 AP 赋予不同权值，提出了一种新的基于分布重叠和特征加权的定位算法。该算法采用瑞利分布重叠计算指纹特征相似度，运算简单，较好地反映了无线信号的相似度；特征权重的引入，突出了离 AP 较近的 AP 在匹配定位中的作用。在典型室内办公环境中进行了定位实验，验证了 MFS 算法采用瑞利分布和特征加权的有效性；和传统 KNN 和 Bayes 定位算法性能对比，MFS 算法定位精度更高，具有较高的实用性。

## 参 考 文 献


[1] Bahl P, Padmanabhan V N. RADAR: an in-building RF-based location and tracking system[C]// Proc. IEEE INFOCOM. Tel-Aviv, Israel. 2000: 775-784

[2] Kushki A, Plataniotis K N, Venetsanopoulos A N. Kernel-based positioning in wireless local area networks[J]. IEEE Transactions on Mobile Computing, 2007, 6(6): 689-705

[3] 徐玉滨，邓志安，马琳. 基于核直接判别和支持向量回归的 WLAN 室内定位算法[J]. 电子与信息学报，2011，33(4)：896-901

[4] 徐凤燕，李楝宾，王宗欣. 一种新的基于区域划分的距离-损耗模型室内 WLAN 定位系统[J]. 电子与信息学报，2008，30(6)：1405-1408

[5] Luca D, Mazzenga F, Monti, et al. Performance evaluation of indoor localization techniques based on RF power measurements from active or passive devices[J]. EURASIP Journal on Applied Signal Processing, 2006(1): 1-11

[6] Youssef M, Agrawala A. The horus location determination system [J]. Wireless Networks, 2008, 14(3): 357-374

[7] 赵方，罗海勇，马严，等. 基于公共信标集的高精度射频指纹定位算法[J]. 计算机研究与发展，2012，49(2)：243-252

[8] Robin W O, Albert K. Indoor location estimation with reduced calibration exploiting unlabeled data via hybrid generative/discriminative learning[J]. IEEE Transactions on Mobile Computing, 2012, 11(11): 1613-1625

[9] Winter S. Location-based similarity measures of regions[OL]. http://www. ifp. uni-stuttgart. de/publications/commIV/winter. pdf

[10] 赵宝贵，李大军. 基于重叠度和匹配距离的面实体匹配方法[C]// 华东六省一市测绘学会第十次学术交流会. 南昌，2007：9-12

[11] 刘婧，孙正兴. 面向视觉交互的室内肤色建模研究[J]. 计算机科学，2008，35(1)：236-239

[12] 杨大成. 移动传播环境[M]. 北京：机械工业出版社，2003：113-115


(上接第 37 页)

## 参 考 文 献


[1] Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M, et al. LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags[C]// Graz, Austria. Proceedings of the 2nd Workshop on RFID Security. New Jersey, USA: IEEE Press, 2006: 137-148

[2] Chien H Y. SASI: A New Ultra-lightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity[J]. IEEE Trans. Dependable and Secure Computing!, 2007, 4(4): 337-340

[3] 吕文纳，王根英，刘云. 基于低成本的 RFID 轻量级安全认证协议的研究[J]. 铁道通信信号，2010，46(12)：32-35

[4] Li Tie-yan. Employing Lightweight Primitives on Low-cost RFID Tags for Authentication [C] // Calgary, BC. Vehicular Technology Conference. 2008: 1-5

[5] Bagheri N, Safkhani M, Naderi M, et al. Security Analysis of LMAP++, an RFID Authentication Protocol[C]// Abu Dhabi. 6th International Conference on Internet Technology and Secured Transactions. 2011: 689-694

[6] Phan R C W. Cryptanalysis of a New Ultralightweight RFID Authentication Protocol—SASI [J]. IEEE Trans on Dependable and Secure Computing, 2009, 6(4): 316-320

[7] Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M, et al. Advances in Ultra-Lightweight Cryptography for Low-cost RFID Tags: Gossamer Protocol[C] // 9th International Workshop on WISA'08. Jeju Island, Korea, Berlin: Springer Berlin Heidelberg, 2009: 56-68

[8] 彭朋，赵一鸣，韩伟力，等. 一种超轻量级 RFID 双向认证协议[J]. 计算机工程，2011，37(16)：140-142

[9] 彭勇，林浒，卜霄菲. 变焦佳点集遗传算法[J]. 计算机科学，2010，37(11)：194-198

[10] 金丽萍，顾翔，纪丽娜. BAN 逻辑及其在认证协议性质分析中的应用研究[J]. 电脑知识与技术，2008，2(12)：500-502