一种新的超轻量级RFID认证协议

张亚力 郭亚军 崔建群 曾庆江
(华中师范大学计算机学院 武汉 430079)

摘 要 RFID(无线射频识别)技术以无线通信的方式广泛运用于生活生产的各个领域,如门禁设备、支付设备等,但阅读器和标签之间无线开放的通信环境使得RFID设备面临更多的恶意攻击和安全威胁。低成本标签只具有非常有限的计算能力和存储空间,一般的分组密码和hash函数等都不能用于低成本标签中。为了解决低成本标签的安全性问题,采用比特位运算密码原语,提出一种新的超轻量级RFID认证协议——SIUAP。SIUAP协议在SIMON类算法的超轻量级轮函数$F(x)$和非线性函数MIXBITS运算的基础上,使用3种简单的比特位运算:比特AND运算、异或运算和循环移位运算,大大降低了计算复杂度。通过GNY逻辑对协议进行形式化的分析,证明了SIUAP协议能够实现阅读器和标签双向合法身份的认证,同时对SIUAP进行安全性分析。与现有的超轻量级认证协议相比,SIUAP协议具有较小的计算开销,能够满足RFID系统低成本、高安全性的需求。

关键词 无线射频识别,超轻量级,双向认证
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.01.035

New Ultra-lightweight RFID Authentication Protocol

ZHANG Ya-li GUO Ya-jun CUI Jian-qun ZENG Qing-jang
(School of Computer, Central China Normal University, Wuhan 430079, China)

Abstract RFID (Radio Frequency Identification) technology is widely applied in many fields of life and production, such as access control equipment, payment equipment and others in wireless communication way. However, the wireless communication environment between the reader and the tag makes the RFID device face more malicious attacks and security threats. Because the low-cost tag only has very limited computing power and storage space, the common block cipher and hash function cannot be used for low cost tag. To solve the security problem of the low cost tag, this paper proposed a new ultra-lightweight RFID authentication protocol—SIUAP by using the bit operation code. Based on the lightweight wheel function $F(x)$ and nonlinear function MIXBITS operations, which belong to SIMON algorithm, SIUAP protocol adopts three simple bit operations: Bits AND operation, XOR and cyclic shift operations, which greatly reduces the computational complexity. Through formally analyzing the protocol by GNY logic, it has been proved that the SIUAP protocol can realize the authentication of the reader and tag. Meanwhile, a security analysis of the SIUAP was also given. Compared with the existing ultra-lightweight authentication protocol, the SIUAP protocol has lower computational cost, which can meet the requirements of the RFID system of low cost and high security.

Keywords Radio frequency identification, Ultra-lightweight, Mutual authentication

1 引言

射频识别(Radio Frequency Identification, RFID)是一种非接触式自动识别的无线通信技术[1],其通过射频信号自动识别目标对象并获取相关数据。由于RFID的设备具有防水、防磁电;耐高温、寿命年限长、读写距离长、数据存储容量大、便于数据的加密等优点,被广泛运用于各种领域,如物品标识、电子票证、商品防伪、身份识别等。尽管RFID系统在实际生活中得到了广泛的应用,但是RFID的阅读器和标签之间的开放的无线通信环境使其面临严重的恶意攻击和安全隐患。攻击者可以实施监听、追踪攻击等来非法攻击RFID系统以获取标签的信息[2]。因此如何有效地对标签进行认证,如何有效地防止非法的阅读器对标签的访问成为了RFID系统安全的关键。由于低成本标签的计算能力弱和存储空间较小,一般的分组密码和hash函数等不能应用于低成本标签中,因此如何制定出低成本、高效、安全的RFID安全认证协议仍是一个亟待解决的问题。

目前国内外学者已经提出不少RFID系统的认证协议和方案[3-5],但都存在一些安全问题。Chien等人根据标签计算能力、电源消耗、存储代价、标签价格和标签所支持的运算将这些协议划分为:重量级认证协议、简单认证协议、轻量级认证协议、超轻量级认证协议[6]。它们的计算复杂性要求越来越低,超轻量级认证协议仅需要基本的比特位运算(与、或、非、异或、移位等)的支持,因此受到更多的青睐,其中最为

到稿日期:2015-11-08 返修日期:2016-05-20 本文受国家自然科学基金(61370108),中央高校基本科研业务费项目(CCNU2015GF0004)资助。
张亚力(1990—),女,硕士生,主要研究领域为信息安全,E-mail:zhangyaliit@163.com;郭亚军(1965—),男,博士,教授,主要研究领域为信息安全、物联网等,E-mail:yj.guo@mail.ccnu.edu.cn(通信作者)。

典型的是 2006 年 Peris 等人首次提出的一系列超轻量级 RFID 认证协议 LAMP[7]，EMAP[8] 和 M2AP[9]，后来被称为 UMAP[10] 协议族，该协议族中标签进行简单的模 2^m 加(mod 2^m(+))、⊕(XOR)、∧(AND)和∨(OR)等简单的算术运算或比特位逻辑运算，但该协议族被指出不能抵抗非同步攻击。2007 年，Chien 等人提出一个典型的超轻量级认证协议 SASI[6]，该协议中标签进行左循环移位(Rot(x,y))、模 2^m 加(mod 2^m(+))、⊕(XOR)、∧(AND)、∨(OR)运算，但 SASI 协议并没有达到预期的目标。2011 年，Arco 等人指出 SASI 协议在完全揭露攻击下攻击者可以获取所有的秘密数据[12]。2008 年，针对 SASI 协议的缺陷，Peris 等人提出了 Gossamer 协议[10]，Gossamer 引进了一个轻量级的非线性函数 MIXBITS，并利用 MIXBITS 函数产生了一个新的随机数来混淆消息的关联。2011 年，Peng 等人证明了 Gossamer 协议也是不安全的[13]。

为了解决现有超轻量级 RFID 认证协议的安全问题，本文提出一种新的超轻量级 RFID 认证协议——SIUAP 协议，SIUAP 协议结合了轻量级轮函数 $F(x)$[17] 和非线性函数 MIXBITS 运算[10]，只涉及 3 种简单的比特位运算：比特 AND 运算、异或运算和循环移位运算。该协议在保证数据隐私性的同时也能够有效地抵制跟踪攻击，满足了低成本标签的要求，提高了执行的效率，同时增加了安全性。

2 SIUAP 协议

2.1 符号说明

为了简化描述，SIUAP 协议的相关符号和操作说明如表 1 所列。

表 1 符号说明

符号	说明
R	阅读器
T	标签
ID	标签唯一的真实的标识符
PID	阅读器和标签共享的标签的匿名
K	标签密钥
?	或运算
·	与运算
⊕	异或运算
<<<	循环左移位
+	模加

2.2 SIUAP 协议描述

鉴于上述安全隐私保护方法存在的缺陷，提出了 SIUAP 协议。SIUAP 协议结合了轮函数 $F(x)$ 和非线性 MIXBITS 函数。轮函数 $F(x)$ 是在美国国家安全局于 2013 年提出的轻量级分组密码算法 SIMON 类算法[17] 中出现的，轮函数 $F(x)$ 采用按位与运算、循环移位运算和异或运算，$F(x)=(x<<<8)\cdot(x<<<1)\oplus(x<<<2)$；轻量级的非线性函数 MIXBITS 首先是由 Gossamer[10] 引进的，它采用了右位移操作(≫)，MIXBITS(x,y)执行的操作如：$Z=x$；for($i=0$；$i<32$；$i++$)$Z=(Z>>1)+Z+Z+y$。将轻量级轮函数 $F(X)$ 和轻量级非线性 MIXBITS 函数相结合可以达到标签和阅读器的双重认证和动态刷新密钥机制的目的，从而实现防止跟踪、机密性等安全需求，其中轮函数 $F(x)$ 和非线性函数 MIXBITS 具有循环移位运算，在一定程度上可以共用电路。总体来说，SIUAP 协议只用到了按位与运算、循环移位运算和异或运算，具有低成本、计算复杂度低等特点。通常认为阅读器和后台服务器是通信安全的，在这里为了便于表示，把阅读器和后台服务器看成阅读器整体。协议的初始状态中，每一个标签都有一个唯一真实的标识符 ID、与阅读器共享的匿名 PID 及密钥 K，在阅读器中设置时间戳 Δt_{max}，时间戳 Δt_{max} 以代数循环的伪随机数代替传统时间戳，可有效降低时钟开销，并由阅读器维护。SIUAP 协议包括 3 个过程：标签识别、双向认证、数据更新。与其它协议不同的是，SIUAP 协议引用了轻量级函数轮函数 $F(x)$，协议的具体过程如下。

(1)标签识别。阅读器通过伪随机数发生器 PRNG 生成两个随机数 r_1，r_2，其中随机数 $g:\{0,1\}^k\rightarrow\{0,1\}^{2k}$，并利用 MIXBITS 函数 $n_1=$MIXBITS(r_1,r_2)将 n_1 和 Hello 发送给阅读器作为质询挑战，此时可能会发生 3 种情况：1)没有标签响应；2)一个标签响应；3)多个标签同时响应。当发生多标签冲突时，会执行一次冲突仲裁(collision arbitration)过程，如二进制搜索算法[18]。这一过程完毕后会从中选取出一个标签与读写器进行信息交互，被选取的标签通过伪随机数发生器 PRNG 生成随机数 r_3，并且利用 MIXBITS 函数得到 $A=$MIXBITS(PID,r_3)，标签将消息 A 发送给阅读器作为应答。

(2)双向认证。阅读器后端数据库收到标签应答消息 A 后，抽取出标签的随机数 r_3 和 PID，搜索自己缓存中的每一个 PID 和密钥 K，其中 $PID=PID^{old}$ 或 $PID=PID^{new}$，$K=K^{old}$ 或者 $K=K^{new}$，计算消息 $B=(PID<<<8)\cdot(r_3<<<1)\oplus(K<<<2)$，阅读器将消息 B 传给标签，标签收到 B 后，计算 $B^*=(PID<<<8)\cdot(r_3<<<1)\oplus(K<<<2)$，若有 $B=B^*$，则阅读器认证通过，阅读器是合法阅读器。标签利用轮函数计算 C，$C=(n_1<<<8)\cdot(r_3<<<1)\oplus(PID<<<2)$，标签将消息 C 发送给阅读器，若有 $C^*=C$，$\Delta t_i\leqslant\Delta t_{max}$，则标签认证成功，认为该标签是合法的；若 $A\neq A^*$ 或 $\Delta t_i>\Delta t_{max}$，则标签认证不通过，过滤此标签。若标签认证成功，则阅读器立即更新。

(3)数据更新。Tag 认证成功后，阅读器立即进行更新操作，更新 $PID^{old}=PID$，$PID^{new}=(PID<<<8)\cdot(ID<<<1)\oplus(n_1<<<2)$，$K^{old}=K$，$K^{new}=(r_1<<<8)\cdot(r_2<<<2)\oplus(r_3<<<2)$，计算 $D=(n_1<<<8)\cdot(r_2<<<1)\oplus(r_3<<<2)$，将消息 D 发送给标签，标签计算 $D^*=(n_1<<<8)\cdot(r_2<<<1)\oplus(r_3<<<2)$，若 $D^*=D$，Tag 进行更新，$K^{new}=(r_1<<<8)\cdot(r_2<<<2)\oplus(r_3<<<2)$，$PID^{new}=(PID<<<8)\cdot(ID<<<1)\oplus(r_3<<<2)$。$K=K^{new}$，$PID=PID^{new}$。SIUAP 协议过程如图 1 所示。

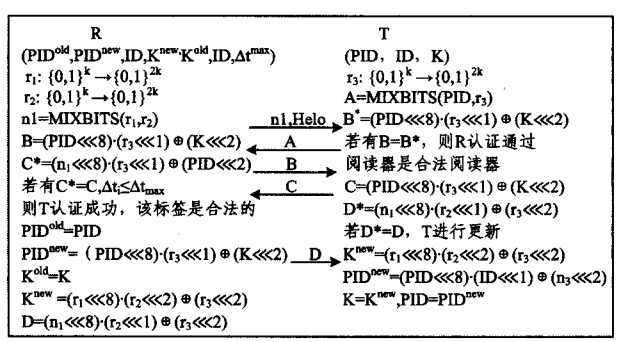

图 1 SIUAP 协议的双向认证

2.3 SIUAP 协议的 GNY 逻辑分析

到目前为止，已经有很多的 RFID 安全协议被提出，但是

大都缺乏严格的形式化分析和证明。1989 年，Burrows 等人提出的 BAN 形式逻辑分析方法[19]是分析安全协议的一个里程碑，BAN 逻辑只关注协议中与认证逻辑直接相关的部分，利用严格的数学推理规则对协议的认证部分进行形式化的分析和证明，从协议的初始化假设阶段推导出协议的目标认证阶段，揭示了一些非形式化方法很难发现的漏洞。例如形式化分析方法发现了 KerBerm 协议和 NS 协议的一些漏洞，而以前其他方法并没有发现这些漏洞[20]。1990 年，宫力等人提出的 GNY 形式逻辑分析方法[20]是对 BAN 进行增强扩充的逻辑推理分析方法，GNY 形式逻辑分析方法比 BAN 逻辑更加全面，扩大了能够分析的协议种类和范围。本文采用 GNY 形式逻辑分析方法对 SIUAP 协议的相互认证进行形式化分析和证明。

(1)协议形式化描述

假设 R 代表读写器，T 表示标签，基于轮函数的超轻量级 RFID 双向认证协议流程如下：

Msg1：$R\rightarrow T$：MIXBITS(r_1，r_2)

Msg2：$T\rightarrow R$：MIXBITS(PID，r_3)

Msg3：$R\rightarrow T$：$(PID<<<8)\cdot(r_3<<<1)\oplus(k<<<2)$

Msg4：$T\rightarrow R$：$(n_1<<<8)\cdot(r_3<<<1)\oplus(PID<<<2)$

Msg5：$R\rightarrow T$：$(n_1<<<8)\cdot(r_2<<<1)\oplus(r_3<<<2)$

用逻辑语言规范以上协议，如下描述：

Msg1：$T<^{*}$ MIXBITS(r_1，r_2)

Msg2：$R<^{*}$ MIXBITS(PID，r_3)

Msg3：$T<^{*}(PID<<<8)\cdot(r_3<<<1)\oplus(k<<<2)$

Msg4：$R<^{*}(n_1<<<8)\cdot(r_3<<<1)\oplus(PID<<<2)$

Msg5：$R<^{*}(n_1<<<8)\cdot(r_2<<<1)\oplus(r_3<<<2)$

(2)协议初始化假设和证明目标

初始化假设如图 2 所示，在本协议中，使用 R 和 T 表示主体，即阅读器、标签。假设①－⑤表示标签、阅读器的拥有；⑥表示阅读器和标签对随机数新鲜性的信任；⑦－⑩表示阅读器和标签对 PID，ID 和 K 是彼此共享的。

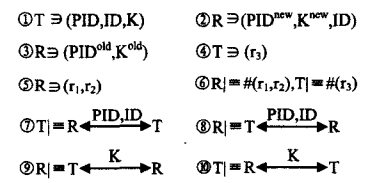

图 2　初始化假设

SIUAP 协议的证明目标主要有两个，即标签和阅读器对彼此交互信息新鲜性的信任。目标的证明公式如下：

$T|\equiv R|\sim\#((PID<<<8)\cdot(r_3<<<1)\oplus(K<<<2))$

$R|\equiv T|\sim\#((n_1<<<8)\cdot(r_3<<<1)\oplus(PID<<<2))$

(3)协议的证明

SIUAP 协议的证明是在初始化假设的基础上进行的，证明过程遵循文献[20]中的逻辑推理规则、告知规则、新鲜规则、拥有规则，消息解释规则遵循了文献[20]中 GNY 逻辑推理规则的书写形式，分别用 T，P，F 和 I 表示。

1)证明 $T|\equiv R|\sim\#\{(PID<<<8)\cdot(r_3<<<1)\oplus(K<<<2)\}$

∵规则 P1：$\dfrac{P<X}{P\ni X}$ 和 Msg3：$T^{*}<\{(PID<<<8)\cdot(r_3<<<1)\oplus(K<<<2)\}$

∴$T\ni\{(PID<<<8)\cdot(r_3<<<1)\oplus(K<<<2)\}$

∵规则 F1：$\dfrac{P|\equiv(X)}{P|\equiv(x,y),P|\equiv\#F((X))}$ 以及假设④$T|\equiv\#(r3)$

∴$T=\#\{(PID)\cdot(r_3)\oplus(K)\}$

∵规则 P2：$\dfrac{P\ni X,P\ni Y}{P\ni(X,Y),P\ni F(X,Y)}$，假设①$T\ni(PID,ID,K)$和假设④$T\ni(r3)$

∴$T\ni\{(PID)\cdot(r3)\oplus(k)\}$

规则 F10：$\dfrac{P|\equiv(X),P\ni X}{P|\equiv\#(H(X))}$ 和 $T=\#\{(PID)\cdot(r_3)\oplus(K)\}$及 $T\ni\{(PID)\cdot(r3)\oplus(k)\}$

∴$T|\equiv\#\{(PID<<<8)\cdot(r_3<<<1)\oplus(K<<<2)\}$

∵规则 I_3：

$$\frac{P\langle H(X,\langle S\rangle),P\ni(X,S),P|\equiv P\leftrightarrow Q,P|\equiv\#(X,S)}{P|\equiv Q|\sim(X,S),P|\equiv Q\sim H(X,\langle S\rangle)}$$

又∵假设⑦$T|\equiv R\overset{PID,ID}{\leftrightarrow}T$ 和⑨$R|\equiv T\overset{K}{\leftrightarrow}R$，Msg3 $T^{*}<\{(PID<<<8)\cdot(r_3<<<1)\oplus(K<<<2)\}$

∴$T|=R\sim\{(PID<<<8)\cdot(r_3<<<1)\oplus(K<<<2)\}$

∵新鲜性定义和 $T=\#\{(PID<<<8)\cdot(r_3<<<1)\oplus(K<<<2)\}$及 $T|=R\sim\{(PID<<<8)\cdot(r_3<<<1)\oplus(K<<<2)\}$

∴$T|\equiv R|\sim\#\{(PID<<<8)\cdot(r_3<<<1)\oplus(K<<<2)\}$

2)证明 $R|\equiv T|\sim\#\{(n_1<<<8)\cdot(r_3<<<1)\oplus(PID<<<2)\}$

完成阅读器对标签的证明。

∵规则 P1：$\dfrac{P<X}{P\ni X}$ 和 Msg4：$R<^{*}\{(n_1<<<8)\cdot(r_3<<<1)\oplus(PID<<<2)\}$

∴$R\ni\{(n_1<<<8)\cdot(r_3<<<1)\oplus(PID<<<2)\}$

∵规则 F1：$\dfrac{P|\equiv\#(X)}{P|\equiv(X,Y),P|\equiv\#(F(X))}$ 和假设⑥$R|\equiv\#(r_1,r_2)$

∴$R|\equiv\#(n_1,r_3,PID)$

∵规则 P1：$\dfrac{P<X}{P\ni X}$ 和 Msg2：$R<^{*}$ MIXBITS(PID，r_3)

∴$R\ni$MIXBITS(PID，r_3)

∵规则 P5：$\dfrac{P\ni F(x,y),P\ni X}{P\ni Y}$，假设②$R\ni(PID^{new},K^{new},ID)$ 和假设③$R\ni(PID^{old},K^{old})$

∴$R\ni r_3$

∵规则 P2：$\dfrac{P\ni X,P\ni Y}{P\ni(X,Y),P\ni F(X,Y)}$ 和假设⑤$R\ni(r_1,r_2)$

∴$R\ni n_1$

∵规则 P2：$\dfrac{P\ni X,P\ni Y}{P\ni(X,Y),P\ni F(X,Y)}$，$R\ni r_3$，$R\ni n_1$ 和假设②$R\ni(PID^{new},K^{new},ID)$及假设③$R\ni(PID^{old},K^{old})$

∴$R\ni\{(n_1)\cdot(r_3)\oplus(PID)\}$

∵规则 F10：$\frac{P|\equiv\#(X),P\ni X}{P|\equiv\#(H(X))},R|\equiv\#(n_1,r_3,PID)$及 $R\ni\{(n_1)\cdot(r_3)\oplus(PID)\}$

∴$R|\equiv\#\{(n_1<<<8)\cdot(r_3<<<1)\oplus(PID<<<2)\}$

∵规则 I3：

$$\frac{P<^{*}H(X,\langle S\rangle),P\ni(X,S),P|\equiv P\leftrightarrow Q,P|\equiv\#(X,S)}{P|\equiv Q|\sim(X,\langle S\rangle),P|\equiv Q|\sim H(X,\langle S\rangle)}$$

又∵假设⑧$R|\equiv T\xleftrightarrow{PID,ID}R$及假设⑩$R$，Msg4：$R<^{*}(n_1<<<8)\cdot(r_3<<<1)\oplus(PID<<<2)$

∴$R|\equiv T|\sim\{(n_1<<<8)\cdot(r_3<<<1)\oplus(PID<<<2)\}$

∵$R|\equiv\#\{(n_1<<<8)\cdot(r_3<<<1)\oplus(PID<<<2)\}$和 $R|\equiv T|\sim\{(n_1<<<8)\cdot(r_3<<<1)\oplus(PID<<<2)\}$

∴$R|\equiv T|\sim\#\{(n_1<<<8)\cdot(r_3<<<1)\oplus(PID<<<2)\}$

通过对本文提出的 SIUAP 协议进行 GNY 逻辑形式化分析，可以在基本假设的基础上推导出预定的设计目标。因此 GNY 推理结果证明了本文提出的 SIUAP 协议的相互认证，能够有效地实现读写器和标签双向合法身份的认证。

3 SIUAP 协议安全性和性能分析

3.1 SIUAP 协议安全性分析

SIUAP 协议安全性是指对于标签 T_0 和 T_1，攻击者 A 窃听、跟踪标签却无法识别、区分标签 T_0 和 T_1，从而无法获得标签的内部信息(如标签的标识符 ID 和密钥 K)。

假设攻击者 A 是一个多项式时间(PPT)算法，阅读器和标签作为协议的参与者。在协议运行期间，攻击者 A 控制标签和阅读器的通信信道，能够监听、跟踪标签和阅读器的信息。可以采用如下随机预言质询来形象化描述攻击者 A 和协议参与者进行交互的攻击能力。

(1)$Execute^{s}(R_i,T_j,m_1,m_2)$。该查询表示攻击者 A 对阅读器和标签实施的被攻击实例 s，攻击者 A 通过监听阅读器和标签执行协议的实例 s，可以获得阅读器和标签之间的交互消息 m_1,m_2。

(2)$SendTag^{s}(T_j,m_1,m_2)$。该查询表示攻击者 A 对标签实施的主动攻击 s，攻击者 A 具有模拟阅读器的能力，通过向标签发送消息 m_1，并且接受标签的应答消息 m_2。

(3)$SendReader^{s}(R_i,m_1,m_2)$。该查询表示攻击者 A 对阅读器实施的主动攻击 s，攻击者 A 具有模拟标签的能力，通过向标签发送消息 m_1，并且接受标签的应答消息 m_2。

(4)$Reveal(T_j)$。该查询表示攻击者 A 获得标签 T_j 的匿名 PID 和密钥 K。

定理 1 SIUAP 协议能够保证标签密钥 K 安全，并且标签的 ID 是匿名的。

在 SIUAP 协议实际运行中，阅读器和标签交换信息 $A=$MIXBITS(PID,r_3)，$B=(PID<<<8)\cdot(r_3<<<1)\oplus(K<<<2)$，$C=(n_1<<<8)\cdot(r_3<<<1)\oplus(PID<<<2)$。交换信息被 MIXBITS$(PID,r_3)$和轮函数 $F(x)$所加密，标签匿名 PID 代替真实的标签标识符 ID 进行传输，匿名信息 PID 被随机数 r_3 所保护，r_3 作为伪随机发生器产生的随机数。

首先证明 SIUAP 协议能够保证标签密钥 K 的安全，构造一个攻击者 A，攻击者 A 与协议中的参与者进行如下的交互过程：

1)攻击者 A 执行 $Execute^{s}(R_i,T_j,m_1,m_2)$，获取标签与阅读器的交互信息 $A=$MIXBITS(PID,r_3)，$B=(PID<<<8)\cdot(r_3<<<1)\oplus(K<<<2)$，$C=(PID<<<8)\cdot(r_3<<<1)\oplus(K<<<2)$。

2)攻击者 A 执行 $SendTag^{s}(T_j,m1,m2)$，若 T 存在，A 向标签发送消息 m_1，标签返回信息 $m2$，攻击者可以获得信息，$C=(PID<<<8)\cdot(r_3<<<1)\oplus(K<<<2)$，$D^{*}=(n_1<<<8)\cdot(r_2<<<1)\oplus(r_3<<<2)$。

3)攻击者 A 执行 $SendReader^{s}(R_i,m1,m2)$，攻击者可以获取信息 $B=(PID<<<8)\cdot(r_3<<<1)\oplus(K<<<2)$。

4)攻击者 A 执行 $Reveal(T_j)$，获取标签密钥 K。

在 4)中，假设攻击者 A 取得标签密钥 K，那么攻击者 A 就可以以不可忽略的优势 ε 成功破解轮函数 $F(x)$，然而这与轮函数 $F(x)$不可被破解[17]相矛盾，故 SIUAP 协议能够保证标签密钥 K 安全。

再证明 SIUAP 协议能够保证标签的标识 ID 是匿名的，标签匿名 PID 代替真实的标签标识符 ID 进行传输。PID 在每次认证的过程中都进行动态更新，$PID^{new}=(PID<<<8)\cdot(ID<<<1)\oplus(r_3<<<2)$，若获取下一个认证过程中 PID 的值必须获取随机数 r_3。构造一个攻击者 A，攻击者 A 选择两个任意的标签 T_0 和 T_1 与阅读器进行如下的交互过程：

1)攻击者 A 执行 $Execute^{s}(R_i,T_j,m_1,m_2)$，获取标签与阅读器的交互信息 $A=$MIXBITS(PID,r_3)，$B=(PID<<<8)\cdot(r_3<<<1)\oplus(K<<<2)$，$C=(PID<<<8)\cdot(r_3<<<1)\oplus(K<<<(2)$，在此过程中伪随机发生器产生了随机数 $r_3,r_3\in\{0,1\}^{2k}$，其中若 $r_3=0$，$T_0\rightarrow r_3$，否则在 $r_3=1$ 时，有 $T_0\rightarrow r_3$。

2)攻击者 A 执行 $Reveal(T_j)$，获取标签的假名 PID。

3)攻击者 A 输出 $b'\in\{0,1\}^{2k}$，比较 b'和 r_3 是否相等。

在 3)中，若 $b'=r_3$，需要分两种情况进行讨论。

第一种情况：$b'=r_3=0$，此时是标签 T_0 所对应的比特位，前面已经假设攻击者能够以不可忽略的优势 ε 窃取标签的信息，故攻击者 A 能够以 ε 的优势区分 T_0。

第二种情况：$b'=r_3=1$，此时是标签 T_1 所对应的比特位，前面已经假设攻击者能够以不可忽略的优势 ε 窃取标签的信息，因此攻击者 A 能够以不可忽略的优势 ε 区分标签的 T_1。

$$\Pr(b'=r_3)=\frac{1}{2}\Pr(b'=r_3=0)+\frac{1}{2}\Pr(b'=r_3=1)=\varepsilon$$

攻击者A能以不可忽略的优势 ε 区分随机数 $b'=b_1$，这与伪随机发生器产生的随机数不可区分相矛盾[22]，攻击者 A 不能获取随机数 r_3，即攻击者 A 不能正确地获取标签匿名 PID，保证了标签 ID 的匿名。

综上所述，攻击者 A 不能获取标签的密钥 K 且标签的 ID 是匿名的，因此定理 1 成立。

3.2 SIUAP 协议性能分析

在标签的存储空间上，LAMP++和 SASI 协议都将上一轮的信息 PID^{old}，$k1^{old}$，$k2^{old}$存储在标签中，而 SIUAP 协议将 PID^{old}，$k1^{old}$，$k2^{old}$和时间戳 Δt_{max}存储在阅读器中，大大节省

了存储空间，并且采用轮函数 $F(x)$ 和非线性的 MIXBITS 函数，并没有增加额外的硬件需求，大大降低了运算硬件的消耗，减少了数据库的计算负担，同时提高了系统的灵活性。表 2 列出 7 种协议的性能分析对比情况，其中 L 为变量长度，此处 L=96bit。

表 2　超轻量级 RFID 认证协议的性能分析对比表

协议	标签上的存储量(bit)	标签上的运算	R-双向认证的总通信代价
LAMP	6L	+、⊕、□、□	4L
EMAP	6L	⊕、□、□	5L
M2AP	6L	+、⊕、□、□	5L
SASI	7L	□、□、⊕、+、ROT(x,y)	4L
Gossamer	7L	+、⊕、ROT(x,y)、MIXBITS(x,y)	4L
RAPP	4L	⊕、ROT(x,y)、Per(x,y)	5L
SIUAP 协议	3L	<<<、⊕、·、MIXBITS(x,y)	5L

结束语　本文提出了一种新的超轻量级 RFID 认证协议(SIUAP)，采用轻量级函数轮函数 $F(x)$ 实现阅读器和标签的应答-挑战，大大减少了运算的计算量，同时在阅读器中设置时间戳 Δt_{max}，增加了攻击者攻击的难度。SIUAP 在保证安全性的同时让有效信息尽可能地存储在阅读器，满足了标签资源受限的特点，其安全性和效率更高，更适合 RFID 系统对低成本、高安全的要求。

参 考 文 献

[1] ZHANG Y, BAI L. Rapid structural condition assessment using radio frequency identification (RFID) based wireless strain sensor[J]. Automation in Construction, 2015, 54(6): 1-11.

[2] WARTHA L N R, LONDHE V. Context-Aware Approach for enhancing security and privacy of RFID[J]. International Journal of Engineering And Computer Science, 2015, 4(1): 1078-1088.

[3] GARICA J, BARBEAU M, KRANAKIS E. Handling security threats to the RFID system of EPC networks[J]. Security of Self-Organizing Networks, 2010, 12(3): 45-64.

[4] DAS M L. Strong Security and Privacy of RFID System for Internet of Things Infrastructure[M]// Security, Privacy, and Applied Cryptography Engineering. Springer Berlin Heidelberg, 2013: 56-69.

[5] JIN Yong-ming, WU Qi-ying, SHI Zhi-qiang, et al. Research and development of RFID lightweight authentication protocol based on [J]. PRF Computer Research and Development, 2014, 51(7): 1506-1514(in Chinese)
金永明，吴棋滢，石志强，等. 基于 PRF 的 RFID 轻量级认证协议研究[J]. 计算机研究与发展，2014，51(7)：1506-1514.

[6] CHIEN H. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity [J]. IEEE Transactions on Dependable and Secure Computing, 2007, 4(4): 337-340.

[7] PERIS-LOPEZ P, HERNANDEZ-CASTRO J C, ESTéVEZ-TAPIADOR J M, et al. LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags[C]// Proceedings of the Workshop on RFID Security. 2006: 12-14.

[8] PERIS-LOPEZ P, HERNANDEZ-CASTRO J C, ESTéVEZ-TAPIADOR J M, et al. EMAP: An efficient mutual-authentication protocol for low-cost RFID tags[C]// Proceedings of the OTM 2006 Workshops on the Move to Meaningful Internet Systems. Springer Berlin Heidelberg, 2006: 352-361.

[9] PERIS-LOPEZ P, HERNANDEZ-CASTRO J C, ESTéVEZ-TAPIADOR J M, et al. M2AP: A minimalist mutual-authentication protocol for low-cost RFID tags[M]// Ubiquitous Intelligence and Computing. Springer Berlin Heidelberg, 2006: 912-923.

[10] PERIS-LOPEZ P, HERNANDEZ-CASTRO J C, TAPIADOR J M E, et al. Advances in Ultralightweight cryptography for low-cost RFID tags: Gossamer protocol [M]// Information Security Applications. Springer Berlin Heidelberg, 2009: 56-68.

[11] SUN H M, TING W C, WANG K H. On the security of Chien's ultralightweight RFID authentication protocol[J]. IEEE Transactions on Dependable and Secure Computing, 2011, 2(8): 315-317.

[12] ARCO P D, SANTIS A D. On ultralightweight RFID authentication protocols[J]. IEEE Transactions on Dep Ependable and Secure Computing, 2011, 8(4): 548-563.

[13] PENG P, ZHAO Y M, HAN W L, et al. Ultra-lightweight RFID Mutual Authentication Protocol [J]. Computer Engineering, 2011, 37(16): 140-142.

[14] TIAN Y, CHEN G, LI J. A New Ultralightweight RFID Authentication Protocol with Permutation[J]. IEEE Communications Letters, 2012, 16(5): 702-705.

[15] WANG shao-hui, HAN zhi-jie, LIU Su-juan, et al. Security Analysis of RAPP an FRID Authentication Protocol based on Permutation[R]. Cryptology ePrint Archive, Report 2012/327, 2012.

[16] AHMADIAN Z, SALMASIZADEH M, AREF M R. Desynchronization attack on RAPP ultralightweight authentication protocol[J]. Information Processing Letters, 2013, 113(7): 205-209.

[17] ABED F, LIST E, LUCKS S, et al. Differential and linear cryptanalysis of reduced-round SIMON[R]. Cryptology EPrint Archive, Report 2013/526, 2013.

[18] ZHANG D, LI G, PAN Z, et al. A new anti-collision algorithm for RFID tag[J]. International Journal of Communication Systems, 2014, 27(11): 3312-3322.

[19] BURROWS M, ABADI M, NEEDHAM R M. A logic of authentication[C]// Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences. The Royal Society, 1989: 233-271.

[20] SAUL E, HUTCHISON A C M. A graphical environment for the facilitation of logic-based security protocol analysis [J]. South African Computer Journal, 2000(26): 196-200.

[21] GONG L, NEEDHAM R, YAHALOM R. Reasoning about belief in cryptographic protocols[C]// Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy. California: IEEE Computer Society Press, 1990: 234-248.

[22] MA Chang-she. Low Cost RFID Authentication Protocol with Forward Privacy[J]. Chinese Journal of Computers, 2011, 34(8): 1387-1398. (in Chinese)
马昌社. 前向隐私安全的低成本 RFID 认证协议[J]. 计算机学报，2011，34(8)：1387-1398