一种超轻量级RFID双向认证协议

刘亚丽[1,2] 秦小麟[1] 王 超[1]
(南京航空航天大学计算机科学与技术学院 南京 210016)[1]
(江苏师范大学计算机科学与技术学院 徐州 221116)[2]

摘 要 开放的无线通信环境,尤其是阅读器和标签间的无线信道,使得无线射频识别(RFID)系统的安全和隐私问题逐渐成为值得关注的焦点,因此设计抗各种恶意攻击和安全威胁的超轻量级RFID认证协议是非常必要的。针对低代价标签提出了一种新的超轻量级RFID双向认证协议,该协议避免了已有RFID认证协议存在的安全隐患。安全分析表明新协议具有较强的安全和隐私属性,并且能够抵抗各种可能的恶意攻击。根据低代价RFID标签资源受限的需求,新协议仅需要在标签上执行两种简单的比特位操作,与其他超轻量级RFID认证协议相比具有更好的性能优势。

关键词 RFID,超轻量级,双向认证,低代价
中图法分类号 TP309 **文献标识码** A

Ultralightweight RFID Mutual-authentication Protocol

LIU Ya-li[1,2] QIN Xiao-lin[1] WANG Chao[1]
(College of Computer Science & Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)[1]
(College of Computer Science & Technology, Jiangsu Normal University, Xuzhou 221116, China)[2]

Abstract Due to the open wireless communication environments in radio frequency identification (RFID) systems, particularly the reader-tag air interface, security and privacy are increasingly becoming noteworthy issues. It is imperative to design ultralightweight RFID authentication protocols to resist various malicious attacks and threats. A new ultralightweight RFID mutual-authentication protocol for low-cost was proposed, which avoids the security omission in the previous RFID authentication protocols. Security analysis shows that the protocol possesses robust security and privacy properties as well as defending against the possible malicious attacks. In terms of the resource-constrained requirements of low-cost RFID tags, the protocol requires only two simple bitwise operations over the tag end and meanwhile it has better performance advantages compared with other ultralightweight RFID authentication protocols.

Keywords RFID, Ultralightweight, Mutual authentication, Low-cost

1 引言

无线射频识别(RFID)系统使用无线射频技术在开放系统环境中进行对象识别,是一种非接触式自动识别技术[1],通过射频信号自动识别目标对象并获取相关数据。由于RFID电子标签具有成本低、体积小、容量大、寿命长、可重复使用等特点,目前RFID技术已被广泛应用于工业自动化、商业自动化、交通运输控制管理等众多领域。尽管RFID系统在实际中得到了广泛的应用,但各种恶意攻击[2,3]和安全隐患[4,5]已成为严重制约其进一步扩展亟需解决的关键问题[6]。近年来,为确保阅读器和标签双方的合法性及通信安全,众多学者提出了多种RFID认证协议,其成为保护标签所有者隐私和安全的最有效途径。

根据计算能力、电源消耗、存储代价、标签价格和标签所支持的运算,Chien等人在文献[7]中将标签分为高代价标签和低代价标签。其中,低代价标签根据价格和体积优势以及无源特点,在实际环境中得到了更加广泛的应用。但由于其极端受限的运算和存储需求[8]:仅能存储数百个比特位,拥有5k~10k逻辑门用于运算,其中仅有250~3k逻辑门实现安全功能,导致低代价标签不能使用传统的加解密方法提供安全保护,因此针对此类标签设计安全和隐私保护方案成为RFID安全领域面临的重要挑战。自从2006年Peris等人首次提出一系列超轻量级RFID认证协议(UMAP协议族[8-10])后,其针对低代价标签构建的超轻量级RFID认证协议成为

到稿日期:2013-03-15 返修日期:2013-06-04 本文受国家自然科学基金项目(61373015),2010年度国家教育部高等学校博士学科点专项科研基金项目(20103218110017),江苏高校优势学科建设工程资助项目(PAPD),南京航空航天大学中央高校基本科研业务费专项基金项目(NP2013307),中央高校基本科研业务费专项:江苏省普通高校研究生科研创新计划资助项目(CX10B_112Z),南京航空航天大学博士学位论文创新与创优基金资助项目(BCXJ10-07)资助。

刘亚丽(1980—),女,博士生,讲师,主要研究方向为物联网安全及隐私保护技术,E-mail:lyl1980115@163.com;秦小麟(1953—),男,教授,博士生导师,主要研究方向为分布式环境的数据管理与安全、信息安全等;王 超(1989—),男,硕士生,主要研究方向为物联网安全。

众多学者关注的焦点[7,11-13]。但已有超轻量级认证协议的典型代表 UMAP 协议族[8-10]被指出存在各种安全隐患且不能抵抗各种恶意攻击[14-18]，如：恶意监听、恶意拦截、重放攻击、伪造攻击、追踪攻击、非同步攻击和全泄露攻击等。

本文提出了一种有效的超轻量级 RFID 双向认证协议，在低代价标签上仅涉及简单比特位运算，满足标签资源受限的需求，提高了协议的执行效率，同时加强了鲁棒性和可靠性。本文主要创新之处如下：

(1)认证周期的前向安全性：每轮认证周期通过动态更新伪随机数、标签假名和密钥，随机化标签和阅读器间的挑战应答，保证不同认证周期间的不可链接性，确保协议具有前向安全性；

(2)挑战应答的同步性：最后一条交互式确认消息采用从阅读器端到标签端发送的方式，确保两者间更新过程和挑战应答的同步性；

(3)双向认证的鲁棒性：阅读器和标签间的双向认证机制加强了协议的鲁棒性，同时确保交互消息和更新数据的真实性和完整性，使得协议不仅具有典型的安全属性，还能够抵抗各种潜在的恶意攻击；

(4)标签运算的超轻量性：通过在低代价 RFID 标签上仅使用模 2^m 加(mod 2^m(+))和左循环移位($Rot(x, y)$)两种简单比特位操作，满足了低代价 RFID 标签超轻量级的运算需求，同时避免了协议[8-10]中类似安全隐患[14-17]的出现。

本文第 2 节对相关工作进行回顾；第 3 节简要介绍 RFID 系统构成和基本设置；第 4 节详细描述我们提出的超轻量级 RFID 双向认证协议(URMAP)；第 5 节对新协议进行详细的安全性分析；第 6 节进行性能评估。最后给出本文总结。

2 相关工作

2003 年 Vajda 等人首次针对低代价 RFID 标签提出轻量级认证协议[19]。2005 年 Juels 提出低代价 RFID 标签中最低限度密码的概念[20]。在文献[19,20]的基础上，Peris 等人于 2006 年提出 3 种超轻量级 RFID 认证协议 LMAP，EMAP 和 M2AP[8-10]，其被称为 UMAP 协议族，引起众多学者的广泛关注。UMAP 协议族[8-10]中标签仅涉及或(OR)、与(AND)、异或(XOR)和模 2^m 加(mod 2^m(+))等简单比特位逻辑运算或算术运算，众多研究团体通过详细的分析发现这些操作的组合存在安全隐患，无法充分保证认证协议的安全性，经过协议的多轮执行指出 UMAP 协议族[8-10]不能抵抗非同步攻击和完全揭露攻击[14-16]。随后，在 LMAP 协议[8]设计策略的基础上，Li 等人提出了 LMAP 协议[8]的扩展版 LMAP+[12]。2011 年，Safkhani 等人在文献[17]中指出 LMAP+[12]不能抵抗跟踪攻击和非同步攻击。

2007 年，Chien 等人提出另一个典型的超轻量级认证协议 SASI[7]，其通过利用比特位异或(XOR)和左循环移位($Rot(x,y)$)操作计算标签和阅读器间的交互信息，但 SASI 协议仍未达到预期的安全性，被指出不能抵抗恶意攻击且数据完整性受到破坏。2011 年，Sun 等人通过重放消息的攻击方法指出 SASI 协议[7]不能抵抗非同步攻击[18]。同年，Arco 等人指出 SASI 协议[7]在完全揭露攻击下攻击者能够获取所有的秘密数据[21]。2012 年，Tian 等人采用轻量级的 Per 运算完成阅读器和标签间的挑战应答过程，提出 RAPP 协议[22]。Wang 等人利用伪造和监听等攻击方法[23]成功攻破 RAPP 协议[22]，造成协议中所有秘密数据的全泄露。2013 年 Ahmadian 等人指出 RAPP 协议[22]不能抵抗非同步攻击[24]。

3 RFID 系统构成和基本设置

典型的 RFID 系统由标签、阅读器和后端数据库 3 部分构成，标签和阅读器间通过挑战-应答方式进行信息交互。超轻量级 RFID 认证协议通常具有以下基本设置：

(1)低代价 RFID 标签是被动无源标签，如第 1 节所述，其具有非常有限的计算和存储能力。标签唯一的静态 ID 存于 ROM，假名 IDS 和密钥存于 EEPROM 用于认证；

(2)阅读器的建立和标签间的无线通信信道，用于两者间交互信息的传递并记录每个认证过程中的交互过程。后台数据库是三者中唯一的可信实体，共享标签的秘密信息(如：标签密钥和静态 ID)；

(3)阅读器和标签间的无线信道较易受攻击者的恶意攻击，通常被认为是不安全信道；而阅读器和后端数据库间的有线信道不易受到恶意攻击，具有较高的安全性，通常被认为是安全信道；

(4)合格的 RFID 认证协议需要在协议层满足基本的安全和隐私需求，而并非在物理层和链路层；

(5)认证协议中涉及的信息长度均为 96 比特位，符合 EPCGlobal 定义的编码标准。

4 超轻量级 RFID 双向认证协议(URMAP)

4.1 符号说明

为简化描述，URMAP 协议中的相关符号和操作说明如表 1 所列。

表 1 符号说明表

符号	说明
R	阅读器
T	标签
TDS	可信后台数据库(包含 IDS 和 K)
PRNG	伪随机数发生器[25]
IDS	当前认证周期的标签假名
IDS^{old}	前一轮认证周期的标签假名
IDS^{new}	下一轮认证周期的标签假名
ID	标签唯一的静态身份
K	标签密钥
K_1, K_2, K_3	当前认证周期中标签密钥 K 的子密钥
$K_1^{old}, K_2^{old}, K_3^{old}$	前一轮认证周期中标签密钥 K 的子密钥
$K_1^{new}, K_2^{new}, K_3^{new}$	下一轮认证周期中标签密钥 K 的子密钥
+	模 2^m 加(mod 2^m(+))，m=96
Rot(x, y)	左循环移位(Rot(x, y)) x 左循环移动(y mod L)位，L=96
P	阅读器和标签间的一次双向认证

4.2 URMAP 协议

URMAP 协议认证过程由 4 个阶段构成：初始化阶段、标签识别阶段、双向认证阶段、更新阶段。下面详细介绍 URMAP 协议的认证过程。

4.2.1 初始化阶段

(1)TDS 选择一个伪随机数发生器 PRNG[25] $g:\{0,1\}^k \rightarrow \{0,1\}^{2k}$ 产生伪随机数；

(2)TDS 产生密钥 $K=K_1|K_2|K_3$，并将其置入合法阅读器 R 和合法标签 T 中；

(3)TDS，合法阅读器 R 和合法标签 T 存储并保密 T 对

应的 IDS 和 K。

4.2.2 标签识别阶段

(1)$R\rightarrow T$:R 向 T 发送“Hello”消息作为挑战,初始化一个新的认证周期;

(2)$T\rightarrow R$:T 收到 R 挑战后,返回当前认证周期的 IDS 给 R 作为应答;

(3)T 识别:R 收到应答后,查询 TDS 是否有匹配的 IDS,其中只有被授权的 R 才能从 TDS 中获取合法 T 相应的秘密信息(密钥 $K=K_1|K_2|K_3$);

①若 R 查询到匹配的 IDS,则将执行后续的双向认证阶段;否则由于此次 T 的应答无效或者 R 为未授权阅读器等因素,导致 R 无法从 TDS 中查询到匹配的 IDS,此时 R 将终止当前认证周期,等待执行下一轮新的认证周期;

②若在 TDS 中匹配的 IDS 为 IDS^{old},则 R 将利用$\{K_1^{old},K_2^{old},K_3^{old}\}$执行后续的双向认证阶段;若匹配的 IDS 为 IDS^{new},则 R 将利用$\{K_1^{new},K_2^{new},K_3^{new}\}$执行后续的双向认证阶段。

4.2.3 双向认证阶段

(1)$R\rightarrow T$:获取匹配 IDS 后,R 利用伪随机数发生器 PRNG[25] 产生一个 96 比特位的伪随机数 n_1,并计算 $A=Rot(IDS+n_1,K_1)+K_2$ 和 $B=Rot(IDS+K_2,n_1)+K_1$,其中 A 用于隐藏伪随机数 n_1,B 用于验证 R 的合法性和 R-T 间交互消息的完整性;R 将消息 $A\|B$ 发送给 T(即 R 向 T 发送随机化挑战)。

(2)R 认证:T 接收到 R 的随机化挑战 $A\|B$ 后,利用自身的 IDS 和子密钥 K_1,K_2 从接收到的消息 A 中提取出伪随机数 n_1,并根据 $B'=Rot(IDS+K_2,n_1)+K_1$ 计算 T 中消息 B'的值。比较收到的消息 B 和计算的消息 B':

①若 B'等于 B,则 R 成功认证且 T 从 R 中正确抽取伪随机数 n_1,即 R 为合法阅读器;

②若 B'不等于 B,则由于此次 R 发出的挑战消息 $A\|B$ 在 R-T 信道传输过程中被攻击者恶意窜改或者 R 为未授权阅读器等因素,导致 B'和 B 两者不一致,T 均认为 R 为非法阅读器,此时 T 将终止当前认证周期,等待执行下一轮新的认证周期。

(3)$T\rightarrow R$:R 被认证为合法阅读器后,T 利用抽取出的伪随机数 n_1 以及自身的子密钥 K_1,K_2 和 ID,计算应答消息 $C=Rot(K_1+n_1,ID)+K_2$,并将 C 发送给 R。

(4)T 认证:R 接收到 T 的应答消息 C 后,根据 $C'=Rot(K_1+n_1,ID)+K_2$ 计算 R 中消息 C'的值。C'中 ID 的值根据当前认证周期的 IDS 从 TDS 中获取。比较收到的消息 C 和计算的消息 C':

①若 C'等于 C,则 T 成功认证,即 T 为合法标签,R 确认具有此 ID 的标签被成功检测。此时,此次双向认证周期 P 被认为是有效认证。

②若 C'不等于 C,则由于此次 T 发出的应答消息 C 在 T-R 信道传输过程中被攻击者恶意窜改或者 T 为未授权标签等因素,导致 C'和 C 两者不一致,R 均认为 T 为非法标签,此时 R 将终止当前认证周期,等待执行下一轮新的认证周期。

(5)$R\rightarrow T$:T 被认证为合法标签后,R 再次利用伪随机数发生器 PRNG[25] 产生一个 96 比特位的伪随机数 n_2,并计算 $D=Rot(K_3+n_2,K_2)$ 和 $E=Rot(K_3+K_2,K_1+n_1)+n_2$,其中 n_1 和 n_2 均用于更新操作。随后,R 将消息 $D\|E$ 发送给 T 后执行下一个阶段的更新操作。

(6)R 进一步认证:T 接收到 R 发送的消息 $D\|E$ 后,利用自身的子密钥 K_2 和 K_3 从接收到的消息 D 中提取出伪随机数 n_2,并根据 $E'=Rot(K_3+K_2,K_1+n_1)+n_2$ 计算 T 中消息 E'的值。比较收到的消息 E 和计算的消息 E':

①若 E'等于 E,则 T 从 R 中正确抽取伪随机数 n_2 且 R 进一步被 T 成功认证,此时 T 将执行更新阶段;

②E'不等于 E,则由于此次 R 发出的消息 $D\|E$ 在 R-T 信道传输过程中被攻击者恶意窜改或者 R 为未授权阅读器等因素,导致 E'和 E 两者不一致,T 均认为 R 为非法阅读器,此时 T 将保持原有 IDS 和 $K=K_1|K_2|K_3$ 的值而不执行更新阶段的操作,同时终止当前认证周期,等待执行下一轮新的认证周期。

4.2.4 更新阶段

R 和 T 成功完成双向认证后,将分别更新自身的 IDS 和 $K=K_1|K_2|K_3$,以保持下一轮认证过程的同步性。

(1)阅读器和 TDS 更新

R 发送消息 $D\|E$ 给 T 后,采取以下方法立即更新自身的 IDS 和 $K=K_1|K_2|K_3$:

$$IDS^{old}=IDS,K_1^{old}=K_1,\ K_2^{old}=K_2,\ K_3^{old}=K_3$$

$$IDS^{new}=Rot(IDS^{old}+n_2,K_2^{old}+n_1)+K_3^{old}+K_1^{old}$$

$$K_1^{new}=Rot(K_1^{old}+n_2,n_1)+K_3^{old}$$

$$K_2^{new}=Rot(K_2^{old}+n_1,n_2)+K_1^{new}$$

$$K_3^{new}=Rot(K_3^{old},n_1+n_2)+K_2^{new}$$

同时,R 保存本轮认证周期的 IDS^{old},K_1^{old},K_2^{old},K_3^{old} 以防止后继认证中的非同步攻击。随后,R 将原值(IDS^{old},K_1^{old},K_2^{old},K_3^{old})和更新值(IDS^{new},K_1^{new},K_2^{new},K_3^{new})发送给 TDS。

(2)标签更新

T 收到消息 $D\|E$ 后,通过检验 E'和 E 的一致性,进一步认证 R。若两者一致性检验成功,T 采取以下方法立即更新自身的 IDS 和 $K=K_1|K_2|K_3$:

$$IDS=Rot(IDS+n_2,K_2+n_1)+K_3+K_1$$

$$K_1=Rot(K_1+n_2,n_1)+K_3$$

$$K_2=Rot(K_2+n_1,n_2)+K_1$$

$$K_3=Rot(K_3,n_1+n_2)+K_2$$

至此,协议执行一轮完整的认证周期,下一轮认证周期从标签识别阶段开始执行。协议的具体步骤如图 1 所示。

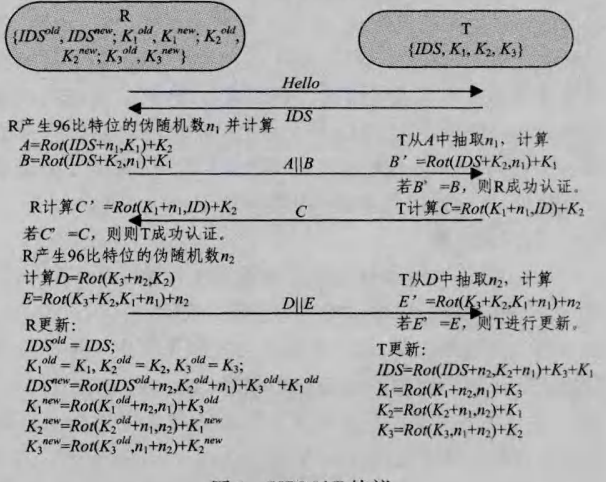

图 1 URMAP 协议

5 安全性分析

本节从 RFID 认证协议的主要安全性能属性以及对典型恶意攻击的抵抗能力两个方面对 URMAP 协议进行详细的安全性能分析。

5.1 数据机密性

URMAP 协议以当前认证周期的 IDS 代替标签独一无二的 ID 作为应答在 R-T 无线信道上传输。通信过程中阅读器和标签间传输的所有公开信息均被秘密值(包括每个认证周期的密钥 $K=K_1|K_2|K_3$ 和动态产生的随机数 n_1, n_2)所保护。随机数在每一轮认证周期中由阅读器动态产生,用以随机化挑战-应答过程,在未知密钥的情况下,攻击者不可能通过截获的交互消息获取合法标签中的任何秘密信息。因此,合法标签的 $K=K_1|K_2|K_3$ 和 ID 被充分保护,确保了数据机密性。

5.2 数据完整性

数据完整性通过比较阅读器和标签间交互信息($A\|B$, $C,D\|E$)的接收版本和自身计算版本进行保障。秘密信息($K=K_1|K_2|K_3,n_1,n_2$)和 IDS 参与交互信息的构建,且进行周期性的动态更新,只有合法阅读器和合法标签才能计算交互信息的有效值。如果攻击者试图修改阅读器和标签间的交互信息,则接收端验证接收消息和自身计算版本的一致性失败,从而识别非法攻击者。因此,URMAP 协议确保了秘密信息以及交互消息的数据完整性。

5.3 标签匿名性

在阅读器和标签的挑战应答过程中,没有明文传送每个标签独一无二的 ID 信息。无线信道上传送的交互信息在每轮认证周期中,根据秘密信息($K=K_1|K_2|K_3,n_1,n_2$)的动态变化进行更新,且对标签 ID 信息进行匿名化处理,实现对标签随机化的访问控制。攻击者即使通过无线信道截获了交互信息,在未知密钥和随机数的情况下,也无法抽取出合法标签的 ID,因此,对非法实体来说标签是匿名的。

5.4 双向认证性

双向认证机制阻止阅读器和标签间未授权的访问,确保只有通过认证的合法实体才能相互通信。合法实体通过分享的密钥信息、产生的随机数构建有效的交互信息,并通过检验接收消息和按照相同算法计算得到自身消息的一致性来达到合法实体的认证功能。具体地,标签通过接收挑战 A 抽取本轮阅读器产生的随机数 n_1 并计算消息 B 和 B'的一致性,来验证阅读器的合法性。若 B 和 B'的一致性验证成功,则标签继续计算 C 并将其发送给阅读器。类似地,只有合法阅读器才能成功验证消息 C 和 C'的一致性,以此验证标签的合法性,并计算 $D\|E$ 发送给标签。因此,只有合法实体才能完成相互认证,从而确保阅读器和标签间的双向认证性。

5.5 前向安全性

每一轮成功认证后,合法实体间的共享密钥 $K=K_1|K_2|K_3$ 和未知随机数 n_1,n_2 均会自动更新。即使 $K=K_1|K_2|K_3$ 在当前认证周期泄露,攻击者也不可能根据历史认证记录推导出之前认证周期中的有效秘密信息($K=K_1|K_2|K_3,n_1,n_2$)。由于所有的交互信息和更新过程均涉及随不同认证周期动态更新的秘密信息($K=K_1|K_2|K_3,n_1,n_2$),且 $K=K_1|K_2|K_3$ 具有周期化和随机化等特点,攻击者若试图根据密钥 K^{new} 的更新方程得出 K^{old},其困难性等价于攻破伪随机数发生器 PRNG[25]。即使标签在当前认证周期被捕获,之前周期的双向认证仍然有效,历史认证记录的安全性得到了保障。因此,URMAP 协议中的密钥进化和认证过程均具有前向安全性。

5.6 抗重放攻击

URMAP 协议通过动态随机化的挑战-应答抵抗恶意攻击者的重放攻击。为了达到重放攻击的目的,攻击者需要存储至少一轮成功认证周期中的交互消息,通过伪装标签或者阅读器在无线通信信道上重放消息,主要有以下 3 种情况。

情况 1 伪装标签重放应答消息 C

假设攻击者在当前认证周期中,伪装标签重放前一轮认证周期的应答消息 C,阅读器很容易发现消息 C 的重放性,因为在每一个不同的认证周期中,应答消息 C 均是独立的且由新挑战中的动态随机数 n_1 进行更新,因此攻击者通过伪造标签重放消息 C 认证失败。

情况 2 伪装阅读器重放挑战消息 $A\|B$

攻击者假装标签在前一轮认证周期中没有完成 IDS 和 $K=K_1|K_2|K_3$ 的更新操作或者攻击者通过采取在公开信道中阻断前一轮认证周期中的最后一条交互消息 $D\|E$ 的手段,而导致标签无法完成正常的更新过程。在此情况下,不论标签的应答是 IDS^{old} 还是 IDS^{new},攻击者均重放在前一轮认证周期中截获的挑战消息 $A\|B$。标签从消息 A 中抽取随机数 n_1 并验证消息 B 的一致性。

(1) 若标签在前一轮认证周期中完成更新操作,由于密钥 K^{new} 不等于 K^{old},标签从消息 A 中抽取的 n_1^{new} 不等于 n_1^{old},导致消息 B 一致性验证失败;

(2) 若标签在前一轮认证周期中未完成更新操作,则密钥 K^{new} 等于 K^{old},标签从消息 A 中抽取的 n_1^{new} 等于 n_1^{old},消息 B 一致性验证成功。标签将重放前一轮认证周期中的应答消息 C 发送给攻击者(伪装的阅读器)。但在此情况下,攻击者通过两次认证周期中相同的标签应答并没有获得合法标签的任何秘密信息,且标签的内部状态没有任何改变,标签和阅读器仍然保持同步性。

情况 3 伪装阅读器重放挑战消息 $D\|E$

假设攻击者在当前认证周期中,伪装阅读器重放前一轮认证周期中最后一条交互消息 $D\|E$。若标签在前一轮认证周期中完成更新操作,则密钥 K^{new} 不等于 K^{old},标签从 D 中抽取的 n_2^{new} 不等于 n_2^{old},导致消息 E 一致性验证失败;若标签在前一轮认证周期中未完成更新操作,则密钥 K^{new} 等于 K^{old},标签从 D 中抽取的 n_2^{new} 等于 n_2^{old},但重放的 E 由前一轮的 n_1^{old} 计算得到,n_1^{old} 和标签在当前认证周期中从新挑战 $A\|B$ 中获取的 n_1^{new} 不匹配,因此 E 的一致性验证失败。

根据以上分析可以得出,重放交互消息 $A\|B$,$D\|E$ 和 C 均不能认证成功,确保了 URMAP 协议能够抵抗重放攻击。

5.7 抗伪造攻击

(1)标签伪造

攻击者试图通过伪造密钥($K'=K_1'|K_2'|K_3'$)假冒一个合法标签达到认证成功的目的。伪造标签收到合法阅读器发送的挑战消息 $A\|B$ 后,将通过抽取的随机数 n_1 验证接收的消息和标签自身计算 B 的一致性。由于伪造密钥($K'=K_1'|$

$K_2'|K_3'$)和合法标签的真实密钥($K=K_1|K_2|K_3$)不匹配，因此伪造标签从 A 中无法抽取出有效的随机数 n_1。即使攻击者通过阅读器和标签间的无线信道截获挑战 $A\|B$，采用修改-测试的方法猜测随机数试图获取合法密钥($K=K_1|K_2|K_3$)，其困难性等价于攻破伪随机数发生器 PRNG[25]。因此，在未知合法密钥($K=K_1|K_2|K_3$)的情况下，伪造标签不可能产生有效的应答消息，标签伪造攻击失败。

(2) 阅读器伪造

攻击者试图通过伪造挑战 $A'\|B'$ 假冒一个合法阅读器达到认证成功的目的。在 $A'\|B'$ 的计算过程中，伪随机数 n_1 由伪造阅读器利用 PRNG[25] 随机产生，密钥($K'=K_1'|K_2'|K_3'$) 由伪造阅读器假冒设定。当合法标签收到伪造阅读器发送的伪造挑战消息 $A'\|B'$ 后，由于($K'=K_1'|K_2'|K_3'$)不等于($K=K_1|K_2|K_3$)，伪造挑战 $A'\|B'$ 认证失败。若攻击者通过无线信道截获合法挑战 $A\|B$，并在下一轮认证周期中伪造阅读器重放 $A\|B$ 试图达到伪造攻击的目的，同样由于合法密钥($K=K_1|K_2|K_3$)的未知性和更新性，合法标签仍然不能认证伪造的阅读器，具体分析见 5.6 节抗重放攻击情况 2 描述。

根据以上分析，URMAP 协议不仅可以抵抗标签伪造攻击，而且可以抵抗阅读器伪造攻击，具有较强的抗伪造性。

5.8 抗追踪攻击

由于动态更新 IDS 和密钥($K=K_1|K_2|K_3$)在每一个成功认证周期中均进行更新，使得不同认证周期中同一标签的应答 IDS 以及阅读器和标签间的交互消息($A\|B,C,D\|E$)均随机化。又根据协议认证周期的不可链接性，攻击者不可能通过截获或者干扰两次或多次挑战-应答过程，获知交互过程中同一标签的相同应答，从而达到追踪标签的攻击目的。因此，URMAP 协议较好地抵抗了追踪攻击，确保了合法标签的位置隐私未得到侵犯。

5.9 抗非同步攻击

URMAP 协议利用在合法阅读器端增加少量的存储空间来阻止恶意攻击者的非同步攻击。主要有以下两种情况：

情况 1　阅读器和标签执行更新过程不同步

攻击者通过阻断最后一条交互消息 $D\|E$ 使得阅读器和标签更新不同步，试图达到非同步攻击的目的。由于 $D\|E$ 是由阅读器发送给标签的最后一条交互消息，攻击者阻断 $D\|E$ 将造成阅读器正常更新而标签不执行更新操作，但在此情况下两者的不同步更新并不会影响下一轮周期的正常认证。因为合法阅读器更新过程中同时存储当前认证周期中的原值(IDS^{old}，K_1^{old}，K_2^{old}，K_3^{old})和更新值(IDS^{new}，K_1^{new}，K_2^{new}，K_3^{new})，下一轮认证过程阅读器仍然可以识别标签应答 IDS^{old}，利用 K^{old} 计算挑战 $A\|B$ 并执行协议后续认证过程。

情况 2　阅读器和标签使用不同随机值更新

攻击者截获公开信道中传输的交互消息 $D\|E$ 并作一定修改变化或者伪造、重放交互消息发送给标签，造成标签提取的随机数和阅读器端产生的原始随机数不一致，但是由于协议的数据完整性保护，无法完成标签端接收消息的一致性验证。具体分析类似 5.7 节抗伪造攻击(2)和 5.6 节抗重放攻击情况 3 描述，在此不再赘述。

根据以上分析可以得出，攻击者不能成功使得阅读器和标签两端更新不同步，URMAP 协议能够抵抗非同步攻击。

6 性能评估

本节从 URMAP 协议认证过程中的资源消耗和安全性能两个方面对其进行详细的性能评估。

6.1 资源消耗分析

由于低代价标签资源极端受限的特点，充分考虑其计算能力、电源消耗和存储代价等因素，我们仅利用简单的控制命令和 3 种原始的算术运算设计 URMAP 协议：伪随机数发生器 PRNG[25]、比特位模 2^m 加(mod 2^m(+))和比特位左循环移位($Rot(x,y)$)，这些操作相比传统的密码算法具有较低的存储量和计算量。为了随机化挑战应答过程，将计算量相对较高的伪随机数产生运算置于阅读器端，标签端仅使用两种简单的比特位运算 mod 2^m(+)和 $Rot(x,y)$ 实现交互信息的验证和计算操作，这两种比特位操作均符合低代价被动 RFID 标签的运算能力。此外，协议并没有增加额外的硬件需求，降低了数据库的计算负担，同时提高了整个系统的灵活性。

URMAP 协议和典型相关协议[8-10]的性能比较见表 2。表 2 中的比较结果表明，URMAP 协议在标签计算代价和存储代价上均优于文献[8-10]协议，通信代价略次于文献[8]协议。URMAP 协议以牺牲少量的通信代价赢得标签存储空间的降低，标签端的计算代价、存储代价和通信代价均能满足低代价 RFID 标签的超轻量级需求。

表 2　性能对比表

	LMAP[8]	EMAP[9]	M2AP[10]	URMAP
标签端的计算代价	$+^2$，$\oplus^2$，OR^1	$\oplus^5$，AND^1，OR1	$+^2$，$\oplus^2$，AND^1，OR^1	$+^4$，Rot^1
标签端的存储代价(包括临时存储参数)	6L	6L	6L	5L
R-T 双向认证的总通信代价	4L	5L	5L	5L

注：(1)L 代表参数的长度，L=96bits；

(2)操作上标代表标签所执行一次计算中此类操作的最大频率。

6.2 安全性对比分析

URMAP 协议和典型相关协议[8-10]的安全性对比见表 3。根据表 3 所列的安全性能对比情况可知，相比文献[8-10]而言，URMAP 协议具有最强的安全和隐私属性，并能够抵抗第 5 节安全性分析中所列出的多种可能的恶意攻击，确保协议具有较强的认证性、数据机密性和完整性以及同步确认等安全隐私属性。

表 3　安全性能对比表

	LMAP[8]	EMAP[9]	M2AP[10]	URMAP
数据机密性	否	否	否	是
数据完整性	否	否	否	是
标签匿名性	否	否	否	是
双向认证性	是	是	是	是
前向安全性	是	是	是	是
抗重放攻击	否	否	否	是
抗伪造攻击	否	否	否	是
抗追踪攻击	否	否	否	是
抗非同步攻击	否	否	否	是

总的来说，表 2 和表 3 中的对比分析表明：URMAP 协议相比已有协议[8-10]具有明显的性能优势，同时具备较优越的安全隐私特征。为了加强协议的鲁棒性、降低标签的计算代价和存储代价，通过牺牲少量的通信代价来更好地满足低代

价 RFID 标签的限制需求，在性能和安全属性间进行了恰当的折中。因此，URMAP 协议是针对低代价 RFID 标签实现超轻量级认证的有效方案，适合资源受限的认证领域。

结束语 本文针对低代价 RFID 标签资源受限的特点，提出了一种超轻量级 RFID 双向认证协议(URMAP)。新协议通过在标签端仅使用两种简单比特位运算的方式实现了阅读器和标签间随机化的挑战-应答，保证了不同认证周期间的不可链接性、前向安全性以及阅读器和标签间的双向认证性。在降低计算代价的同时，确保了在资源受限的低代价标签上完成超轻量级 RFID 双向认证过程。安全性分析表明 URMAP 协议具备较完善的安全和隐私属性，同时能够抵抗多种潜在的恶意攻击，加强了鲁棒性，提高了执行效率，恰当地平衡了安全性和低代价标签资源极端受限的需求。与已有相关超轻量级 RFID 认证协议相比，URMAP 协议具有更加优越的性能，能够恰当地应用于资源受限的轻量级分布式认证系统。

参 考 文 献

[1] Juels A. RFID Security and Privacy: A Research Survey [J]. IEEE Journal on Selected Areas in Communications, 2006, 24 (2): 381-394

[2] Juels A. Strengthening EPC Tag against Cloning [C]// Proceedings of the 4th ACM Workshop on Wireless Security. ACM, 2005: 67-76

[3] Liu Ya-li, Qin Xiao-lin, Li Bo-han, et al. A Forward-Secure Grouping-proof Protocol for Multiple RFID tags [J]. International Journal of Computational Intelligence Systems, 2012, 5 (5): 824-833

[4] Chien H Y, Chen C H. Mutual Authentication Protocol for RFID Conforming to EPC Class-1 Generation-2 Standards [J]. Computer Standards and Interfaces, 2007, 29(2): 254-259

[5] Rotter P. A Framework for Assessing RFID System Security and Privacy Risks [J]. IEEE Pervasive Computing, 2008, 7(2): 70-77

[6] Zuo Y. Survivable RFID Systems: Issues, Challenges, and Techniques [J]. IEEE Transactions on Systems, Man, and Cybernetics-Part C: Applications and Reviews, 2010, 40(4): 406-418

[7] Chien H Y. 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

[8] 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]// Proc. Second Workshop RFID Security. Graz, Austria, 2006: 12-14

[9] Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M, et al. EMAP: An Efficient Mutual Authentication Protocol for Low-Cost RFID Tags [C]// Proc. OTM Federated Conf. and Workshop: IS Workshop (IS'06). LNCS 4277, Springer-Verlag, Berlin Heidelberg, 2006: 352-361

[10] Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M, et al. M2AP: A Minimalist Mutual-Authentication Protocol for Low-Cost RFID Tags [C]// Proc. Int'l Conf. Ubiquitous Intelligence and Computing (UIC'06). LNCS 4159, 2006: 912-923

[11] Lo N W, Shie H S, Yeh K H. A Design of RFID Mutual Authentication Protocol Using Lightweight Bitwise Operations [C]// Proc. the 3rd Joint Workshop on Information Security (JWIS 2008). Seoul, Korea, 2008

[12] Li Tie-yan. Employing Lightweight Primitives on Low-cost RFID Tags for Authentication [C]// Proc. Vehicular Technology Conference 2008 (VTC'08). IEEE, 68th, 2008: 1-5

[13] Burmester M, Munilla O. Lightweight RFID Authentication with Forward and Backward Security [J]. ACM Transactions on Information and System Security (TISSEC), 2011, 14(1): 11-37

[14] Li Tie-yan, Deng R. Vulnerability Analysis of EMAP-An Efficient RFID Mutual Authentication Protocol [C]// The Second International Conference on Availability, Reliability and Security (ARES'07). IEEE, 2007: 238-245

[15] Li Tie-yan, Wang Gui-lin. Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols [C]// New Approaches for Security, Privacy and Trust in Complex Environments. Springer US, 2007, 232: 109-120

[16] Chien H Y, Huang C W. Security of Ultra-Lightweight RFID Authentication Protocols and Its Improvements [J]. ACM Operating System Rev., 2007, 41(2): 83-86

[17] Safkhani M, Bagheri N, Naderi M, et al. Security Analysis of LMAP++, an RFID Authentication Protocol [C]// Proc. 2011 International Conference for Internet Technology and Secured Transactions (ICITST'11). IEEE, 2011: 689-694

[18] 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, 8(2): 315-317

[19] Vajda I, Butty'an L. Lightweight Authentication Protocols for Low-cost RFID Tags [C]// Proc. Second Workshop on Security in Ubiquitous Computing-Ubicomp (UBICOMP'03). 2003

[20] Juels A. Minimalist Cryptography for Low-cost RFID Tags [C]// SCN' 04 Proceedings of the 4th International Conference on Security in Communication Networks. Springer Berlin Heidelberg, 2005: 149-164

[21] Arco P D, De Santis A. On Ultralightweight RFID Authentication Protocols [J]. IEEE Transactions on Dependable and Secure Computing, 2011, 8(4): 548-563

[22] Tian Yun, Chen Gong-liang, Li Jian-hua. A New Ultralightweight RFID Authentication Protocol with Permutation [J]. IEEE Communications Letters, 2012, 16(5): 702-705

[23] Wang Shao-hui, Han Zhi-jie, Liu Su-juan, et al. Security Analysis of RAPP An RFID Authentication Protocol based on Permutation [R]. Cryptology ePrint Archive, Report 2012/327, 2012

[24] Ahmadian Z, Salmasizadeh M, Aref M R. Desynchronization Attack on RAPP Ultralightweight Authentication Protocol [J]. Information Processing Letters, 2013, 113(7): 205-209

[25] Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M, et al. LAMED-A PRNG for EPC Class-1 Generation-2 RFID Specification [J]. Computer Standards and Interfaces, 2009, 31: 88-97