DOI:10.19651/j.cnki.emt.2209135

# 基于 PUF 和 LED 算法的轻量级 RFID 安全认证协议*

王 者[1,2] 王争光[1,2] 宋贺伦[1,2]
(1.中国科学技术大学纳米技术与纳米仿生学院 合肥 230026;2.中国科学院苏州纳米技术与纳米仿生研究所 苏州 215123)

**摘 要:** 无线射频识别技术是目前推动物联网发展的重要技术之一,具有不易涂抹,成本低廉等优势。由于无线射频信号在传输过程中易收到攻击,RFID 系统需要建立完善的完全保障机制。本文基于 RFID 系统的安全要求和技术现状,提出了一种轻量级 RFID 安全认证协议,该协议基于 LED 密码技术和物理不可克隆函数,利用 PUF 的挑战-响应信号对进行身份验证,LED 算法对 PUF 的响应信号进行加密传输保证认证信息安全,每次认证结束后都会更新服务器内的标签信息。本文使用 Verilog 语言对认证过程进行电路实现与仿真,并基于 40 nm 平台的标准单元库对电路进行综合分析。仿真和综合结果表明该轻量级 RFID 安全认证协议可有效抵御常见攻击,并且标签存储、计算的硬件开销都较低,适用于资源受限的场景。

**关键词:** RFID;认证;协议;密码算法
**中图分类号:** TP309 **文献标识码:** A **国家标准学科分类代码:** 510

# Lightweight RFID security authentication protocol based on PUF and LED algorithm

Wang Zhe[1,2] Wang Zhengguang[1,2] Song Helun[1,2]
(1. School of Nano-Tech and Nano-Bionics, University of Science and Technology of China, Hefei 230026, China;
2. Suzhou Institute of Nano-Tech and Nano-Bionics, Chinede Academy of Science, Suzhou 215123, China)

**Abstract:** Radio frequency identification technology is one of the important technologies currently promoting the development of the Internet of Things. Because the wireless radio frequency signal is easy to be attacked during the transmission process, the RFID system needs to establish a complete and complete guarantee mechanism. Based on the security requirements and technical status of RFID systems, this paper proposes a lightweight RFID security authentication protocol. The protocol is based on LED cryptography and physical unclonable function, and uses the challenge-response signal pair of PUF for authentication. The LED algorithm encrypts and transmits the response signal of the PUF to ensure the security of the authentication information. After each authentication, the label information in the server will be updated. This paper uses the Verilog language to implement and simulate the circuit certification process, and conduct a comprehensive analysis of the circuit based on the standard cell library of the 40 nm platform. Simulation and comprehensive results show that the lightweight RFID security authentication protocol can effectively resist common attacks, and the hardware overhead of tag storage and calculation is low, which is suitable for resource-constrained scenarios.

**Keywords:** RFID;authentication;protocol;cryptographic algorithm

## 0 引 言

无线射频识别(RFID)技术是一种利用射频技术进行身份识别的技术,通过非接触式通信实现自动识别。RFID 技术具有存储量高、可移植性强、安全性好、自动识别等特点,是物联网的核心技术之一。将 RFID 技术和移动通信、互联网和云技术等结合应用,可以实现全球范围内的物体跟踪与通信,实现物与物之间和人与物之间的信息传输[1]。RFID 系统分为电子标签、阅读器、服务器 3 部分。服务器负责数据计算和存储。服务器会存储所有标签的身份标识和相关信息,并负责标签的防伪认证、数据加解密、信息更新等数据计算操作。阅读器的主要功能为通过 RFID 天线

收稿日期:2022-03-02
* 基金项目:纳米真空互联试验站(2018-000052-73-01-000356)、江苏省"六大人才高峰"高层次人才项目(XYDXX-211)资助

和标签进行通信，作为服务器和标签之间的信息交互。部分功能复杂的阅读器还可以在与标签通信时，实现数据的奇偶校验以及多个标签之间的防碰撞等功能[2-3]。RFID 标签存储目标物体的信息及唯一身份识别码，作为数据载体，RFID 标签可存储的信息量大，且不容易被涂抹或撕破，因此相比于条形码，RFID 标签的安全性更高。

服务器和阅读器之间的信息传输通常通过有线信道进行，可以使用传统的网络安全协议和密码体制来保障信息安全。阅读器和标签之间使用无线信号传输信息[4]，安全隐患巨大，目前对于无线信道的攻击手段有很多种，例如假冒、篡改、窃听、克隆、重放、去同步化攻击等，标签内部的信息很容易暴露，因此 RFID 标签的安全机制一直是研究关注的重点。一个完善的 RFID 系统应同时具备安全性和可用性[5]。为满足安全需求，RFID 系统需有一套安全机制保护标签和服务器内部的信息安全。此外，电子标签的硬件资源有限，因此如何在低成本低功耗的要求下设计一个可抵御当前常见攻击手段的 RFID 安全机制是目前亟需解决的问题。

基于 RFID 安全的现状，本文在对现有的几种 RFID 认证协议进行分析比较后提出了一种改进的认证方案，基于物理不可克隆函数(PUF)和 LED 轻量级加密算法，可消耗更少的硬件资源实现对 RFID 系统信息安全的保护。本文对此协议的认证过程进行了详细描述，并使用 Verilog 语言和 VCS 仿真平台对认证过程进行了仿真模拟，通过对攻击手段的模拟仿真证明本协议的安全性，通过电路综合结果证明本协议对硬件资源消耗更少，功耗更低。

## 1　研究现状

### 1.1　RFID 认证协议

目前对于 RFID 安全机制的研究主要分为两个方向：基于物理方法的机制和基于密码算法的机制。基于物理方法的 RFID 安全机制包括 kill/sleep 指令机制、阻塞标签法等[6]。物理安全机制往往需要额外的设备辅助和资源消耗，且易对标签造成不可逆的损伤，具有局限性，因此目前的研究更多集中于密码安全机制。使用密码安全机制来保护 RFID 系统的通信安全面临的挑战有三点，一是 RFID 电子标签的成本受限，标签的存储能力和计算能力难以支持复杂度高的密码算法；二是标签和阅读器之间的无线通信过程；三是出于对系统真实性的要求，通信双方必须进行双向身份认证，密码安全机制中最关键的就是 RFID 安全认证协议[7]。认证协议根据使用的密码算法复杂度，可以划分为重量级、轻量级和超轻量级安全协议。重量级安全认证协议基于重量级密码算法，例如对称加密算法 DES、AES、SM4 和非对称加密算法 ECC、RSA 等。此类协议安全性高但可用性差，密码算法消耗的硬件资源多，因此近年来提出了轻量级和超轻量级安全认证的概念。超轻量级安全认证依靠硬件中的简单逻辑门运算，与、或、异或等，适用于对安全性要求不高的场景，比如 HB 族认证协议、Gossamer 认证协议等。相比之下，轻量级安全认证协议使用占用资源更少的密码算法，比如哈希函数、循环冗余校验、伪随机数函数算法等[6]。轻量级安全认证协议可以在成本需求和安全性需求之间找到平衡点，因此是目前研究关注的重点方向。本文的研究方向即为针对低成本 RFID 电子标签的轻量级安全认证协议。

### 1.2　PUF

目前的轻量级认证协议大多使用 Hash 函数进行信息加密，典型的有 HashLock 协议、随机化 HashLock 协议、Hash-Chain 协议、基于 Hash 的 ID 变化协议、分布式询问-应答协议、LCAP 协议等。但此类方案存在很多安全漏洞，无法抵御克隆攻击、去同步攻击等。

随着 PUF 技术的发展，PUF 被发现可以有效抵御 RFID 系统面临的克隆攻击。PUF 靠微延迟电路实现，对该电路输入随机挑战信号可产生相应的响应信号，我们称这些输入和对应的输出为挑战-响应信号对[8-9]。由于电路生产过程中存在不可避免的微小差异，因此每个 PUF 的挑战-响应对都不同。这些差异无法预测，无法复制，所以 PUF 具有随机性和不可克隆性，每个 PUF 的挑战-响应对都具有唯一性且无法被仿制。基于其特点，将 PUF 应用于密码安全机制中有明显优势：响应信号由电路生成，无需存储在易受攻击的硬件中；PUF 的工作原理依靠物理介质中固有的差异和熵，而非未经证实的数论假设，因此无法通过数学手段破解。

近年来已有许多研究者将 PUF 和 Hash 函数结合，应用于 RFID 安全认证。Akgun 等[10]提出了一种将 PUF 的响应信号作为标签 ID，利用哈希函数加密传输的 RFID 认证方案，但这种方案需要服务器在每次搜索时使用 Hash 函数计算所有记录在内的标签 ID，性能损耗巨大。之后 Bendavid 等[11]提出了一种由 PUF 响应信号计算 ID 的认证方案，但这种方案需在标签内部存储计算所需参数，无法抵御物理攻击和去同步攻击等。随后 Gope 等[12]提出了一个只存储一组身份 ID 和挑战信号的认证方案，每次认证成功后更新 PUF 的挑战-响应对，此方案可抵御去同步攻击，但此方案需要服务器预先为标签注册一系列挑战-响应对作为身份验证手段，一旦挑战响应对消耗完，还需要重新注册。为改进这一缺陷，Zhu[13]提出了在每次认证过程中生成新的挑战响应对的方案，这种方案可抵御物理攻击，但需要标签增加随机数生成电路，消耗硬件面积。基于 RFID 安全认证协议的现状和安全要求，本文提出了一种改进的 RFID 安全认证方案，和现有的认证方案相比，可在有抵御现有攻击手段能力的情况下消耗更少的硬件资源。

此外，传统的 HASH 函数使用的硬件成本较高，例如常用的 MD4、MD5、SHA-256 等算法需要大概 7 350～10 868 个逻辑门电路实现[14]。而一个 RFID 电子标签内部的逻辑门通常在 1 000～10 000 个之间[15]，可用于信息安

全的门电路大概在 200～2 000 个之间。因此对于 RFID 标签而言,传统 Hash 函数的硬件实现成本过高。针对此问题,本文提出一种将 LED 算法应用于 RFID 电子标签安全认证的方法。LED 算法是 Guo 等提出的一种轻量级 Hash 函数算法[16],具有硬件实现简单、能耗低、需要的存储空间小等特点,应用于资源受限的 RFID 电子标签中有天然优势。

基于此,本论文提出一个基于物理不可克隆函数和 LED 算法的 RFID 安全认证方案,可在保证安全需求的前提下,进一步降低电子标签的硬件使用面积。

## 2　基于 PUF 和 LED 算法的 RFID 安全认证协议

### 2.1　系统模型

本文提出的协议基于 Vaudenay 安全隐私模型[17],该模型由 Serge Vaudenay 团队提出,规定了一种可实现强隐私的 RFID 架构和攻击者的能力模型。

本文以张菁等[18]提出的 RFID 安全架构为基础作了适当修正,具体如下:

1) $SetupServer(1^{\lambda}) \rightarrow (ID, C)$

基于安全参数 λ 为服务器生成标签唯一身份标识 ID 及挑战信号 $C$,给每个标签分配 ID 并存储挑战信号 $C$ 和对应响应信号 $R$;

2) $SetupTag$

生成一个拥有身份标识码 ID、PUF 电路和 Hash 函数算法的标签。每个标签的信息在注册阶段存储在服务器的后端数据库中;

3) $IdentTag(\#) \rightarrow out$

服务器、阅读器和标签在协议 # 中进行通信,如果服务器和标签之间的双向认证成功,out=1,反之 out=0.

攻击者可利用以下八步循环运行的算法:

1) $CreatTagb(ID)$

通过质询 SetupTag 获得一个自由标签,标签可以是合法的也可以是不合法的,合法标签 $b=1$,不合法标签 $b=0$;

2) $DrawTag(distr) \rightarrow (vtag1, b1, \cdots vtagn, bn,)$

根据分配概率 distr,随机选取标签进行访问,根据 $b$ 判断标签是否合法;

3) $FreeTag(vtag)$

将合法标签设为空白,使服务器无法访问该标签;

4) $Launch(\#)$

通过读写器端初始化认证协议;

5) $SendReader(a, \#) \rightarrow a'$

在协议 # 的执行下,给服务器发送消息 $a$ 并得到响应 $a'$;

6) $SendTag(a, vtag) \rightarrow a'$

向标签 vtag 发送质询 $a$ 并得到响应 $a'$;

7) $Result(\#)$

如果攻击成功,输出结果为 1,反之为 0;

8) $Corrupt(vtag)$

识别标签 vtag 的当前状态,判断标签是否拥有合法身份。

### 2.2　环境参数

1)标签 T 使用的函数和参数

(1)物理不可克隆函数 $P$:通过 PUF 电路实现,输入挑战信号 $C$ 可得到响应信号 $R$。对于同一个 PUF,输入不同 $C$ 得到的 $R$ 不同,对于不同的 PUF,相同的输入信号 $C$ 得到的输出信号 $R$ 不同。

(2)轻量级 HASH 函数算法 LED:单向函数,无法通过输出结果分析出输入信号。LED 为公开算法,所有标签和攻击者都能使用。

(3)ID:在注册阶段,由服务器派发给标签的唯一身份标识。服务器会存储所有合法标签的 ID 信息,每个标签存储自己的 ID。

2)服务器 S 使用的函数和参数

(1)LED:和标签内部相同的 LED 算法。

(2)存储每个标签的 ID 和挑战响应对 $\{C_i, R_i\}$。

3)计算符号

⊕:异或运算,是一个具有单向性的运算,从 $a \oplus b$ 的结果无法推知 $a$ 和 $b$ 的数值;

‖:连接符;

### 2.3　协议认证过程

本文提出的协议具有如下假设:

1)协议包括 RFID 标签注册和认证两部分,每个标签投入使用前需预先向服务器认证,得到合法身份。本文假设认证过程使用安全通道。

2)每个标签都有 LED 加密模块和物理不可克隆函数 PUF 模块。

3)服务器和阅读器之间的通信信道是安全的,阅读器和标签之间的通信信道易受到攻击。

协议注册过程包括:

1) $T \rightarrow S:\{hello\}$

标签向服务器发送注册请求;

2) $S \rightarrow T:\{ID, C_i\}$

服务器根据 SetupServer 函数生成一个标签身份标识码 ID 和挑战信号 $C_i$,发送给标签;

3) $T \rightarrow S:\{R_i\}$

标签存储 ID,将 $C_i$ 作为 PUF 的输入,得到 $R_i = P(C_i)$,发送给服务器,服务器存储该标签的 ID 及对应的 $(C_i, R_i)$。

认证过程如图 1 所示。

1) $S \rightarrow T:\{hello\}$

服务器通过阅读器向标签发送认证请求;

2) $T \rightarrow S:\{ID\}$

标签收到认证请求后向阅读器发送自己的 ID;

3) $S \rightarrow T:\{C_i\}$

服务器在后台数据库中查找对应 ID 信息,如果数据库

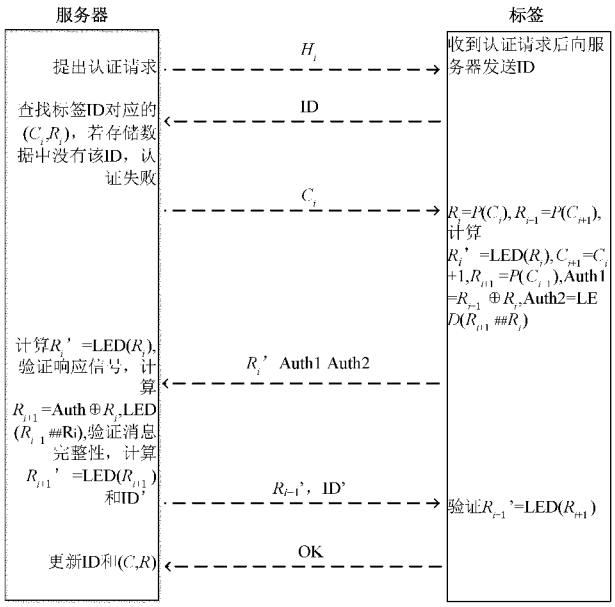


图 1　认证过程

中没有存储该 ID，认证失败；若找到该 ID 则向标签发送该 ID 对应的挑战信号 $C_i$；

4) $T \rightarrow S:\{R_i', Auth1, Auth2\}$

标签收到阅读器发送的 $C_i$，首先使用 PUF 模块得到 $C_i$ 的响应信号 $R_i$，然后根据式(1)计算 $R_i'$作为标签身份验证信息。接下来通过式(2)、(3)更新挑战响应对，利用式(4)、(5)计算 $Ri'$，$Auth1$ 和 $Auth2$ 返回给阅读器。

$$R_i' = LED(R_i) \tag{1}$$

$$C_{i+1} = C_i + 1 \tag{2}$$

$$R_i + 1 = P(C_i + 1) \tag{3}$$

$$Auth1 = R_{i+1} \oplus R_i \tag{4}$$

$$Auth2 = LED(R_{i-1} \# \neq R_i) \tag{5}$$

5) $S \rightarrow T:\{R_{i+1}', ID'\}$

服务器收到响应后，利用式(1)验证内部存储的 $R_i$ 和标签的返回值是否相等，若不相等，认证失败；若相等，证明标签身份合法。验证标签身份后根据式(6)和(5)计算 $R_{i-1}$ 与 $Auth2$，对比收到的 $Auth2$ 验证消息完整性，若计算结果与标签发送的相同，说明消息未经篡改，否则终止认证。得到正确的 $R_{i-1}$ 后通过式(7)和 SetupServer 函数计算 $R_{i+1}'$和新的标签身份码 ID′返还给标签。$R_{i+1}'$的作用是验证服务器身份，由于异或计算的单向性，只有拥有正确 $R_i$ 的服务器才能获得 $R_{i+1}$。

$$R_{i+1} = Auth1 \oplus R_i \tag{6}$$

$$R_{i+1}' = LED(R_{i+1}) \tag{7}$$

6) $T \rightarrow S:\{ok\}$

标签收到信息后验证服务器发送的 $R_{i-1}'$与自己的计算结果是否相同，若相同说明服务器身份合法，将 ID 替换为 ID′，向服务器发送认证通过信号，认证完成。服务器收到认证成功信号后将标签信息更新为 ID′和($C_{i+1}$，$R_{i+1}$)，原本的 ID 依旧保存，直至至下一次认证成功，这种方法可以抵御去同步攻击。

在认证过程中，如果有任何步骤验证失败，认证立刻终止，在证明标签和服务器身份皆合法后才能进行下一步通信。

### 2.4　模拟仿真

本文使用 verilog 语言对此协议中服务器、阅读器、标签之间的通信过程进行模拟。结构设计如图 2 所示。

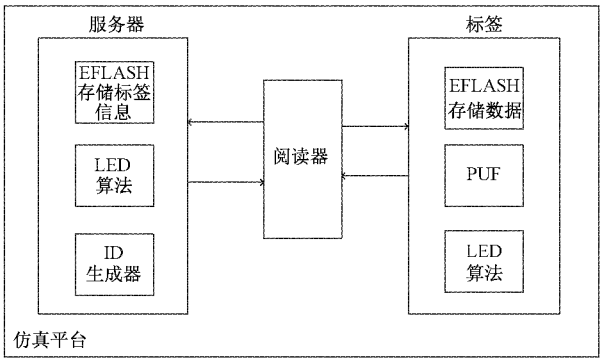


图 2　系统框图

服务器存储标签相关信息，接收阅读器信息并进行处理，通过阅读器对标签进行读写；标签通过阅读器与服务器进行双向认证，认证成功后允许服务器对标签内部信息进行读写操作；阅读器负责数据传输和显示。本文通过 VCS 仿真平台模拟三者的信息传输过程，以此验证协议的可行性和安全性。认证过程如图 3 所示。


图 3　服务器认证过程

服务器查找标签信息后，验证服务器发送的响应信号正确性与完整性，并更新标签信息，包括标签 ID 和挑战-响应对，认证通过后对标签内部信息进行读写，如图 4 所示。


图 4　阅读器显示信息

阅读器负责信息传递，以及必要的信息显示，例如标签 ID 以及认证结果，如图 5 所示。

标签通过内部的 PUF 模块和 LED 算法模块进行身份验证，在认证通过后允许服务器对内部存储信息读取和修改。


图 5　标签认证过程

## 3　协议分析

### 3.1　安全性分析

在本协议中,若 RFID 双向认证失败,标签和阅读器不会进行下一步通信,此方法可保障标签和服务器内部敏感信息的安全,满足 RFID 系统的机密性要求。对于认证过程,本文基于 Vaudenay 攻击者模型,针对目前常见的无线信道攻击手段进行了安全分析。

1)假冒攻击

首先攻击者 A 假冒合法服务器,向标签 T 发送认证请求,获得标签的 ID 后,攻击者生成一个随机数 C 伪造成挑战信号。收到标签的返回数据后,攻击者若想进行下一步认证,必须从$\{R_i', Auth1, Auth2\}$中获得 $R_{i+1}$。由于 Hash 函数和异或运算的单向性,从 $Auth1=R_{i+1}\oplus R_i$ 无法推知 $R_{i+1}$ 和 $R_i$,从 $Auth2=\mathrm{LED}(R_{i+1}\#\#R_i)$亦无法逆推得 $R_{i-1}\#\#R_i$。因此攻击者无法通过下一步认证。本文在 vcs 仿真平台上对此种攻击情况进行了模拟,结果如图 6 所示,攻击者在第 5 步无法返回正确的 $R'_{i-1}$,无法通过认证。


图 6　假冒服务器

伪造标签身份同理,基于 PUF 的不可克隆性,攻击者 A 收到挑战信号 $C_i$ 后无法得到 $R_i$ 的具体数值,从而无法回复正确的响应信号。利用仿真平台的模拟结果如图 7 所示。


图 7　假冒标签

若攻击者假冒标签参与认证,由于没有 PUF 模块,无法得到能通过认证的 $R_i$。若认证不通过,标签不会进行下一步通信,因此在本协议中,攻击者通过假冒服务器或标签无法成功破解认证过程。

2)篡改攻击

篡改攻击指攻击者在信息传输过程中截取敏感信息,篡改后重新发送。若协议传输的敏感信息被篡改,在接下来的认证中攻击者可以使用篡改后的消息进行身份认证,比如若攻击者成功篡改本协议中的 $R_{i+1}$,便可破解认证。本协议通过 Hash 函数来保证无线信道传输数据的完整性。服务器接收到 $R_{i+1}$ 后会利用 Auth 的 Hash 函数结果进行比较,若 $R_{i-1}$ 被篡改,服务器会发现计算值和 Auth2 不匹配,从而结束认证。因此攻击者无法通过篡改攻击破解认证。仿真结果如图 8 所示,攻击者 A 篡改第 4 步或第 5 步的信息都会导致认证失败,如图 9 所示。


图 8　篡改第 4 步发送的数据


图 9　篡改第 5 步发送的数据

3)窃听攻击

攻击者可截获认证过程中的传输信息,若攻击者可以通过分析截获数据得到系统敏感信息,该协议过程即为非安全。对本协议而言,敏感信息是标签更新的响应信号 $R_{i+1}$。标签通过发送 $R_{i+1}\oplus R_i$ 将新的响应信号 $R_{i-1}$ 传递给服务器,可以看做把 $R_i$ 当做加密密钥,对 $R_{i+1}$ 进行了加密,由于异或运算的单向性,如果攻击者不知道 $R_i$ 的具体数值,就无法获得 $R_{i+1}$。$R_i$ 由 PUF 电路生成,不存储在标签内部,且不以明文形式传输,因此即使攻击者通过窃听手段获取传输内容,也无法确定 $R_{i+1}$ 和 $R_i$。此外,标签发送的 $R'$和 $Auth2$ 通过 LED 算法进行加密,获得加密结果也无法反推出 $R_{i+1}$ 和 $R_i$,服务器发送的 $R_{i-1}$ 同理。因此窃听攻击只能获取标签的身份信息,无法破解认证过程的重要信息 $R_i$ 和 $R_{i+1}$,但标签 ID 在每次认证成功后都会更新,获得 ID 对破解认证没有帮助。

4)去同步攻击

去同步攻击属于常见 RFID 系统攻击方式,攻击者通

过拦截认证一方发出的信息，使双方信息更新不同步。对本协议而言，每次认证服务器都会存储新旧两个 ID，若攻击者拦截标签发出的认证成功信号，标签认为认证成功，更新身份码为 ID′，服务器认为认证失败，不会更新标签信息，但会存储发给标签的 ID′。下一次认证时，标签发送 ID′，此 ID 在服务器中依然被存储为该标签的身份码之一，因此服务器依然可以查找到标签信息并发送其对应的挑战信号 C。对标签而言，除 ID 外，标签内部不存储其他参数，因此不受去同步攻击的影响。仿真结果如图 10 所示。

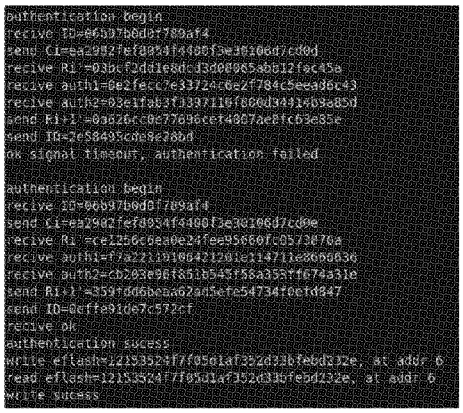


图 10　受到去同步攻击的两次认证

5)克隆攻击

攻击者通过仿制合法标签，制造和合法标签数据相同的芯片从而取代合法标签的手段称为克隆攻击。本协议中的标签可使用 PUF 模块抵抗克隆攻击，PUF 本身无法被复制，因此攻击者不可能对标签数据进行完全仿制。不过根据最新研究显示，如果攻击者能获得一个 PUF 足够多的挑战-响应对，就可以通过建模算法对 PUF 的输出结果进行预测[19]。但在本协议中，攻击者无法获得 PUF 响应信号的明文输出，无法获得大量的 PUF 具体输入输出值，就无法建立模型进行破解。

6)重放攻击

重放攻击指攻击者记录在通信过程传输的消息，并在接下来的认证过程中使用。本协议中，每次认证都会更新挑战-响应对，因此每次认证中发送的$\{R_i', Auth1, Auth2\}$并不相同，服务器不会通过验证。如图所示，本文通过模拟两次认证过程来验证该结论，如图 11 所示。

7)物理攻击

假设攻击者通过对合法标签进行物理探测，获得标签内部的存储信息，攻击者也无法获取能对系统安全构成威胁的信息。因为认证的重要信息为 PUF 的响应信号，该信号通过延迟电路生成，不会进行存储，且如果通过物理手段破解会改变 PUF 的输出。

8)前向安全性和后向安全性[20]

每次认证成功后，标签的 ID 和挑战响应对都会更新，且基于 PUF 输出的随机性，每个响应信号 R 之间不具有


图 11　重放攻击

关联性。即使攻击者通过窃听等手段获取其中一轮的{ID，$C$，$R$}，也无法推导出前一轮或后一轮的 $R$ 值。PUF 可为本协议的前向安全性和后向安全性提供保障。

综上，对于目前常见的 RFID 无线信道攻击手段，本协议都有抵御措施，可保证系统的机密性。

### 3.2　可用性分析

1)硬件资源消耗

本文在使用 verilog 语言实现 LED 算法后，使用 40 nm 工艺平台下的标准单元库对电路进行综合，综合结果显示，实现 LED 算法只需要 1 641 个门电路(如图 12 所示)。

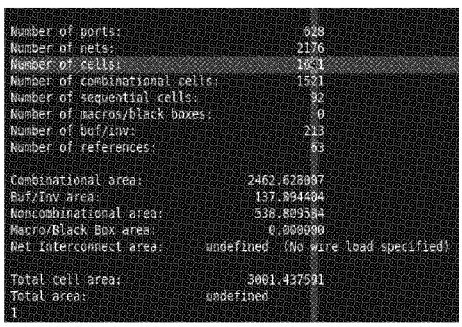


图 12　LED 算法的电路综合结果

此外本文利用相同的标准单元库对目前常见的 Hash 函数 MD5、SHA-256、SM3 的电路进行综合分析，对比结果如表 1 所示，可以看出 LED 算法所需门电路最少。

**表 1　各算法面积对比**

| 算法 | Cells | Combinational area | Tolal area |
|---|---|---|---|
| SM3 | 42 090 | 404 788 | 420 068 |
| MD5 | 8 001 | 18 362 | 21 756 |
| SHA-256 | 10 868 | 30 196 | 38 725 |
| LED | 1 641 | 2 463 | 3 001 |

2)协议安全性

从抗攻击能力的角度，将本文提出的认证协议与前文所述的 AKgun 协议[10]、BenDavid 协议[11]、Gope 协议[12]和 ZhuFeng 协议[13]对比，结果如表 2 所示。

**表 2　安全性能比较**

| 可抵御攻击类型 | 文献[10] | 文献[11] | 文献[12] | 文献[13] | 本协议 |
|---|---|---|---|---|---|
| 窃听攻击 | √ | √ | √ | √ | √ |
| 假冒攻击 | √ | √ | √ | √ | √ |
| 重放攻击 | × | × | × | × | √ |
| 篡改攻击 | √ | √ | √ | √ | √ |
| 去同步攻击 | √ | × | × | √ | √ |
| 标签跟踪 | × | √ | √ | √ | √ |
| 物理攻击 | × | × | √ | √ | √ |

从对比结果可知,和现有的基于 PUF 和 Hash 函数的 RFID 安全认证协议相比,本文提出认证方案能够够抵御更多攻击手段。

3)总结分析

从资源消耗角度分析,本协议使用的 LED 算法和其它 Hash 函数相比消耗的硬件资源更少,且不需要额外的密码算法或随机数发生器;从安全性角度分析,本协议的认证过程可抵御更多攻击手段。因此本协议的可用性更强,应用于 RFID 电子标签中可在达到更高安全性要求的情况下减小标签成本和面积。

## 4　结　　论

本文针对低成本无源 RFID 电子标签提出了一个基于 PUF 和 LED 算法的 RFID 安全认证协议。协议的突出特点是使用 PUF 和 LED 算法实现标签与服务器之间的双向身份认证,无需标签存储任何秘密参数,也无需使用随机数发生器。通过安全性分析与仿真结果证明本协议可提供的多种安全保障,可抵御目前常见的多种攻击方式。

本文提出的认证方案可应用于目前的无线通信网络,与现有的轻量级认证协议相比,本协议的算法复杂度低,硬件资源消耗少,具有成本低、实用性强、安全性高等优势。未来工作可引入更多加密算法机制,为 RFID 系统的安全提供进一步保障。

## 参考文献


[1] 叶乔. 采用 PUF 的云服务 RFID 系统认证协议的研究[D]. 无锡:江南大学,2021,DOI:10.27169/d.cnki.gwqgu.2021.001752.

[2] 张瑾瑾,张浩军. 物理不可克隆函数在 RFID 认证中的应用[J]. 中原工学院学报,2014,25(4):11-15.

[3] 李忠建,张雪凡,叶旸,等. 多标签环境下 RFID 系统的受限链路[J]. 电子测量技术,2016,39(1):9-13,DOI:10.19651/j.cnki.emt.2016.01.003.

[4] 李军. 自主标准 RFID 信令的分析设计及实践[J]. 国外电子测量技术,2017,36(9):82-85.

[5] 王冬生. 试分析物联网中的 RFID 技术及物联网的构建[J]. 中国信息化,2021(8):73-74.

[6] 曾飞. 面向物联网的轻量级 RFID 安全认证协议研究[D]. 北京:北京交通大学,2014.

[7] 丁杰. RFID 系统的安全认证协议研究与实现[D]. 南京:南京邮电大学,2019,DOI:10.27251/d.cnki.gnjdc.2019.001213.

[8] 刘登科,刘伟,宋贺伦,等. 一种 0.11 μm SRAM PUF 芯片的测试与分析[J]. 电子测量技术,2019,42(17):88-94,DOI:10.19651/j.cnki.emt.1902719.

[9] 张家梁. 一种基于 BCH 算法的 SRAM PUF 片的设计、测试与分析[D]. 合肥:中国科学技术大学,2021,DOI:10.27517/d.cnki.gzkju.2021.001719.

[10] AKGUN M, CAGLAYAN M U. Providing destructive privacy and scalability in RFID systems using PUFs[J]. Ad Hoc Netw, 2015, 32:32-42.

[11] BENDAVID Y, BAGHERI N, SAFKHANI M, et al. IoT device security: Challenging "A lightweight RFID mutual authentication protocol based on physical unclonable function"[J]. Sensors, 2018, 18(12), DOI:10.3390/s18124444.

[12] GOPE P, LEE J, QUEK T. Lightweight and practical anonymous authentication arotocol for RFID systems using physically unclonable functions[J]. IEEE Transactions on Information Forensics & Security, 2018, DOI:10.1109/TIFS.2018.2832849.

[13] ZHU F. New lightweight two-way RFID authentication protocol: PUF-LMAP[J]. Microcomputer and Application,2016,35(1):1-4.

[14] MANIFAVAS C, HATZIVASILIS G, FYSARAKIS K, et al. Lightweight cryptography for embedded systems-A comparative analysis[M]. Berlin Heidelberg:Springer, 2014:333-349.

[15] JUELS S A. Authenticating pervasive devices with human[J]. Proc Crypto, 2005, 3621:293-308.

[16] XU L, GUO J, CUI J, et al. Key-recovery attacks on LED-like block ciphers[J]. 清华大学学报自然科学版(英文版), 2019, 24(5):585-595.

[17] VAUDENAY S. On privacy models for RFID[J]. Advances in Cryptology ASIACRYPT 2007, Springer Berlin Heidelberg, 2007: 68-87.

[18] 张菁,余意,梅映天. 一种基于 PUF 的面向低成本标签的轻量级 RFID 安全认证协议[J]. 安徽水利水电职业技术学院学报,2019,19(2):48-51.

[19] RÜHRMAIR U, SEHNKE F, SÖLTER J, et al. Modeling attacks on physical unclonable functions[C]. Proceedings of the 17th ACM Conference on Computer and Communications Security,2010:237-249.

[20] 贺章擎,李红,万美琳,等. 一种基于 PUF 的两方认证与会话密钥交换协议[J]. 计算机工程与应用,2018,54(18):17-21.


## 作者简介


**王者**,工学硕士,主要研究方向为数字集成电路设计和测试验证。

**宋贺伦**(通信作者),博士,研究员,主要研究方向为半导体器件集成技术研究及应用。

E-mail:hlsong2008@sinano.ac.cn