基于多 PUF 模组的身份标识与身份认证机制研究

谢 峰,孟 坤*,张 旺,许嘉鑫,王启源
(北京信息科技大学 计算机学院,北京 100101)

摘 要: 身份认证是保护用户数据的第一道防线,为用户数据安全提供重要的保证。现有的身份认证方法均依赖于凭证服务提供商(CSP)等权威中心,信任其自身管控性和安全防护能力。但是,权威中心对身份标识具有绝对管控权,权威中心一旦失效将带来信息安全隐患。基于此,提出了一种基于多 PUF 模组的身份标识生成及身份认证机制,将 PUF 硬件指纹引入认证机制中,设计了一种去中心化身份认证机制。物理不可克隆功能(Physical Unclonable Function,PUF)描述了一种具有唯一性、不可篡改性的物理功能,已在身份认证领域得到了广泛应用,但其易受到使用环境等的影响而失效。现有的基于 PUF 的身份认证方法均未提供对 PUF 芯片失效的容忍方案。该文利用多 PUF 模组关联的方式,提出了提高身份认证机制可用性的解决方案。最后,对所提出的机制从安全性、可行性和可靠性三个方面进行了讨论和证明。

关键词: 去中心化; 物理不可克隆功能; 身份认证; 可靠性; 硬件指纹
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 1673-629X(2024)08-0073-05
doi: 10.20165/j.cnki.ISSN1673-629X.2024.0147

Research on Identity Generation and Identity Authentication Mechanism Based on Multi-PUF Modules

XIE Feng,MENG Kun*,ZHANG Wang,XU Jia-xin,WANG Qi-yuan
(School of Computer Science,Beijing Information Science and Technology University,Beijing 100101,China)

Abstract: Identity authentication serves as the primary line of defense for safeguarding user data,providing crucial assurance for the security of user information. Existing identity authentication methods rely on authoritative centers such as Credential Service Providers (CSP), trusting their self-control and security capabilities. However,authoritative centers possess absolute control over identity,and any failure in these centers may pose security risks to information. Considering this,we propose an identity generation and authentication mechanism based on multi-PUF modules,introducing PUF hardware fingerprints into the authentication process and designing a decentralized identity authentication mechanism. Physical Unclonable Function (PUF) describes a physically unique and tamper-resistant function widely applied in the field of identity authentication. However,PUFs are susceptible to environmental influences,leading to potential failures. Existing PUF-based identity authentication methods have not provided tolerance solutions for PUF chip failures. We propose a solution to enhance the usability of identity authentication mechanisms by utilizing a correlated approach with multiple PUF modules. Finally,we discuss and demonstrate the proposed mechanism in terms of security,feasibility,and reliability.

Key words: decentralization; physical unclonable function; identity authentication; reliability; hardware fingerprints

0 引 言

随着互联网技术的不断成熟,互联网用户的数量不断增加,对于互联网的安全性也越来越高。身份认证作为保护用户信息的第一道防线,为用户安全提供了重要的保证。根据 NIST SP 800-63(Digital Identity Guidelines)中定义的用于身份验证的通用模型,身份认证机制主要由数字身份(身份标识)和身份证明两部分构成。身份标识是用来唯一标识人或物身份的一种凭证,身份证明是确认一个主体在一定的可信度下就是其声称的对象,即验证身份标识的过程。因此身份标识是身份认证机制的核心要素,传统的身份标识主要包括三个方面:知识因素、内在因素和占有因素,用于回答“你知道什么”“你是谁”和“你拥有什么”这三个基本问题[1]。其中,前两种身份标识主要用于识别人的身份,而所有权则主要用于识别物的身份。身份证明使用挑战-应答的方式对身份标识进行对比验证,以实现对身份标识的识别。目前,主流的身份认证机制都将凭证服务提供商(CSP)颁发的凭证作为唯一

收稿日期: 2023-11-11 **修回日期:** 2024-03-14
基金项目: 北京教委 2019 年度科技计划一般项目(KM201911232002)
作者简介: 谢 峰(1999-),男,硕士研究生,研究方向为数据安全和身份认证;通信作者:孟 坤(1980-),男,副教授,博士,硕导,CCF 会员(18468),研究方向为数据安全和身份认证、网络安全与性能评价。

标识,CSP是指发现或注册订阅器的受信任实体,并通过挑战-应答的方式验证订阅者标识符的有效性[2-5]。该文将这种身份认证机制定义为中心化身份认证机制,中心化身份认证机制信任于权威中心的两个特点:自我管控性和安全防护。自我管控即保证自身不会作恶,安全防护即保证难以被外部攻击成功。当中心节点存在恶意行为,例如篡改用户认证信息时,用户自身无法阻止,其他用户也无法察觉,从而给用户的信息安全带来重大风险。因此,中心化身份认证面临着安全性和可靠性等方面的挑战,需要考虑更高效、更安全的替代方案。

去中心化是指摆脱绝对管控方,使得身份标识能够不受人为因素的影响,从而正确地标识身份。其目的在于使用一种超越现有认知水平的手段来阻止任何人或物对身份标识进行影响、控制。区块链技术通过由大量用户维护公共账本,依靠各个用户之间所持有信息的高度一致性来保证信息的正确性[6]。另一种方式是基于量子计算技术的身份标识。与传统的数字身份标识不同,量子身份标识使用量子比特来存储和处理身份信息。任何用户也无法对量子态进行篡改,摆脱绝对管控[7]。随着科技和互联网技术的快速发展,为适应物联网时代的需求,身份认证机制需要在保障安全性的前提下,确保认证高效、低成本、低功耗。如上所述,区块链技术需要大量用户维护网络内信息的正确性,要求大量存储空间且认证检索效率较低[8]。量子计算实现的身份标识在硬件、软件、网络等方面都需要高度专业化的支持[9],运行成本相对较高。因此,在实现去中心化的身份认证方式的同时,需要评估不同方案的安全性、效率以及成本等因素,以寻找最优解决方案。

物理不可克隆功能(Physical Unclonable Function,PUF)特性依赖于芯片特性和制造过程中随机差异,如工作环境、制作工艺等,产生的重要信息[10-11]。这些随机差异使得PUF具有不可克隆性和不可预测性,无法模拟和复制,为低成本高安全性的身份认证机制提供了安全保障[12]。这些不稳定的特性也导致PUF在不同的工作环境、工作电压等条件生成的CRPs对不稳定,甚至失效[13-14]。基于此,该文提出了一种基于多PUF模组的身份标识生成及身份认证机制,在机制中利用PUF硬件指纹生成身份标识,设计一种摆脱绝对管控方的去中心化身份认证机制。同时,利用多PUF模组关联的方式,提出了提高身份认证机制可用性的方案,保证在PUF功能出现故障时身份认证系统的可靠性以及用户数据的安全性。

该方案主要有以下贡献:

(1)将可信第三方替换成不可操控的物理特性(PUF)的背书,通过物理特性来生成身份标识保证去中心化。

(2)提出通过多PUF芯片组成PUF模组,提高PUF芯片失效后身份标识的可用性。

1 相关工作

PUF描述了一种具有唯一性、不可篡改性的物理功能,能够很好地保证身份标识所需要的特性。目前,最常被使用的PUF功能有基于仲裁器的PUF及其变体,环形振荡器PUF(RO-PUF),SRAM-PUF等。利用其生产制作过程中的随机特征,产生多个具有唯一性和不可复制特性的PUF输出。这种具有独特性质的PUF输出可以应用于密钥生成、IP保护和身份认证等多种领域。近几年的科学研究[15-23],验证了这一点。尽管PUF在身份认证领域已经得到了广泛的应用,但仍然存在着如绝对管控等问题。

Jiang Qi[13]等提出了用于车联网的AKE协议,协议中引入了PUF功能以确保用户设备或传感器受到损害,但需要将PUF的CRP信息存储在服务器中,如果攻击者控制了服务器,那么用户的信息安全就得不到保障。Chaterjee等[21]提出了一种基于私有PUF的方案,该方案确保即使PUF实例对用户是私有的,它也允许受信任方(组管理员或GM)对应用程序提供商(AP)的认证,并且不需要在一个安全的数据库中存储原始的CRP,从而使对手更难对部署的PUF发起建模攻击。但协议存在缺陷,当AP受到损害时,可能允许特定用户验证并使用该服务。Qureshi和Munir[23]提出了一种基于PUF的物联网设备认证身份保护协议,在认证事件期间,通过混淆技术来存储有关注册设备PUF的模糊信息,而不是存储明文CRP。但仍容易收到重放攻击,且存在安全单点故障问题。

2 基于多PUF模组的身份认证方案

该方案利用PUF的特性,生成可靠的身份标识,验证通信双方的身份合法性。方案采用无存储的方式进行身份标识的对比验证,实现去中心化。为避免PUF功能故障后的方案失效,该方案采用多PUF芯片关联形成PUF模组,通过PUF模组生成鲁棒性更高的身份标识,从而提高身份认证机制的可靠性。为了能够更好地说明工作过程,对提议的方案提供了详细的描述,表1列出了符号和描述。

提出的方案分为两个部分,即身份标识注册和身份证明。首先,用户需要在配置有PUF芯片的设备上进行身份标识注册。如果用户已经注册成功,下一步可与其他用户交换验证消息和生成会话密钥,以便进行进一步通信。

表 1　符号表述

符号	描述
U,V	用户名、身份标识
C	PUF 函数挑战问题
$P(*)$	PUF 函数描述
g,N	g 为随机素数, $\gcd(g,N)=1$
$\mathrm{hash}(*)$	哈希函数
$\varphi(*)$	欧拉函数

2.1　身份标识注册

相关方确认配置 PUF 驱动的身份认证机制,进行身份标识的注册。注册过程包括以下步骤: 首先,输入注册用户的名称 U; 接着,确认随机数 g,N 以及测量参数的实例; 最后,根据这些输入参数生成唯一的身份标识。具体流程如图 1 所示。

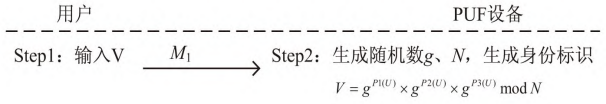

图 1　身份标识注册流程

2.2　身份认证机制流程

认证双方在公共通道上进行身份验证。该方案的认证过程如图 2 所示。

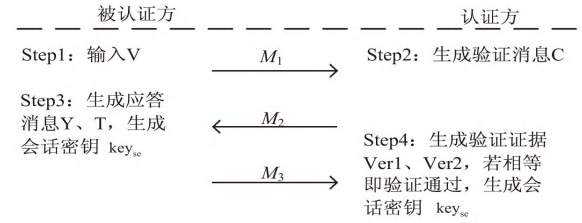

图 2　身份认证机制流程

Step1: 被认证方 → 认证方: $\{M_1\}$。被认证方发送或广播“身份名称+身份标识”消息,并向认证方发起请求 $M_1=<\mathrm{Request},U,V>$。

Step2: 认证方 → 被认证方: $\{M_2\}$。认证方收到请求访问后,选择随机数 x,生成身份认证验证信息 $C=g^x \bmod N$,并向被认证方发送消息 $M_2=<C,V>$。

Step3: 被认证方 → 认证方: $\{M_3\}$。被认证方生成应答信息 $Y=g^{P_1(C)\times P_2(C)\times P_3(C)} \bmod N$,

$$T=[\mathrm{hash}(Y)\times P_1(C)\times P_2(C)\times P_3(C)+P_1(U)+P_2(U)+P_3(U)] \bmod \varphi(N)$$

并生成会话密钥 $\mathrm{key}_{se}=C^{P_1(U)\times P_2(U)\times P_3(U)} \bmod N=V^x \bmod N$,之后向认证方发送消息 $M_3=<Y,T>$。

Step4: 认证方计算身份验证证据,认证方通过对方发送的信息 M_3 计算 $\mathrm{Ver}_1=V\times Y^{\mathrm{hash}(Y)} \bmod N$ 和 $\mathrm{Ver}_2=g^T \bmod N$。当 $\mathrm{Ver}_1=\mathrm{Ver}_2$ 时身份认证通过,并生成会话密钥; 否则认证失败。

2.3　PUF 功能失效容忍策略

文章提出的机制中,当 PUF 功能出现故障时将会输出缺省值 FAULT。计算验证证据时,仅当所有 PUF 输出均为默认值或 PUF 输出非来自原 PUF 时验证失败。所提出的机制保证当 PUF 芯片失效个数小于 3 时均可验证通过。

3　方案分析

一个优秀的身份认证机制可以保护系统免受非法攻击,为了分析方案在不同攻击模式下的安全性,假设通信双方之间的通信通道是不安全的,攻击者可以拦截和篡改该通道上传输的信息。在本节中,将进行该机制的可行性、安全性和可靠性分析。

3.1　可行性分析

该机制的设计是为了确保通信双方之间能够实现去中心化的相互验证,同时容忍 PUF 芯片失效,对此将用数学推理的角度从理论上说明该机制的可行性。

定理: 方案中的身份标识能够保证唯一性、不可篡改以及身份标识的验证性。

证明: 身份标识采用 PUF 功能生成的特定 CRPs 生成,由 PUF 本身的特性能够保证身份标识的唯一性。该方案采用离散对数对身份标识关键信息进行隐藏,并在认证过程中使用 hash 函数确保认证信息未被篡改。利用挑战应答的方式计算验证证据,当验证证据符合条件时即可验证通过。

推论一: 认证方拥有 PUF 芯片 P_1, P_2 和 P_3,在 PUF 芯片运行正常的情况下,身份验证机制能够正常验证身份标识。

证明: 在正常情况下计算身份验证证据

$$\mathrm{Ver}_1=V\times Y^{\mathrm{hash}(Y)} \bmod N=g^{P_1(U)}\times g^{P_2(U)}\times g^{P_3(U)}\times g^{\mathrm{hash}(Y)\times P_1(C)\times P_2(C)\times P_3(C)} \bmod N$$

和 $\mathrm{Ver}_2=g^T \bmod N$。由扩展欧拉定理:

$$g^x=g^{x \bmod \varphi(N)},\ \gcd(g,N)=1$$

可得:

$$\mathrm{Ver}_2=g^T \bmod N=g^{P_1(U)}\times g^{P_2(U)}\times g^{P_3(U)}\times g^{\mathrm{hash}(Y)\times P_1(C)\times P_2(C)\times P_3(C) \bmod N}=\mathrm{Ver}_1$$

当 $\mathrm{Ver}_1=\mathrm{Ver}_2$ 时,关键认证信息 $\mathrm{puf}(\cdot)$ 相等,即验证认证信息来自同一合法的 PUF 设备,验证通过。

推论二: 设认证方在持用 PUF 芯片有两个及以下芯片失效的情况下,身份验证机制能够正常验证身份标识。

证明: 机制设置当 PUF 芯片失效时,设置 PUF 输出为默认值 FAULT。在计算验证信息之前,当且仅当 $Y=g^{\mathrm{FAULT}^3} \bmod N$,即 3 个 PUF 均失效时立即返回验证失败信息。

3.2　安全性分析

在本节中,通过假设认证双方之间的通信通道并不安全,分析了该协议在应对部分与身份认证相关的

常见安全威胁时的系统安全保障机制。

(1) 伪装攻击。

伪装是指某个实体可以窃听、截取通信信道中标签和读取器所传输的信息,并利用这些信息伪造参数,欺骗系统的认证。在该方案中,使用离散对数来隐藏 PUF 关键信息。在不安全的信道中通信,即使攻击者截取了信道中的认证信息,想破解离散对数获得 PUF 信息来伪造参数是相当困难的。

(2) 重放攻击。

攻击者成功捕获合法用户的认证信息,并利用该信息请求认证,以欺骗合法用户或服务器。这种类型的攻击适用于不及时更新密钥的机制。相比之下,在提出的机制中,攻击者不能控制 PUF 的挑战。每次认证过程中,认证方会生成随机的挑战 $C = g^x \bmod N$ 来进行认证,尽管攻击者成功捕获了某一次的认证信息,也无法进行重放攻击。

(3) 防克隆。

该方案利用 PUF 芯片在制作过程中的独特差异,随机生成 CRPs 作为关键信息。而这些差异使得 PUF 芯片无法通过复制等手段获得一个 PUF 副本,因此该方案能够防止克隆关键信息。

(4) 防篡改。

该机制使用 hash 函数和质询-响应的概念来验证消息的来源、完整性和新鲜度。接收方可以使用 hash 函数来识别接收到的消息的任何更改。

3.3 可靠性分析

该方案采用 3 个 PUF 芯片组成 PUF 模组,其中 PUF 芯片之间互相独立、互不干扰,利用每个 PUF 芯片产生的应答消息生成的身份标识。一旦确定了单个 PUF 的质量指标,就可以计算出 PUF 模组的质量指标。理想情况下,假设每个 PUF 部件输出是独立的,设 PUF 的故障率分别为 λ_1,λ_2,λ_3。通过对比验证不同关联关系以及不同关联个数的故障率来说明方案的可靠性。

(1) PUF 输出的关联关系。

(a) 异或⊕: 对 PUF 的输出进行逐位异或运算,此时 PUF 模组的故障率为 $\lambda = 1 - (1 - \lambda_1) \times (1 - \lambda_2) \times (1 - \lambda_3)$。使用异或操作时,PUF 模组中个别 PUF 出现故障则不能产生正确响应。

(b) 级联||: 对 PUF 输出进行简单的拼接操作,此时 PUF 模组的故障率为 $\lambda = \lambda_1 \times \lambda_2 \times \lambda_3$。这种情况下,每个 PUF 部件的输出都相对独立互不影响。

(c) 嵌套◁: 将 puf1 的响应作为 puf2 的挑战,此时 puf2 的挑战空间由 puf1 控制,PUF 模组的故障率为 $\lambda = 1 - (1 - \lambda_1) \times (1 - \lambda_2) \times (1 - \lambda_3)$,这种情况下,单一 PUF 的出错会导致整个 PUF 模组的故障响应。

根据不同关联关系的特性可以看出,异或操作和嵌套操作在可靠性方面与级联相比较为不足且耦合性较高。同时,异或与嵌套在设计复杂度和计算复杂度上开销也更大。因此,该方案选择使用实现较为简单且可靠性较高的级联操作进行 PUF 模组的设计。

(2) 实验分析。

实验环境: 操作系统: Windows10; PUF 类型: Sram PUF。

图 3 为所用 PUF 实现路径,以上电作为 PUF 的挑战,对应 Sram 单元的内存值为应答。该文提取了 Sram 单元的 256 位作为 PUF 的应答值。由于 Sram 单元的物理特性,部分单元在不同次上电中会存在零与一之间随机跳转的现象,因此该文采用了 31 位 BCH 编码,对 Sram PUF 值进行纠正。

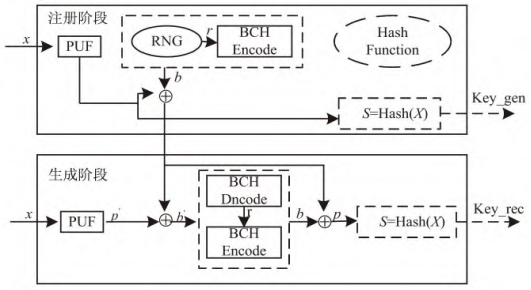

图 3 Sram PUF 工作流程

在对 PUF 进行 3 000 次上电挑战后,统计 PUF 出现故障次数,如图 4 所示,PUFs 的平均故障率为 0.518%。

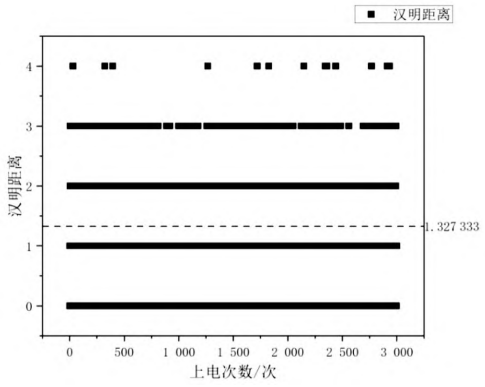

图 4 Sram PUF 应答汉明距离

表 2 批量实验对比

PUF 个数	故障率/%
2	0.268
3	0.139
4	0.072

采用上述设计进行 1 000 次批量实验,计算方案的成功率。多次实验后计算平均值(见表 2),显示当级联 PUF 个数为 2 时,方案失败率为 0.268%; 当级联 PUF 个数为 3 时,方案失败率为 0.139%; 当级联 PUF 个数为 4 时,方案失败率为 0.072%。实验表明当有

PUF 功能失效时,机制能够正常运行。随着 PUF 个数的增加,机制的容错率随之增加,但同时带来的体积负担也随之增加。

4　结束语

提出了一种基于多 PUF 模组的身份标识生成与身份认证机制,并从数学上证明了身份标识的可验证性。该方案通过 PUF 芯片注册身份标识来实现去中心化,使用多 PUF 级联的方式,保证有一个 PUF 芯片正常即可通过验证,提高身份认证机制的可靠性,并通过实验对可靠性进行了进一步的验证。实验表明该方案具有可行性、安全性和可靠性,为去中心化身份认证机制提供了新的研究思路。

参考文献:

[1] WANG C,WANG Y,CHEN Y,et al.User authentication on mobile devices: approaches,threats and trends [J].Computer Networks,2020,170: 107118.

[2] MA S,FENG R,LI J,et al.An empirical study of sms one-time password authentication in android apps [C]//Proceedings of the 35th annual computer security applications conference.San Juan: ACM,2019: 339-354.

[3] JIANG Q,ZHANG X,ZHANG N,et al.Three-factor authentication protocol using physical unclonable function for IoV [J].Computer Communications,2021,173: 45-55.

[4] SIDDIQUI Z,GAO J,KHAN M K.An improved lightweight PUF - PKI digital certificate authentication scheme for the Internet of Things [J].IEEE Internet of Things Journal,2022,9(20): 19744-19756.

[5] YADAV B P,PRASAD C S S,PADMAJA C,et al.A coherent and privacy-protecting biometric authentication strategy in cloud computing [J].IOP Conference Series: Materials Science and Engineering,2020,981(2): 022043.

[6] MONRAT A A,SCHELÉN O,ANDERSSON K.A survey of blockchain from the perspectives of applications,challenges,and opportunities [J].IEEE Access,2019,7: 117134-117151.

[7] PADAMVATHI V,VARDHAN B V,KRISHNA A V N.Quantum cryptography and quantum key distribution protocols: a survey [C]//2016 IEEE 6th international conference on advanced computing (IACC).Bhimavaram: IEEE,2016: 556-562.

[8] LI X,JIANG P,CHEN T,et al.A survey on the security of blockchain systems [J].Future Generation Computer Systems,2020,107: 841-853.

[9] SINGH A,DEV K,SILJAK H,et al.Quantum internet—applications,functionalities,enabling technologies,challenges,and research directions [J].IEEE Communications Surveys & Tutorials,2021,23(4): 2218-2247.

[10] LIANG W,LIAO B,LONG J,et al.Study on PUF based secure protection for IC design [J].Microprocessors and Microsystems,2016,45: 56-66.

[11] IGIER M,VAUDENAY S.Distance bounding based on PUF [C]//Cryptology and network security: 15th international conference.Milan: Springer,2016: 701-710.

[12] AL-HAIDARY M,NASIR Q.Physically unclonable functions (PUFs): a systematic literature review [C]//2019 advances in science and engineering technology international conferences (ASET).Dubai: IEEE,2019: 1-6.

[13] 徐太忠,杨天池,程　娟,等.基于纠错码模糊提取器的 SRAM-PUF 设计方法 [J].计算机科学,2016,43(S2): 373-376.

[14] LIANG W,XIE S,ZHANG D,et al.A mutual security authentication method for RFID-PUF circuit based on deep learning [J].ACM Transactions on Internet Technology,2021,22(2): 1-20.

[15] AYSU A,GULCAN E,MORIYAMA D,et al.End-to-end design of a PUF-based privacy preserving authentication protocol [C]//Cryptographic hardware and embedded systems-CHES 2015: 17th international workshop.Saint-Malo: Springer,2015: 556-576.

[16] 张效林,谷大武.一种基于 PUF 的可证明安全消息认证算法及应用 [J].中国科学: 信息科学,2022,52(12): 2336-2350.

[17] BARBARESCHI M,DE BENEDICTIS A,MAZZOCCA N.A PUF-based hardware mutual authentication protocol [J].Journal of Parallel and Distributed Computing,2018,119: 107-120.

[18] 徐　森,刘佳鑫,杨　硕,等.基于切比雪夫混沌映射和 PUF 的 RFID 三方认证协议 [J/OL].计算机应用研究: 1-6 [2023-10-29].https://doi.org/10.19734/j.issn.1001-3695.2023.06.0263.

[19] BANSAL G,NAREN N,CHAMOLA V,et al.Lightweight mutual authentication protocol for V2G using physical unclonable function [J].IEEE Transactions on Vehicular Technology,2020,69(7): 7234-7246.

[20] LEE T F,CHEN W Y.Lightweight fog computing-based authentication protocols using physically unclonable functions for internet of medical things [J].Journal of Information Security and Applications,2021,59: 102817.

[21] CHATERJEE U,MUKHOPADHYAY D,CHAKRABORTY R S.3PAA: a private PUF protocol for anonymous authentication [J].IEEE Transactions on Information Forensics and Security,2020,16: 756-769.

[22] CHUANG Y H,LEI C L.PUF based authenticated key exchange protocol for IoT without verifiers and explicit CRPs [J].IEEE Access,2021,9: 112733-112743.

[23] QURESHI M A,MUNIR A.PUF-IPA: a PUF-based identity preserving protocol for Internet of Things authentication [C]//2020 IEEE 17th annual consumer communications & networking conference (CCNC).Las Vegas: IEEE,2020: 1-7.