Artificial Intelligence and Robotics Research 人工智能与机器人研究, 2026, 15(1), 222-231
Published Online January 2026 in Hans. https://www.hanspub.org/journal/airr
https://doi.org/10.12677/airr.2026.151022

Hans汉斯

去中心化的身份标识与认证方案

庞　晖，孟　坤，王启源

北京信息科技大学计算机学院，北京

收稿日期：2025年12月11日；录用日期：2025年12月31日；发布日期：2026年1月13日

摘　要

传统身份认证中私钥重复使用及中心化密钥管理带来一定的安全隐患。本文引入物理不可克隆函数(Physical Unclonable Functions, PUF)技术，代替传统公钥基础设施(PKI)分发密钥，通过利用PUF的高度随机性和唯一性，实现同一用户在不同系统或应用场景中动态生成独立且唯一的私钥，避免了私钥重复使用导致的撞库攻击风险以及私钥静态存储带来的内存泄漏攻击风险。该方法不仅增强了身份认证过程的安全性和隐私保护，还提升了多场景身份隔离能力，为构建去中心化、可信赖的身份认证体系提供了新的技术路径。安全分析表明，该方案能有效抵御撞库、身份伪造、内存泄漏等攻击，适用于隐私保护要求高的身份认证场景。实验结果表明，在具体的应用场景中验证了方案的可行性和有效性。

关键词

物理不可克隆函数，椭圆曲线，身份标识，身份认证，去中心化

Decentralized Identity Identification and Authentication Scheme

Hui Pang, Kun Meng, Qiyuan Wang

Computer School, Beijing Information Science & Technology University, Beijing

Received: December 11, 2025; accepted: December 31, 2025; published: January 13, 2026

Abstract

In traditional authentication systems, the reuse of private keys and centralized key management introduce certain security risks. This paper introduces Physical Unclonable Function (PUF) technology to replace the traditional Public Key Infrastructure (PKI) for key distribution. By leveraging the high randomness and uniqueness of PUFs, the method enables the dynamic generation of independent and unique private keys for the same user across different systems or application scenarios, thereby preventing credential-stuffing attacks caused by private-key reuse and memory-leakage

文章引用: 庞晖, 孟坤, 王启源. 去中心化的身份标识与认证方案[J]. 人工智能与机器人研究, 2026, 15(1): 222-231.
DOI: 10.12677/airr.2026.151022

attacks arising from static private-key storage. This approach not only enhances the security and privacy protection of the authentication process but also improves identity isolation across multiple scenarios, offering a new technical pathway for building decentralized and trustworthy authentication systems. Security analysis shows that the proposed scheme can effectively resist credential-stuffing, identity forgery, memory-leakage, and other attacks, making it suitable for authentication scenarios with high privacy-protection requirements. Experimental results demonstrate the feasibility and effectiveness of the scheme in specific application contexts.

Keywords

Physical Unclonable Function, Elliptic Curve, Identity Identification, Authentication, Decentralization

1. 引言

身份认证技术是在计算机网络中确认操作者身份的一种有效手段，其核心目标是解决“你是谁”的问题。通过特定的验证机制，该技术确保只有经过授权的合法用户才能访问受保护的资源或服务[1]。身份标识则是用于证明个人或机构身份的法定凭证，其基本作用是向系统或他人表明“我是谁”[2]。这类标识具有排他性，必须由身份主体本人持有和使用。可以说，身份标识是身份认证的前提，而身份认证则是验证该标识真实性和有效性的过程。由于身份认证能够有效确认用户身份的合法性，因此在信息安全体系中具有关键作用。缺乏可靠的认证机制，系统就无法准确识别访问者，从而容易导致数据泄露、非法访问等安全风险。基于椭圆曲线密码学(Elliptic Curve Cryptography, ECC)的身份标识与认证技术近年来在信息安全领域得到广泛关注[3]。与传统公钥加密算法相比，ECC 通过更短的密钥长度即可实现相同甚至更高的安全强度，其计算效率高、资源消耗低、适应性强，特别适用于物联网设备、智能终端等资源受限环境。椭圆曲线算法的核心优势在于其基于离散对数问题的数学困难性，使得从公钥推算私钥几乎不可行，从而确保身份标识的唯一性与认证过程的抗攻击性。相比传统的 RSA 等算法，ECC 在密钥管理与认证交互中的数据传输量更小、执行速度更快，可以有效降低身份认证系统的计算负担与通信延迟，为构建轻量化、高强度的身份安全机制提供了坚实的数学基础[4]。因此，基于椭圆曲线的身份标识与认证在保证安全性的同时，兼具高效性与可扩展性，成为新一代可信身份管理体系的重要发展方向。

在身份标识过程中，私钥的管理与使用方式仍是影响系统整体安全的关键问题。传统身份体系中普遍存在同一用户在不同系统或平台上重复使用相同私钥的现象，这种做法虽然在使用上具有便利性，却潜藏严重的安全隐患。用户通常为了减少密钥管理的复杂度、避免频繁生成与备份新密钥，选择在多个应用场景中使用相同的私钥。一旦某一平台的密钥或认证数据被泄露，攻击者即可利用已知的私钥信息在其他平台上进行批量尝试，从而通过“撞库”手段实现身份冒用[5]。此类攻击不依赖算法漏洞，而是利用用户行为上的重复使用密钥特性实现跨系统的身份伪造，使得身份标识的唯一性和独立性受到破坏。私钥重复使用还使得不同平台之间的身份信息产生可关联性，进一步增加了隐私泄露与身份跟踪的风险。因此，在基于椭圆曲线的身份标识体系中，如何防止私钥重复使用并确保其不可滥用，成为影响认证安全性的核心问题之一。

在身份认证过程中，认证方希望认证过程安全可靠，能够确认通信对象确为其声称的身份，防止冒

充与伪造；而被认证方则希望在完成认证的同时，其私钥及真实身份信息不被泄露或记录，防止被追踪与滥用。传统的身份认证机制通常依赖中心化的 PKI 架构或服务器数据库，通过证书管理机构(Certificate Authority, CA)实现密钥生成与分发[6]。在该体系中，CA 负责为用户生成或签发公钥证书，认证服务器通过验证证书签名与公钥绑定关系来确认身份。密钥分发过程包括密钥生成、证书颁发、传输与存储等环节，这一流程在理论上确保了身份认证的可验证性与可信性。然而，在实际应用中，密钥分发的中心化特征带来了新的安全风险[7]。一方面，CA 或密钥管理服务器作为信任节点，一旦遭受攻击或被恶意控制，攻击者便可能伪造证书或篡改公钥，导致大规模的身份伪造事件；另一方面，密钥分发与存储过程往往需要在通信信道中传输公钥或证书数据，如果加密或认证机制不完善，攻击者可以通过中间人攻击或数据篡改破坏密钥完整性。此外，用户在认证时通常需要向服务器提交签名或凭证，服务器会将这些身份数据记录或存储，用于后续验证或审计，这在无形中增加了身份信息泄露的风险。虽然这种中心化密钥管理体系能够实现基本的身份验证功能，但在面对数据库泄露、重放攻击以及多平台关联分析时，难以同时满足认证方的安全要求与被认证方的隐私保护需求。认证方虽然能够验证用户身份，但一旦认证服务器或 CA 被攻破，用户的密钥数据及身份映射信息将面临大规模泄露；而被认证方在认证过程中，其身份特征会长期保留在中心服务器中，缺乏有效的隐私防护与动态更新机制。这种依赖集中管理的体系在分布式、异构网络环境下安全性脆弱，难以支撑高安全和高隐私要求的身份认证需求。

为解决上述问题，物理不可克隆函数(Physically Unclonable Function, PUF)被引入到基于椭圆曲线的身份标识与认证体系中，成为保障密钥安全与提升身份可信性的有效手段。PUF 利用硬件制造过程中随机形成的微观物理差异，为每个设备提供唯一且不可复制的物理特征，可被视为设备层面的“硬件指纹”[8]。通过将 PUF 作为私钥生成的设备，可以在不依赖非易失性存储器的情况下动态地产生私钥，从而避免私钥的长期保存，彻底消除因密钥因存储而导致的泄露风险[9]。PUF 的输出依赖于设备的固有物理特性，即使攻击者掌握系统结构，也无法通过建模或复制获得相同的响应。PUF 的一个重要优势在于其对输入挑战的高度敏感性，只要输入不完全相同，PUF 就会产生截然不同的响应。基于这一特性，同一用户可以在不同的系统或应用场景中通过不同的挑战输入，动态生成各自独立且唯一的私钥。这种机制有效避免了传统身份认证中因私钥重复使用而导致的撞库攻击风险。具体而言，用户使用同一 PUF 设备生成私钥，通过使用不同的挑战进而输出不同的私钥，使得每个系统中的身份标识相互独立，无法通过一处泄露推导出其他场景下的身份密钥。由此，PUF 不仅增强了私钥的动态性和唯一性，还实现了多场景下身份隔离和隐私保护，极大提升了整体身份认证体系的安全性和抗攻击能力。同时，在认证方利用 PUF 存储被认证方的公钥，使得不同认证方的数据库中存储的同一被认证方的公钥信息各不相同。即使是同一个被认证方，其在不同认证方处的公钥也无法被关联或复用。因此，即便攻击者试图冒充被认证方并篡改认证方数据库中的公钥信息，由于缺乏对应的 PUF 响应验证，篡改行为无法通过身份验证，从而有效防止了公钥伪造和身份冒用的风险，显著提升了身份信息管理的安全性和可信度。综上，PUF 在基于椭圆曲线的身份标识与认证体系中[10]，不仅从根本上提升了私钥的安全性与唯一性，也在身份信息管理和隐私保护方面发挥了关键作用，为构建去中心化、安全可信的身份认证机制提供了新的解决方案。

因此，本文提出了一种基于 PUF 的去中心化身份标识与认证方案，无需存储私钥，使同一被认证方在不同认证方中可生成不同的公私钥对，从而有效缓解因身份信息重复使用而导致的撞库攻击风险。该方案不仅适用于用户，也适用于智能体、物联网设备、软件程序等多种身份主体，具备广泛的适用性与扩展性。本文的主要贡献如下：

1) 设计一种适用于不同身份标识的生成方法，为同一被认证方生成多个彼此无关联且难以伪造的身份标识；

2) 提出一种去中心化身份认证方案，该方法结合 PUF 与椭圆曲线，有效增强对抗攻击者的能力。

2. 方案设计

利用 PUF 的独特特性生成用户身份标识，构建去中心化的身份认证机制，适用于多种场景和主体交互，为不同应用环境提供安全可靠的身份认证方案。表 1 中列出了各符号的具体含义。

Table 1. Symbol meaning
表 1. 符号含义

符号	含义
sk	私钥
pk	公钥
G	椭圆曲线的基点
Q	椭圆曲线的阶
PUF(*)	PUF 函数
HASH(*)	哈希函数
u	用户名
c	挑战

2.1. 设计身份标识

该身份标识的设计要为用户或设备在不同的场景中生成不同的身份标识，用户或设备有极大的自主权，可以自主决定并定制在不同场景中的身份标识。

2.1.1. 选择数据项

用户可以自主选择参与身份标识生成的具体数据项内容及其数量，以实现个性化和可控的身份管理，同时增强可扩展性。用户选择的数据项数量越多，且所选内容中包含具有强唯一性的标识(如身份证号等)，就能为身份认证过程提供更高的安全保障，有效降低身份被冒用或仿造的风险。同时，由于不同场景下用户可根据需求灵活搭配不同的数据项组合，而非依赖固定的单一标识，这可以有效避免因信息重复而导致的“撞库”问题，让身份管理在安全与灵活性之间达到更优平衡。

2.1.2. 数据处理

为确保后续计算环节对不同类型与格式的数据项实现统一化处理，需首先对用户或设备选定的数据进行处理操作。具体而言，去除数据中包含的空格、特殊符号等非必要字符，并将所有数据统一转换为二进制格式，以保证后续计算的一致性。若用户未选择任何数据项，则直接跳过该处理步骤。

在上述步骤完成后，对有效数据项执行逐位异或运算。为确保运算的正确性，需要对所有参与运算的数据项进行长度对齐处理，即通过在最前端补“0”的方式，使所有数据项的二进制长度与最长数据项保持一致，并逐位执行异或运算。若未选择数据项或仅选择单个数据项，则无需执行异或操作。

为增强随机性，将认证方的 ID 作为输入参数传递给 PUF 模块，由该模块生成的输出结果将作为盐值，并与异或运算结果按顺序进行拼接，从而得到最终的输入参数\mu。该设计确保了即便在数据项缺失的情况下，仍能通过盐值机制维持基本的安全特性。并且，由于不同用户拥有的 PUF 不同，使得最终得到的输入参数也就不同，呈现出更强的随机性和不可预测性。

2.1.3. 身份标识生成

得到输入参数后，对其进行哈希，并计算哈希值 $h = HASH(\mu)$。将 h 输入到 PUF 中，所得输出作为

私钥。只要是用户本人以及其所拥有的 PUF，即可无需存储任何信息，每次都能重新生成相同的私钥，用于身份认证。然后基于椭圆曲线密码学生成对应的公钥，即：

$$sk = PUF(h) \tag{1}$$

$$pk = sk * G \tag{2}$$

最终，得到可用于不同场景中的身份标识(sk, pk)。

2.2. 身份注册流程

图 1 所示为身份注册的流程图。在身份注册过程中，主要是由被认证方将其公钥发送给认证方，从而完成身份信息的注册与认证准备。当被认证方首次参与认证过程时，其身份注册的具体流程如下(其中 PUF_1 为被认证方拥有的 PUF， PUF_2 为认证方拥有的 PUF)：

1) 被认证方首先计算其身份标识，并向认证方发送包含用户名与公钥的信息，即消息$\{u, pk\}$。

2) 认证方接收到该信息后，计算

$$P = PUF_2(pk) \tag{3}$$

存储 u 和 P。由于 PUF 的不可克隆特性，使用此存储公钥的方式，对于同一被认证方，不同认证方所保存的各不相同。这使得攻击者若想通过篡改认证方数据库中的公钥来实施攻击，将面临极大的难度。

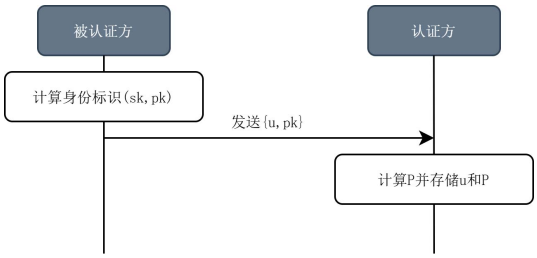

Figure 1. Identity registration flowchart
图 1. 身份注册流程图

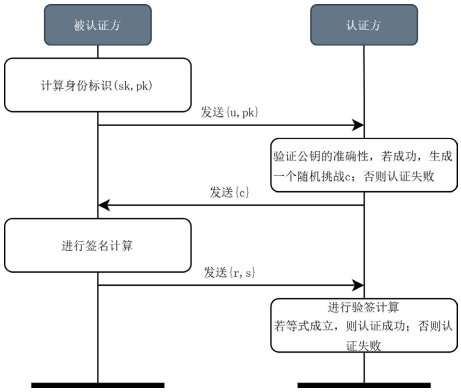

Figure 2. Identity authentication flowchart
图 2. 身份认证流程图

2.3. 身份认证流程

身份认证流程结合了 PUF 和椭圆曲线，实现单向的身份认证。图 2 所示为身份认证流程图。具体步

骤如下(其中 PUF_1 为被认证方拥有的 PUF， PUF_2 为认证方拥有的 PUF)：

1) 被认证方首先计算其身份标识，并向认证方发送包含用户名和公钥的信息，即 $\{u, pk\}$ 。

2) 认证方接收到该信息后，验证公钥的准确性，即计算 $PUF_2(pk)$ 并将计算结果与预存的 P 进行对比。若二者不一致，则说明不是被认证方本人，或者数据库中存储的公钥有误，即认证失败；若一致，则继续进行签名认证，由认证方生成并发送一个随机挑战 $\{c\}$ 给被认证方。

3) 被认证方接收到挑战后，选取随机数

$$k = PUF_1(u)PUF_1(c) \bmod q \tag{4}$$

计算过程借助了 PUF 的随机性特性，从而显著提升了随机数的随机性。同时，计算过程中，该随机数与认证方发来的信息 c 进行绑定，确保签名认证是专为该认证方参与本次认证过程而进行的。此设计还显著提升了本方案的抗攻击能力，有效防范重放的安全威胁。得到随机数后 k，被认证方进行签名计算：

$$kG = (x_1, y_1) \tag{5}$$

$$e = HASH(c) \tag{6}$$

$$r = x_1 \bmod q \tag{7}$$

$$s = k^{-1}(e + r \cdot sk) \bmod q \tag{8}$$

签名计算完成后，被认证方将结果发送给认证方 $\{r, s\}$ 。

4) 认证方接收到签名消息后，进行验签计算：

$$e = HASH(c) \tag{9}$$

$$u_1 = es^{-1} \bmod q \tag{10}$$

$$u_2 = rs^{-1} \bmod q \tag{11}$$

$$u_1 \cdot G + u_2 \cdot pk = (x_2, y_2) \tag{12}$$

认证方验证 $r = x_2 \bmod q$ 是否成立。若成立，则认证成功；否则，认证失败，签名无效。

2.4. 实现与验证说明

为验证所提出方案的可行性，本文在本地实验环境中进行了初步实现与测试。实验所采用的 PUF 为 SRAM PUF 设备，使用 C 语言实现，选取 P-256 椭圆曲线、SHA-256 哈希函数来实现身份认证过程。通信部分基于 Winsock 提供的套接字接口，实现客户端与服务器之间的身份认证交互。

3. 安全性分析

为了全面评估本方案的有效性与鲁棒性，本文从非形式化分析与形式化证明两个层面对其进行综合分析。在非形式化分析方面，主要从以下维度展开探讨：抗内存泄漏攻击能力、抗撞库攻击能力、抗伪造攻击能力和抗重放攻击能力。在形式化证明方面，本文借助 Scyther 工具对协议的关键安全属性进行建模与自动化验证，以确保其在逻辑层面具备严密的安全保障。

3.1. 非形式化分析

3.1.1. 抵抗内存泄露攻击

在传统身份认证系统中，私钥通常被加载并存储在主内存中。然而，此类设计易受到冷启动攻击的威胁。该攻击方式通过在设备断电后迅速重启系统，利用动态随机存取存储器(Dynamic Random Access

Memory, DRAM)在短时间内数据不完全失效的特性，从中恢复内存中残留的私钥信息。一旦攻击者成功窃取私钥，便可伪造用户身份或实施克隆攻击，对系统安全性构成严重威胁[11]。而在本方案中，身份标识的生成是在每次认证过程中动态生成的，并不会使用任何的内存，从根本上规避了此类安全问题。

3.1.2. 抵抗撞库攻击

撞库攻击通常利用用户在多个平台上重复使用相同密码的习惯进行入侵[12]。而 PUF 所具有的随机性特征，能够有效降低此类攻击的风险。具体而言，只要 PUF 的输入略有不同，其输出就会发生显著变化，这种变化高度不可预测，且在统计上趋近于均匀分布。PUF 输出的高度随机性确保了不同输入所对应的响应在整个输出空间中呈现出强离散性和最小相关性。这一特性不仅显著降低了攻击者通过建模或重构手段还原 PUF 行为的可能性，也为防范撞库攻击提供了有效解决方案。

3.1.3. 抵抗伪造攻击

攻击者通过伪造合法用户的身份标识，试图绕过认证机制，从而获得对系统资源的非法访问[13]。本方案通过将身份信息与 PUF 设备的物理特性进行强绑定，来抵御此类伪造攻击。每个用户都拥有一个专属的 PUF，只有其本人及其 PUF 设备能够生成有效的身份标识，确保身份认证的唯一性与不可伪造性。PUF 通过提取硬件在制造过程中自然形成的微观结构随机差异，生成具有物理唯一性的数字指纹。这种基于半导体工艺偏差产生的随机响应，既无法通过软件算法模拟或预测，也难以借助物理逆向工程进行复制，其输出结果具备高度的唯一性与稳定性。依托 PUF 的硬件级防护机制，从物理层面实现了密钥在硬件中生成、在硬件中使用、永不离开硬件的安全闭环，有效阻断了身份伪造的技术路径。

3.1.4. 抵抗重放攻击

尽管攻击者无法伪造有效的认证数据，但仍可能通过截获并重放先前的认证数据包，冒充合法用户，从而实施重放攻击[14]。为防范此类攻击，必须确保每次认证过程中所使用的消息均不重复。本身份认证方案通过对挑战 c 进行签名，且每次认证均使用不同的挑战 c，从根本上避免了消息的重复使用。此外，签名过程中所用随机数 k 的选取依赖于 PUF 设备，进一步增强了其随机性与唯一性，有效提升了对重放攻击的抵抗能力。因此，在本方案中，只要能确保每次认证过程中的挑战 c 各不相同，就可以做到抵抗重放攻击。

3.2. 形式化证明

为了验证所提方案的安全性，本文采用了开源形式化分析工具 Scyther [15]，该工具由 Cas Cremers 开发，主要基于 Dolev-Yao 模型对协议的安全性进行验证。它通过安全协议描述语言定义协议，能够检测密钥泄露、伪装攻击等多种安全漏洞，并以可视化方式展示攻击路径。Scyther 支持无限会话验证和多协议并行分析，同时具备高效的搜索算法，有效避免状态爆炸问题，适合分析参与方较少且依赖第三方加密的安全协议。它广泛应用于安全协议的设计验证、漏洞检测以及学术研究中，帮助用户确保协议的安全性和可靠性。

本文在 Scyther 中对方案进行建模，设定了两个通信实体：角色 A 表示被认证方，角色 B 表示认证方。鉴于 Scyther 工具对运算模型的支持具有一定限制，本文将方案中的 PUF 函数抽象为哈希函数处理，其余密码操作则依据方案实际流程建模。通过设置 Secret 声明验证密钥与会话密钥的机密性安全性，设置 Alive 声明验证通信对方是否确实参与过协议执行。分析结果表明 Scyther 工具在当前建模与攻击假设下未发现针对所提协议的有效攻击路径，表明该协议具备较好的安全性。由于在 WSL (Windows Subsystem for Linux)环境下部署的 Scyther 工具未启用图形化界面(GUI)支持，实验结果主要通过命令行输出和日志分析进行验证。Scyther 工具分析结果如图 3 所示。

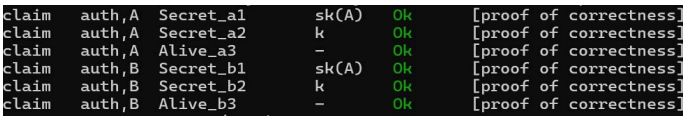

Figure 3. Analysis results of the Scyther
图 3. Scyther 工具分析结果图

4. 应用场景与实现方案

该身份标识与认证方案可以广泛适用于各种应用场景中。本节中具体写该方案在智能物联网医疗设备身份认证场景中的实现过程。

4.1. 场景描述

随着医疗信息化和物联网技术的快速发展，现代医院逐步引入大量智能医疗设备，如可穿戴健康监测仪、输液泵、血糖监测仪、远程心电采集终端等。这些设备能够通过无线网络实时采集患者的生理数据，并将数据传输至医院云端系统进行分析与存储，从而实现远程诊断、智能预警与个性化治疗。

但在医疗物联网场景中具有以下显著特征：设备数量庞大且分布广泛，医院内外联网设备众多，设备身份管理复杂；终端计算与存储能力有限，设备芯片资源受限，无法承担高强度密码学运算；传输的是患者实时生理数据，属于个人敏感信息，任何泄露或篡改都可能引发医疗事故与法律风险；通信环境复杂多变，无线传输易受干扰和攻击，如窃听、伪造、重放等。因此，建立一个既安全可靠又轻量高效的身份标识与认证机制，对保障医疗物联网系统的可信运行具有关键意义。

现假设用户 A 需要使用三个医疗设备进行健康检测，即用于采集心电信号的智能心电监测仪、用于监测血压变化的智能血压计和用于检测血糖水平的智能血糖监测仪。

4.2. 身份标识生成过程

对于心电监测仪设备，用户 A 自主选择用户 ID、手机号和设备 ID 作为生成身份标识的信息，即“A + 12312341234 + 心电监测仪”，并将信息输入到用户 A 拥有的 PUF_1 中。PUF_1 对“A”计算得到 data，接着对“A + 12312341234 + 心电监测仪 + data”进行计算，其结果作为用户 A 私钥 sk_1，并计算相应的公钥 pk_1，得到用户 A 在心电监测仪设备中可以使用的身份标识 (sk_1, pk_1)。

对于血压计设备，用户 A 自主选择用户 ID、身份证号和设备 ID 作为生成身份标识的信息，即“A + 111111200001018888 + 血压计”，后续采取和上述相同的步骤，得到用户 A 在血压计设备中可以使用的身份标识 (sk_2, pk_2)。

对于血糖监测仪设备，用户 A 自主选择用户 ID、性别、家庭住址和 IP 地址作为生成身份标识的信息，即“A + 男 + 中国 + 192.168.1.100”，后续采取和上述相同的步骤，得到用户 A 在血糖监测仪设备中可以使用的身份标识 (sk_3, pk_3)。

此身份标识生成过程，在不同的设备中身份标识亦不相同，若心电监测仪的私钥丢失而信息泄露，并不会导致血压计和血糖监测仪的信息也遭受泄露，因此可以抵抗撞库攻击。

4.3. 身份认证方案流程

用户 A 首次使用心电监测仪时，由用户 A 拥有的 PUF_1 发送用户名和公钥到心电监测仪设备，其使用自己拥有的 PUF_2 计算 P_1，并存储用户名和 P_1。

在后续使用心电监测仪时，用户 A 将用户 ID、手机号和设备 ID 输入到 PUF_1 中，由 PUF_1 发送用户

名和公钥到心电监测仪设备，设备验证公钥的准确性，并给用户 A 发送一个随机挑战，然后用户 A 计算签名并给设备发送签名，最终由设备验证签名，接着双方进行身份认证，完成身份认证过程。

用户 A 在使用血压计和血糖监测仪进行身份认证时也执行和上述同样的操作。

用户 A 用于每个设备的私钥并不会进行存储，而是在使用时计算得到的，因此并不存在内存泄漏的危险。由于 PUF 具有极强的随机性，以及用户 A 拥有的 PUF_1 只有本人可以使用，因此可以有效抵抗伪造攻击。设备会在不同的认证过程中给用户 A 发送不同的挑战，并且用户 A 在计算签名时 k 值的选取利用了 PUF 的随机特性，降低了重放攻击的可能性。

4.4. 场景总结

数字签名是一种基于公钥密码体制的安全技术，可用于验证消息的真实性，确保信息确实来源于合法发送者，还可用于验证消息的完整性，防止内容在传输过程中被篡改，以及用于确认签名者的身份，保证签名操作由持有对应私钥的合法主体执行。然而，在实际应用中，数字签名体系通常依赖中心化机构分发和管理身份标识，这种结构存在潜在的安全风险。例如，数据库中私钥的泄露将直接影响系统的整体安全性与数据的可信性，可能导致身份冒用、签名伪造以及数据篡改等问题；若中心机构遭受攻击、被伪造或管理不当，亦可能导致整个信任体系的崩溃。所以，此方案摒弃传统中心化的身份标识分发机制，转而由用户利用 PUF 生成有效的身份标识，无需存储私钥，而是通过计算方式在每次使用时动态生成，从而在保证安全性的同时提升系统的去中心化与抗攻击能力。

此方案与高敏感、高安全要求的智能医疗物联网场景尤为契合。通过为每个医疗设备赋予唯一的身份标识，系统能够在防止内存泄漏、撞库、伪造及重放攻击的同时，保证认证过程的高效与可靠。

5. 总结

本文提出了一种基于 PUF 的身份标识生成与身份认证方法，不仅适用于多样化的应用场景中，还可覆盖人、设备、智能体等多类型主体的身份管理需求。该方法通过在不同系统间保持身份标识的唯一性，实现身份信息的隔离与风险控制，并可以动态生成密钥，有效避免私钥因存储带来的泄露风险。最后，通过形式化和非形式化的安全性分析表明，该方案具备抗多种攻击的能力，包括撞库攻击、伪造攻击等。因此，该方案在提升认证安全性以及保护用户隐私方面具有良好的实用价值。

参考文献

[1] Burrows, M., Abadi, M. and Needham, R. (1990) A Logic of Authentication. *ACM Transactions on Computer Systems*, **8**, 18-36. https://doi.org/10.1145/77648.77649

[2] Blue, J., Condell, J. and Lunney, T. (2018) A Review of Identity, Identification and Authentication. *International Journal for Information Security Research*, **8**, 794-804. https://doi.org/10.20533/ijisr.2042.4639.2018.0091

[3] Kaushalya, J. and Sai, R.V. (2020) A Survey on Efficient and Secure Implementation of ECDSA against Fault Attack. *International Journal of Emerging Trends in Engineering Research*, **8**, 2945-2954. https://doi.org/10.30534/ijeter/2020/11872020

[4] Shaaban, M.A., Alsharkawy, A.S., AbouKreisha, M.T., *et al*. (2024) Efficient ECC-Based Authentication Scheme for Fog-Based IoT Environment. *International journal of Computer Networks & Communications*, **15**, 55-71. https://doi.org/10.5121/ijcnc.2023.15404

[5] Holthouse, R., Owens, S. and Bhunia, S. (2025) The 23andMe Data Breach: Analyzing Credential Stuffing Attacks, Security Vulnerabilities, and Mitigation Strategies. https://arxiv.org/pdf/2502.04303

[6] Zhang, H. and Zhao, F. (2023) Cross-Domain Identity Authentication Scheme Based on Blockchain and PKI System. *High-Confidence Computing*, **3**, Article 100096. https://doi.org/10.1016/j.hcc.2022.100096

[7] Manasrah, A., Yaseen, Q., Al-Aqrabi, H. and Liu, L. (2025) Identity-Based Authentication in VANETs: A Review. *IEEE Transactions on Intelligent Transportation Systems*, **26**, 4260-4282. https://doi.org/10.1109/tits.2025.3528932

[8] Gebali, F. and Mamun, M. (2022) Review of Physically Unclonable Functions (PUFs): Structures, Models, and Algorithms. *Frontiers in Sensors*, **2**, Article 751748. https://doi.org/10.3389/fsens.2021.751748

[9] Suh, G.E. and Devadas, S. (2007) Physical Unclonable Functions for Device Authentication and Secret Key Generation. 2007 44*th ACM*/*IEEE Design Automation Conference*, San Diego, 4-8 June 2007, 9-14.

[10] Rullo, A., Felicetti, C., Vatalaro, M., De Rose, R., Lanuzza, M., Crupi, F., *et al*. (2025) PUF-Based Authentication-Oriented Architecture for Identification Tags. *IEEE Transactions on Dependable and Secure Computing*, **22**, 66-83. https://doi.org/10.1109/tdsc.2024.3387568

[11] Moriyama, D., Matsuo, S. and Yung, M. (2013) PUF-Based RFID Authentication Secure and Private under Memory Leakage. https://eprint.iacr.org/2013/712

[12] Ba, M.H.N., Bennett, J., Gallagher, M., *et al*. (2021) A Case Study of Credential Stuffing Attack: Canva Data Breach. 2021 *International Conference on Computational Science and Computational Intelligence* (*CSCI*), Las Vegas, 15-17 December 2021, 735-740. https://doi.org/10.1109/csci54926.2021.00187

[13] Roy, P., Kumar, R. and Morshed, M.N. (2024) AAF-SCM: An Authenticated Framework for Supply Chain Management. 2024 *International Conference on Intelligent Systems and Advanced Applications* (*ICISAA*), Pune, 25-26 October 2024, 1-4. https://doi.org/10.1109/icisaa62385.2024.10829139

[14] Alhasan, A.Q.A., Rohani, M.F. and Abu-Ali, M.S. (2024) Ultra-Lightweight Mutual Authentication Protocol to Prevent Replay Attacks for Low-Cost RFID Tags. *IEEE Access*, **12**, 50925-50934. https://doi.org/10.1109/access.2024.3386100

[15] Le, T.M.C., Pham, X.T. and Le, V.T. (2024) Advancing Security Protocol Verification: A Comparative Study of Scyther, Tamarin. *Journal of Technical Education Science*, **19**, 43-53. https://doi.org/10.54644/jte.2024.1523