

物联网设备接入信息系统的安全认证与身份管理

薛曾毅¹ 刘洋紫玉² (通讯作者)

1. 四川蓉氢科技有限公司 四川省 成都市 610041

2. 新华水利控股集团有限公司 北京市 100053

【摘要】：随着物联网技术的广泛应用，海量异构设备接入信息系统所带来的安全风险日益突出。物联网设备普遍存在计算资源受限、部署环境复杂、身份管理缺失等问题，传统基于证书和中心化的安全认证机制难以直接适配。本文从物联网设备接入信息系统的实际需求出发，系统分析了设备身份管理的核心挑战，提出了基于轻量化密码算法的设备认证协议设计思路，并构建了面向资源受限设备的统一认证框架。在此基础上，引入零信任安全理念，探讨了动态身份管理架构。通过安全性与性能分析表明，所提方案在保障认证强度的同时有效控制了资源消耗，为物联网设备的安全接入提供了可行路径。

【关键词】：物联网安全；身份认证；轻量化密码；零信任架构；设备身份管理

1 引言

物联网的快速普及深刻改变了信息系统的接入边界。据预测，全球物联网设备连接数量已达数百亿规模，广泛部署于工业控制、智慧城市、智能交通、能源管理等关键领域。然而，物联网设备的大规模接入也使信息系统的攻击面急剧扩大，安全形势愈发严峻。

与传统信息系统不同，物联网设备接入面临三重特殊约束：其一，设备算力弱、存储小、供电有限，无法承载复杂的密码运算；其二，设备部署于开放物理环境，易遭受侧信道攻击和物理篡改；其三，设备身份管理普遍缺失，大量设备仍使用默认口令运行。传统安全认证机制依赖于中心化、资源密集型的加密计算与密钥管理方式，难以适配边缘节点的实际条件。

因此，构建面向物联网设备接入的安全认证与身份管理体系，已成为保障信息系统整体安全的关键课题。本文围绕这一主题展开系统论述。

2 物联网设备身份管理的关键问题

2.1 设备身份标识体系的缺失

在传统信息系统中，用户身份通常以账号密码、数字证书等形式统一管理。然而，物联网设备身份管理面临根本性困难：所有设备缺乏统一、规范的身份标识体系，仅依靠静态 IP 或 MAC 地址进行简单区分，而这两种标识极易被攻击者伪造。攻击者只需通过技术手段伪装成合法设备的地址，就能轻松接入目标网络。这从根本上动摇了信息系统对设备身份的基本信任。

2.2 身份全生命周期的管理需求

物联网设备的身份管理贯穿设备全生命周期，涵盖初始注册、运行中身份保持、状态变更、废弃撤销等阶段。2025 年发布的团体标准《物联网边缘节点轻量化安全认证实施指南》明确提出，应涵盖设备接入前认证、运行中身份保持、远程重认证、

密钥更新等核心技术要求。这意味着身份管理不是一次性的静态操作，而是持续运行的动态过程。

2.3 跨域身份管理的挑战

物联网设备往往需要在不同管理域之间移动或协作。例如，车载设备跨区域行驶时需接入不同的路边单元，工业传感器可能同时向多个平台上报数据。基于设备真实身份实现跨域认证存在隐私泄露的风险，而匿名认证方案又存在难以追踪恶意设备的隐患。如何在身份可验证性与隐私保护之间取得平衡，是跨域身份管理的核心难题。

3 物联网设备安全认证技术

3.1 认证协议的基本框架

物联网设备安全认证的核心目标，是确保接入信息系统的设备身份真实可信。认证协议通常涉及设备端、网关/服务器端以及认证服务端三方实体。其基本流程可概括为：设备发起接入请求，认证服务端对设备身份进行验证，验证通过后建立安全会话密钥用于后续通信保护。

设设备身份标识为 ID ，认证过程中设备需证明其拥有与 ID 绑定的秘密信息 SD 。传统方案多采用基于证书的公钥基础设施 (PKI)，其认证强度可表示为：

$$Authstrength = f(|Kpriv|, Hashtype, Signscheme)$$

其中 $|Kpriv|$ 为私钥长度， $Hashtype$ 为哈希函数类型， $Signscheme$ 为签名方案。在同等安全强度下，不同密码体制的计算开销差异显著。

3.2 轻量化密码算法的适配

针对物联网设备的资源约束，轻量化密码算法成为关键支撑技术。美国国家标准与技术研究院 (NIST) 已于 2025 年正式发布轻量级加密标准，基于 Ascon 算法族提供经过验证的加

密和哈希工具，在保持强大安全性的同时，有效降低能源消耗、内存使用量和运算需求。Ascon 的算法结构更容易配合掩码等防护措施实现，降低攻击者通过功耗或运算时间分析窃取信息的可能性。

算法类型	典型方案	密钥长度	计算时间（相对值）	存储需求
ECC签名	ECDSA-256	256 bit	1.0（基准）	中等
轻量级哈希	Ascon-Hash	128 bit	0.3	低
轻量级AEAD	Ascon-128	128 bit	0.4	低
格密码	Kyber-512	~800 byte	1.2	较高

在实际部署中，应依据设备的能力等级（高 / 中 / 低）匹配合适的算法组合。

3.3 基于物理不可克隆函数的认证

物理不可克隆函数（Physical Unclonable Function, PUF）利用芯片制造过程中的物理差异生成唯一“指纹”，为设备提供硬件级身份锚定。基于SRAM PUF密钥生成器（SPUF-KG）的轻量级认证协议，在设备到服务器（D2S）和设备到设备（D2D）场景下均表现出良好性能，通信成本较现有 PUF 方案分别降低 18.99% 和 5.09%。

PUF 认证的基本原理可形式化描述为：对于激励信号 c_i ，设备产生响应 $r_i = \text{PUF}(c_i)$ 。认证服务器预存激励-响应对 $\{c_i, r_i\}$ ，认证时选取新的激励 c_{new} ，验证设备返回的响应 $r_{new} = \text{PUF}(c_{new})$ 与预期值是否匹配。由于不同芯片的 PUF 响应互不相关且不可克隆，该机制能有效抵御物理伪造攻击。

4 零信任架构下的身份管理

4.1 零信任的核心原则

传统“边界防护”模型假设内部网络可信，而物联网设备的广泛部署使边界变得模糊甚至消失。零信任架构基于“永不信任、始终验证”的核心逻辑，要求对每一次接入请求都进行严格的身份验证和权限评估。

零信任在物联网场景中的适用性体现在三方面：一是设备接入的动态性——设备可能随时加入或离开网络，静态信任假设不再成立；二是通信路径的不确定性——设备间的通信可能跨越多个信任域；三是威胁的内外模糊性——攻击既可能来自外部，也可能来自被攻陷的内部设备。

4.2 动态信任评估机制

在零信任框架下，设备身份不再是静态的“一次性认证”，而是伴随持续行为评估的动态信任值。信任评估函数可表示为：

$$T_{device}(t) = \alpha \cdot T_{base} + \beta \cdot B(t) - \gamma \cdot A(t)$$

其中 T_{base} 为初始认证信任值， $B(t)$ 为行为合规性评分， $A(t)$ 为异常行为检测值， α, β, γ 为权重系数。

当 $T_{device}(t)$ 低于预设阈值时，系统可触发重认证、权限收缩乃至接入阻断。这种动态信任机制使身份管

轻量化算法的选择需综合考量安全强度与资源消耗。以椭圆曲线密码（ECC）与轻量级对称密码为例，其计算开销对比如下：

理从“接入时的一次判断”演进为“运行中的持续管控”。

4.3 统一认证框架的设计

综合上述分析，物联网设备接入信息系统的安全认证与身份管理，应采用分层统一的框架设计，如下图所示：



该框架自下而上由密码基础层、协议层、认证服务层和应用层构成。密码基础层提供轻量级加密、PUF 等基础安全能力；协议层实现设备与系统间的认证与密钥协商；认证服务层负责身份生命周期管理和信任评估；应用层则对接具体的访问控制与安全策略。

5 安全性与性能分析

5.1 安全性分析

所提方案的安全性可从以下维度进行论证。在身份伪造攻击方面，基于 PUF 的硬件指纹机制使攻击者无法克隆设备身份；在中间人攻击方面，认证协议中嵌入的密钥协商过程确保会话密钥的机密性和完整性；在重放攻击方面，协议通过随机数或时间戳保证每次认证消息的新鲜性。

对于跨域认证场景，基于区块链的可追踪匿名方案利用单向哈希链和无证书密码生成多个无关联的假名身份，既保护了设备隐私，又可恢复恶意设备的真实身份进行追责。BAN 逻辑正确性分析和形式化安全证明表明该方案具有较高的安全性。

5.2 性能分析

轻量化认证方案的性能优势主要体现在计算开销、通信开销和存储开销三个维度。在计算开销方面，轻量级对称密码运算（如 Ascon）较传统 ECC 方案减少约 60%~70% 的运算时间。

在通信开销方面, 单次认证的交互消息量可控制在 $1 \sim 2$ KB 以内, 适应低带宽物联网通信场景。在存储开销方面, 服务器端存储较现有方案降低约 17.4%。

对于格加密与区块链结合的轻量级方案, 在 100 比特安全级别下, 认证与密钥协商时间约为 $257.401 \mu s$, 单次认证通信开销为 1052 比特。这些指标表明, 轻量化方案在保障安全强度的同时, 有效满足了物联网设备的资源约束条件。

6 结语

物联网设备接入信息系统的安全认证与身份管理, 是保障

物联网生态安全的基础性工作。本文系统分析了物联网设备身份管理的核心挑战, 探讨了轻量化密码算法适配、PUF 硬件认证等关键技术, 提出了分层统一认证框架的设计思路, 并引入零信任理念实现动态身份管理。未来研究方向可包括: 面向大规模异构设备的自动化身份编排、抗量子计算威胁的轻量级密码方案、以及人工智能驱动自适应信任评估机制。构建安全可信的物联网设备接入体系, 需要学术界与产业界的持续协同推进。

参考文献

- [1] T/XZBX 0071-2025, 物联网边缘节点轻量化安全认证实施指南[S]. 2025.
- [2] 汪秋丽, 任志宇, 吴翔宇, 等. 基于区块链的物联网可追踪匿名跨域认证方案[J]. 计算机科学, 2025, 52(5): 337-344.
- [3] 智慧园区物联深耕: 零信任全维度解析[EB/OL]. 阿里云开发者社区, 2025.
- [4] SPUF-KG and SSL-TRNG Enhanced lightweight IoT authentication and key exchange protocol[J]. Journal of King Saud University - Computer and Information Sciences, 2025, 37: 279.
- [5] Blockchain based lightweight authentication scheme for internet of things using lattice encryption algorithm[J]. Computer Standards & Interfaces, 2025, 93: 103981.
- [6] NIST. Lightweight Cryptography Standard: Ascon Algorithm Family[S]. 2025.

作者简介: 薛曾毅 (1983—), 男, 汉族, 硕士, 研究方向为物联网工程。