Computer Science and Application 计算机科学与应用, 2025, 15(11), 338-348
Published Online November 2025 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2025.1511309

Hans汉斯

基于线性同态签名的敏感物联网设备后量子安全接入认证

谢金红[1,2]，乔建辉[3*]，李溪峰[1]，车小亮[1,3]

[1]武警工程大学密码工程学院，陕西 西安
[2]武警云南总队临沧支队，云南 临沧
[3]网络与信息安全武警部队重点实验室，陕西 西安

收稿日期：2025年10月23日；录用日期：2025年11月20日；发布日期：2025年11月27日

摘　要

当敏感设备批量请求接入物联网时，对其接入认证过程的安全性与效率提出了更高要求。一方面，设备接入认证方案需具备抵御量子计算攻击的能力，以适应后量子时代的安全需求；另一方面，还需高效处理海量终端设备的并发认证请求，高效处理批量设备请求验证。本文提出一种基于线性同态签名的物联网设备接入认证方案，旨在实现批量设备的安全接入和高效认证。该方案首先基于NTRU密码签名体制与格理论困难问题，设计一种新型线性同态签名算法，使其不仅具备抗量子安全性，还能够支持对多个签名进行线性聚合与高效验证，将该算法嵌入认证服务中心与网关，实现对设备身份与传输数据的联合批量验证；再次，设计了高效的分层认证故障设备定位协议，并利用PUF技术实现密钥管控，提高了方案的可行性。安全性分析表明，该方案可有效抵御量子计算环境下的伪造与篡改攻击；性能评估显示，在千级设备规模下，在存储开销保持可行范围内，实现高效批量验证。

关键词

物联网，格密码，线性同态签名，后量子密码

Post-Quantum Secure Access Authentication for Sensitive IoT Devices Based on Linear Homomorphic Signature

Jinhong Xie[1,2], Jianhui Qiao[3*], Haofeng Li[1], Xiaoliang Che[1,3]

[1]College of Cryptographic Engineering, Engineering University of People's Armed Police, Xi'an Shaanxi
[2]Lincang Detachment, Yunnan Provincial Corps of People's Armed Police, Lincang Yunnan
[3]Key Laboratory of Network and Information Security of People's Armed Police, Xi'an Shaanxi

[*]通讯作者。

文章引用: 谢金红, 乔建辉, 李溪峰, 车小亮. 基于线性同态签名的敏感物联网设备后量子安全接入认证[J]. 计算机科学与应用, 2025, 15(11): 338-348. DOI: 10.12677/csa.2025.1511309

Received: October 23, 2025; accepted: November 20, 2025; published: November 27, 2025

Abstract

When a large number of sensitive devices request access to the Internet of Things (IoT) in batches, higher requirements are put forward for the security and efficiency of their access authentication process. On the one hand, device access authentication schemes need to have the ability to resist quantum computing attacks to meet the security needs of the post-quantum era; on the other hand, they also need to efficiently handle concurrent authentication requests from massive terminal devices and verify batch device access requests. This paper proposes an IoT device access authentication scheme based on linear homomorphic signatures, aiming to achieve secure access and efficient authentication of batch devices. First, based on the NTRU cryptographic signature scheme and hard problems in lattice theory, the scheme designs a new linear homomorphic signature algorithm. This algorithm not only has post-quantum security, but also supports linear aggregation and efficient verification of multiple signatures. It is embedded in the authentication service center (ASC) and gateways to realize the joint batch verification of device identities and transmitted data. Second, an efficient hierarchical authentication protocol for faulty device localization is designed, and Physical Unclonable Function (PUF) technology is used to realize key management and control, which improves the feasibility of the scheme. Security analysis shows that the scheme can effectively resist forgery and tampering attacks in the quantum computing environment; performance evaluation indicates that under the scale of thousands of devices, efficient batch verification is achieved while the storage overhead remains within a feasible range.

Keywords

Internet of Things (IoT), Lattice-Based Cryptography, Linear Homomorphic Signature, Post-Quantum Cryptography

1. 引言

在工业、医疗和军事等敏感领域中，物联网发挥着不可替代的重要作用，它通过各种传感器、智能设备及通信技术，建起严密的感知与响应体系，极大提升安全性、可靠性与应对效率。比如，物联网通过分布式光纤传感网络实时监测核电站物理入侵与设备故障[1]；借助联邦学习实现隐私保护的医疗数据分析[2]；从“连接”迈向“智能协同”，构建起高效的信息交互桥梁，使各军兵种、各作战单元间实现信息实时共享与无缝对接[3]等。物联网设备的认证接入需要考虑多方面因素，就前沿通用物联网技术而言，网络层面采用的分布式架构和零信任动态认证技术[4]，解决中心化单点故障问题，实现动态认证。安全层面引入抗量子签名算法[5]-[7]、轻量级协议[8] [9]等，在保证安全的同时，提高认证效率；在硬件层面，利用芯片制造工艺偏差生成设备唯一硬件指纹[10]等技术，提升抗物理攻击能力。

线性同态签名[11]能在没有签名私钥的情况下，允许任何实体对已认证的数据进行线性同态运算生成新数据，并得到新数据的有效签名，其在物联网领域具有很好的应用成效[12]。而随着量子计算发展使传统签名算法面临被破解风险，尤其是敏感设备数据接入物联网中对安全性要求更高。保证接入算法安全性的同时，需要兼顾接入认证的效率，以保证实用性。基于格的抗量子线性同态签名在资源受限设备上表现优

异，签名生成耗时短，认证成功率高，为物联网安全提供有力支撑，对物联网在各领域的可靠应用不可或缺。Chen 等人[13]在标准模型下提出了首个格基线性同态签名，方案使用了文献[14]的两整数格相交法实现安全签名，并利用盆景树格基委派算法[15]绑定数据集标签，从而实现了标准模型下的可证明安全性。Lin 等人[5]提出的格基线性同态签名方案，利用满秩差分哈希函数替代线性同态编码，相对于 Chen 等人提出的方案，公钥矩阵数量减少，消除了公钥尺寸的标签长度的依赖，但运算维度增加了，导致运算效率不高。特别是近年来，随着 NIST 后量子算法的广泛征集，大量高效格基签名算法涌现。比如，Falcon 算法[5]是 NIST 后量子密码标准化选定的数字签名算法，基于 NTRU 格构建，融合快速傅里叶变换实现安全高效签名。Hawk 算法[16]是基于二次型格同构[17]问题设计的 NTRU 型签名算法，其参数选取更小，签名运算效率更高，入选 NIST 算法评比第二轮。Dilithium 算法[18]困难性依赖于理论上的模块学习误差(MLWE)和 MSIS 问题，它是基于多项式环上的高效签名算法，2022 年被 NIST 选为量子安全签名标准。

本文综合考虑抗量子同态签名算法综合性能，根据多项式环计算的高效性，设计一种 NTRU 型线性同态签名算法，并结合敏感物联网设备接入，给出了线性同态签名算法应用物联网模型。通过安全性和整体性能分析，构建的方案模型可实现物联设备高效接入认证的安全性和可靠性。

2. 基础知识

本文使用粗体小写字母表示向量，如向量$\boldsymbol{b}$。使用粗体大写字母表示矩阵，如矩阵$\boldsymbol{A}$。$\mathbb{Z}_q$表示模q整数域。使用$\|\cdot\|$表示向量的欧几里得范数(L2 范数)。

2.1. 数学知识

2.1.1. 多项式环

NTRU 算法的核心代数结构是有限域上的循环多项式环，标准形式为：$R_q=\mathbb{Z}_q[x]/(x^n+1)$。$\mathbb{Z}_q[x]$为模$q$的整数环($q$为大素数或 2 的幂)；$(x^n+1)$为分圆多项式($n$为 2 的幂)，作为环的零化多项式，使环中满足$x^n\equiv -1 \bmod (x^n+1)$，进而$x^{2n}\equiv 1$，形成循环结构。$R_q$中任意多项式可表示为次数小于等于$n-1$的多项式，即元素形式为$a=a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1}$，其中$a_i\in\mathbb{Z}_q$。

2.1.2. 格与格上困难问题

格是由一组线性无关向量的所有整系数线性组合构成的向量全体。令$\{\mathbf{b}_1,\mathbf{b}_2,\cdots,\mathbf{b}_n\}$为$n$个线性独立的向量，由$\{\mathbf{b}_1,\mathbf{b}_2,\cdots,\mathbf{b}_n\}$生成的$n$维格定义为：$\mathcal{L}(\mathbf{B})=\left\{\sum_{i\in[n]}c_i\mathbf{b}_i, c_i\in\mathbb{Z}\right\}$，其中$\{\mathbf{b}_1,\mathbf{b}_2,\cdots,\mathbf{b}_n\}$为矩阵$\mathbf{B}$的列向量，为格的一组基，基向量的个数$n$定义为格的维数。

格的多项式表示：将R中多项式作为$\mathbb{Z}^n$中的向量，则R中的理想对应$\mathbb{Z}^n$中理想格。

最近向量问题(NVP)：给定格$\mathcal{L}$和目标向量$\mathbf{t}\in\mathbb{Z}^n$，找到格点$\mathbf{b}\in\mathcal{L}(\mathbf{B})$使得$\|\mathbf{t}-\mathbf{b}\|$最小。

定义 1 SIS 困难问题[14] [15]：(小整数解(short integer solution, SIS))问题：给定一个均匀随机的矩阵$\mathbf{A}\in\mathbb{Z}_q^{n\times m}$以及参数$n,m,q,\beta$，$\mathrm{SIS}_{n,m,q,\beta}$问题的目标是找到一个非零整数向量$\mathbf{v}\in\mathbb{Z}_q^m$，使得$\|\mathbf{v}\|\le\beta$且$\mathbf{Av}=0(\bmod q)$。

定义 2 NTRU-SIS 困难问题[14] [15]：给定公钥$h\in R_q$，寻找非零多项式对$\sigma\in R$，使得：$h\cdot\sigma\equiv 0 \bmod q$且$\|\sigma\|\le\beta$。

困难性：NTRU-SIS 问题的困难性可归约到理想格上最短向量的最坏情况困难性，量子算法无法在多项式时间内求解，确保抗量子攻击安全。

2.1.3. Babai 算法

Babai 算法是格密码学中用于求解最近向量问题(Nearest Vector Problem, NVP)的经典近似算法，其核心

目标是在给定格中找到与目标向量距离最近的格点。具体算法详见文献[19]，Babai 算法可简要的表达为：

$\mathrm{Babai}(\mathbf{B},\mathbf{t})$：输入一个优质格基 $\mathbf{B}$ 和一个目标向量 $\mathbf{t}\in\mathbb{Z}^n$。输出一个格点 $\mathbf{b}\in\mathcal{L}(\mathbf{B})$，使得 $\|\mathbf{t}-\mathbf{b}\|$ 相对较小。

在多项式环计算中，优质格基 $\mathbf{B}$ 是由私钥多项式生成的基，而 $\mathbf{t}$ 是由目标多项式生成的向量。

2.1.4. 离散高斯分布

离散高斯分布是定义在整数格 $\mathcal{L}$ 上的概率分布，参数为“中心 $\mathbf{c}\in\mathbb{R}^d$”和“标准差 σ”，概率质量函数为：

$$\mathcal{D}_{\mathcal{L},\mathbf{c},\sigma}(\mathbf{v})=\frac{\exp\left(-\frac{\|\mathbf{v}-\mathbf{c}\|^2}{2\sigma^2}\right)}{\sum_{\mathbf{w}\in\mathcal{L}}\exp\left(-\frac{\|\mathbf{w}-\mathbf{c}\|^2}{2\sigma^2}\right)} \tag{1}$$

核心性质：当 σ 足够大时(通常 $\sigma\geq\sqrt{\log d}\cdot\det(\mathcal{L})^{1/d}$)，采样结果以高概率是格中的短向量($\|\mathbf{v}\|\leq O\left(\sigma\sqrt{d}\right)$)；

NTRU 中的采样：在 R_q 中，离散高斯采样等价于对多项式系数采样，即每个系数 r_i (或 s_i)独立从 $\mathcal{D}_{\mathbb{Z},0,\sigma}$ 采样，确保 r, s 为短多项式。

2.2. 物联网设备接入认证框架

当前基于物联网设备安全接入认证模型已经超越了简单的账号密码或单身证书的验证模式，正向自适应、自动化、去中心化和能抵抗未来威胁的方向演进。基于签名算法的常用接入认证框架设计遵循“建立认证服务中心－签发设备准入凭证－设备接入请求－认证服务中心验证－授权与会话”的概要流程来设计。

(1) 建立认证服务中心：基于云服务器或去中心化的信任机制建立的数据运算中心，实现用户身份验证、授权和数据全周期管理等。

(2) 签发设备准入凭证：认证服务中心(AS)生成签名的公、私钥对。设备向 AS 注册申请唯一身份标识，AS 向设备签发私钥并绑定设备身份。

(3) 设备接入请求：接入设备利用自身凭证，生成一个接入认证消息，并发送至网络接入点。

(4) 认证服务中心验证：AS 接收网络接入点收集的关于设备的数据信息，使用公钥信息进行验证。

(5) 授权与会话：认证通过后，AS 会向网关下发授权令牌，或直接为设备生成会话密钥，并建立安全的数据通道。

当有批量设备进行接入认证时，AS 在高峰期可能需要同时验证成千上万台设备的接入请求。传统的签名方案需要逐个验证每个设备的签名，计算开销巨大，容易成为性能瓶颈。

3. 基于线性同态签名的物联网设备接入认证

线性同态签名允许对多个已签名的消息进行线性组合，并生成一个新的、有效的签名。这个新签名可以被任何拥有公钥的人验证，且验证者可以确信：原始数据中的线性组合确实是由合法的签名者生成的。在物联网接入认证框架中，网关或认证中心可以将多个设备的认证请求聚合成一个请求和一个聚合签名，只需验证一次聚合签名，就能同时完成对所有设备身份的认证，极大提升效率。

3.1. NTRU 型线性同态签名方案

基于格上同态签名算法具有较好的抗量子攻击特性，由于运算的复杂性致使运算效率不高。NTRU 型

同态签名算法是基于环多项式环上数学困难问题的简易算法，保证安全性的同时，运算效率较高，是用于设计抗量子安全的物联网认证的较好选择。本节提出一种 NTRU 型的线性同态签名算法，实现不同设备签名的聚合验证。

(1) 密钥生成

输入安全参数 λ，输出私钥 sk 和公钥 pk：

a) 参数选择：根据 λ 确定多项式环维度 n、模数 q。其中 $q \equiv 1 \bmod 2n$，且 x^n+1 在 $\mathbb{Z}_q[x]$ 中可分解，所有的运算均在环 R_q 上进行。

b) 生成公私钥多项式：

采样可逆多项式 $f \in R_q$ 和随机多项式 $g \in R_q$，系数均从$\{-1, 0, 1\}$中随机选择，满足 $f \cdot f^{-1} \equiv 1 \bmod q$；计算 $h = g \cdot f^{-1} \bmod q$。令私钥 $sk = (f, g)$，公钥 $pk = h$。

(2) 签名生成

$\mathrm{Sign}(sk, m)$：对签名消息进行预处理，进行全域哈希转成小系数多项式 $m \in R_q$。通过离散高斯采样随机短多项式 $e \in R$，输入私钥 $sk = (f, g)$，调用 Babai 算法，找到小范数多项式 (s, r)，使得：

$$f \cdot s - g \cdot r = f \cdot m + e \pmod q \tag{2}$$

多项式 $e \in R$ 是误差项，且 $\|e\|_\infty \le \gamma$ (γ 很小)。输出签名消息 $\sigma = (s, r)$。

(3) 签名验证

$\mathrm{Verify}(pk, m, \sigma)$：输入公钥 pk、消息 $m \in R_q$ 和签名 (s, r)，输出“接受 1”或“拒绝 0”：

a) 计算 $d = s - h \cdot r - m \pmod q$：

b) 验证 $\|d\| \le B$ (其中 $B < \dfrac{q \cdot 2^{-\lambda/n} - 1}{2}$)是否成立，若成立则输出“接受 1”，否则“拒绝 0”。

(4) 线性同态运算

$\mathrm{Hom}(pk, \sum m_i, \sum \sigma_i)$：对多个签名线性同态运算，输入公钥 pk，消息 m_i 及其签名 $\sigma_i = (s_i, r_i)$。其中 $1 \le i \le t$。对于整数系数 c_i，输出组合消息 m^* 的签名 σ^*：

$$m^* = \sum_{i=1}^{t} c_i m_i \bmod q; \sigma^* = (s^*, r^*) = \left(\sum_{i=1}^{t} c_i s_i \bmod q, \sum_{i=1}^{t} c_i r_i \bmod q\right) \tag{3}$$

调用验证算法 $\mathrm{Verify}(pk, m^*, \sigma^*)$ 进行验证。

a) 计算 $d^* = s^* - h \cdot r^* - m^* \pmod q$：

b) 验证 $\|d^*\| \le B \sum_{i=1}^{t} c_i$ 是否成立，若成立则输出“接受 1”，否则“拒绝 0”。

验证算法的正确性：

单个签名的验证可得 $f \cdot d = e \pmod q$，即 $\|f \cdot d\| = \|e\|$。所以 $\|d\| \ge \dfrac{\|e\|}{\|f\|_1}$，此时对于 $\|d\|$ 的上界 B 可以取较大的值，但需要使攻击者伪造签名的概率可忽略，则要满足 $\left(\dfrac{2B+1}{q}\right)^n < 2^{-\lambda}$，可得 $B < \dfrac{q \cdot 2^{-\lambda/n} - 1}{2}$。

对于多个签名消息的聚合验证，$\|f \cdot d^*\| = \sum_{i=1}^{t} c_i \|e\| \pmod q$，进而需要验证 $\|d^*\| \le B \sum_{i=1}^{t} c_i$ 是否成立。

3.2. 基于线性同态签名的物联网设备接入认证模型

3.2.1. 物联网认证模型构建

线性同态签名算法应用到物联网设备的接入认证中，使接入设备从逐个验证转变为批量验证。敏感设备接入物联网需要严格的接入环境和安全的接入认证算法，在此基础上还需要考虑验证效率。本节基于上节 NTRU 线性同态签名算法设计的物联网设备接入认证模型如图 1 所示。

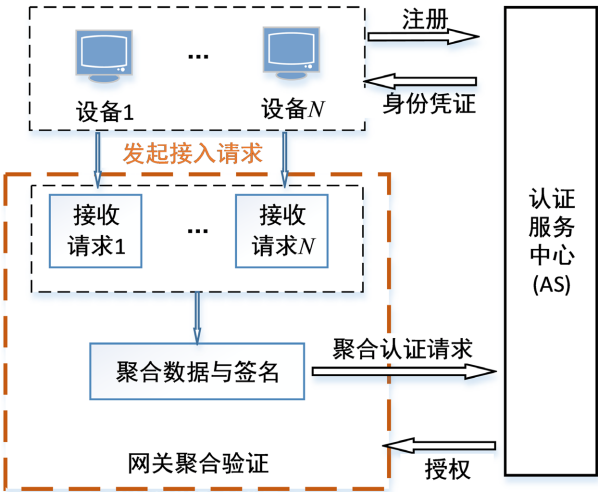

Figure 1. LHS-based networked device access authentication framework
图 1. 基于 LHS 的联网设备接入认证框架

第 1 阶段：系统初始化与设备预配

1) 认证服务中心(AS)设置：生成同态签名方案的主密钥对(sk, pk)，公钥 pk 公开。

2) 设备注册与凭证签发：每个设备在入网时，向 AS 注册其唯一身份标识 ID_i。

AS 使用主私钥 sk 与设备 ID_i 绑定签发一个与设备身份关联的专属同态签名私钥 $sk_i = (sk, \mathrm{ID}_i)$，并通过安全密钥通信渠道分发至设备的安全元件中。

第 2 阶段：接入认证流程

1) 设备发起请求：设备 i 需要接入网络时，生成一个认证消息 m_i。使用自己的同态签名私钥 sk_i 中的 sk 对消息 m_i 进行签名，得到 $\sigma_i = \mathrm{Sign}(sk, m_i)$。

设备将认证数据 (σ_i, m_i) 发送给网络接入网关。

2) 网关聚合：网关在短时间内(如一个时间窗口)收集到来自 N 个设备的认证请求：$(\sigma_1, m_1), \cdots, (\sigma_n, m_n)$。计算聚合消息和聚合签名：

$$m^* = (c_1 m_1 + c_2 m_2 + \cdots + c_n m_n),\ \sigma^* = (c_1\sigma_1 + c_2\sigma_2 + \cdots + c_n\sigma_n) \tag{4}$$

3) 认证服务中心验证：

网关将聚合后的数据 (m^*, σ^*) 以及设备数量等信息发送给 AS。

AS 收到后，使用主公钥 pk 对聚合签名进行验证：$\mathrm{Verify}(pk, m^*, \sigma^*)$。

4) 验证结果：

如果成功，意味着 AS 可以确信：所有参与聚合的原始消息 m_i 都是由拥有合法私钥 sk_i 的设备签名的。AS 因此批准这 n 台设备的接入请求。

如果失败，则意味着至少有一个设备的签名无效。此时，AS 可要求网关减小聚合批次重新提交验证，利用故障定位协议，查找恶意设备。

第 3 阶段：授权与会话建立

1) 认证通过后，AS 会向网关下发授权令牌，或直接为这批设备生成会话密钥。

2) 网关通知各设备认证成功，并建立安全的数据通道。

3.2.2. 故障定位协议

设计的接入认证模型中，恶意设备的检测定位功能十分重要，本节设计一种分层认证的故障定位协

议。根据设备数量 N，将设备分 K 层 M 组，选取合适的正整数 N,K,M，使 $N/M^2 \le 2$，且 $N/M, N/M^2, M^3/N$ 均为整数。

1) 协议配置

设 $H(*)$ 为 SHA-256 哈希函数，利用 AS 为每个设备生成的 ID_i 生成认证码 $AC_i = H(sk \| \mathrm{ID}_i)$。网关对接入设备按树形划分 K 层，对于不大于千级的设备数，可取 $K=3$。

2) 子聚合生成

利用 $H(*)$ 函数生成所有设备的认证码 $AC_i = H(sk \| \mathrm{ID}_i)$，绑定对应设备生成的签名 σ_i。

第 3 层：将 N/M^2 个设备划分 1 个小细组，并聚合每个小组的设备签名 σ_j^* $(1 \le j \le \frac{N}{M^2})$，计算该小组所有设备的认证码 $AC_{3,j} = H(AC_1 \| AC_2 \cdots \| AC_{N/M^2})$，绑定 $AC_{3,j}$ 和 σ_j^*。

第 2 层：将第 3 层 M 设备为 1 小组划分成 N/M 个小组，并聚合每个小组的设备签名 σ_t^* $(1 \le t \le \frac{N}{M})$，计算该小组所有设备的认证码 $AC_{2,t} = H(AC_{3,1} \| AC_{3,2} \cdots \| AC_{3,M})$，绑定 $AC_{2,t}$ 和 σ_t^*。

第 1 层：聚合第 2 层所有小组的子聚合签名得到最终聚合签名 σ^*，计算所有 $AC_{3,t}$ 的认证码摘要 $AC^* = H(AC_{2,1} \| AC_{2,2} \cdots \| AC_{3,N/M})$，绑定 AC^* 和 σ^*。

3) 验证定位

第一次定位：AS 验证总签名 σ^* 失败时，要求网关上传第 2 层所有认证码和签名 $(AC_{2,t}, \sigma_t^*)$，AS 先验证每个子聚合签名的有效性，若验证 σ_t^* 签名失败，则恶意设备就可定位在第 t 组。

第二次定位：AS 验证 t 组所有签名 σ_j^* 的有效性，若验证 σ_j^* 签名失败，则定位恶意设备在 j 组内；

第三次定位：在 j 组内最多有 2 个设备，可逐一验证其签名的有效性，最终定位到恶意设备。

该故障定位协议基于 SHA-256 哈希函数，利用主密钥生成每一层的哈希摘要 AC_i 认证码，在 SHA-256 哈希函数安全条件下，攻击者无法伪造。对于千级设备量的设备而言，使用构造的分组认证故障定位协议发展总签名验证失败时，最快可经过 3 次签名验证、最多也就经过 $(M + N/M)$ 次验证就可定位故障设备，查找定位信息效率较高。

3.2.3. 模型密钥管理

保证设备使用的密钥安全是确保模型中签名不可伪造性的前提。设计的物联网设备接入认证模型中第一阶段的密钥分发是密钥管理的关键阶段。本节使用物理不可克隆函数 PUF 技术[10]，将生成的设备专属密钥从 AS 中的静态存储到设备端的重构，并贯穿密钥的安全分发、安全存储、更新和撤销整个过程。

1) 密钥安全分发机制

密钥分发涉及到密钥封装等加密技术，PUF 技术生成根密钥后，需要使用稳定的根密钥对设备专属密钥加密后分发至设备，使用的具有抗量子安全的加密算法，构建的认证接入模型采用层级化密钥分发架构。

核心层：AS 生成主密钥对 (sk, pk)，私钥 sk 存储于 AS 安全模块，公钥 pk 利用可信安全渠道广播下发至所有网关，确保公钥的完整性和不可篡改性。

设备层：结合使用 PUF 技术实现设备专属密钥的分发。设备首次入网请求时，携带专属物理不可克隆标识 ID_i 向 AS 发起注册请求，AS 验证设备标识合法性，并向设备的 PUF 施加一个挑战 C，设备 PUF 基于物理特性生成对应的响应 R 和辅助数据 S，并向 AS 输出加密密钥 K。AS 基于主私钥 sk 为设备生成专属同态签名私钥 sk_i，并利用 K 对 sk_i 加密分发至各设备，设备接收后通过 PUF 验证解密，得到专属签名 sk_i。

2) 密钥存储、更新及撤销机制

密钥存储：在 AS 侧，主私钥采用硬件常用的硬件加密与多副本冷备份相结合的存储方式，避免物理

攻击与逻辑泄露。在网关侧，仅存储主公钥与临时聚合签名缓存，不存储任何私钥，降低网关被攻击后的密钥泄露风险。在设备侧，设备专属私钥通过 PUF 动态生成，避免私钥以明文形式存储在易被读取的闪存/内存中，私钥仅允许签名算法调用时单次加载，用完清除。

密钥更新：模型密钥更新采用双密钥过渡期机制策略，为密钥设置专用备用位置，根据算法需要更新密钥时，在主密钥继续使用的同时，将待更新密钥加载备用位置，并设置更换过渡期，过渡期间模型可支持两套密钥使用，并在过渡期内使用旧密钥完成一次完整的设备认证后，利用新密钥重新生成接入认证消息签名，完成新旧密钥更替。

密钥撤销：密钥的撤销以证书撤销列表(CRL)记录为依据，由 AS 主导，关联网关与设备。AS 设置不同优先级别的 CRL 推送策略，并定期更新列表。

当设备正常退出时，AS 检测设备 30 日未发起接入请求，将该设备专属密钥标记“待用”，若再合法启用，需重新申请，否则加入 CRL 中禁用；当设备异常接入时，网关检测到设备签名验证失败次数超过 5 次，或 AS 检测到设备伪造消息，则由 AS 将密钥标识加入 CRL 禁用。当检测到大规模伪造攻击时，AS 紧急使用最优先级推送 CRL 新增列表，同步密钥撤销信息，降低攻击扩散风险。

3.3. 性能分析

3.3.1. 模型安全性分析

物联网设备接入认证的安全性主要是防止签名的伪造和篡改。本文提出的接入认证模型是基于格线性同态签名算法设计的，其安全性一方面基于线性同态签名算法本身的抗量子攻击特性，有效抵御量子级别攻击，防止签名的伪造和篡改；另一方面是得利于线性同态运算的优良性能，在验证过程中保护设备本身数据的隐私性。

抗量子安全：设计的 NTRU 型线性同态签名算法，其安全性是基于 NTRU-SIS 困难问题，攻击者要基于算法本身伪造或篡改出一个合法的签名，即要寻找另一个非零多项式对 $\sigma' \in R$，使得：$h \cdot \sigma' \equiv 0 \bmod q$ 且 $\|\sigma'\| \le \beta$。进一步可得 $h \cdot (\sigma - \sigma') \equiv 0 \bmod q$，解此多项式的困难性归约到破解 NTRU-SIS 困难问题上，所以算法具有良好的抗量子攻击特性。

隐私保护：在设备接入认证过程中，AS 只能看到聚合结果，无法获取单个设备的敏感数据 m_i，保护敏感数据不被第三方获取。

3.3.2. 算法运算效率分析

物联网接入认证模型的效率主要取决于线性同态签名算法本身的效率。在满足抗量子安全条件下，将本文提出的 NTRU 型线性同态签名方案与 Chen 等人[13]和 Li 等人[5]提出的格基线性同态签名方案进行生成效率对比分析。并与同样基于多项式运算的典型 Dilithium 签名方案的性能进行对比。上述方案应用于物联网接入认证，当同时处理 N 台设备时，不考虑故障定位协议带来的计算影响，具体签名生成及验证时间如表 1 所示。

由表 1 可知，本文设计的方案在单签名生成和验证效率上，比文献[5]和[13]提出的线性同态签名方案较优，但不如 Dilithium 方案高效。生成的单个签名的尺寸比文献[5]和[13]方案生成的签名尺寸小，与 Dilithium 方案生成的签名尺寸相近。由于本文方案和文献[5]和[13]方案均满足线性同态性，所以在进行批量验证时，先对签名进行聚合而后进行验证，其验证效率与单个签名验证效率相近，而 Dilithium 方案需要对 N 个用户逐一进行验证。本文设计的方案核心优势在于处理批量签名验证，假设在同等计算复杂度系数条件下，设安全参数 $\lambda = 128$，多项式维度 $n = 1024$，模数 $q = 2048$，设备数量 $N = 1000$，签名消息长度 $L = 256$ 比特，NTT 乘法系数设为 0.5，多项式加法系数设为 0.1。设计的 NTRU 型方案批量验证用时约为 132.4 ms，而 Dilithium 方案完成批量验证用时大约 265.6 ms，主要原因是由于 Dilithium 方案的非同态性质。

Table 1. Comparative analysis of generation efficiency and performance
表 1. 生成效率及性能对比分析

性能指标	Chen 等人方案[13]	Lin 等人方案[5]	本文方案	Dilithium 方案[18]
单签名生成时间	$O\left(n^3\right)$	$O\left(m^3\right)$	$O\left(n^2\log q\right)$	$O\left(n\log n\log q\right)$
单签名验证时间	$O\left(nhr\right)$	$O\left(nm\right)$	$O\left(n\log n\log q\right)$	$O\left(n\log n\right)$
批量验证时间	$O\left(nhr\right)$	$O\left(nm\right)$	$O\left(nN+n\log n\log q\right)$	$O\left(Nn\log n\right)$
单签名大小	$O\left(rn\log_2\left(n^{\frac{3}{2}}\log n\right)\right)$	$O\left(m\log_2\left(m\log q\right)\right)$	$2n\log_2 q$	$O\left(n\log n\right)$
抗量子性	是	是	是	是
同态性	是	是	是	否

参数说明：Lin 等人方案中设定的格维度 $m=6n\log q$，Chen 等方案中设定的矩阵行数 $h=\left\lfloor\frac{n}{6\log q}\right\rfloor$、标签长度 $r=O\left(\log n\right)$。

3.3.3. 算法通信开销分析

物联网接入认证模型的通信开销主要集中于“设备－网关－AS”之间的交互。设备向网关发送认证消息和签名信息，以及网关向 AS 发送聚合消息和聚合签名占用大量的通信开销，AS 向网关返回验证结果及授权，网关向设备返回认证结果等通信开销可以忽略不计。设单设备认证消息长度为 L，针对 $N=1000$ 级别数量的验证，同样在不考虑故障定位协议产生的通信负荷时，通信开销对比分析结果如表 2 所示。

Table 2. Comparison and analysis of communication overhead
表 2. 通信开销对比及分析

方案类型	单设备开销	N 台设备总通信开销	结果
Chen 等人方案[13]	$O\left(rn\log_2\left(n^{\frac{3}{2}}\log n\right)\right)$	$(N+1)\left[L+O\left(rn\log_2\left(n^{\frac{3}{2}}\log n\right)\right)\right]$	中等
Lin 等人方案[5]	$O\left(m\log_2\left(m\log q\right)\right)$	$(N+1)\left[L+O\left(m\log_2\left(m\log q\right)\right)\right]$	最大
Dilithium 方案[18]	$O\left(n\log n\right)$	$2N\left[L+O\left(n\log n\right)\right]$	较小
本文方案	$2n\log_2 q$	$(N+1)\left[L+2n\log_2 q\right]$	较小

由于 Dilithium 方案的非同态性质，在物联网千级设备认证时，需要同时处理 N 台设备，并通过网关转发，所以通信开销增加 2 倍。通过表 2 可以看出，再进行单台设备通信时，Dilithium 方案通信开销具有较大优势，但同时处理 N 台设备认证时，本文方案与 Dilithium 方案通信开销优势相近，远小于文献[5]和[13]方案的通信开销。

3.3.4. 模型可行性分析

计算资源受限环境下的可行性：可采用转载算力的方式来解决，在签名生成过程中，Babai 算法迭代

求解相对比较耗时，可根据实际应用环境要求将 Babai 算法转载。比如，当网关算力高于设备端，可将 Babai 算法转载至网关，设备采样生成小多项式 e 并设置好运算参数后，将最复杂的运算转载网关运算。

通信资源受限环境下的可行性：针对通信环境较差的应用场景中，对方案本身选择小规模参数，压缩生成信息空间，减小设备与网关、AS 之间的通信负担；采用密钥封装，将密钥集成于安全元件或是 PUF 中，减小 AS 与设备、网关之间的通信负担；分段传输聚合签名，每段适配窄带宽传输要求，降低带宽占用率。

4. 结束语

本文提出的基于线性同态签名的敏感物联设备接入认证，为大规模、高并发物联网设备接入场景提供了一种有效的解决方法。设计的 NTRU 型线性同态签名算法能抵御量子攻击的同时，支持数据聚合验证，有效提升物联网网关接入验证效率。相比于传统的物联网接入认证算法(比如对称签名算法等)，该线性同态签名算法还存在签名生成复杂度高、通信开销大等弊端，这也是提高安全性而带来的弊端。本研究对高并发、高安全需求的物联网场景提供了一种可行的认证解决方案。

基金项目

武警工程大学基础前沿创新项目(WJY202419)。

参考文献

[1] Liu, C.W., Liu, Y., Du, L., *et al*. (2023) Enhanced Sensing of Optomechanically Induced Nonlinearity by Linewidth Suppression and Optical Bistability in Cavity-Waveguide Systems. *Optics Express*, **31**, 9236-9250. https://doi.org/10.1364/oe.482075

[2] Yang, J.M., Liu, F., Wang, B.Y., *et al*. (2021) Blood Pressure States Transition Inference Based on Multi-State Markov Model. *IEEE Journal of Biomedical and Health Informatics*, **25**, 237-246. https://doi.org/10.1109/jbhi.2020.3006217

[3] Zsiborács, D. (2025) Human-Machine Teaming in Modern Warfare: Evolving Collaboration at Edge on the Battlefield. https://www.karveinternational.com/insights/human-machine-teaming-in-modern-warfare

[4] Aleisa, M.A. (2025) Blockchain-Enabled Zero Trust Architecture for Privacy-Preserving Cybersecurity in IoT Environments. *IEEE Access*, **13**, 18660-18676. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10839415 https://doi.org/10.1109/ACCESS.2025.3529309

[5] Lin, C., Xue, R., Yang, S., Huang, X. and Li, S. (2020) Linearly Homomorphic Signatures from Lattices. *The Computer Journal*, **63**, 1871-1885. https://doi.org/10.1093/comjnl/bxaa034

[6] Wu, B., Wang, C. and Yao, H. (2021) A Certificateless Linearly Homomorphic Signature Scheme for Network Coding and Its Application in the IoT. *Peer-to-Peer Networking and Applications*, **14**, 852-872. https://doi.org/10.1007/s12083-020-01028-8

[7] Fouque, P.A., Hoffstein, J., Kirchner, P., *et al*. (2018) Falcon: Fast-Fourier Lattice-Based Compact Signatures over NTRU. Submission to the NIST's Post-Quantum Cryptography Standardization Process.

[8] Shah, A., Pandya, H., Soni, M., Karimov, A., Maaliw, R.R. and Keshta, I. (2023) PUF-Based Lightweight Authentication Protocol for IoT Devices. In: *Lecture Notes in Networks and Systems*, Springer, 401-412. https://doi.org/10.1007/978-981-99-3177-4_29

[9] Rana, M., Mamun, Q. and Islam, R. (2022) Lightweight Cryptography in IoT Networks: A Survey. *Future Generation Computer Systems*, **129**, 77-89. https://doi.org/10.1016/j.future.2021.11.011

[10] 李进. 基于物理不可克隆函数的芯片安全技术研究[D]: [硕士学位论文]. 成都: 电子科技大学, 2022.

[11] Johnson, R., Molnar, D., Song, D. and Wagner, D. (2002) Homomorphic Signature Schemes. In: *Lecture Notes in Computer Science*, Springer, 244-262. https://doi.org/10.1007/3-540-45760-7_17

[12] Zhou, X., Zhou, T., Tian, Y., Zhong, W. and Yang, X. (2024) Linearly Homomorphic Signature Scheme with High-Signature Efficiency and Its Application in IoT. *IEEE Internet of Things Journal*, **11**, 38126-38136. https://doi.org/10.1109/jiot.2024.3443282

[13] Chen, W., Lei, H. and Qi, K. (2016) Lattice-Based Linearly Homomorphic Signatures in the Standard Model. *Theoretical Computer Science*, **634**, 47-54. https://doi.org/10.1016/j.tcs.2016.04.009

[14] Cash, D., Hofheinz, D., Kiltz, E. and Peikert, C. (2012) Bonsai Trees, or How to Delegate a Lattice Basis. *Journal of Cryptology*, **25**, 601-639. https://doi.org/10.1007/s00145-011-9105-2

[15] Boneh, D. and Freeman, D.M. (2011) Homomorphic Signatures for Polynomial Functions. In: *Lecture Notes in Computer Science*, Springer, 149-168. https://doi.org/10.1007/978-3-642-20465-4_10

[16] Léo, D., Eamonn, W., Ludo, N.P., *et al*. (2022) Hawk: Module LIP makes Lattice Signatures Fast, Compact and Simple. http://eprint.iacr.org/2022/1155

[17] Léo, D.S. and Wessel, V.W. (2021) On the Lattice Isomorphism Problem, Quadratic Forms, Remarkable Lattices, and Cryptography. *Lecture Notes in Computer Science*, **13277**, 643-673. https://doi.org/10.1007/978-3-031-07082-2_23

[18] Jackson, K.A., Miller, C.A. and Wang, D. (2024) Evaluating the Security of Crystals-Dilithium in the Quantum Random Oracle Model. In: *Lecture Notes in Computer Science*, Springer, 418-446. https://doi.org/10.1007/978-3-031-58751-1_15

[19] Babai, L. (1986) On Lovász' Lattice Reduction and the Nearest Lattice Point Problem. *Combinatorica*, **6**, 1-13. https://doi.org/10.1007/bf02579403