研究与开发

一种基于格的轻量级物联网群签密认证方案

徐川[1,2]，艾星好[1]，王杉杉[1]，赵国锋[1,2]，韩珍珍[1,2]
（1. 重庆邮电大学通信与信息工程学院，重庆 400065；
2. 四川易景智能终端有限公司，四川 宜宾 644000）

摘　要：5G时代为物联网高速发展带来了机遇，身份认证是保障物联网安全的基础。然而在面对量子攻击时，由于物联网节点众多，基于签密的身份认证方案生成节点密钥将消耗大量资源，难以满足物联网低开销的需求。为此，设计了一种基于格的轻量级群签密认证方案。在密钥生成阶段，设计了改进陷门对角矩阵，优化生成密钥所需的原像采样算法，减小了生成大量密钥时所需的整体时间；在身份认证阶段，基于剩余哈希引理和签密性质，在一个逻辑步骤内对消息同时进行签名和加密，提出了低次数的点乘与哈希运算的交互流程，完成组长代替群组成员进行的接入认证。仿真实验表明，该方案降低了物联网设备接入时的交互次数，减少了身份认证阶段的计算开销，对比现有方案，签密与解签密的总开销降低了至少7%，同时证明了该方案能在物联网中抵抗量子攻击。

关键词：群组认证；抗量子；物联网；轻量级
中图分类号：TN918；TP309
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2024094

A lightweight lattice-based group signcryption authentication scheme for Internet of things

XU Chuan[1,2], AI Xinghao[1], WANG Shanshan[1], ZHAO Guofeng[1,2], HAN Zhenzhen[1,2]
1. School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
2. Sichuan Yijing Intelligent Terminal Co., Ltd., Yibin 644000, China

Abstract: The 5G era has brought opportunities for the rapid development of the Internet of things. Identity authentication is the basis for ensuring the security of the Internet of things. However, in the face of quantum attacks due to the large number of nodes in the Internet of things, the signcrypt-based identity authentication scheme will consume a

收稿日期：2024−01−12；**修回日期：**2024−03−22
通信作者：徐川，xuchuan@cqupt.edu.cn
基金项目：国家自然科学基金资助项目（No.62171070）；重庆市博士后科学基金资助项目（No.CSTB2022NSCQ-BHX0043）；2022宜宾市引进高层人才项目（No.2022YG05）；重庆邮电大学博士研究生人才培养项目（No.BYJS202204）
Foundation Items: The National Natural Science Foundation of China (No. 62171070), Chongqing Postdoctoral Science Foundation (No. CSTB2022NSCQ-BHX0043), 2022 Yibin City Introduced High-level Talents Project (No. 2022YG05), Chongqing University of Posts and Telecommunications Doctoral Talent Training Program (No.BYJS202204)

lot of resources to generate node keys, which is difficult to meet the low cost requirements of the Internet of things. Therefore, a lightweight lattice-based group signcryption authentication scheme was designed. In the key generation stage, the improved trapdoor diagonal matrix was designed to optimize the original image sampling algorithm required for key generation and reduce the overall time required for generating a large number of keys. In the identity authentication stage, based on the residual Hash lemma and the signcryptic property, the message was signed and encrypted in one logical step at the same time, and the interaction flow of dot multiplication and Hash operation with low frequency was proposed to complete the access authentication performed by the group leader on behalf of the group members. Simulation experiments show that this scheme reduces the number of interactions during the access of Internet of things devices, reduces the computing cost of identity authentication stage, and reduces the total cost of signcryption and decryption by more than 7% compared with the existing schemes. Furthermore, the simulation results prove that this scheme can resist quantum attacks in the Internet of things.

Key words: group authentication, quantum-resistant, Internet of things, lightweight

0　引言

近年来，物联网产业发展迅速，物联网接入设备众多，身份认证是系统安全的第一道防线[1-2]。物联网中设备的局限性（有限的计算能力、存储空间等资源限制）[3]，使得传统的认证协议在物联网环境中并不适用[4-5]。因此，急需设计出适用于物联网场景的接入认证方案。

签密技术[6]因其计算和通信成本低于传统的先签名后加密的方案，被引入资源受限的物联网场景中[7]。牛淑芬等[8]提出了基于异构密码系统的混合签密方案，私钥生成器和密钥生成中心能够分别在基于身份的密码体制（identity based cryptography，IBC）和无证书密码体制（certless cryptography，CLC）中产生自己的系统主密钥，利用群组成员协作解签密提高方案的安全性。Mandal 等[9]在物联网环境中设计了一种新的基于三因素认证的用户访问控制方案（certificateless signcryption-based three-factor user access control scheme for Internet of things environment，CSUA-IoT），通过执行 CSUA-IoT 的登录和访问控制阶段，注册用户和指定智能设备可通过物联网环境中特定单元的可信网关节点相互授权和验证。Chen 等[10]在物联网环境中提出了一种改进的无证书在线/离线签密方案（certificateless online/offline signcryption scheme，CLOOSC），云服务器作为半可信的密钥生成中心，负责分发整个系统的公共参数，消息验证阶段外包给边缘服务器。但该方案未考虑离线计算时的开销，且在验证阶段使用双线性导致运算开销增大。Dohare 等[11]在工业物联网中提出了一种无证书的聚合签密方案（certificateless aggregated signcryption scheme，CLASS），在双线性迪菲-赫尔曼（quadratic bilinear Diffie-Hellman，QBDH）的假设下能够抵抗选择密文攻击下的不可区分性（indistinguishability under chosen-ciphertext attack，IND-CCA2）和自适应选择消息攻击下满足存在不可伪造性攻击（existential unforgeability under chosen message attack，EUF-CMA）。但其注册时实体间生成密钥步骤烦琐，身份认证阶段通信和计算复杂度高。综上，现有物联网场景下的签密方案在设计注册和身份认证阶段所需的开销较大。

随着后量子时代的到来，大多数认证协议所依赖的离散问题和质数问题都能够在多项式时间内得到解决[12]，传统方案无法抵御量子攻击。而量子计算机解决基于格结构的数学问题仍需要指数级时间[13]，因此格密码被认为是一种具有较高安全性的密码算法[14-15]，可用于构造相应的认证方案。但是，现有抗量子签密方案密钥生成运算多，签密与解签密的计算量大。Zhu 等[16]提出了

一种基于代理签密的抗量子方案，该方案在构造中引入了区分函数，根据输入的发送方和接收方的密钥情况保障算法的加密、签名和签密的对称性，方案中密钥尺寸为$m^2n\log q$；Li等[17]提出了基于格的异构签密安全方案，其安全性是基于多项式环上带误差学习的判定和小多项式比判定两个困难问题假设的，但该方案计算和通信复杂度较高，其加密计算量为$9T_h+4T_{em}+7T_{ea}$，解密计算量为$10T_h+5T_{em}+4T_{ea}$。若将此类抗量子签密方案引入物联网认证场景，将加重注册阶段生成各实体所需密钥的负载，增大身份认证阶段物联网设备发送认证请求与设备组聚合认证的开销。

综上所述，为解决现有的物联网认证方案中存在的开销过大问题，本文提出了一种基于格的群签密轻量级认证方案，主要贡献如下。

（1）针对大量群组成员签密时所需资源开销问题，本文摒弃传统的群组密钥，改为只在无证书注册阶段分配部分密钥，在认证阶段再生成完整密钥，同时提出改进陷门的对角矩阵以及扰动向量的协方差矩阵，优化生成密钥所需的原像采样算法，减小生成大量密钥时所需的整体时间。

（2）针对身份认证阶段，现有方案的群组成员与组长交互运算次数多，导致组长聚合运算复杂度高的问题，本文在构建抗量子攻击方案时，基于剩余哈希引理以及签密的性质，在一个逻辑步骤内对消息同时进行签名和加密，提出了一种低运算次数与复杂度的交互认证流程，其签密与解签密阶段主要采用无双线性配对运算，哈希运算总量为5次以下。

（3）基于BAN（Burrows-Abadi-Needham）形式逻辑证明了该方案的正确性，通过随机oracle模型进行轮询安全性分析，证明了该方案具有不可伪造性，可抵抗重放攻击、中间人攻击和量子攻击。仿真实验表明，本文方案降低了物联网设备接入时的交互次数，相较于现有方案，能够将注册阶段的公钥与私钥生成时间降低30%，签密与解签密的总开销同比降低7%。

1 系统模型与相关理论

1.1 格理论及困难问题

本文在物联网场景下认证方案的构建与安全性的证明中，相关符号及其意义见表1。

表1 相关符号及其意义

符号	符号定义
Q	大质数
m	传输的数据消息
n	系统安全参数
s	系统高斯参数
d_i	用户设备部分私钥
c	加密后的密文
σ	离散正态分布参数
ω	复杂性函数
M	随机整数
l	满足$l>5n\log q$
D	离散正态分布
t_i	秘密值
b_i	用户设备部分公钥
H_1	哈希函数满足$H_1:\{0,1\}^*\times\{0,1\}^*\to Z_q^n$
H_2	哈希函数满足$H_2:Z_q^{2n}\times\{0,1\}^*\to\{h,h\in\{-1,0,1\}^k\}$
Z_q	剩余类环
ID_i	用户设备身份
MPK	系统公钥
MSK	系统私钥
pk_i	用户设备完整公钥
sk_i	用户设备完整私钥
params	公开参数

给定一个M行和M列的可逆矩阵$\boldsymbol{B}=[\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_M]\in Z^{M\times M}$，其中，$M$个向量$\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_M\in \mathrm{R}^N$线性无关，由矩阵$\boldsymbol{B}$生成的$M$维整数格定义为：

$$\Lambda=\{y\in Z^M\Big|y=\boldsymbol{B}\boldsymbol{c}=\sum_{i=1}^{M}c\boldsymbol{b}_i,c\in Z^M\},\quad \boldsymbol{B}=\{\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_M\}\in \mathrm{R}^{N\times M} \tag{1}$$

其中，这些向量被称为格的基。格的维数与向量 $\mathrm{span}(\Lambda)=\{\boldsymbol{B}y \mid y\in \boldsymbol{R}^M\}$ 所在的线性空间相关，其中，矩阵 $\boldsymbol{B}=\{\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_M\}\in \boldsymbol{R}^{N\times M}$ 为格的基。对格基由 $\tilde{\boldsymbol{b}}_i=\boldsymbol{b}_i-\sum_{j=1}^{i-1}\mu_{ij}\tilde{\boldsymbol{b}}_j$ 定义，其施密特正交化矩阵为 $\tilde{\boldsymbol{B}}=\{\tilde{\boldsymbol{b}}_1,\tilde{\boldsymbol{b}}_2,\cdots,\tilde{\boldsymbol{b}}_M\}$，其中，$\mu_{ij}=\frac{<\boldsymbol{b}_i,\tilde{\boldsymbol{b}}_j>}{<\boldsymbol{b}_j,\boldsymbol{b}_j>}$。

给定矩阵 $\boldsymbol{A}\in Z_q^{M\times N}$，$Z_q^{m\times n}$ 为包含 M 行和 N 列的残差相关矩阵环，其中，M、N 和 q 均为正整数，有相应的 M 维格定义为：

$$\Lambda^{\perp}(\boldsymbol{A})=\{e\in \mathrm{Z}^M:\boldsymbol{A}\cdot e=0\bmod q\} \tag{2}$$

$$\Lambda_M^{\perp}(\boldsymbol{A})=\{e\in \mathrm{Z}^M:\boldsymbol{A}\cdot e=u \bmod q\} \tag{3}$$

对于任意 $s>0$，以 c 为中心格的离散高斯函数定义为：

$$\rho_{s,c}(x)=\exp\left(\frac{-\pi\|x-c\|^2}{s^2}\right) \tag{4}$$

其中，定义域为 R^N。对于标量矩阵 $\boldsymbol{\Sigma}=s^2\cdot\boldsymbol{I}$，$\rho_{s,c}(x)$ 为高斯函数，$s>0$。将格上的离散高斯分布定义为：

$$D_{\Lambda,\sqrt{\Sigma},c}(x)=\frac{\rho_{\boldsymbol{B},\sqrt{\Sigma},c}(x)}{\rho_{\boldsymbol{B},\sqrt{\Sigma},c}(\Lambda)} \tag{5}$$

对于任意的 $\varepsilon>0$，满足 $\rho(s\cdot\Lambda^*)\leqslant 1+\varepsilon$ 的最小 s 为平滑参数，用 $\eta_\varepsilon(\Lambda)$ 表示。

定义 1　给定一个正整数 $N\geqslant 1$，χ 为 Z_q^M 上的高斯噪声分布，其中，模量 $q\geqslant 2$。概率分布 $A_{s,\chi}$ 可通过如下方法得到：均匀选择矩阵 $\boldsymbol{\alpha}\in Z_q^{N\times M}$ 和向量 $\boldsymbol{s}\in Z_q^N$，从高斯噪声分布 χ 中随机提取噪声向量 $\boldsymbol{e}\in Z_q^M$。

此外输出 $(\boldsymbol{A},\boldsymbol{A}^{\mathrm{T}}s+e)$ 主要有以下两个版本的误差学习（learning with errors，LWE）问题：

（1）搜索性 LWE 问题：给定 m 个独立样本 $(\boldsymbol{A},\boldsymbol{A}^{\mathrm{T}}s+e)$ 服从分布 $A_{s,\chi}$，以不可忽略的概率输出 $s\in Z_q^N$。

（2）确定性 LWE 问题：区分上述算法得到的每个样本 $(\boldsymbol{A},\boldsymbol{A}^{\mathrm{T}}s+e)$，主要区别是样本是否服从分布 $A_{s,\chi}$ 或者样本是否在 $Z_q^{N\times M}\times Z_q^{N\times M}$ 上的均匀分布中随机选择。

1.2　系统模型

5G 物联网接入认证场景如图 1 所示，5G 物联网接入认证场景包括密钥生成中心（key generation center，KGC）、认证单元（authentication management function，AMF）、物联网设备（Internet of things device，IOTD）和物联网设备组组长（group leader，GL）。同一区域内的窄带物联网（narrowband Internet of things，NB-IoT）节点根据功能特性划分为一组，同一节点群组中成员属于同一应用服务器，会根据节点计算能力、电池容量等情况选择一个节点作为群组组长。群组中的 NB-IoT 节点若在同一时刻需要接入网络，会将接入请求信息发送给设备组组长，由组长代替所有相关的组成员与认证单元交互完成认证。

接入认证过程主要分为 3 个阶段：初始化阶段、注册阶段和身份认证阶段。初始化阶段主要由密钥生成中心负责生成注册和认证所需的相应系统参数，并设置安全参数；注册阶段各实体自身生成实体间交互认证所需的签名和加密密钥；身份认证阶段则由物联网设备向认证单元发起接入认证请求，认证单元验证签名等参数的合法性，对物联网设备完成身份认证。

物联网认证流程主要存在两方面的问题，一是在注册和身份认证阶段的资源开销问题，注册阶段群组成员会生成大量的密钥，身份认证阶段群组成员在发送认证请求与组长交互以及组长聚合消息时，签名和加密需要的运算次数和复杂度较高。二是物联网设备交互认证时的安全问题，身份认证阶段，物联网设备与组长进行交互以及组长聚合请求消息后向认证单元统一认证时，存在中间人攻击、重放攻击、量子攻击等安全威胁。

为解决上述问题，本文提出了基于格的轻量级群组认证方案，主要功能与流程如下。

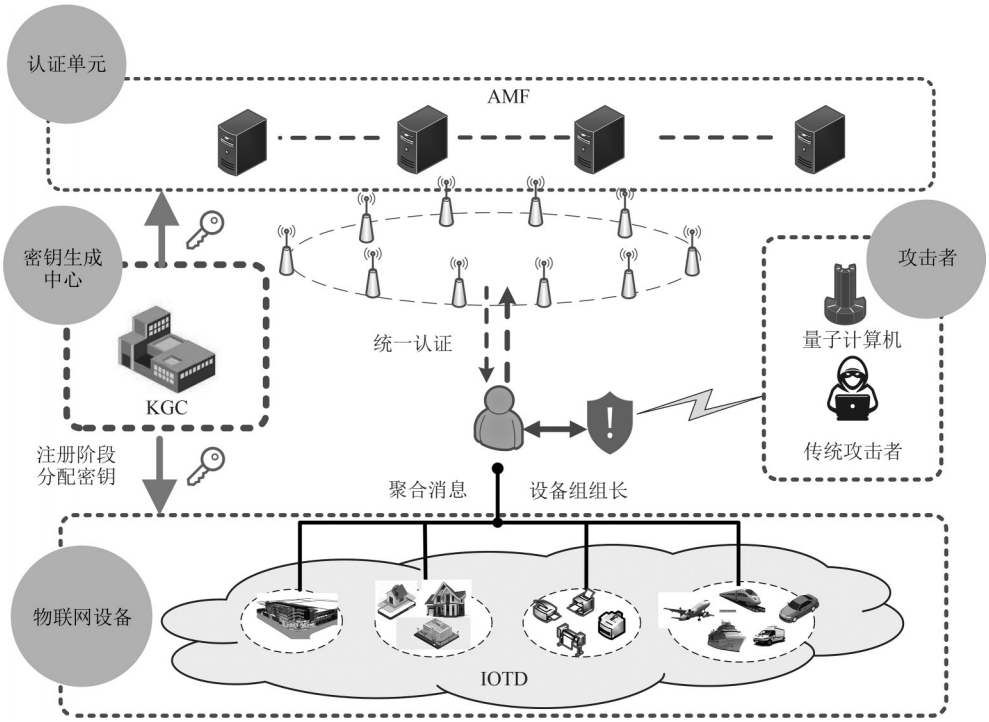


图1　5G物联网接入认证场景

（1）密钥生成中心（KGC）：本文方案中密钥生成中心作为半可信实体，初始化阶段负责生成系统所需的关键参数和安全参数，并在注册阶段根据各个实体的身份标识，采用基于多项式二次型陷门（multivariate quadratic polynomial trapdoor12，MP12）方案的改进抽样算法为AMF、IOTD和GL分配部分密钥。

（2）认证单元（AMF）：作为认证节点，在身份认证阶段根据组长发送的聚合签名对同一群组内的物联网设备进行统一认证，并对IOTD发送的数据进行解密，生成聚合认证响应消息返回给物联网设备。

（3）物联网设备（IOTD）：在注册阶段通过密钥生成中心分配的部分密钥生成签名和加密所需的完整公私钥，在认证阶段生成签名和密文，并将接入认证请求信息统一发送给设备组组长，由组长代替物联网设备组成员进行统一认证。

2　基于格的群签密轻量级认证方案

2.1　基于MP12的改进抽样算法

本文提出了一种基于MP12的改进抽样算法，降低了密钥生成时间，提高了整个认证流程的效率。算法采用的陷门结构为完全并行化，当固定参数N、M和$\boldsymbol{R}$时，需要更小的模量q使得密钥更小，从而提高生成效率。

假设$q\geqslant 3$，$M\geqslant 5n\log q$，随机选择矩阵$\boldsymbol{A}\in Z_q^{N\times M}$，整数格$\Lambda^{\perp}(\boldsymbol{A})$上的短基$\boldsymbol{T}_{\boldsymbol{A}}\in Z^{N\times M}$，高斯参数$s\geqslant \|\boldsymbol{T}_{\boldsymbol{A}}\|\omega(\sqrt{\log n})$。对于任意的$\boldsymbol{u}\in Z_q^N$，存在有效的多项式时间算法SamplePre$(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},s,\boldsymbol{u})$。该算法在统计上近似从离散高斯分布$G_{\Lambda u(\boldsymbol{A}),s}$中提取的向量$\boldsymbol{v}\in\Lambda^{\boldsymbol{u}}(\boldsymbol{A})$。根据高斯分布的性质，$\boldsymbol{v}$以压倒性的概率满足$\|\boldsymbol{v}\|\leqslant s\sqrt{M}$。原像采样算法可以很容易的扩展到矩阵，即对于任意矩阵$\boldsymbol{U}\in Z^{N\times k}$，其基本参数与基本的原像采样算法相同。由一种扩展的多项式时间算法

SamplePre($\boldsymbol{A}, \boldsymbol{T}_A, s, \boldsymbol{u}$)，其统计近似算法为在离散 $G_{\Lambda u(\mathbf{A}),s}$ 和 $\boldsymbol{Av}=\boldsymbol{U} \bmod q$ 中得到矩阵高斯分布 $\boldsymbol{v} \in \Lambda^{\boldsymbol{u}}(\boldsymbol{A})$，同时 $\|\boldsymbol{v}\| \leqslant s\sqrt{m}$ 具有压倒性的概率。设 $\eta=\eta_{\varepsilon}(\boldsymbol{R}^M)=\eta_{\varepsilon}(Z^{NM})$ 为整数格的平滑参数，其中，$\varepsilon \in (0,1)$ 将陷门 $\tilde{\boldsymbol{R}}$ 的最大奇异值表示为 $s_1(\tilde{\boldsymbol{R}})$。令 $\Lambda \in \boldsymbol{R}^N$ 的格基为 $\boldsymbol{B}$，则对于任意的 $\varepsilon>0$ 有 $\eta_{\varepsilon}(\Lambda) \leqslant \left\|\tilde{\boldsymbol{B}}\right\| \cdot \sqrt{\ln(2N(1+1/\varepsilon))/\pi}$，故可知 $\sigma_g=\sqrt{b^2+1} \cdot \eta \geqslant \eta_{\varepsilon}(\Lambda_v^{\perp}(g^t))$，现假设环上误差学习小整数解（ring-LWE with small integer solution，R-SIS）上界为 $\sqrt{NM}$，原像高斯宽度为 $s=\sqrt{\sigma_g^4/\sigma_g^4-\eta^2 \cdot (s_1^2(\tilde{\boldsymbol{R}})+\eta^2 \boldsymbol{I}_M)}$。

陷门生成算法如算法 1 所示，原像采样算法如算法 2 所示，其中，扰动的采样不依赖于目标 u。

算法 1　陷门生成算法

输入　安全参数

输出　陷门与密钥

步骤 1　执行 SamplePre $(f, g_1, g_2, \cdots, g_{k-1}) \leftarrow \chi^k$；

步骤 2　令 $\tilde{\boldsymbol{R}}=\mathrm{diag}(f, g_1, g_2, \cdots, g_{k-1})$；

步骤 3　$a^t=g^t \cdot (f^{-1} \cdot \tilde{\boldsymbol{R}})^{-1}$；

步骤 4　返回 $\tilde{\boldsymbol{R}}$ 与 a。

算法 2　原像采样算法

输入　目标 $u \in \boldsymbol{R}q$ 与陷门 $\tilde{\boldsymbol{R}}$

输出　原像 u

步骤 1　采样扰动 $p \leftarrow \mathrm{D}_{R^M, \sqrt{\Sigma p}}$；

步骤 2　令 $\tilde{a}^t=f^{-1} \cdot a^t, \tilde{\boldsymbol{u}}=\boldsymbol{u} \cdot f^{-1}, \boldsymbol{v}=\tilde{\boldsymbol{u}}-\tilde{a}^t \cdot p$；

步骤 3　采样 $x \leftarrow \mathrm{D}_{\Lambda_v^{\perp}(gt), \sigma g}$；

步骤 4　返回 $y=\tilde{\boldsymbol{R}} \cdot x+p$。

本文基于格的群签密轻量级认证方案主要分为 3 个阶段：初始化阶段、注册阶段和身份认证阶段，具体步骤见第 2.2 节至第 2.4 节。

2.2　初始化阶段

初始化阶段，KGC 执行以下步骤来完成系统的初始化。给定一个安全参数 n，KGC 执行初始化算法并输出公共参数。

（1）KGC 选择系统所需的相应基本参数 $q=\mathrm{ploy}(n)$，$\alpha \in \{0,1\}$，$k=[\log q]$，$N=2nk$，$M=O(\log q)$。

（2）设 $\chi_{\beta}=D_{Z, q\alpha}$ 表示误差分布，KGC 选择误差分布参数 $B=q\alpha \cdot \omega(\sqrt{\log n})$。假设 $g^{\mathrm{T}}=(1, 2, 4, \cdots, 2^{k-1}) \in Z_q^k$ 是一个 k 维向量，KGC 计算 $\boldsymbol{G}=\mathbf{I}_n \otimes g^{\mathrm{T}}$，其中，$\mathbf{I}_n$ 表示 n 阶单位向量。

（3）KGC 选择两个防碰撞的哈希函数：

$$H_1: \{0,1\}^* \times \{0,1\}^* \rightarrow Z_q^n \tag{6}$$

$$H_2: Z_q^{2n} \times \{0,1\}^* \rightarrow \{h, h \in \{-1,0,1\}^k\} \tag{7}$$

（4）KGC 执行陷门构造函数 TrapGen $(1^n, 1^N, q) \rightarrow (\boldsymbol{A}, \boldsymbol{R})$，并计算：

$$\boldsymbol{A}=(\bar{\boldsymbol{A}} | \boldsymbol{G}-\bar{\boldsymbol{A}}\boldsymbol{R}) \in Z_q^{n \times N} \tag{8}$$

其中，$\bar{\boldsymbol{A}} \leftarrow Z_q^{n \times nk}$，$\boldsymbol{R} \leftarrow D_{z, s_1}^{nk \times nk}$。

（5）离散高斯分布的误差为 $s_1=5\omega(\sqrt{\log n})$，离散高斯分布参数 $\sigma \leqslant \alpha\lambda s\sqrt{6l}$，其中，$s \geqslant \|\boldsymbol{R}\| \omega(\sqrt{\log n})$，$\lambda$ 为随机整数，l 为满足 $l \geqslant 5n \log q$ 的正实数。

（6）KGC 令 $(\mathrm{MPK}, \mathrm{MSK})=(\boldsymbol{A}, \boldsymbol{R}) \in Z_q^{n \times N} \times Z_{\boldsymbol{B}}^{nk \times nk}$，原像采样算法参数 $s_2=\sqrt{6(s(\boldsymbol{R})^2)+1}$，$S(\boldsymbol{R})$ 为 $\boldsymbol{R}$ 的奇异值。最后将参数 $\{\boldsymbol{A}, H_1, H_2, s_1, s_2, \chi_B\}$ 作为系统参数公开。

2.3　注册阶段

在此阶段 KGC 为 AMF、IOTD 和组长生成部分密钥，AMF、IOTD 和组长根据身份 ID 选择出的秘密值计算出所需的公私钥。每个 IOTD 设备和 AMF 首先注册并提供其部分私钥，获取由 KGC 生成的另一部分私钥。之后，KGC 将各自的另一部分私钥分别发送到 IOTD 和 AMF。至此，每个用户都拥有一个唯一且合法的身份 ID。AMF、GL 和 IOTD 将自己的身份标识 ID 和群组身份标识（group ID，GID）嵌入注册请求信息中，向 KGC 发出注册请求。KGC 收到注册请求信息后，验证 IOTD 的设备组身份标识 GID，在

确定IOTD为有效组成员后，为IOTD、AMF和GL分配部分密钥。注册阶段如图2所示，具体执行步骤如下。

（1）KGC在收到各个通信实体的注册请求后为IOTD分配部分密钥：KGC计算$u_i=H_1(\mathrm{ID}_i)$，其中，$\mathrm{ID}_i\in\{0,1\}^*$，且$i\in\{\mathrm{S},\mathrm{V}\}$。KGC从矩阵$\boldsymbol{A}=(\bar{\boldsymbol{A}}|\boldsymbol{G}-\bar{\boldsymbol{A}}\boldsymbol{R})\in Z_q^{n\times N}$中提取出前$nk$列子矩阵。KGC提取部分私钥$d_i\leftarrow\mathrm{SampleD}(\bar{\boldsymbol{A}},\boldsymbol{R},\boldsymbol{u},s_2)$，其中，$d_i\in Z_q^N$；如果满足$\boldsymbol{A}d_i=u_i$，且$\|d_i\|\leqslant s_2\sqrt{N}\cdot\omega(\sqrt{\log n})$，则KGC将部分密钥$d_i$传输给身份$\mathrm{ID}_i$的$\mathrm{IOTD}_i$。

（2）为AMF分配部分密钥：KGC计算$u_a=H_1(\mathrm{ID}_a)$，其中，$\mathrm{ID}_a\in\{0,1\}^*$，且$a\in\{\mathrm{S},\mathrm{V}\}$。KGC从矩阵$\boldsymbol{A}=(\bar{\boldsymbol{A}}|\boldsymbol{G}-\bar{\boldsymbol{A}}\boldsymbol{R})\in Z_q^{n\times N}$中提取出前$nk$列子矩阵$\bar{\boldsymbol{A}}$。KGC提取部分私钥$d_a\leftarrow\mathrm{SampleD}(\bar{\boldsymbol{A}},\boldsymbol{R},u_a,s_2)$，其中，$d_a\in Z_q^N$。如果满足$\boldsymbol{A}d_a=u_a$，且$\|d_a\|\leqslant s_2\sqrt{N}\cdot\omega(\sqrt{\log n})$，KGC将部分密钥$d_a$传输给身份$\mathrm{ID}_a$的AMF。

（3）为组长分配部分密钥：KGC计算$u_G=H_1(\mathrm{ID}_G)$，其中，$\mathrm{ID}_G\in\{0,1\}^*$，且$G\in\{\mathrm{S},\mathrm{V}\}$。KGC从矩阵$\boldsymbol{A}=(\bar{\boldsymbol{A}}|\boldsymbol{G}-\bar{\boldsymbol{A}}\boldsymbol{R})\in Z_q^{n\times N}$中提取出前$nk$列子矩阵。KGC提取部分私钥$d_G\leftarrow\mathrm{SampleD}(\bar{\boldsymbol{A}},\boldsymbol{R},u_G,s_2)$，其中，$d_G\in Z_q^N$。如果满足$\boldsymbol{A}d_G=u_G$，且$\|d_G\|\leqslant s_2\sqrt{N}\cdot\omega(\sqrt{\log n})$，KGC将部分密钥$d_G$传输给身份$\mathrm{ID}_G$的组长。最后KGC将需要分配给通信实体的部分密钥嵌入注册消息中，返回注册响应。

收到KGC返回的注册响应后，IOTD根据分配的部分密钥生成完整的公私钥。IOTD获取$T_i\leftarrow(\boldsymbol{A},R_i,T_A,\sigma_R)$，计算$Q_i=\boldsymbol{A}R_i^{-1}$，其中，$R_i=H_1(\mathrm{ID}_u)$，$\|T_i\|\leqslant\sigma R/\omega(\sqrt{\log m})$，$\sigma R\geqslant\|\tilde{T}_A\|(\sigma\sqrt{m}\cdot\omega(\sqrt{\log^{3/2}m}))$，$i=1,2,\cdots,l,r$，$\mathrm{ID}_r\in\{U,\mathrm{ID}_r\}$，$\mathrm{U}=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_l\}$，其中，$\mathrm{ID}_s\in U$为签密者身份标识，$\mathrm{ID}_r\notin U$为解签密者身份标识。具有身份$\mathrm{ID}_i$的$\mathrm{IOTD}_i$选择秘密值$t_i\leftarrow\chi_B^n$，并设置私钥$\mathrm{sk}_i=(t_i,d_i)\in Z_q^n\times Z_q^N$。然后$\mathrm{IOTD}_i$计算其公钥$\mathrm{pk}_i$，选择矩阵$\boldsymbol{B}_i\leftarrow Z_q^{n\times M}$，向量$o_i\leftarrow\chi_B^n$，计算$b_i=\boldsymbol{B}_i^{\mathrm{T}}x+2o_i \bmod q\in Z_q^M$，计算公钥$\mathrm{pk}_i=(b_i|\boldsymbol{B}_i^{\mathrm{T}})\in Z_q^{M\times(1+n)}$。

具有身份ID_a的AMF选择秘密值$t_a\leftarrow\chi_b^n$，并设置私钥$\mathrm{sk}_a=(t_a,d_a)\in Z_q^n\times Z_q^N$。然后AMF计算其公钥$\mathrm{pk}_a$，选择矩阵$\boldsymbol{B}_a\leftarrow Z_q^{n\times M}$，向量$o_a\leftarrow\chi_B^n$，计算$b_a=\boldsymbol{B}_a^{\mathrm{T}}x+2o_a \bmod q\in Z_q^M$，计算公钥$\mathrm{pk}_a=(b_a|\boldsymbol{B}_a^{\mathrm{T}})\in Z_q^{M\times(1+n)}$。

具有身份ID_G的组长选择秘密值$t_G\leftarrow\chi_b^n$，并设置私钥$\mathrm{sk}_G=(t_G,d_G)\in Z_q^n\times Z_q^N$。然后组长计算其公钥$\mathrm{pk}_G$，选择矩阵$\boldsymbol{B}_G\leftarrow Z_q^{n\times M}$，向量$o_G\leftarrow\chi_B^n$，

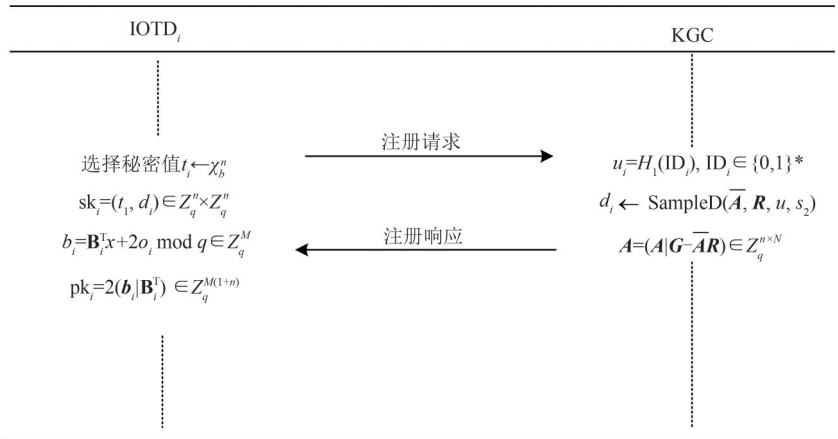


图2　注册阶段

计算 $b_G=\boldsymbol{B}_G^{\mathrm{T}}x+2o_G \bmod q\in Z_q^M$，计算公钥 $\mathrm{pk}_G=(b_G\|\boldsymbol{B}_G^{\mathrm{T}})\in Z_q^{M\times(1+n)}$。

2.4　身份认证阶段

身份认证阶段如图 3 所示，IOTD_i将接入认证请求发送给设备组组长 GL 进行聚合，由 AMF 通过验证组长聚合后的签名，完成对群组中所有物联网设备的统一认证。

IOTD_i在完成注册阶段的密钥生成后，根据相应的公私钥对消息 m_i进行加密，将加密后的消息嵌入接入认证请求中发送给组长，IOTD_i执行如下操作：IOTD_i随机选择向量 $\boldsymbol{y}=[y_1,y_2,y_3]^{\mathrm{T}}\in Z^{3t}$，其中，$y_1\leftarrow D_\sigma^t$，$y_2\leftarrow D_\sigma^t$，$y_3\leftarrow D_\sigma^t$。随机选择 $r\leftarrow\{0,1\}^M$，$w\leftarrow\chi_B^n$，$e_1\leftarrow\chi_B^n$，$e_2\leftarrow\chi_B^n$，令 $h=H_2(\boldsymbol{AB}_G\boldsymbol{y},m_i)$，$x=\mathrm{sk}_i h\in Z^{3t}$ 且 $\varepsilon=x+y$，输出签名 $\sigma'=\varepsilon+h$，概率 $P\geqslant(1,D_\sigma^{3l}(\varepsilon)/MD_{\sigma,w}^{3l}(\varepsilon))$，得到 $\sigma_i=\mathrm{encode}(\sigma_i')\in Z_q^n$，计算 $v_1=\sigma+\boldsymbol{B}_v r\in Z_q^n$，$v_2=\boldsymbol{A}^{\mathrm{T}}w+2e_2\in Z_q^N$，$v=(m_i+\langle bv,r\rangle+\langle w,H_1(\mathrm{ID}_S,\mathrm{ID}_V)\rangle+2ov) \bmod q$，得到密文 $c_i=(v\|v_1\|v_2)$。随机选择 (k_{i_0},k_{i_1})服从分布 χ_B，获取当前时间戳 T_G，计算 $M_i=\mathrm{ID}_i\|\mathrm{ID}_a\|c_i\|T_G$，将签名 o_i和 M_i嵌入接入请求信息中，最后发给组长。

组长收到组中所有成员的访问请求信息后，执行以下步骤：首先验证签名，若等式成立，则签名有效，具体为计算 $h'=H_2(\varepsilon\boldsymbol{A}-H_1(\mathrm{ID}_S,\mathrm{ID}_V)h,m)$，如果 $\|\varepsilon\|\leqslant 2\sigma\sqrt{3l}$ 且 $h'=h$，则签名有效。聚合密文 $c=\sum_{i=1}^{n}c_i$，由 $h=H_2(y,c)$，$x=\mathrm{sk}_G h\in Z^{3t}$ 生成签名 $\sigma_G'=\varepsilon+h$，得到 $\sigma_G=\mathrm{encode}(\sigma_G')\in Z_q^n$，随机选择 (k_{G_0},k_{G_1})服从分布 χ_B，计算 $M_G=\mathrm{ID}_G\|\mathrm{ID}_a\|c\|T_S$，组长将新生成的签名和 M_G嵌入聚合请求信息中发送给 AMF。

在收到聚合请求消息后，AMF 将执行以下步

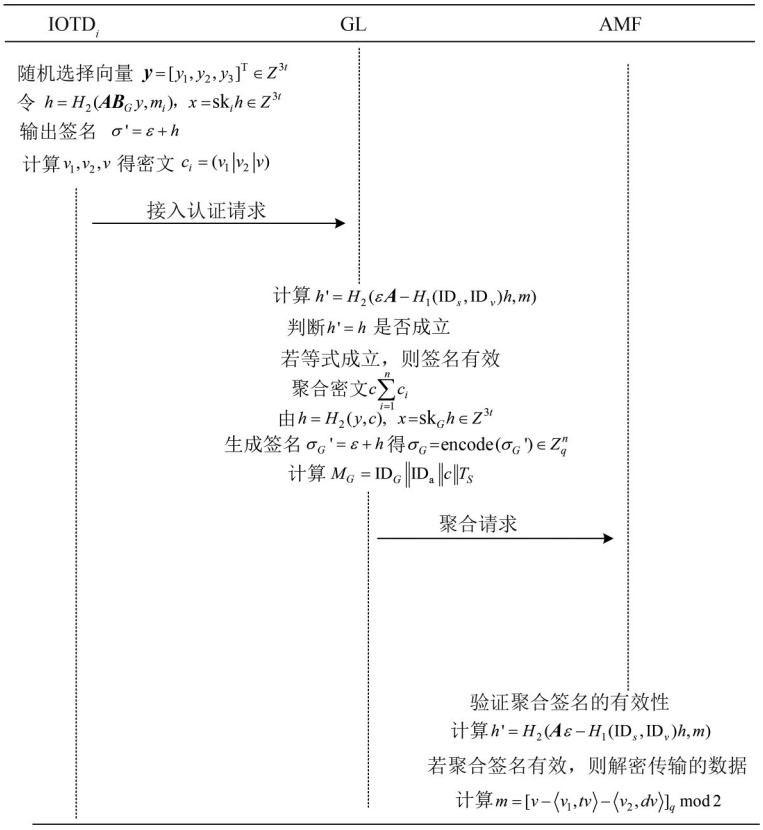


图3　身份认证阶段

骤：首先验证时间戳T_S的有效性，若有效则通过$\sigma_G'=(H_2(y,\sum_{i=1}^{n}c_i),\mathrm{sk}_G h+\sum_{i=1}^{n}\mathrm{pk}_i)$验证签名，若等式$\sigma'=\sigma$成立则签名有效，AMF在验证签名有效后可通过计算$m=[v-\langle v_1,t_v\rangle-\langle v_2,d_v\rangle]_q \bmod 2$解密要传输的数据$m$。

3 安全评估

3.1 安全模型

本文方案安全模型将从挑战者（challenger，C）和攻击者（attacker1，A_1）、（Attacker2，A_2）的角度进行相关描述，安全模型定义如下。

游戏1：首先C运行设置算法来生成系统参数，C将系统参数发送给攻击者，同时秘密保存主密钥。

阶段1 由A_1进行多项式时间的自适应查询。

公钥查询：A_1选择一个标识ID_i并查询其部分私钥。C通过运行密钥提取算法来获得部分密钥，并将其发送给A_1。A_1提交一个关于身份ID_i的公钥查询。最后，C输出公钥给A_1。

私钥查询：如果身份ID_i的公钥没有被替换，C将完整的私钥发送给A_1，否则停止游戏。

公钥替换：A_1在合适的范围内用一个新的公钥pk_i'替换之前的公钥pk_i。

签密查询：A_1对签密者的身份ID_s，解签密者的身份ID_v及消息m进行签密查询。C通过运行签密算法返回密文c。

解签密查询：A_1对签密者身份ID_s，解签密者身份ID_v以及密文c进行解签密查询。C通过运行解签密算法返回结果。

挑战：A_1停止阶段1的自适应查询，选择两个等长的消息(m_0,m_1)和两个身份(ID_s^*,ID_v^*)，其中，ID_s^*为签密者身份，ID_v^*为解签密者身份。阶段1中，A_1无法提取身份ID_v^*上的完整私钥。

阶段2 A_1可以同阶段1一样执行自适应查询，然而A_1不能在ID_v^*上执行私钥查询。如果在挑战阶段之前替换了身份ID_v^*的公钥，A_1就不能查询其部分私钥。挑战阶段后，A_1无法向C*的解签密查询器提交查询。

假设：A_1输出一个假设b^*。如果满足$b^*=b$，则C输出LWE问题的解。攻击者优势被定义为$Adv(A_1)=\left|\Pr[b^*=b]-1/2\right|$，其中，$\Pr|b^*=b|$为$b^*=b$的概率。

游戏2：在此阶段只改变了游戏1的系统公钥生成过程，其余步骤与游戏1相同。

3.2 安全分析

3.2.1 正式的安全性分析

（1） 正确性

引理1 假设$x\leftarrow D_{Z^n,s}$，当$s\geqslant\omega\sqrt{\log n}$时，不等式$\|x\|\leqslant s\sqrt{n}$和$\|x\|\leqslant s\omega(\sqrt{\log n})$能够以概率$1-\mathrm{negl}(n)$成立。

由引理1可知签密算法不能统计区分分布，因此存在$\|\varepsilon\|\leqslant 2\sigma\sqrt{3l}$，有式（9）成立。

$$v-<v_1,t_v>-<v_2,d_v>=(m_2+2\mathrm{error})\bmod 2 \quad (9)$$

对于C有$v-<v_1,t_v>-<v_2,d_v>=(m_2+2\mathrm{error})\bmod 2$，因此，如果$|2\mathrm{error}|<q/2$总会有$m=[v-<v_1,t_v>-<v_2,d_v>]q \bmod 2$。

证明：

$$|2\mathrm{error}|=\left|2e+2o_s^t r-2d_v^t e_2\right|<\frac{q}{2} \quad (10)$$

当$|2\mathrm{error}|=\left|2e+2o_s^t r-2d_v^t e_2\right|<\frac{q}{2}$时，等式$m=[v-<v_1,t_v>-<v_2,d_v>]q \bmod 2$成立。

（2）保密性

接下来的交互游戏中，第一类多项式时间攻击者A_1可以改变用户的公钥，但不知道主密钥，第二类多项式时间攻击者A_2知道主密钥，但不能更改用户的公钥。

定理1 在随机oracle模型中，最多进行q_1密钥生成查询、q_2部分私钥查询、q_3公钥替换和q_4秘密值查询。假设签密方案被A_1打破优势，那

么挑战者C可以由式$\xi c \geqslant 1-(1/q_1)^{q_2}/q_1 \cdot \xi - \mathrm{negl}(n)$解决LWE问题，且时间间隔不超过$q_1t_1+q_2t_2+q_3t_3+q_4t_4$，其中，$t_1$是密钥生成查询的时间，$t_2$是部分私钥查询的时间，$t_3$是公钥替换查询的时间，$t_4$是秘密值查询的时间。

证明：假设C是A_1的挑战者。游戏i=1意味着A_1在游戏i中获胜，那么|Pr[游戏$_i$=1]−1/2|是A_1在游戏i中的一个显著优势，其中，$i \in \{0,1,2\}$。

游戏0：首先，C运行设置算法生成系统参数和主私钥R。C发送参数给A_1，并保留主私钥R。且A_1不知道主私钥。C使用3个列表（L_1,L_2,L_3）用于后续查询存储，列表初始为空。

阶段1　由A_1执行一系列自适应查询且每个查询都依赖于前面的查询结果。

H_1查询：A_1对身份ID_i发出H_1查询。C检查(ID_i,u_i)是否已经存在于列表L_1中。如果有一个匹配的元组，C将u_i返回给A_1，否则，它返回一个从Z_q^n中选择的随机向量u_i，并在列表L_1中存储(ID_i,u_i)。

H_2查询：A_1进行一个H_2查询。C检查$(\boldsymbol{A},\boldsymbol{B}_s,y,m)$是否已经存在于列表$L_2$中。如果有一个匹配的元组，C返回$h$作为应答，否则，它返回其选择的随机数$h \in \{-1,0,1\}^k$，并在列表$L_2$中存储$(\boldsymbol{A},\boldsymbol{B}_s,y,m)$。

部分私钥查询：A_1选择一个标识ID_i并查询其部分私钥。C运行提取算法，生成与ID_i对应的部分私钥d_i。最后，C将其发送到A_1并将(ID_i,d_i)存储在列表中。

请求公钥：A_1提交一个关于身份ID_i的公钥查询。如果pk_i存在于列表L_3中，则C将其发送给A_1，否则，C选择矩阵$\boldsymbol{B}_i$和向量$\boldsymbol{b}_i$来计算身份ID_i的pk_i。最后，C返回公钥$pk_i \leftarrow (\boldsymbol{b}_i \| \boldsymbol{B}_i^{\mathrm{T}}) \in Z_q^{M\times(1+n)}$，并将$(ID_i,t_i,\boldsymbol{b}_i,\boldsymbol{B}_i,o_i)$添加到列表$L_3$中。

私钥查询：如果没有替换标识ID_i的公钥，C运行密钥生成算法生成与ID_i对应的私钥。C将完整的私钥(d_i,t_i)发送到A_1，并存储(ID_i,d_i,t_i)在列表L_3中。如果身份ID_i的公钥被替换，C将停止游戏。

公钥替换：A_1选择的合适范围内的新公钥pk替换之前的pk_i，并使用$(ID_i,t_i,\boldsymbol{b}_i,\boldsymbol{B}_i,o_i)$更新列表。

签密查询：A_1选择签密者的身份ID_s，解签密者的身份ID_v，消息m，C选择一个随机数$t \in \{1,2,3,4,\cdots,q\}$。如果$ID_S^* = ID_t$，C调用签密算法并将密文$c$返回$A_1$，否则C从$Z^{n\times M}$中随机从$Z$和$\boldsymbol{B}_v$中随机选择$y$计算$h$，并在列表$L_2$中存储$(\boldsymbol{A},\boldsymbol{B}_v,y,h)$。然后，C继续计算：

$$\sigma' = \varepsilon + h \tag{11}$$

$$v_1 = \sigma + \boldsymbol{B}_v r \in Z_q^n \tag{12}$$

$$v_2 = \boldsymbol{A}^{\mathrm{T}} w + 2e_2 \in Z_q^N \tag{13}$$

$$v = (m + < b_v, r > + < w, H_1(ID_s, ID_v) > + 2ov) \bmod q \tag{14}$$

并返回密文$c=(v \| v_1 \| v_2)$给A_1。如果$ID_s \neq ID_t$，C返回空值标识“⊥”给A_1。

解签密查询：A_1发出签密者的身份ID_s、解签密者的身份ID_v和密文c的解签密密文。如果$ID_s \neq ID_t$，C返回一个解签密结果，否则C计算h'并通过以下等式恢复m：

$$h' = H_2(\boldsymbol{B}_s \boldsymbol{A}\varepsilon - H_1(ID_s, ID_v) pk_s h, m) \tag{15}$$

$$m = [v - < v_1, t_v > - < v_2, d_v >] q \bmod 2 \tag{16}$$

最后，当且仅当$h'=h$时，C返回m，否则，C返回“⊥”。

挑战：A_1决定停止第一阶段的自适应查询，并选择等长度的消息(m_0,m_1)、发送者的身份ID_s^*和接收者的身份ID_v^*。在第一阶段中，A_1无法提取身份ID_v*上的完整私钥。假设C已经查询了H_0和部分私钥、公钥和私钥，C必须考虑两种情况来回答此挑战查询。

情况1：如果ID_v*=ID_t，C从{0,1}中随机选择b，且$\boldsymbol{y}^* = [y_1,y_2,y_3]^{\mathrm{T}} \in Z$，通过以下等式计算

(v^*, v_1^*, v_2^*)：

$$h = H_2(\boldsymbol{A}\boldsymbol{B}_v \boldsymbol{y}^*, mb) \tag{17}$$

$$x^* = \mathrm{sk}_s^* h^* \tag{18}$$

$$\sigma^* = \mathrm{encode}(\sigma') \in Z_q^n \tag{19}$$

$$v_1^* = \sigma^* + \boldsymbol{B}_v r \in Z_q^n \tag{20}$$

$$v_2^* = \boldsymbol{A}^{\mathrm{T}} W + 2e_2^* \in Z_q^n \tag{21}$$

$$v^* = (mb + < b_v, r > + < w, H_1(\mathrm{ID}_s^*, \mathrm{ID}_v^*) > + 2o) \bmod q \tag{22}$$

最后，C在列表L_2中存储(v^*, v_1^*, v_2^*)，并输出$c^* = (v^*, v_1^*, v_2^*)$作为挑战密文。

情况2：如果$\mathrm{ID}_v^* \neq \mathrm{ID}_t$，则C失败并终止此游戏。

阶段2 A_1可执行与阶段一相同步骤的查询，但A_1不能在$(\mathrm{ID}_s^*, \mathrm{ID}_v^*)$上执行私钥查询。若在挑战阶段之前替换了身份$\mathrm{ID}_v^*$的公钥，$A_1$就不能查询其部分私钥。在挑战阶段后，$A_1$无法向$c^*$的解签密协议提交查询。

假设：如果$b' = b$，A_1输出一个猜测b'，C输出LWE问题的解决方案。

游戏1：从游戏0中提取用户的部分私钥且游戏1只改变提取算法，C选择$d_i \leftarrow D_{Z^N, s_2 \cdot \omega(\log n)}$计算$u_i = \boldsymbol{A} d_i$，若$u_i$未在在列表$L_1$中，C使$H_1(\mathrm{ID}_i) = u_i$，否则C采用预形成提取算法得到$d_i$。根据原像采样算法的性质，游戏0和游戏1的私钥分布无法区分，即A_1无法区分游戏0和游戏1，因此：

$$\left|\Pr[\text{游戏}1 = 1] - \Pr[\text{游戏}0 = 1]\right| = \mathrm{negl}(n) \tag{23}$$

游戏1的其余步骤与游戏0相同。

游戏2：在游戏2中，除了游戏1的系统公钥的生成过程外，游戏1的其余步骤与游戏0相同。A_1在游戏1中不使用矩阵的陷门$\boldsymbol{R}$来提取用户的部分私钥。由$(\boldsymbol{A}, \boldsymbol{R}) \leftarrow \mathrm{TrapGen}(1^n, 1^m, q)$和$\boldsymbol{A} \in Z_q^{n \times l}$可知，$\boldsymbol{A}$的分布不可区分。即$A_1$不可区分游戏1和游戏2，因此：

$$\left|\Pr[\text{游戏}2 = 1] - \Pr[\text{游戏}1 = 1]\right| = \mathrm{negl}(n) \tag{24}$$

$$\xi - \left|\Pr[\text{游戏}2 = 1] - \frac{1}{2}\right| = \left|\Pr[\text{游戏}0 = 1] - \frac{1}{2}\right| -$$
$$\left|\Pr[\text{游戏}2 = 1] - \frac{1}{2}\right| \leqslant \left|\Pr[\text{游戏}0 = 1]\right| -$$
$$\left|\Pr[\text{游戏}1 = 1]\right| - \left|\Pr[\text{游戏}2 = 1]\right| \leqslant \mathrm{negl}(n) \tag{25}$$

因此，$\left|\Pr[\text{游戏}2 = 1] - 1/2\right| \geqslant \xi - \mathrm{negl}(n)$成立。

由于在游戏2中的$\boldsymbol{A}$为随机选择，所以具体的步骤为：C运行设置算法，得到系统参数$\mathrm{params} = \{\boldsymbol{A}, H_1, H_2, s_1, s_2, \chi_B\}$，其中，$\boldsymbol{A}$为随机选择。此后，C向攻击者$A_1$传递参数。

阶段3 公钥查询、H_0查询、H_1查询、信号加密查询和非信号加密查询与游戏0中的查询相同，对其他查询的描述如下。

部分私钥查询：A_1选择一个标识ID_i并查询其部分私钥。C运行部分私钥提取算法，生成与ID_i对应的部分私钥d_i。然后C将其交付到A_1并存储$(\mathrm{ID}_i, u_i, d_i)$在列表中。

公钥替换：C将$(\mathrm{ID}_i, u_i, d_i, x_i, \boldsymbol{B}_i, o_i)$替换为$(\mathrm{ID}_i, u_i, b_i, \boldsymbol{B}_i)$。

挑战：在进行自适应查询后，A_1输出两个不同的挑战明文m_0、m_1和两个身份$(\mathrm{ID}_s^*, \mathrm{ID}_v^*)$到C。C应答查询如下：

1）如果$\mathrm{ID}_v^* \neq \mathrm{ID}_t$，C失败并终止游戏；否则C获取$(\mathrm{ID}_v, u^*, x_t, b_t, \boldsymbol{B}_t, o_t)$或$(\mathrm{ID}^*, u^*)$。其中，前者表示$\mathrm{ID}_v^*$的公钥未被替换，后者表示其公钥已被替换。

2）如果没有替换ID_v^*的公钥$\left((b^*, \boldsymbol{B}^*) = (b_t', \boldsymbol{B}_t')\right)$，则C继续执行2），否则C执行3）。

3）验证已替换的公钥$(b_t', \boldsymbol{B}_t')$。如果不是有效的公钥，C停止游戏，否则C令$(b^*, \boldsymbol{B}^*) = (b_t', \boldsymbol{B}_t')$。

4）C选择$y \leftarrow Z_q^{1+n}$和$r \in \{0,1\}^M$，然后将$(b_t, \boldsymbol{B}_t, y)$和$(b_t, \boldsymbol{B}_t, (rTb_t \| \boldsymbol{B}_t r))$发送给$A_1$。如果$A_1$可以用$1-\mathrm{negl}(n)$的概率来区分它们，那么公钥

$(b_t', \boldsymbol{B}_t')$就会是一个有效的公钥。

5）C 令 $(v^*, v_1^*, v_2^*)=(v', w^{\mathrm{T}}u_t, \boldsymbol{A}^{\mathrm{T}}w+2ov)$，并将挑战密文 $c^*=(v^*, v_1^*, v_2^*)$输出到 A_1。

假设：如果 $b'=b$，则 A_1输出一个假设 b'，C 输出 LWE 问题的解。

挑战过程中，A_1可以通过调用密钥生成算法轻松获得有效的公钥；相反，若提供了一个无效的公钥，A_1失败的概率为 1-negl(n)。因为 A_1在游戏中获胜，所以我们有理由假设 A_1提供了一个有效公钥的概率为 1。C 的优势为 ξ_{C}，它等于以下 3 个事件同时发生的概率。

事件 a_1：当查询部分私钥时，游戏没有终止。

事件 a_2：满足 $\mathrm{ID}_v^*=\mathrm{ID}_t$。

事件 a_3：A_1成功地区分了挑战性的密文。

如果上述游戏没有终止，A_1在游戏 2 中的显著优势是 $\left|\Pr[\text{游戏}2=1]-1/2\right|\geqslant\xi-\mathrm{negl}(n)$，即 $\Pr[a_3|a_2\cap a_1|]\geqslant\mathrm{negl}(n)$。因此，如果 A_1能以优势 ξ 打破签密方案，则 C 以优势 $\xi_C\geqslant(1-1/q_1)q_2/q_1\cdot\varepsilon-\mathrm{negl}(n)$用 A_1解决 LWE 问题，且时间间隔不超过 $q_1t_1+q_2t_2+q_3t_3+q_4t_4$。

定理 2　随机 oracle 模型中，如果 A_2可以优势 ξ 打破签密方案，则 C 可以解决 LWE 问题，时间间隔不超过 $q_1t_1+q_2t_2+q_3t_3$，优势 $\xi_C\geqslant(1-1/q_1)q_2/q_1\cdot\xi-\mathrm{negl}(n)$。其中，$t_1$是一个关键生成查询的时间，$t_2$是一个部分私钥查询的时间，$t_3$是秘密值查询的时间。

证明：假设 C 是攻击者 A_2的挑战者，游戏在 A_2和 C 之间构造如下。

初始阶段：通过运行设置算法获得私钥 R 和系统参数 $\mathrm{params}=\{\boldsymbol{A}, H_1, H_2, s_1, s_2, \chi_{\mathrm{B}}\}$，C 将参数和 R 传递给 A_2。

阶段 4　除以下查询外，A_2提交了一系列作为定理 1 的自适应查询。

请求公钥：如果输入 $i=t$，则设置 $b_t=b^*$ 和 $\boldsymbol{B}_t=\boldsymbol{B}^*$，否则，C 选择 $\boldsymbol{B}_i\leftarrow Z_q^{n\times M}$，$x_i\leftarrow\chi_B^n$和 $o_i\leftarrow\chi_B^M$。然后 C 进行计算：

$$b_i=\boldsymbol{B}_i^{\mathrm{T}}x_i+2o_i \bmod q \tag{26}$$

C 将 $(\mathrm{ID}_i, b_i, \boldsymbol{B}_i, o_i)$添加到列表 L_1 中，并将 $(\mathrm{ID}_i, b_i, \boldsymbol{B}_i)$传递到 A_2。

挑战：A_2完成第一阶段的自适应查询后，A_2输出两个不同的挑战明文 m_0和 m_1，以及身份信息 $(\mathrm{ID}_S^*, \mathrm{ID}_V^*)$，如果 $\mathrm{ID}_V^*=\mathrm{ID}_t$则判定失败并终止游戏，否则 C 检查列表 L_1获得 $(\mathrm{ID}_V^*, b^*, \boldsymbol{B}^*)$并计算 $d_t\leftarrow\mathrm{Extract}(\mathrm{ID}_t, \mathrm{params})$，$u_t=H_1(\mathrm{ID}_t)$。C 设置 $c^*=(v^*, v_1^*, v_2^*)=(v'+w^{\mathrm{T}}u_t, \boldsymbol{A}^{\mathrm{T}}w+2ov)$，并将挑战密文 c^*传递给 A_2。

假设：A_2输出一个假设 b'。如果 $b'=b$，C 输出 LWE 问题实例的解。

（3）不可伪造性

定理 3　对于多项式时间攻击者 A_1，签密方案的不可伪造性是基于 R-SIS 假设。假设 $\mathrm{Adv}(\mathrm{A}_1)=\xi$，则在多项式时间内挑战者 C 以优势 $\mathrm{Adv}_{\mathrm{C}}=\xi(1-2^{-\omega\log n})$解决 R-SIS 问题。

证明：假设攻击者 A_1可以制造一个签密密文。那么 A_1和它的挑战者 C 之间的游戏可以构建为：首先，C 调用设置算法获得系统参数 $\mathrm{params}=\{H_0, H_1, s_1, s_2, \chi_{\mathrm{B}}\}$和系统私钥 R，然后返回参数给 A_1但保留系统私钥 R。C 维护两个哈希列表 L_1和 L_2以及密钥列表 L_3，列表最初为空。

查询：A_1提交一系列自适应查询，包括定理 1 中第一阶段的各种查询。

伪造：A_1输出一个伪造文件 $(c', \mathrm{ID}_S', \mathrm{ID}_V')$到 C。当且仅当密文有效时，C 成功，$\mathrm{A}_1$可以输出另一个伪造文件 $(c, \mathrm{ID}_S', \mathrm{ID}_V')$。

由于 $\boldsymbol{A}(\varepsilon'-\varepsilon'+d_V(h'-h))=0$ 成立，对于 ε^* 与 h^* 有 $\varepsilon'\leqslant2\sigma\sqrt{3l}$，$h'\leqslant\lambda$，故 $\varepsilon^*-\varepsilon'+d_V(h'-h^*)\leqslant8\sigma\sqrt{2l}+4s\lambda\sqrt{2l}$ 以压倒性的概率成立。

由原像采样函数和最小熵性质可得 $\varepsilon^*-\varepsilon'+d_V(h'-h^*)=0$ 的概率最多为 $1-2^{-\omega\log n}$，因此 C 成

功解决R-SIS问题的概率为$\mathrm{Adv}_C=\xi(1-2^{-\omega\log n})$。

3.2.2 非正式的安全分析

（1）相互认证

本文方案使物联网设备组和AMF之间能够实现相互认证。物联网设备依据密钥生成中心分配的部分密钥生成签密信息，此后向认证单元发送认证请求并由组长进行聚合，认证单元根据判断聚合签密的有效性来对群组内的物联网设备进行批量认证。若攻击者缺乏相应的私钥则无法获得有效的签密和聚合签密。在认证单元经由设备组组长完成对群组的统一认证后，群组成员可依据AMF返回的认证响应来判断此节点的合法性。

（2）不可链接性

本文方案中，每个物联网设备发送请求消息时都使用注册阶段由部分私钥产生的完整独立密钥。由于存在一个防碰撞哈希函数H，因此没有任何有用的信息可以链接两个签名。在身份认证的聚合阶段，每个物联网设备对于消息与签名的聚合都为匿名。在R-SIS问题下，对于私钥所产生的多个签名σ_i和σ_i'，攻击者将不能判断签名来源是否为同一物联网设备。

3.3 BAN逻辑证明

本节使用BAN逻辑证明了该方案的正确性，它作为一种形式逻辑，被广泛用于验证认证和密钥协议的有效性。该方案的安全目标是实现5G物联网组与网络侧AMF之间的相互认证和安全的数据传输。

（1）P和Q代表通信实体；

（2）K_{ab}表示通信实体的共享会话密钥；

（3）K_a和K_b表示通信实体的公钥；

（4）$K_{a^{-1}}$和$K_{b^{-1}}$表示通信实体的密钥；

（5）X和Y表示协议中传递的消息；

（6）$P|\equiv X$：P认为消息X为真；

（7）$P\lhd X$：P曾收到包含X的消息；

（8）$P|\sim X$：P曾发送包含X的消息；

（9）$P|\Rightarrow X$：P控制X；

（10）$\#(X)$：消息X是新鲜的；

（11）$P\overset{K}{\longleftrightarrow}Q$：P和Q用共享对称密钥$K$相互通信；

（12）K：用密钥加密消息X所获得的密文；

（13）$<X>Y$：X和Y的组合，Y是一个秘密值，其存在表示Y的所有者的身份；

（14）(X,Y)：X和Y之间相关；

（15）$\mathrm{rule}_1/\mathrm{rule}_2$：$\mathrm{rule}_2$可以从$\mathrm{rule}_1$中推导出来。

为了使BAN逻辑进行正确性分析，对BAN逻辑模型的一些相关推理规则描述如下：

消息含义规则：

$$\frac{P|\equiv Q\overset{K}{\longleftrightarrow}P,P\lhd\{X\}_K}{P|\equiv Q|\sim X} \tag{27}$$

如果P相信P和Q之间的共享会话密钥K以及P接收到由K加密的消息[3]K，则P认为Q曾经发送了消息X。

Nonce验证规则：

$$\frac{P|\equiv\#(X),P|\equiv Q|\sim X}{P|\equiv Q|\equiv X} \tag{28}$$

如果P相信消息X是新鲜的，且P相信Q曾发送信息X，则P相信消息X。

管辖权规则：

$$\frac{P|\equiv Q\Rightarrow X,P|\equiv Q|\equiv X}{P|\equiv X} \tag{29}$$

如果P相信Q对有管辖权，而P相信Q相信X，那么P就相信信息X。

新鲜度规则：

$$\frac{P|\equiv\#(X)}{P|\equiv\#(X,Y)} \tag{30}$$

如果P相信X是新鲜的，则P相信(X,Y)是新鲜的。

会话密钥规则：

$$\frac{P\left|\equiv \#(K), P\right|\equiv Q\left|\equiv X\right.}{P\left|\equiv P\overset{K}{\longleftrightarrow}Q\right.} \tag{31}$$

查看规则：

$$\frac{P\left|\lhd (X,Y)\right.}{P\left|\lhd X\right.} \tag{32}$$

$$\frac{P\left|\equiv P\overset{K}{\longleftrightarrow}Q, P\lhd \{X\}_K\right.}{P\left|\lhd X\right.} \tag{33}$$

如果P接收到一条消息，并且P知道该消息的相关密钥，则P接受该消息的组件。

本文提出方案的安全目标描述如下：

G1：$\mathrm{AMF}\left|\equiv \mathrm{IOTD}_i\overset{m_i}{\longleftrightarrow}\mathrm{AMF}\right.$

G2：$\mathrm{IOTD}_i\left|\equiv \mathrm{AMF}\overset{m_{\mathrm{AMF}}}{\longleftrightarrow}\mathrm{IOTD}_i\right.$

本文提出方案的理想形式信息描述如下：

M1：访问请求信息

由IOTD_i发出

$$\mathrm{AMF}<\left\{\mathrm{ID}_{\mathrm{IOTD}_i},\mathrm{ID}_{\mathrm{AMF}},\{\mathrm{IOTD}_i\overset{m_i}{\longleftrightarrow}\mathrm{AMF}\}K_A,\ T_S,\{\mathrm{ID}_{\mathrm{IOTD}_i},\mathrm{ID}_{\mathrm{AMF}},\{\mathrm{IOTD}_i\overset{m_i}{\longleftrightarrow}\mathrm{AMF}\}K_A,\ T_S\}\mathrm{K}_{i-1}\right\}$$

M2：访问响应消息

由AMF发出：

$$\mathrm{IOTD}_i<\left\{\mathrm{ID}_{\mathrm{AMF}},\mathrm{ID}_{\mathrm{IOTD}_i},\{\mathrm{AMF}\overset{m_{\mathrm{AMF}}}{\longleftrightarrow}\mathrm{IOTD}_i\}K_i,\ T_S,\{\mathrm{ID}_{\mathrm{AMF}},\mathrm{ID}_{\mathrm{IOTD}_i},\{\mathrm{IOTD}_i\overset{m_{\mathrm{AMF}}}{\longleftrightarrow}\mathrm{AMF}\}K_i,\ T_S\}K_{A-1}\right\}$$

本文方案将做出以下假设：

H1：$\mathrm{IOTD}_i\left|\equiv \overset{K_{\mathrm{AMF}}}{\longrightarrow}\mathrm{AMF}\right.$

H2：$\mathrm{AMF}\left|\equiv \overset{K_i}{\longrightarrow}\mathrm{IOTD_i}\right.$

H3：$\mathrm{IOTD}_i\left|\equiv \#(T_S)\right.$

H4：$\mathrm{AMF}\left|\equiv \#(T_S)\right.$

H5：$\mathrm{AMF}\left|\equiv \mathrm{IOTD}_i\right|\Rightarrow \mathrm{IOTD}_i\overset{m_i}{\longleftrightarrow}\mathrm{AMF}$

H6：$\mathrm{IOTD}_i\left|\equiv \mathrm{AMF}\right|\Rightarrow \mathrm{AMF}\overset{m_{\mathrm{AMF}}}{\longleftrightarrow}\mathrm{IOTD}_i$

最后，由定义的BAN逻辑规则和假设可得到本文方案的理想化形式分析如下：由M1和H2，根据消息含义规则$\left[(P\left|\equiv \overset{K}{\longrightarrow}Q, P\lhd \{X\}K-1)/(P\right|\equiv Q\left|\sim X\right.)\right]$可推出：

S1：$\mathrm{AMF}\left|\equiv \mathrm{IOTD}_i\right|\sim \mathrm{IOTD}_i\overset{m_i}{\longleftrightarrow}\mathrm{AMF}$

由M2和H1，根据消息含义规则$\left[(P\left|\equiv \overset{K}{\longrightarrow}Q, P\lhd \{X\}_{K^{-1}})/(P\right|\equiv Q\left|\sim X\right.)\right]$可推出：

S2：$\mathrm{IOTD}_i\left|\equiv \mathrm{AMF}\right|\sim \mathrm{AMF}\overset{m_{\mathrm{AMF}}}{\longleftrightarrow}\mathrm{IOTD}_i$

由S1和H4，根据nonce验证规则$\left[(P\left|\equiv \#(X), P\right|\equiv Q\sim X)/(P\left|\equiv Q\right|\equiv X)\right]$可推出：

S3：$\mathrm{AMF}\left|\equiv \mathrm{IOTD}_i\right|\equiv \mathrm{IOTD}_i\overset{m_i}{\longleftrightarrow}\mathrm{AMF}$

由S2和H3，根据nonce验证规则$\left[(P\left|\equiv \#(X), P\right|\equiv Q\left|\sim X\right.)/(P\left|\equiv Q\right|\equiv X)\right]$可推出：

S4：$\mathrm{IOTD}_i\left|\equiv \mathrm{AMF}\right|\equiv \mathrm{AMF}\overset{m_{\mathrm{AMF}}}{\longleftrightarrow}\mathrm{IOTD}_i$

由S3和H5，根据管辖权规则$\left[(P\left|\equiv Q\right|\Rightarrow X, P\left|\equiv Q\right|\equiv X)/(P\left|\equiv X\right.)\right]$可推出：

S5：$\mathrm{AMF}\left|\equiv \mathrm{IOTD}_i\overset{m_i}{\longleftrightarrow}\mathrm{AMF}\right.$

由S4和H6，根据管辖权规则$\left[(P\left|\equiv Q\right|\Rightarrow X, P\left|\equiv Q\right|\equiv X)/(P\left|\equiv X\right.)\right]$可推出：

S6：$\mathrm{IOTD}_i\left|\equiv \mathrm{AMF}\overset{m_{\mathrm{AMF}}}{\longleftrightarrow}\mathrm{IOTD}_i\right.$

由S5和S6可得初始设定的安全目标G1和G2验证成功。

4　仿真实验与分析

本节将从安全性和计算开销两个方面对方案进行性能分析，与文献[9-11]的签密方案和文献[16-17]的抗量子方案进行对比分析。本文采

用Win10操作系统，Intel-i7-12700F处理器，内存为16 GB，利用OPENSSL库实现各个方案。对于签密认证方案，计算开销是性能测量的重要指标之一。密码运算时间的符号表示见表2。

4.1 签密方案性能对比

根据美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）的安全参数，为了达到与AES-128相同的安全级别，假设哈希算法的输出为128 bit，时间戳TS为32 bit，随机数为128 bit，标识ID大小为128 bit。由于本文对比的方案[9-11]使用了基于椭圆曲线的签密方式，在对方案CSUAC-IoT[9]、CLOOSC[10]和CLASS[11]进行仿真对比时做出如下设置：首先生成阶为q的加法群，其中生成元为P，P为度为2的超奇异椭圆曲线上的点，p为1 024 bit素数，q为256 bit的素数。在签密与解签密方面，本文假设参与群组认证的组成员个数为m，本文方案与文献[9-11]的方案进行对比，签密开销对比见表3。

Mandal等[9]通过用户密码、生物识别技术以及移动设备作为方案中认证的3个因素构造认证方案。通过可信第三方（trust authority，TA）针对椭圆曲线离散对数问题设置$E_q(a,b):y^2=+x^3+ax+b(\mathrm{mod}\,q)$相应参数并公开$\{G,E_q\{a,b\},Y_T\}$。该方案的注册阶段分多个部分，方案中的多步骤注册为该方案开销增大的原因之一，其第一部分由网关节点和物联网设备以及TA进行交互；当注册一个网关节点时，TA会分配一个唯一的标识$\mathrm{ID}_{\mathrm{GN}}$，一个随机私钥并计算其相应的公钥$Y_G=x_G\cdot G$，其中，TA会用各自的网关节点加载物联网设备的参数$\{\mathrm{ID}_{S_i},Y_{S_i}\}$。在Mandal所设计的方案[9]中，TA会再次选择随机密钥Z_i以保障物联网设备与其对应的网关节点进行安全通信；第一部分的注册结束后会有移动设备与TA进行二次注册并在此部分使用生物识别技术，移动设备会再次选择秘密值与相应的标识ID，且会通过用户进行两次签密操作$\mathrm{Sign}_G=H(C_1\|T_1\|T_{2i}\|S_1\|S_{2i})\cdot k_u+x_u(\mathrm{mod}\,q)$。本文所设计的方案中，注册阶段由物联网设备与认证单元AMF在密钥生成中心KGC进行统一注册，避免了多次的重复计算，本文方案由于采用无证书密码体制，密钥生成中心仅为物联网设备以及认证单元分配部分密钥$d_i\leftarrow\mathrm{SampleD}(\overline{\boldsymbol{A}},\boldsymbol{R},u,s_2)$，IOTD根据分配的部分密钥生

表2 密码运算时间的符号表示

密码运算名称	英文	运算时间的符号表示
ECC乘法运算	Elliptic curve multiplication	T_{em}
ECC加法运算	Elliptic curve addition	T_{ea}
双线性配对运算	Bilinear pairing operation	T_{p}
模指数运算	Modular exponential operation	T_{m}
哈希函数运算	Hash function operations	T_{h}
NTRU乘法运算	NTRU multiplication	T_{lm}
NTRU加法运算	NTRU addition operation	T_{la}

表3 签密开销对比

方案	签密	解签密	运算总量	运算代价/ms
Mandal等[9]	$12T_{\mathrm{h}}+10T_{\mathrm{em}}+3T_{\mathrm{ea}}+4T_{\mathrm{m}}$	$16T_{\mathrm{h}}+7T_{\mathrm{em}}+7T_{\mathrm{ea}}$	$28T_{\mathrm{h}}+17T_{\mathrm{em}}+10T_{\mathrm{ea}}+4T_{\mathrm{m}}$	92.502
Dohare等[11]	$5T_{\mathrm{h}}+4T_{\mathrm{em}}+2T_{\mathrm{ea}}$	$4T_{\mathrm{h}}+3T_{\mathrm{em}}+2T_{\mathrm{ea}}$	$9T_{\mathrm{h}}+7T_{\mathrm{em}}+4T_{\mathrm{ea}}$	35.914
Chen等[10]	$4T_{\mathrm{h}}+T_{\mathrm{p}}+6T_{\mathrm{em}}+3T_{\mathrm{ea}}$	$4T_{\mathrm{h}}+T_{\mathrm{p}}+5T_{\mathrm{em}}+2T_{\mathrm{ea}}$	$8T_{\mathrm{h}}+11T_{\mathrm{em}}+5T_{\mathrm{ea}}+2T_{\mathrm{p}}$	137.581
本文方案	$2T_{\mathrm{h}}+4T_{\mathrm{lm}}+5T_{\mathrm{la}}+T_{\mathrm{m}}$	$2T_{\mathrm{h}}+2T_{\mathrm{lm}}+2T_{\mathrm{la}}+T_{\mathrm{m}}$	$4T_{\mathrm{h}}+6T_{\mathrm{lm}}+7T_{\mathrm{la}}+2T_{\mathrm{m}}$	34.332

成完整的公私钥。IOTD 获取 $T_i \leftarrow (A, R_i, T_A, \sigma_R)$，计算 $Q_i = AR_i^{-1}$，其中 $R_i = H_1(\mathrm{ID}_u)$，$\|T_i\| \leqslant \sigma R / \omega(\sqrt{\log m})$，$\sigma R \geqslant \|\tilde{T}_A\|(\sigma\sqrt{m} \cdot \omega(\sqrt{\log^{3/2} m}))$，$i = 1, 2, \cdots, l, r$，$\mathrm{ID}_r \in \{\mathrm{U}, \mathrm{ID}_r\}$，$\mathrm{U} = \{\mathrm{ID}_1, \mathrm{ID}_2, \cdots, \mathrm{ID}_l\}$，其中，$\mathrm{ID}_s \in \mathrm{U}$ 为签密者身份标识，本文所提出的方案相较于 Mandal 等[9]的方案在保证注册阶段的安全通信的同时免去了多次注册的繁琐步骤。Mandal 方案[9]的算法签密所需要的开销为 $12T_{\mathrm{h}} + 10T_{\mathrm{em}} + 3T_{\mathrm{ea}} + 4T_{\mathrm{m}}$，解签密需要的开销为 $16T_{\mathrm{h}} + 7T_{\mathrm{em}} + 7T_{\mathrm{ea}}$。本文所提方案的签密需要的开销为 $2T_{\mathrm{h}} + 4T_{\mathrm{lm}} + 5T_{\mathrm{la}} + T_{\mathrm{m}}$，解签密需要的开销为 $2T_{\mathrm{h}} + 2T_{\mathrm{lm}} + 2T_{\mathrm{la}} + T_{\mathrm{m}}$。

Chen 等[10]通过离线计算的方式在物联网场景下构建了一种无证书的加密方案，采用云服务器负责分发整个系统的关键参数，假设云服务器传输信息的信道是安全的。离线计算时，首先给定发送方的身份 ID_S 和相应的公钥 $\mathrm{PK}_{\mathrm{IDS}}$ 和私钥 $\mathrm{SK}_{\mathrm{IDS}}$，随机选择 $r_1 \in Z_p^*$，$\beta \in Z_p^*$，$\mu \in Z_p^*$，$\gamma \in Z_p^*$，$r_2 \in \{0, 1\}^*$，计算 $U = \mu P$。该方案的离线阶段使用哈希函数 H_2 计算 $H_2(r_2, \mathrm{ID}_S, U, \mathrm{PK}_{\mathrm{ID}_S})$，并计算 $W = e(P, P)^{r_1} = g^{r_1}$，$C_1 = \alpha^{-1} r_1 P$，$C_2 = r_1(\beta + s)P = r_1(\beta P + P_{\mathrm{pub}})$，由 (U, W, C_1, C_2, T, r_2) 构成离线密文。该方案的在线签密阶段将由消息 m 以及离线密文进行计算 $C = k \oplus (m \| r_2 \| \mathrm{ID}_S)$，并在签密阶段由离线密文所得值继续计算 $h = H_4(C_3, C, r_2, \mathrm{ID}_S, \mathrm{ID}_R, C_1, C_2, \mathrm{PK}_{\mathrm{ID}_S}, \mathrm{PK}_{\mathrm{ID}_R})$，得到最后的密文 $\sigma = (U, T, C_1, C_2, C_3, C, t)$，该方案虽然通过离线计算的方式减小了该部分物联网设备的相应开销，但此后的解签密和验证阶段消息发送者与接收者由于密文的两次加密会在解签密进行大量计算，并验证 $e(P_{\mathrm{pub}} + q_{\mathrm{ID}_S} P, tT) = e(U, hP) e(U, \mathrm{PK}_{\mathrm{ID}_S})$，$e(C_1, P)^{\alpha} = W$ 同时导致整体开销增加。该方案的算法中签密所需要的开销为 $4T_{\mathrm{h}} + T_{\mathrm{p}} + 6T_{\mathrm{em}} + 3T_{\mathrm{ea}}$，解签密所需要的开销为 $4T_{\mathrm{h}} + T_{\mathrm{em}} + 5T_{\mathrm{ea}} + 2T_{\mathrm{p}}$。

Dohare 等[11]通过无证书聚合签密的方式构建认证方案，该方案中包含工业云服务器、密钥生成中心、数据持有者、数据使用者和雾节点。签密部分发送者 u_i 由身份标识 ID_R 和消息 msg_i 执行计算过程 $\psi_1 = g^{w_i} \cdot (\mathrm{OSK}_i^{w_i})$ 与 $\psi' = H_2(\mathrm{ID}_R, \psi_1, \Omega_i) \oplus \mathrm{msg}_i$，签密阶段通过数据持有者用自己的私钥和由密钥生成中心生成的密钥对数据进行签密，之后将签密的数据上传到工业云服务器 ICS，数据使用者利用相应的参数进行验证和解密，计算 $Q_i = \mu_1(H_1(\mathrm{ID}_R, \psi', \alpha_i) \cdot \mathrm{PK}_i + \mathrm{SK}_i + D_i)$，$V_i = \mu_1 H_3(\mathrm{ID}_s, \alpha_i, \mathrm{PK}_i, \psi') + x_i H_3(\mathrm{ID}_s, \alpha_i, \beta_i, \psi')$，在 Dohare 方案[11]中签密阶段雾节点采用的算法与 SignC $(PP, \mathrm{msg}, \mathrm{SK}_s, \psi') \rightarrow \zeta$ 子算法相同，执行 $\mathrm{OSign(OSK)} \rightarrow \psi'$。在此处雾节点用于执行外包部分签名，其余签名在工业云服务器上执行，Dohare 在签密阶段后由聚合签密器对 $\zeta_i = (\psi', \alpha_i, \beta_i, V_i)$ 进行聚合。虽然该方案在签密阶段与聚合签密时采用了将计算量较大的部分在工业云服务器和雾节点上执行，能够减小一定量的开销，但该方案在验证聚合签密部分由用户执行，且数据使用者需要对雾层上的聚合数据执行解签密过程 $C'' = H_3(\beta_i, C_i', x_R \beta_i, \mathrm{ID}_R)$，其中，$C_i' = \beta_i \cdot (x_i + D_i)$。该方案算法中签密所需要的开销为 $5T_{\mathrm{h}} + 4T_{\mathrm{em}} + 2T_{\mathrm{ea}}$，解签密所需要的开销为 $4T_{\mathrm{h}} + 3T_{\mathrm{em}} + 2T_{\mathrm{ea}}$。

本文方案根据安全性证明对比了文献[9-11]的安全性能见表 4。

不同阶段的通信开销如图 4 所示，不同阶段

表 4　安全性能对比

对比项	CSUAC-IoT[9]	CLOOSC[10]	CLASS[11]	本文方案
是否抵抗伪造攻击	N	N	Y	Y
是否抵抗重放攻击	Y	Y	Y	Y
是否抵抗中间人攻击	Y	Y	Y	Y
是否抵抗量子攻击	N	N	N	Y

的计算开销如图5所示。图4和图5描述了在身份认证阶段固定群组成员大小的情况下，签密与解签密运算总量的开销对比，由于文献[9-10]中多次使用双线性配对，且验证时类似 $\mathrm{Sign}_G \cdot G = H(G_1 \| T_1 \| T_{2i} \| S_1 \| S_{2i} \| W_{\mathrm{SK}} \| L_U \| TS_U \| x_1')$这样的运算占据了大量开销，Mandal方案[9]中通过用户进行两次签密操作 $\mathrm{Sign}_G = H(C_1 \| T_1 \| T_{2i} \| S_1 \| S_{2i}) \cdot k_u + x_u (\mathrm{mod}\, q)$，经由网关节点进行第一次签密验证并计算 $L_U = L_{\mathrm{mod}} \oplus H(Z_i \| TS_{GN})$ 后，将消息 $\{m_i, TS_{GN}, \mathrm{ID}_{S_i}, L_{\mathrm{mod}}\}$转发给智能设备进行第二次签密验证。在Mandal的方案[9]中为增强安全通信将物联网设备、网关节点以及移动设备的注册过程拆分成了两次注册阶段，其多次选择身份标识信息以及由随机私钥计算公钥的过程造成三因素认证方案开销增大，且从图5中可以看出，本文方案相较于文献[9-10]在签密和解签密阶段的运算量更小。虽然相较于文献[11]在签密阶段所需要的开销略大，其签密的运算量为 $5T_{\mathrm{h}}+4T_{\mathrm{em}}+2T_{\mathrm{ea}}$，但签密和解签密的运算总量更低，本文方案为34.33 ms，优于文献[11]。

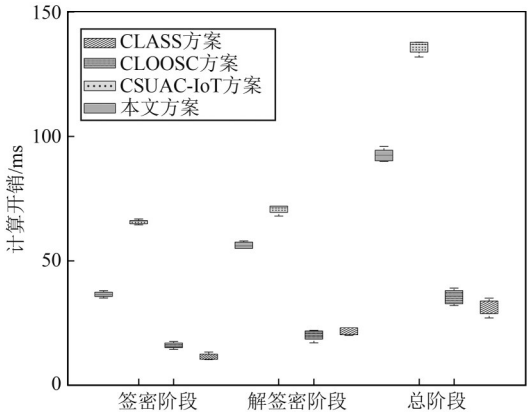


图4 不同阶段的通信开销

认证开销随群组成员变化如图6所示，图6描述了在身份认证阶段，本文方案与文献[9-11]在不同群组认证人数情况下所有组成员完成统一签密认证所需要的时间。对比的群组成员动态变化范围为0~100个，从图6中可看出本文方案和文献[9-11]的方案都随着群组成员数量增多而认证开销逐渐增大，其开销增大的原因为文献[9-11]中 $S_{2i} = v_i / r_i + k_U (\mathrm{mod}\, q)$，$W_{\mathrm{SK}} = H(r_i \| TS_U) \oplus H(v3 \| K_U \cdot Y_G)$等计算量较大的运算会随着设备接入数量增多。从图6中可以看出，本方案认证所需的计算开销在设备数量较小时与文献[9-11]接近，但随着群组设备的不断接入，本文方案计算开销相比文献[9-11]的开销差值逐渐增大，从图6中可以看出，本文所提方案的认证开销在群组设备接入数量较大时小于文献[10-11]，且远小于文献[9]。

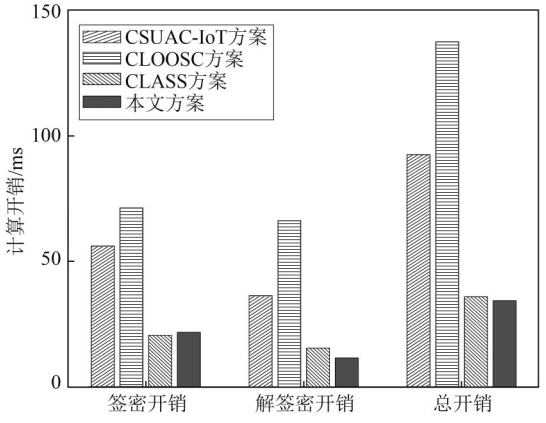


图5 不同阶段的计算开销

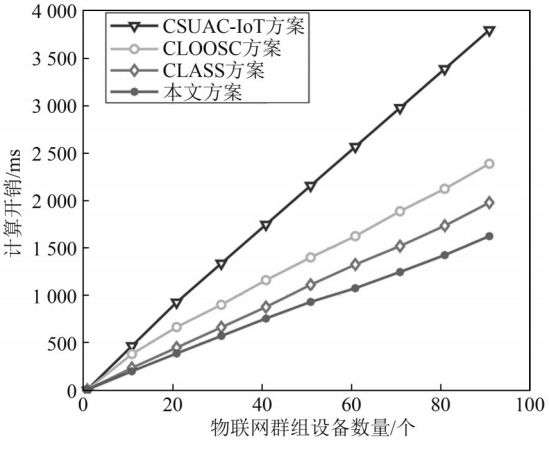


图6 认证开销随群组成员变化

通信实体生成密钥所需时间如图 7 所示，图 7 描述了在注册阶段，本文方案的通信实体生成密钥所需的时间与文献[9-11]的通信实体生成密钥所需的时间的对比。本文方案优化了生成密钥所需的原像采样算法，简化了扰动向量的协方差矩阵。算法采用的陷门结构为完全并行化，当固定参数 N、M 和 $\boldsymbol{R}$ 时，只需要更小的模量 q 使得密钥更小，生成效率更高。从图 7 中可以看出，在公钥与私钥生成阶段及总的密钥生成开销，本文方案明显优于文献[9-11]。

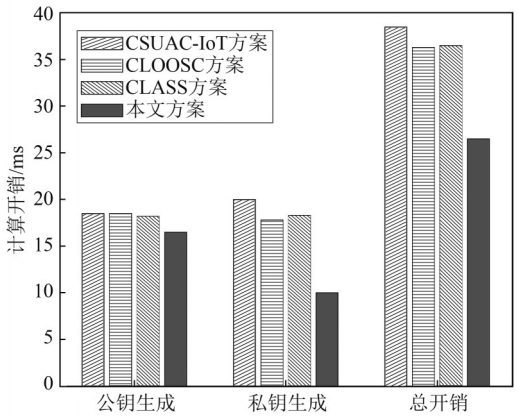


图7　通信实体生成密钥所需时间

4.2　与抗量子方案对比

抗量子签密方案对比见表 5，针对抗量子签密方案从签密与解签密运算总量和密文大小进行比较。由于目前的抗量子签密方案多为理论研究并主要针对区块链场景，面向物联网场景的研究较少，因此本文选择相同理论支撑的文献[16-17]进行对比，其抗量子方案均基于格密码设计。从表 5 中可以看出，文献[16-17]在签密、解签密和运算总量各阶段与本文方案对比，本文所采用的哈希、乘法等运算量均低于文献[16-17]，同时，本文方案密钥尺寸为 $2nm\log q$，低于文献[16-17]的 $m^2n\log q$ 和 $3nm\log q$。

表5　抗量子签密方案对比

方案	签密	解签密	运算总量	密钥尺寸
Zhu 等[16]	10_h+10 T_{em}+3T_{ea}	7T_h+11 T_{em}+7T_{ea}	17T_h+ 21T_{em}+10T_e	$m^2n\log q$
Li 等[17]	9T_h+4 T_{em}+7T_{ea}	10T_h+5 T_{em}+4T_{ea}	19T_h+9T_{em}+ 11T_{ea}	$3nm\log q$
本文方案	2T_h+4T_{lm}+ 5T_{la}+T_m	2T_h+2T_{lm}+ 2T_{la}+T_m	4T_h+6T_{lm}+ 7T_{la}+2T_m	$2nm\log q$

5　结束语

面向物联网的轻量级群组认证是解决物联网各种应用场景下多个设备并行认证的有效方法。然而，现有的群组认证方案存在众多安全隐患，无法抵抗量子攻击，计算代价相对较高，无法适用于物联网节点资源受限的情况。本文提出了一种基于格的轻量级物联网群签密认证方案，该方案利用群组认证的方式对多个用户进行统一签密，同时利用基于格的签密方法抵抗量子攻击。方案满足正确性、机密性，并且可以抵抗伪造、重放、冒充等恶意攻击。同时，本文方案利用优化后的原像采样算法为通信实体分配认证所需的加密密钥，相较于其他方案，能够以更高的效率完成密钥生成。但本文所提的方案也具有相应的不足之处，在面对多个群组的同时接入时，由于群组设备的差异性可能存在设备间使用不同密码体制。本文所提方案仅考虑在无证书密码环境下的设备交互问题，面对基于传统公钥密码体制的设备接入基于身份密码体制的设备时，本文方案将难以适用，即本文所提方案在异构密码体制的环境下缺乏一定程度上的兼容性。与现有面向物联网的群组认证方案相比，本文方案总体上具有更高的安全性和较低的计算开销，更适用于海量认证请求的物联网场景，可以有效地满足物联网场景下资源受限节点的轻量级群组认证需求。

参考文献：

[1] NING H S, SHI F F, CUI S, et al. From IoT to future cyber-enabled Internet of X and its fundamental issues[J]. IEEE Internet of Things Journal, 2021, 8(7): 6077-6088.

[2] NAYAK P, SWAPNA G. Security issues in IoT applications using certificateless aggregate signcryption schemes: an overview[J]. Internet of Things, 2023(21): 100641.

[3] WEI L X, CHEN Y R, WANG H, et al. BBIL: a bounding-based iterative method for IoT to localize things[J]. IEEE Internet of Things Journal, 2020, 7(2): 1413-1425.

[4] 杨毅宇, 周威, 赵尚儒, 等. 物联网安全研究综述: 威胁、检测与防御[J]. 通信学报, 2021, 42(8): 188-205.
YANG Y Y, ZHOU W, ZHAO S R, et al. Survey of IoT security research: threats, detection and defense[J]. Journal on Communications, 2021, 42(8): 188-205.

[5] JUNG J, KIM B, CHO J, et al. A secure platform model based on ARM platform security architecture for IoT devices[J]. IEEE Internet of Things Journal, 2022, 9(7): 5548-5560.

[6] NIU S F, SHAO H L, HU Y, et al. Privacy-preserving mutual heterogeneous signcryption schemes based on 5G network slicing[J]. IEEE Internet of Things Journal, 2022, 9(19): 19086-19100.

[7] LOHIYA R, THAKKAR A. Application domains, evaluation data sets, and research challenges of IoT: a systematic review[J]. IEEE Internet of Things Journal, 2021, 8(11): 8774-8798.

[8] 牛淑芬, 杨喜艳, 李振彬, 等. 基于异构密码系统的混合签密方案[J]. 计算机工程与应用, 2019, 55(3): 61-67.
NIU S F, YANG X Y, LI Z B, et al. Hybrid signcryption scheme based on heterogeneous system[J]. Computer Engineering and Applications, 2019, 55(3): 61-67.

[9] MANDAL S, BERA B, SUTRALA A K, et al. Certificateless-signcryption-based three-factor user access control scheme for IoT environment[J]. IEEE Internet of Things Journal, 2020, 7(4): 3184-3197.

[10] CHEN J S, WANG L L, WEN M, et al. Efficient certificateless online/offline signcryption scheme for edge IoT devices[J]. IEEE Internet of Things Journal, 2022, 9(11): 8967-8979.

[11] DOHARE I, SINGH K, AHMADIAN A, et al. Certificateless aggregated signcryption scheme (CLASS) for cloud-fog centric industry 4.0[J]. IEEE Transactions on Industrial Informatics, 2022, 18(9): 6349-6357.

[12] CHENG C, LU R X, PETZOLDT A, et al. Securing the Internet of Things in a quantum world[J]. IEEE Communications Magazine, 2017, 55(2): 116-120.

[13] WU C, KE L, DU Y. Quantum resistant key-exposure free chameleon hash and applications in redactable blockchain[J]. Information Sciences, 2021, 548 (1): 438-449.

[14] EL-ZEKEY M, MEDINA J, MESIAR R. Lattice-based sums[J]. Information Sciences: an International Journal, 2013(223): 270-284.

[15] XIE C, WENG J, WENG J, et al. Scalable revocable identity-based signature over lattices in the standard model[J]. Information Sciences, 2020(518): 29-38.

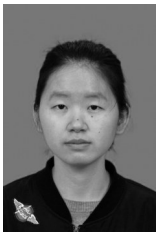
[16] ZHU H, WANG Y, WANG C, et al. An efficient identity-based proxy signcryption using lattice[J].Future Generation Computer Systems, 2021(117): 321-327.

[17] LI F Y, YU S Q, LI G S, et al. Intelligent federated learning on lattice-based efficient heterogeneous signcryption[J]. International Journal of Intelligent Systems, 2022, 37(11): 9480-9507.

[作者简介]

徐川（1980– ），男，博士，重庆邮电大学通信与信息工程学院教授、博士生导师，主要研究方向为网络体系结构、网络安全、网络建模。

艾星好（1999– ），男，重庆邮电大学通信与信息工程学院硕士生，主要研究方向为物联网的接入认证方案。



王杉杉（1996– ），女，重庆邮电大学通信与信息工程学院博士生，主要研究方向为天地一体化网络安全。

赵国锋（1972– ），男，博士，重庆邮电大学通信与信息工程学院教授、博士生导师，主要研究方向为天地一体化网络体系结构、工业物联网、网络安全。

韩珍珍（1989– ），女，博士，重庆邮电大学通信与信息工程学院讲师，主要研究方向为天地一体化网络体系结构、跨层路由、网络安全。