计 算 机 研 究 与 发 展
Journal of Computer Research and Development
https://crad.ict.ac.cn
62(12): 3106−3121, 2025

车载自组织网络中基于格的无抽样条件隐私保护聚合认证

张 静 杨 志 崔 杰 许 艳 仲 红
(安徽大学计算机科学与技术学院 合肥 230039)
(zjing@ahu.edu.cn)

Lattice-Based Conditional Privacy-Preserving Aggregate Authentication Without Sampling in Vehicular Ad Hoc Network

Zhang Jing, Yang Zhi, Cui Jie, Xu Yan, and Zhong Hong
(*School of Computer Science and Technology*, *Anhui University*, *Hefei* 230039)

Abstract Vehicular ad hoc network is the foundation of the intelligent transportation system, which can effectively improve traffic efficiency and enhance road safety. However, due to the openness of its wireless communication environment, the edge nodes in vehicular ad hoc networks are vulnerable to various external attacks. In order to balance privacy protection and traceability, also ensure secure authentication, an effective method is to adopt the conditional privacy-preserving authentication scheme in vehicular ad hoc networks. Although various privacy-preserving authentication schemes have been proposed successively, the security of these schemes almost all relies on the difficult assumptions of traditional number theory, and it is difficult to have post-quantum security characteristics. Therefore, aiming at the security and efficiency problems of existing lattice-based conditional privacy-preserving authentication schemes in vehicular ad hoc networks, and in order to solve the key escrowing problem, by leveraging the decisional learning with errors over rings (RLWE) hardness assumption and the ring-learning with errors (RLWE) small integer solution (SIS) hardness assumption on structured lattices, and combining with the rejection sampling technique, a lattice-based sampling-free conditional privacy preserving aggregate authentication scheme is designed. It is proved that the proposed scheme can achieve adaptive security in the random oracle. In addition, the performance evaluation shows that the proposed scheme is superior to the scheme based on the general lattice in terms of computation cost.

Key words lattice; conditional privacy-preserving; ring small integer solution; ring learning with errors; vehicular ad hoc network (VANET)

摘 要 车载自组织网络(vehicular ad hoc network, VANET)是构建智能交通系统的基础,其能够有效提高交通效率以及增加道路安全性.但由于其自身无线通信环境的开放性,车载自组织网络中的边缘节点易遭受到各种外部攻击.为了兼顾隐私保护和可追溯性并确保安全认证,一种有效的方法是采用车联网条件隐私保护认证方案.虽然目前已有各种车联网条件隐私保护认证方案被相继提出,但这些方案的安全性几乎都依赖于传统数论困难假设,难以具备后量子安全特性.因此,针对现有基于格的车联网条件隐私保护认证方案的安全和效率问题,同时为解决密钥托管问题,利用结构化格上的环上带误差学习决策

收稿日期: 2024-06-05; **修回日期**: 2025-06-24
基金项目: 国家自然科学基金项目(U23A20308, 62472003, 62202008);安徽省自然科学基金项目(2408085JX010);安徽大学协同创新计划项目(GXXT-2022-049)
This work was supported by the National Natural Science Foundation of China (U23A20308, 62472003, 62202008), the Natural Science Foundation of Anhui Province (2408085JX010), and the Anhui University Collaborative Innovation Program Project (GXXT-2022-049).
通信作者: 崔杰 (cuijie@mail.ustc.edu.cn)

困难假设以及环上小整数解困难假设，并结合拒绝抽样技术，设计了一种车联网中基于格的无抽样条件隐私保护聚合认证方案，并在随机预言机模型下证明了所提方案能够达到适应性安全. 此外，通过性能评估展示了该方案在计算开销方面优于基于一般格的聚合认证方案.

关键词 格；条件隐私保护；环上小整数解；环上带误差学习；车载自组织网络

中图法分类号 TP309

DOI: 10.7544/issn1000-1239.202440454 **CSTR:** 32373.14.issn1000-1239.202440454

随着社会数字化迅猛发展，车载自组织网络(vehicular ad hoc network, VANET)与人们的安全交通出行越发紧密相关，例如：智能车辆和智能交通服务的出现与升级. 典型的 VANET 环境设置通常包括可信权威机构(trusted authority, TA)、路侧单元(road side unit, RSU)和车载单元(on board unit, OBU)的车辆，其中 RSU 和车辆为保证实时获悉车辆和道路相关信息，彼此间通过 OBU 周期性地交换通信数据. 这种通信方式可以是车对车(vehicle to vehicle, V2V)、车对基础设施(vehicle to infrastructure, V2I)或者车对一切(vehicle to everything, V2E)，为实现这些通信功能可以借助专用短程无线通信(dedicated short range communication, DSRC)协议[1-2]. 具体来说，配置 DSRC 协议后的车辆能够使用其 OBU 以每 100~300 ms 的频率向附近其他车辆以及 RSU 广播通信消息，这些通信数据涵盖了车辆有关信息(位置和速度)和附近的道路状况(道路拥堵程度、道路缺陷情况以及天气状况). VANET 中的每个 RSU 在接收到其管辖范围内车辆广播的相关信息后，需要将验证通过的交通信息打包发送给 TA. 然后相关技术人员可以针对这些信息进行数据挖掘和分析，以促进业务决策以及更长期的城市规划的制定，例如：确定交通阻塞点或事故多发地区.

确保消息完整性是基于 VANET 的交通系统所需考虑的首要问题，由于 VANET 中的节点处于开放的无线通信环境中，因此假设敌手可以拦截、修改、重放以及删除 VANET 中传输的数据是比较合理的. 当然，考虑恶意车辆向 VANET 内的其他车辆或者 RSU 广播恶意消息的问题也是必要的，因为在网络攻击中，这种恶意行为可能会造成毁灭性的后果[3]. 故确保车辆和 RSU 接受来自其他网络节点消息的合法性和完整性十分重要. 同时，确保条件隐私保护特性对于车联网安全认证至关重要，即一方面能够避免恶意车辆通过未经授权的监视手段获取车辆的身份隐私信息，另一方面又能够在特定环境下及时提取恶意车辆的真实身份信息. 故此，需要在身份隐私保护和可追溯责任性之间做好权衡. 不妨假设以下场景，在一场涉及恐怖分子通过注入恶意构造的交通信息，从而招致交通事故的刑事调查中，快速获取犯罪分子的车辆真实身份十分关键.

Hubaux 等人[4]于 2004 年率先对 VANET 中的智能车辆面临的各种安全威胁与挑战做出系统化阐述，并对实现车联网安全认证所需的各种安全和隐私需求做出正式的定义. 紧随其后，2007 年 Raya 等人[5]提出了一种概念性的安全体系结构，并设计了一套基于公钥基础设施(public key infrastructure, PKI)的安全通信协议. 然而遗憾的是，借助这种方式实现的安全通信，车辆必须预存储大量公私钥对以及相应的数字证书，以确保车辆身份的真实性. 由于在每轮通信会话中，车辆都需随机地选取 1 对公私钥对来确保消息的完整性认证，因此不可避免地给车辆和 TA 带来巨大的存储开销负担. 此外，TA 难以实现恶意车辆真实身份的可追溯性. 2008 年，Lu 等人[6]设计了一种高效条件隐私保护协议. 在该协议中，车辆需要在每次车载通信中从附近的 RSU 获取新的数字证书. 故而，这种频繁的证书更新势必会导致车联网内部沉重的通信开销负担. 为了缓解这一问题，同年，Zhang 等人[7]提出了 RSU 辅助的批量消息聚合认证协议，其中车辆在驶出当前 RSU 通信管辖范围才会更新数字证书. 2015 年，Shao 等人[8]利用新的群签名技术设计了一种支持可追溯的高效匿名认证方案. 然而，这类方案都基于 PKI，因此需要大量的存储空间用于数字证书的管理.

针对复杂的证书管理问题，2014 年 Li 等人[9]利用基于身份的签名[10]思想，设计了一种车联网中条件隐私保护认证框架. 但由于方案中涉及频繁的双线性配对操作，所以不可避免地带来繁重的计算开销. 为了解决这一问题，He 等人[11]提出了一种基于身份的无配对条件隐私保护认证方案. 该方案显著降低计算和通信开销，同时支持消息聚合认证. 2020 年，Ogundoyin[12]构造了一种可证明安全的轻量级条件隐私保护认证方案. 然而，这类方案都存在密钥托管问题.

为解决这类基于身份密码系统的认证方案固有的密钥托管问题,相关研究人员设计了一系列基于无证书的条件隐私保护认证方案. 2015 年, Horng 等人[13] 设计了一种基于无证书密码体制的条件隐私保护聚合认证方案. 之后, Mei 等人[14] 在 2020 年设计了一种支持条件隐私保护的无证书聚合认证方案,该方案利用全聚合技术降低计算开销,以及借助假名机制实现条件隐私保护. 2021 年, Gupta 等人[15] 运用签密技术设计了一种高效的条件隐私保护认证方案. 但这类方案都是基于传统数论困难假设,所以并不具备后量子安全特性.

为了有效抵御量子计算机的攻击,迄今为止已有研究人员提出基于格的认证方案. 2019 年, Mukherjee 等人[16] 首次利用一般格中的最短向量问题(shortest vector problem, SVP),在 VANET 中设计了支持条件隐私保护的聚合认证方案,但方案的安全性规约不紧凑且计算效率不高. 2020 年, Dharminder 等人[17] 利用一般格的代数结构设计了一种支持可撤销的聚合认证方案,方案设计较为复杂且方案证明不够正式化. 此外,该方案同前述基于格的条件隐私保护认证方案一样,所有车辆的 OBU 中均存储着系统主私钥,因此恶意攻击者可借助侧信道攻击尝试获取密钥泄露信息,从而对安全通信构成极大威胁. 2022 年, Li 等人[18] 利用一般格上的非齐次小整数解(inhomogeneous small integer solution, ISIS)问题[19],结合一般格中传统格陷门函数设计了一种格上身份基条件隐私保护认证方案. 该方案利用假名机制实现匿名认证. 但由于其假名身份构造存在固定部分,且在验证阶段暴露了 OBU 的公钥信息,因此该方案不能实现消息的不可链接性功能. 2023 年, Wen 等人[20] 基于结构化格上的模上带误差学习(module learning with errors, MLWE)问题[21],并利用环签名技术设计了一种可撤销的条件隐私保护认证方案. 但由于环签名固有的签名尺寸与环成员数量成线性正相关的问题,以及该方案并不支持聚合认证,所以在高移动性的 VANET 环境中的适用性受到一定程度的制约.

由此可见,目前关于格密码体制下的车联网条件隐私保护认证方案的研究仍然较为匮乏,同时已有认证方案大都基于一般格构造,存在效率不高、安全功能特性兼具不全面、安全性规约不紧凑的问题,而仅有的基于结构化格构造的认证方案[20] 未能够具备聚合认证特性,并未能很好契合实际车联网场景. 因此,本文利用结构化格上的新陷门函数并结合拒绝抽样技术,提出了一种车联网中基于格的无抽样条件隐私保护聚合认证方案. 主要贡献包括 3 个方面:

1)丰富的安全功能特性. 本文方案详细地分析了满足各种需要的主要安全特性,能够同时支持消息认证、身份隐私保护、可追溯性、消息不可链接性. 此外,除了能够抵御常见类型的攻击,例如中间人攻击、篡改攻击、假冒攻击等,还能够抵御量子计算机的攻击.

2)实用的结构化格设计. 本文方案利用结构化格中新陷门下的陷门生成算法、原像采样算法分别生成系统主公私钥对和提取局部签名密钥,并结合拒绝抽样技术实现完整签名密钥提取. 实验结果表明,与基于一般格的聚合认证方案相比,所提方案计算效率更优.

3)严格的安全性证明. 本文方案在随机预言机模型中,可达到适应性选择身份与消息下的不可伪造特性,方案的底层安全性依赖于环上带误差学习问题以及环上小整数解问题,具体地,方案的主公钥伪随机安全性依赖于 RLWE(ring learning with errors)困难假设,而不可伪造性可规约到 RSIS(ring small integer solution)困难假设,这 2 类困难假设均与结构化格上的 SVP 一样困难.

1 预备知识

1.1 符号定义

本文的安全参数为 n; 用$\mathbb{R}$表示实数域, $\mathbb{Z}$表示整数域. 给定正整数k, 记$k=1,2,\cdots$. 本文所涉及的向量均默认为行向量. 向量$\boldsymbol{a}$和向量$\boldsymbol{b}$的内积记为$\boldsymbol{a}\odot\boldsymbol{b}$. 令$\boldsymbol{a}=(a_1,a_2,\cdots,a_m)\in\mathbb{R}^m$, 则$\boldsymbol{a}$的$\ell_1$, ℓ_2, ℓ_∞范数分别为$\|\boldsymbol{a}\|_1=\sum_{i=0}^{m}|a_i|$, $\|\boldsymbol{a}\|_2=\sqrt{\sum_{i=0}^{m}a_i^2}$和$\|\boldsymbol{a}\|_\infty=\max_i\{|a_i|\}$. 如无特殊说明,则默认为$\ell_1$范数. 对于任意给定的概率分布$D$和集合$E$, $d\leftarrow_{\$}D$表示$d$是从概率分布$D$中随机抽样的, $e\leftarrow_{\$}E$表示$e$是从集合$E$中随机采样的. 矩阵$\boldsymbol{R}\in\mathbb{R}^{n\times m}$的范数和最大奇异值分别记为$\|\boldsymbol{R}\|=\max_i\|\boldsymbol{r}_i^{\mathrm{T}}\|$和$s_1(\boldsymbol{R})=\max_{\boldsymbol{x}}\|\boldsymbol{R}\boldsymbol{x}^{\mathrm{T}}\|$, 其中$\boldsymbol{r}_i^{\mathrm{T}}$为$\boldsymbol{R}$的第$i$个列向量, $\boldsymbol{x}$为m维的单位向量. 易知, $s_1(\boldsymbol{R})\geqslant\|\boldsymbol{R}\|$. 记矩阵$\boldsymbol{R}$的 Gram-Schmidt 正交化矩阵为$\tilde{\boldsymbol{R}}$, 则$\|\tilde{\boldsymbol{R}}\|\leqslant\|\boldsymbol{R}\|$. 对于矩阵$\boldsymbol{A}\in\mathbb{R}^{n\times\tilde{m}}$和$\boldsymbol{B}\in\mathbb{R}^{n\times m}$以及矩阵$\boldsymbol{A}\in\mathbb{R}^{w\times m}$和$\boldsymbol{B}\in\mathbb{R}^{k\times m}$, 其行连接和列连接分别记为$[\boldsymbol{A}|\boldsymbol{B}]\in\mathbb{R}^{n\times(\tilde{m}+m)}$, $[\boldsymbol{A},\boldsymbol{B}]=\begin{bmatrix}\boldsymbol{A}\\ \boldsymbol{B}\end{bmatrix}\in\mathbb{R}^{(w+k)\times m}$. 对于结构化格下的多项式环$\mathcal{R}$可将其表示为如下形式: $\mathcal{R}=\mathbb{Z}[x]/F(x)$, 其中$F(x)$是$n$阶分圆多项式, 当$n$是 2 的整数次幂时, $F(x)=x^n+1$. 环$\mathcal{R}$与

$\mathbb{Z}^n$是同构的，环$\mathcal{R}$中的每个元素$f=\sum_{i=0}^{n-1}a_i x^i$可对应于系数向量$(\boldsymbol{a}_0,\boldsymbol{a}_1,\cdots,\boldsymbol{a}_{n-1})\in\mathbb{Z}^n$，范数$\|f\|$表示相应系数向量的范数. 本文所采用的多项式环$\mathcal{R}$表示为$\mathcal{R}_q=\mathbb{Z}_q[x]/(x^n+1)$，其中$q\equiv 1 \bmod 2n$.

本文方案的所有参数均与n相关，所以可将n看作方案的安全参数. 以n为参数的可忽略函数记为$negl(n)=O(n^{-c})$，其中c为任意的正数. 如果某个事件不发生的概率是可忽略的，则称该事件以极大概率发生. 对于给定的可数集合D及其上的2个概率分布X和Y，$\Delta(X,Y)=\frac{1}{2}\sum_{z\in D}|X(z)-Y(z)|$表示为$X$与$Y$间的统计距离. 如果2个概率分布的统计距离是可忽略的，则称这2个概率分布统计接近. 给定2个分布集合$\{X_n\}_{n\in\mathbb{N}}$和$\{Z_n\}_{n\in\mathbb{N}}$，若对于任意的非均匀概率多项式时间算法PPT(probabilistic polynomial time)，恒有$|Pr_{y\leftarrow_{\$}X_n}[\mathcal{A}(y)=1]-Pr_{y\leftarrow_{\$}Z_n}[\mathcal{A}(y)=1]|=negl(n)$，则称$X_n$和$Z_n$是计算不可区分的.

1.2 格及离散高斯分布

定义 1. 令m为任意正整数，矩阵$\boldsymbol{B}\in\mathbb{R}^{m\times m}$由$m$个线性无关列向量组成，则由$\boldsymbol{B}$生成的$m$维格$\Lambda$定义为$\Lambda=L(\boldsymbol{B})=\{\boldsymbol{B}\boldsymbol{c}^{\mathrm{T}}:\boldsymbol{c}\in\mathbb{Z}^m\}$，其中$\boldsymbol{B}$称为$L(\boldsymbol{B})$的基.

本文主要关注环$\mathcal{R}$上的q模结构化格，其定义如下：

给定正整数n，m和q，多项式向量$\boldsymbol{a}\in\mathcal{R}_q^{l\times m}$和多项式$u\in\mathcal{R}_q$定义如下2类格：

$$\Lambda^{\perp}(\boldsymbol{A})=\{\boldsymbol{x}\in\mathcal{R}^m:\boldsymbol{a}\odot\boldsymbol{x}=0 \bmod q\},$$

$$\Lambda^{u}(\boldsymbol{A})=\{\boldsymbol{x}\in\mathcal{R}^m:\boldsymbol{a}\odot\boldsymbol{x}=u \bmod q\}.$$

特别地，对于任意满足$\boldsymbol{a}\odot\boldsymbol{x}=u \bmod q$的多项式向量$\boldsymbol{v}$，有$\Lambda^{u}(\boldsymbol{a})=\Lambda^{\perp}(\boldsymbol{a})+\boldsymbol{v}$.

离散高斯分布[22-23]是格密码学中的重要概念. 记以$\boldsymbol{c}\in\mathbb{R}^m$为中心，实数$s>0$为参数的$m$维高斯函数为$\rho_{s,\boldsymbol{c}}(\boldsymbol{x})=\exp\left(-\pi\frac{\|\boldsymbol{x}-\boldsymbol{c}\|^2}{s^2}\right)$，其中$\boldsymbol{x}\in\mathbb{R}^m$.

定义 2. 给定向量$\boldsymbol{c}\in\mathbb{R}^m$和实数$s>0$，则$m$维格$\Lambda$上的离散高斯分布为

$$\forall\boldsymbol{x}\in\Lambda,\ \mathcal{D}_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{x})=\frac{\rho_{s,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{s,\boldsymbol{c}}(\Lambda)},$$

其中$\rho_{s,\boldsymbol{c}}(\Lambda)=\sum_{\boldsymbol{x}\in\Lambda}\rho_{s,\boldsymbol{c}}(\boldsymbol{x})$.

当$\boldsymbol{c}=\boldsymbol{0}$时，记$\rho_{s,\boldsymbol{0}}$和$\mathcal{D}_{\Lambda,s,\boldsymbol{0}}$分别为$\rho_s$和$\mathcal{D}_{\Lambda,s}$.

类似地，记以$\boldsymbol{c}\in\mathbb{Z}^m$为中心，实数$\sigma>0$为参数的$m$维正态高斯测量函数为

$$\rho_{\sigma,\boldsymbol{c}}^m(\boldsymbol{x})=(1/\sqrt{2\pi\sigma^2})^m\times\exp(-\|\boldsymbol{x}-\boldsymbol{c}\|^2/2\sigma^2).$$

定义 3. 给定向量$\boldsymbol{c}\in\mathbb{R}^m$和实数$\sigma>0$，则$m$维格$\Lambda$上的离散正态高斯分布为

$$\forall\boldsymbol{x}\in\Lambda,\ \mathcal{D}_{\Lambda,\sigma,\boldsymbol{c}}^m(\boldsymbol{x})=\rho_{\sigma,\boldsymbol{c}}^m(\boldsymbol{x})/\rho_{\sigma,\boldsymbol{c}}^m(\Lambda),$$

其中$\rho_{\sigma,\boldsymbol{c}}^m(\Lambda)=\sum_{\boldsymbol{x}\in\Lambda}\rho_{\sigma,\boldsymbol{c}}^m(\boldsymbol{x})$.

当$\boldsymbol{c}=\boldsymbol{0}$时，记$\rho_{\sigma,\boldsymbol{0}}^m$和$\mathcal{D}_{\Lambda,\sigma,\boldsymbol{0}}^m$分别为$\rho_\sigma^m$和$\mathcal{D}_{\Lambda,\sigma}^m$.

平滑参数[22]是关于高斯参数的另一个重要概念. 以下引理给出了平滑参数大小的一个上界[23].

引理 1. 设$\boldsymbol{B}\in\mathbb{R}^{m\times m}$是$m$维格$\Lambda$的任意一组基，给定任意的实数$\epsilon\in(0,1)$，则平滑参数$\eta_\epsilon(\Lambda)$满足$\eta_\epsilon(\Lambda)\leqslant\|\tilde{\boldsymbol{B}}\|\sqrt{\ln(2n(1+1/\epsilon))/\pi}$.

特别地，对任意的函数$\omega(\sqrt{\lg n})$，除可忽略的概率外，总有$\eta_\epsilon(\Lambda)\leqslant\|\tilde{\boldsymbol{B}}\|\omega(\sqrt{\lg n})$.

离散高斯分布具有如下典型性质[22-23]：

引理 2. 给定m维格$\Lambda\subset\mathbb{Z}^m$及其上任意一组基$\boldsymbol{B}\in\mathbb{Z}^{m\times m}$，任意向量$\boldsymbol{c}\in\mathbb{R}^m$和实数$\epsilon\in(0,1)$，如果高斯参数$s\geqslant\|\tilde{\boldsymbol{B}}\|\omega(\sqrt{\lg n})$，则有下面关系成立：

$$Pr[\|\boldsymbol{x}-\boldsymbol{c}\|\geqslant s\sqrt{m}|\boldsymbol{x}\leftarrow_{\$}D_{\Lambda,s,\boldsymbol{c}}]\leqslant\frac{1+\epsilon}{1-\epsilon}\times 2^{-m}.$$

引理 3. 给定整数$m\geqslant 2$和格$\Lambda\subset\mathbb{Z}^m$，实数$\epsilon\in(0,1)$和高斯参数$s\geqslant 2\eta_\epsilon(\Lambda)$，对于中心$\boldsymbol{c}\subset\mathbb{Z}^m$和任意的向量$\boldsymbol{x}\in\Lambda$，则$\mathcal{D}_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{x})\leqslant 2^{-m}(1+\epsilon)/(1-\epsilon)$，特别地，当$\epsilon<1/3$时，$\mathcal{D}_{\Lambda,s,\boldsymbol{c}}$的最小熵至少为$m-1$.

对于从环$\mathcal{R}^{m\times k}$中按照离散高斯分布选取的矩阵，其最大奇异值满足以下条件[24]：

引理 4. 设对任意给定的实数$s>0$，如果矩阵$\boldsymbol{R}$是从离散高斯分布$\mathcal{D}_{\mathcal{R}^{m\times k},s}$中随机采样的，那么矩阵$\boldsymbol{R}$的最大奇异值将以压倒性概率满足$s_1(\boldsymbol{R})\leqslant s\sqrt{n}O(\sqrt{w}+\sqrt{k}+\omega(\sqrt{\lg n}))$，其中隐含的常数因子约为$\frac{1}{\sqrt{2\pi}}$.

文献[23]给出了平滑引理，如引理5所示.

引理 5. 对于任意给定的正整数$n\geqslant 4$，$q\geqslant 2$和$m\geqslant 2\lceil\lg q\rceil+2$，实数$s\geqslant\omega(\sqrt{\lg mn})$和随机向量$\boldsymbol{a}\in\mathcal{R}_q^{1\times m}$，如果$\boldsymbol{x}$是从离散高斯分布$\mathcal{D}_{\mathcal{R}^m,s}$中随机采样的向量，那么$\boldsymbol{a}\odot\boldsymbol{x}$的分布统计接近于$\mathcal{R}_q$上的均匀分布.

离散正态高斯分布具有如引理6所示的有趣性质[25].

引理 6. 给定任意实数$\sigma>0$和正整数m，则有如下关于离散正态高斯分布的概率公式成立：

$$Pr[\|\boldsymbol{x}\|>2\sigma\sqrt{m}|x\leftarrow_{\$}D_{\mathbb{Z},\sigma}^m]<2^{-m},$$

$\sigma\geqslant 3/\sqrt{2\pi}$时，对于任意的$\boldsymbol{x}\in\mathbb{Z}^m$，总有$D_{\mathbb{Z}^m,\sigma}^m(\boldsymbol{x})\leqslant 2^{-m}$，即说明离散正态高斯分布$D_{\mathbb{Z}^m,\sigma}^m(\boldsymbol{x})$的最小熵至少为$m$.

引理 7. 拒绝抽样技术[25]. 假定集合V是$\mathbb{Z}^m$中的任意子集，且集合V中的所有向量的ℓ_2范数均小于值T，实数σ满足条件$\sigma=\omega(T\sqrt{\lg m})$，$h:V\to\mathbb{R}$是从集合$V$

映射到实空间$\mathbb{R}$上的任意一种概率分布. 则存在一个小的正常数$M=O(1)$, 使得实际分布与理想分布的统计距离在可忽略范围$2^{-\omega(\lg m)}/M$内, 且实际分布以$(1-2^{-\omega(\lg m)})/M$的较大概率输出有效值, 特别的, 当$\sigma=\alpha T$, α是任意的正实数时, 满足$M=\exp(12/\alpha+1/(2\alpha)^2)$, 实际分布与理想分布的统计距离在$2^{-100}/M$之内, 且实际分布至少以$(1-2^{-100})/M$的概率输出对应结果. 其中实际分布可划分成3个阶段: 首先$\boldsymbol{v}\leftarrow_{\$}h$, 其次$\boldsymbol{z}\leftarrow_{\$}D^m_{\mathbb{Z},\sigma,\boldsymbol{v}}$, 最后以$\min(D^m_{\mathbb{Z},\sigma}/MD^m_{\mathbb{Z},\sigma,\boldsymbol{v}},1)$的概率输出结果$(\boldsymbol{z},\boldsymbol{v})$; 理想分布的3个阶段可表示为: 首先$\boldsymbol{v}\leftarrow_{\$}h$, 然后$\boldsymbol{z}\leftarrow_{\$}D^m_{\mathbb{Z},\sigma}$, 最后以$1/M$的概率输出结果$(\boldsymbol{z},\boldsymbol{v})$.

为提高方案的实现效率, 本文采用定义在环$\mathcal{R}=\mathbb{Z}_q[x]/(x^n+1)$上的结构化格来构造方案, 同时利用拒绝抽样技术引理进一步提高方案在消息签名阶段的效率. 注意到, 环$\mathcal{R}$上的m维格相当于$\mathbb{Z}$上的nm维格.

本文方案的安全性基于RLWE决策困难问题和RSIS困难问题.

定义 4. 给定随机向量$\boldsymbol{a}\in\mathcal{R}_q^m$和实数$\beta>0$, RSIS问题是找到非零向量$\boldsymbol{x}\in\mathcal{R}_q^m$, 满足$\|\boldsymbol{x}\|\leqslant\beta$且$\boldsymbol{a}\odot\boldsymbol{x}=0 \bmod q$.

根据文献[26]可知, 对于任意的多项式函数$\beta(n)$, 当$q\geqslant\beta\sqrt{n}\times\omega(\lg n)$时, 求解上述RSIS问题的困难性程度不亚于求解最坏情况下近似因子为$\gamma(n)\geqslant\beta\sqrt{n}\times\omega(\lg n)$格上SVP问题.

定义 5. 给定秘密值$s\in\mathcal{R}_q$和噪声分布χ, 若$\boldsymbol{a}\leftarrow\mathcal{R}_q$且$\boldsymbol{e}\leftarrow\chi$, 则$(\boldsymbol{a},\boldsymbol{b}=\boldsymbol{a}\cdot s+\boldsymbol{e})$是服从RLWE分布$\psi_{s,\chi}$上的随机抽样. 定义RLWE决策问题是敌手$\mathcal{A}$能以不可忽略的概率区分$\psi_{s,\chi}$上的随机抽样和$\mathcal{R}_q\times\mathcal{R}_q$.

依据文献[27]的论证结果, 对于任意给定的实数$\alpha\in(0,1)$, 若素数$q\equiv 1 \bmod 2n$满足条件$\alpha q>\omega\left(\sqrt{\lg(2n)}\right)$, 则破解RLWE决策问题的困难性程度不亚于求解多项式结构化格上近似因子为$\tilde{O}(\sqrt{n}/\alpha)$的SVP, 特别地, 当误差分布$\chi$为离散高斯分布$\mathcal{D}_{\mathcal{R},\sigma}$时, 高斯参数$\sigma$需满足$\sigma>\sqrt{n}\times\omega\left(\sqrt{\lg(2n)}\right)$.

1.3 格陷门及其应用

格陷门是分析格密码学的重要工具之一, 而传统意义上的格陷门即格内较短的一组基[23]. 本文采用的格陷门函数形如$f(\boldsymbol{x})=\boldsymbol{a}\odot\boldsymbol{x}$, 其中$\boldsymbol{a}\in\mathcal{R}_q^{1\times m}$, $\boldsymbol{x}\in\mathcal{R}^m$. 在选择合适的参数后, 上述函数为满射, 即对函数值域空间中的任意一个元素, 都存在至少1个定义域空间中的元素与其对应. 如果限制函数值对应的原像范数较小, 则求解该原像是困难的, 除非已知函数的陷门.

本节介绍Micciancio等人[28]提出的格陷门概念和相关算法.

定义 6. 给定正整数$w,q\geqslant 2$, 令$k=\lceil\lg q\rceil$, 向量$\boldsymbol{g}=(1,2,\cdots,2^{k-1})\in\mathcal{R}_q^k$. 定义向量$\boldsymbol{a}\in\mathcal{R}_q^{w+k}$的$\boldsymbol{g}$陷门为$\boldsymbol{R}\in\mathcal{R}^{w\times k}$满足$\boldsymbol{a}\begin{bmatrix}\boldsymbol{R}\\ \boldsymbol{I}_k\end{bmatrix}=h\boldsymbol{g}$, 其中$\boldsymbol{I}_k$为单位矩阵, $h\in\mathcal{R}_q$为可逆多项式, 称为$\boldsymbol{R}$的标签.

陷门$\boldsymbol{R}$的好坏可以通过比较$\boldsymbol{R}$的最大奇异值来确定, $s_1(\boldsymbol{R})$越小则$\boldsymbol{R}$越好. 由文献[28]可知, 对任意整数$q\geqslant 2$, 格$\Lambda^{\perp}(\boldsymbol{g})$存在一个基$\boldsymbol{S}\in\mathbb{Z}^{k\times k}$满足$\|\tilde{\boldsymbol{S}}\|\leqslant\sqrt{5}$. 因此, 如果$\boldsymbol{a}$存在较好的陷门$\boldsymbol{R}$, 则可以容易求出函数$f(\boldsymbol{x})$的原像, 使其范数较小.

令高斯参数$s\geqslant\sqrt{7(s_1(\boldsymbol{R})^2+1)}\times\omega(\sqrt{\lg n})$, 对任意的$u\in\mathcal{R}_q$, 利用$\boldsymbol{a}$的$\boldsymbol{g}$-陷门$\boldsymbol{R}\in\mathcal{R}^{w\times k}$可以计算小向量$\boldsymbol{x}\in\mathcal{R}^m$满足$\boldsymbol{a}\odot\boldsymbol{x}=u \bmod q$, 其中$m=w+k$. 具体过程如下:

首先随机地采样扰动向量$\boldsymbol{p}\leftarrow\mathcal{D}_{\mathcal{R}^m,\sqrt{\Sigma_p}}$, 其中$\Sigma_{\boldsymbol{p}}=s^2\boldsymbol{I}_m-5\omega(\lg n)\begin{bmatrix}\boldsymbol{R}\\ \boldsymbol{I}_k\end{bmatrix}[\boldsymbol{R}^{\mathrm{T}}|\boldsymbol{I}_k]$, $\sqrt{\Sigma_{\boldsymbol{p}}}$的计算采用Cholesky的分解方法; 然后根据格$\Lambda^{\perp}(\boldsymbol{g})$的短基$\boldsymbol{S}$计算小向量$\boldsymbol{y}\in\mathcal{R}^k$满足$\boldsymbol{g}\odot\boldsymbol{y}=h^{-1}(u-\boldsymbol{a}\odot\boldsymbol{p})$, 最后输出$\boldsymbol{x}^{\mathrm{T}}=\boldsymbol{p}^{\mathrm{T}}+[\boldsymbol{R},\boldsymbol{I}_k]\boldsymbol{y}^{\mathrm{T}}$易验证如下等式:

$$\begin{aligned}\boldsymbol{a}\odot\boldsymbol{x}=&\boldsymbol{a}\odot\boldsymbol{p}+\boldsymbol{a}[\boldsymbol{R},\boldsymbol{I}_k]\boldsymbol{y}^{\mathrm{T}}=\boldsymbol{a}\odot\boldsymbol{p}+h\boldsymbol{g}\boldsymbol{y}^{\mathrm{T}}=\\&\boldsymbol{a}\odot\boldsymbol{p}+hh^{-1}(\boldsymbol{u}-\boldsymbol{a}\odot\boldsymbol{p})=\boldsymbol{u} \bmod q.\end{aligned}$$

文献[28]给出了2个新$\boldsymbol{g}$陷门下的有效算法, 分别可以生成随机向量$\boldsymbol{a}$及其陷门$\boldsymbol{R}$, 以及利用陷门$\boldsymbol{R}$采样得到较小的$\boldsymbol{x}\in\mathcal{R}^m$, 满足$\boldsymbol{a}\odot\boldsymbol{x}=u$, 其中$u\in\mathcal{R}_q$注意到, 新$\boldsymbol{g}$陷门下的陷门生成和原像采样算法具有比传统陷门下相关算法更高的实现效率.

引理 8. 陷门生成算法[28]. 令整数$b,q\geqslant 2$, $k=\lceil\log_b q\rceil$, $w=2$. 给定随机环元素a、合适的高斯参数$\sigma>\sqrt{n}\times\omega(\lg(2n))$以及可逆的环标签$h\in\mathcal{R}_q$. 则有PPT算法GenTrap-RLWE$(a,h,\sigma)$通过从离散高斯分布$\mathcal{D}_{\mathcal{R}^{1\times k},\sigma}$中随机抽取2个环向量$\boldsymbol{z}_1$和$\boldsymbol{z}_2$, 然后计算$\boldsymbol{a}=[1|a|h\boldsymbol{g}-(\boldsymbol{z}_1+a\boldsymbol{z}_2)]\in\mathcal{R}_q^{1\times(2+k)}$, 并令$\boldsymbol{R}=(\boldsymbol{z}_1,\boldsymbol{z}_2)$, 最后输出环向量$\boldsymbol{a}$及其对应标签$h$的陷门矩阵$\boldsymbol{R}$, 使得$\boldsymbol{a}$以压倒性概率与$\mathcal{R}^{2+k}$上的均匀分布计算不可区分.

引理 9. 原像采样算法[28]. 令正整数$b,q,w\geqslant 2$, $k=\lceil\log_b q\rceil$. 给定$\boldsymbol{a}\in\mathcal{R}_q^{w+k}$、可逆标签$h\in\mathcal{R}_q$及其陷门$\boldsymbol{R}\in\mathcal{R}^{w\times k}$, 对于任意给定的环元素$u\in\mathcal{R}_q$以及高斯参数$\sigma\geqslant\sqrt{(b^2+3)(s_1(\boldsymbol{R})^2+1)}\times\omega(\sqrt{\lg n})$, 存在PPT算法$SamplePre(\boldsymbol{a},\boldsymbol{R},h,u,\sigma)$将输出$\boldsymbol{x}\in\mathcal{R}^{w+k}$, 使其概率分布统计接近于$D_{\Lambda^u(\boldsymbol{a}),\sigma}$且满足$\boldsymbol{a}\odot\boldsymbol{x}=\boldsymbol{u} \bmod q$.

为简便起见, 本文将标签h设为1.

2 系统描述

2.1 系统模型

本文设计的车联网中基于格的无抽样条件隐私保护聚合认证方案囊括了车辆、RSU、应用服务器(application server, AS)和 TA 4 类实体，其系统模型如图 1 所示.

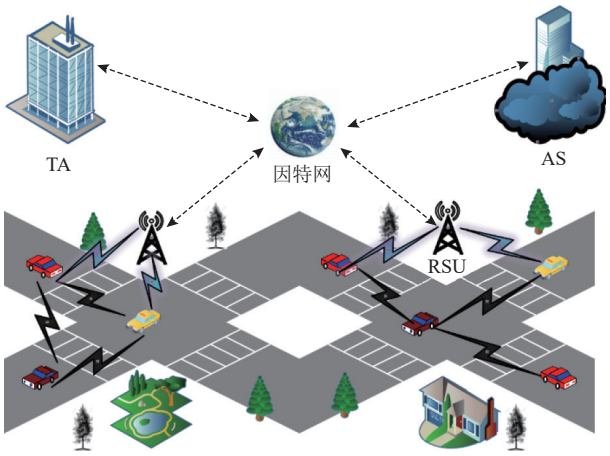


Fig. 1 Illustration of system model

图 1 系统模型示意图

其中 TA 和 AS 位于双层网络拓扑结构的上层，彼此间借助安全套接字层 SSL(secure socket layer)协议进行通信，处于底层的 RSU 和车辆则可以利用 DSRC 协议进行彼此间通信，AS 提供的相关服务可确保整个系统的通信安全. 各个实体的具体描述如下所示：

1)TA. TA 肩负着车辆注册中心和密钥生成中心双重角色，其拥有强大的计算能力. TA 的核心功能在于负责生成系统参数，并依据车辆的 OBU 身份为每个车辆的 OBU 分配相应局部签名密钥，再通过离线方式将相关参数预加载到车辆的 OBU 中. TA 是唯一能够从车辆广播的通信数据中提取车辆真实身份的第三方实体.

2)AS. AS 提供特定应用服务的支持，通过与其他网络元素的交互来管理交通数据，支持决策和控制，实现更智能化、高效化的车联网服务.

3)RSU. RSU 是部署在路边的无线通信设备. RSU 肩负着为其管控辖域内的车辆供应网络接入服务的责任. 在每次通信中，RSU 需要验证车辆广播消息的真实性，并在必要时将通过完整性验证的消息通过有线通信的方式转发给 TA 和 AS.

4)车辆. 为获得 OBU 的私钥，车辆会向 TA 提交注册请求. 每个车辆都预装载了防篡改设备 OBU，以防止密钥信息泄露. 车辆通过 OBU 将道路交通信息广播给附近的 RSU 和其他车辆.

定义 7. 车联网中无抽样条件隐私保护聚合认证方案. 构建一个完整的车联网中无抽样条件隐私保护聚合认证方案需要具备 5 个核心的 PPT 算法，其构成元素分别对应系统创建算法(*Setup*)、局部密钥提取算法(*Par-Extract*)、完整签名密钥提取算法(*Ful-Extract*)、消息签名算法(*MesSig*)以及签名验证算法(*Verify*)，具体描述如下：

1) $Setup(1^n)$. 该算法交由 TA 执行，用于生成系统的初始参数. 算法输入系统安全参数 n，输出系统主公钥 $\boldsymbol{mpk}$ 和主私钥 $\boldsymbol{msk}$.

2) $Par\text{-}Extract(\boldsymbol{mpk},\boldsymbol{msk},id_{OBU_i})$. 该算法仍由 TA 执行，其核心作用是利用主私钥提取出对应身份 id_{OBU_i} 下的私钥 $\boldsymbol{sk}_{OBU_i}$. 算法输入系统主公钥 $\boldsymbol{mpk}$、主私钥 $\boldsymbol{msk}$ 和 OBU 身份 id_{OBU_i}，输出对应的 OBU_i 公私钥对 $(pk_{OBU_i},\boldsymbol{sk}_{OBU_i})$.

3) $Ful\text{-}Extract(\boldsymbol{sk}_{OBU_i},\boldsymbol{m}_i,T_i)$. 该算法交由 OBU 执行，其主要功能是生成车辆的完整签名密钥 $\boldsymbol{sk}_{V_i}$ 和用于匿名的假名身份 ANS_i. 此算法输入包括了 OBU_i 的私钥 $\boldsymbol{sk}_{OBU_i}$、消息 $\boldsymbol{m}_i$ 和当前系统时间戳 T_i，输出对应于时间戳 T_i 下，关于消息 $\boldsymbol{m}_i$ 的假名身份 ANS_i 以及对应消息 $\boldsymbol{m}_i$ 的签名密钥 $\boldsymbol{sk}_{V_i}$.

4) $MesSig(\boldsymbol{sk}_{V_i},\boldsymbol{m}_i,\mu_i)$. 该算法由车辆自身执行，其核心功能在于生成消息 $\boldsymbol{m}_i$ 的合法签名 $\boldsymbol{\sigma}_i$，用于后续的完整性验证. 算法接受签名私钥 $\boldsymbol{sk}_{V_i}$、消息 $\boldsymbol{m}_i$ 和系统时间戳 T_i 作为输入，输出车辆对应于消息 $\boldsymbol{m}_i$ 的签名 $\boldsymbol{\sigma}_i$.

5) $Verify(ANS_i,T_i,\boldsymbol{\sigma}_i,\boldsymbol{m}_i)$. 该算法由 RSU 或者消息接收方车辆执行，主要用于验证消息发送方车辆生成关于消息 $\boldsymbol{m}_i$ 的签名 $\boldsymbol{\sigma}_i$ 的有效性. 根据验证算法 *Verify* 验证消息数量的差异性，进一步可将其细分为 2 个子算法 *Single-Verify* 和 *Batch-Verify*. 对于单一验证算法，算法输入消息 $\boldsymbol{m}_i$、系统时间戳 T_i 和消息 $\boldsymbol{m}_i$ 的签名 $\boldsymbol{\sigma}_i$，算法输出“1”或者“0”. 如果算法输出“1”则表示签名 $\boldsymbol{\sigma}_i$ 是合法签名，反之则表示签名 $\boldsymbol{\sigma}_i$ 是非法签名. 而批量聚合验证算法则以关于身份列表 $\{id_{OBU_1},id_{OBU_2},\cdots,id_{OBU_i}\}$ 对应的时间戳列表 $\{T_1,T_2,\cdots,T_i\}$、相应的消息列表 $\{\boldsymbol{m}_1,\boldsymbol{m}_2,\cdots,\boldsymbol{m}_i\}$ 和假名身份列表 $\{ANS_1,ANS_2,\cdots,ANS_i\}$，以及在消息集合 $\{\boldsymbol{m}_1,\boldsymbol{m}_2,\cdots,\boldsymbol{m}_i\}$ 上的聚合签名 $\sum_i \boldsymbol{\sigma}_i$ 作为输入，输出“1”或者“0”. 如果算法输出“0”则表示聚合签名 $\sum_i \boldsymbol{\sigma}_i$ 是无效签名，反之

则表示签名σ_i是有效签名.

对于任意一个车联网中无抽样条件隐私保护聚合认证方案来说，如果方案设计各阶段的参与者都严格遵循协议正确地执行各个算法，那么 PPT 算法 *Verify* 返回有效值“1”的概率是压倒性的.

2.2 安全模型及目标

车联网中无抽样条件隐私保护聚合认证方案需要具备不可伪造性这一重要的安全性需求，为了达到适应性安全，需要对敌手$\mathcal{A}$的能力进行合理的假设. 本文设计的方案允许敌手$\mathcal{A}$可以适应性地对任意的 OBU 身份进行局部私钥提取询问、向车辆签署消息的密钥进行完整私钥提取询问以及对任意消息进行签名询问. 本文根据文献 [29] 所提的适应性安全模型，合理地界定以下车联网中无抽样条件隐私保护聚合认证方案的适应性安全模型.

定义 8. 不可伪造性. 如果对于任意的多项式时间敌手$\mathcal{A}$，在以下交互式模拟游戏$\mathcal{F}$中获得胜利的概率近乎可忽略不计，那么可以判定该车联网中无抽样条件隐私保护聚合验证方案满足适应性选择身份和消息攻击下的不可伪造性. 注意到，该交互式游戏$\mathcal{F}$主要由系统创建阶段、局部私钥提取询问阶段、完整私钥提取询问阶段、签名询问阶段以及伪造阶段这 5 个阶段组成.

1) 系统创建阶段. 在此阶段，挑战者C扮演 TA 的角色. 挑战者C执行$Setup(1^n)$算法输出系统公私钥对$(\boldsymbol{mpk},\boldsymbol{msk})$，并将$\boldsymbol{mpk}$返回给敌手$\mathcal{A}$.

2) 局部私钥提取询问阶段. 当敌手$\mathcal{A}$适应性地对身份为id'_{OBU_i}的OBU_i私钥进行询问时，挑战者C执行算法$Par\text{-}Extract(\boldsymbol{mpk},\boldsymbol{msk},id'_{OBU_i})$计算出车载单元$OBU_i$私钥$\boldsymbol{sk}_{OBU_i}$，并将其返回给敌手$\mathcal{A}$.

3) 完整签名密钥提取询问阶段. 当敌手$\mathcal{A}$适应性地对身份标志为id'_{OBU_i}的车辆关于消息$\boldsymbol{m}_i$的签名密钥进行问询时，挑战者C运行算法$Ful\text{-}Extract(\boldsymbol{sk}_{OBU_i},\boldsymbol{m}_i,T_i)$获得关于消息$\boldsymbol{m}_i$的签名密钥$\boldsymbol{sk}_{V_i}$，并将其发送给敌手$\mathcal{A}$.

4) 签名询问阶段. 敌手$\mathcal{A}$可对 OBU 的身份为id'_{OBU_i}的车辆关于消息$\boldsymbol{m}_i$的签名进行适应性询问，挑战者C为响应敌手$\mathcal{A}$的签名询问，随后执行算法$MesSig(\boldsymbol{sk}_{V_i},\boldsymbol{m}_i,T_i)$，并计算出对应当前时间戳$T_i$关于消息$\boldsymbol{m}_i$的签名$\boldsymbol{\sigma}_i$，最后将有效签名$\boldsymbol{\sigma}_i$发送给敌手$\mathcal{A}$.

5) 伪造阶段. 敌手$\mathcal{A}$伪造一个关于身份$id^*_{OBU_i}$的消息签名对$(\boldsymbol{m}_i^*,\boldsymbol{\sigma}_i^*)$，如若敌手$\mathcal{A}$未对 OBU 的身份$id^*_{OBU_i}$进行过局部私钥提取询问和完整签名密钥提取询问、消息$\boldsymbol{m}_i^*$未被敌手$\mathcal{A}$签名询问过且验证算法$Verify(ANS_i^*,T_i^*,\boldsymbol{\sigma}_i^*,\boldsymbol{m}_i^*)=1$，则敌手$\mathcal{A}$获得游戏$\mathcal{F}$胜利.

保障通信安全和维护车辆隐私，是确保车联网实现隐私保护下安全认证的决定性因素. 本文所提方案能够达到以下安全目标：

1)消息认证.RSU 和消息接收方车辆可以验证消息来源车辆广播消息的完整性，同时可以轻易检测出消息是否遭到恶意篡改.

2)身份隐私保护和可追溯性. 为保障车辆的真实身份隐私信息不被暴露，车辆通过系统时间戳T_i下的匿名身份ANS_i来广播道路交通状况消息. 值得注意的是，若恶意车辆广播虚假或者恶意交通信息，除了 TA 其他任何第三方实体都无法从恶意车辆通信消息中提取出车辆的真实身份信息.

3)不可链接性. 对于车辆先后广播的任意 2 条消息，以及对应消息所使用的匿名身份，RSU 和恶意敌手都无法找到其间的对应关系，即恶意敌手无法以不可忽略的优势区分任意 2 个假名身份.

4)抵御各种类型攻击. 基于格的无抽样条件隐私保护聚合认证协议除了能够免疫各种常见类型攻击，如篡改攻击、中间人攻击、假冒攻击、重放攻击和窃取验证表攻击. 此外，本文方案还能够对量子计算机威胁表现得极具健壮性.

3 方案描述

3.1 方案构造

1)系统建立算法$Setup(1^n)$.

定义集合$V=\{f(x)\in\mathcal{R}_3:\|f\|_1=\kappa\}$，TA 输入安全参数$n$；选定模素数$q\equiv 1 \bmod 2n$；并选取整数$b\geqslant 2$、$k=\lceil\log_b q\rceil$、3 个高斯参数$(\sigma_1,\sigma_2,\sigma_3)$、公开的辅助向量$\boldsymbol{g}=(1,b,\cdots,b^{k-1})\in\mathcal{R}_q^k$，以及3个安全的单向抗碰撞哈希函数$H_1:\{0,1\}^*\to\mathcal{R}_q$，$H_2:\{0,1\}^*\to\mathcal{R}$，$H_3:\{0,1\}^*\to V$，其中$m=k+2$. TA 执行如下过程：

① 选定高斯参数$\sigma_1\geqslant\sqrt{n}\times\omega(\sqrt{\lg(2n)})$，随机选取环元素$y\in\mathcal{R}_q$，运行算法$GenTrap\text{-}RLWE(y,1,\sigma_1)$，获得随机环向量$\boldsymbol{a}\in\mathcal{R}_q^{1\times(2+k)}$及相应的陷门矩阵$\boldsymbol{R}=(\boldsymbol{z}_1,\boldsymbol{z}_2)\in\mathcal{R}_q^{2\times k}$.

② TA 输出系统公钥$\boldsymbol{mpk}=\boldsymbol{a}$和主私钥$\boldsymbol{msk}=\boldsymbol{R}$. 该阶段总的时间复杂度为$O(1)+O(kn\lg n)+O(kn\lg n)=O(kn\lg n)$.

2)局部私钥提取算法$Par\text{-}Extract(\boldsymbol{mpk},\boldsymbol{msk},id_{OBU_i})$.

TA 首先将系统主公钥$\boldsymbol{mpk}$、主私钥$\boldsymbol{msk}$以及关于OBU_i的对应身份$id_{OBU_i}\in\{0,1\}^*$作为算法的输入项，

其次执行下列相应步骤：

① TA 计算$p_i=H_1(id_{OBU_i})$，令OBU_i的公钥为$pk_{OBU_i}=p_i$.

② 对于给定的合适大小高斯参数$\sigma_2\geqslant\sqrt{(b^2+3)(s_1(\boldsymbol{R})^2+1)}\times\omega(\sqrt{\lg n})$，TA 运行原像采样算法$SamplePre(\boldsymbol{a},\boldsymbol{R},1,p_i,\sigma_2)\rightarrow\boldsymbol{\psi}_i$.

③ TA 输出OBU_i的私钥$\boldsymbol{sk}_{OBU_i}=\boldsymbol{\psi}_i$.

④ 车辆在未接入车联网环境阶段需要完成 OBU 的初始化. 具体地，首先车辆需要在线下阶段向 TA 提交注册请求，然后 TA 将依次为每个合法车辆配备相应的 OBU，其次OBU_i将验证等式$\boldsymbol{a}\odot\boldsymbol{\psi}_i=p \bmod q$是否成立，进而可判断 TA 的合法权威性. 通过合法性验证后，车辆同意 TA 将车辆的真实身份 RID、登录校验密码 PWD 以及OBU_i的私钥$\boldsymbol{\psi}_i$预加载到车辆相应的OBU_i中.

该阶段的总的时间复杂复为$O(1)+O(n\lg n)+O(1)+O(n\lg n)=O(n\lg n)$.

3）完整签名密钥提取算法$Ful\text{-}Extract(\boldsymbol{sk}_{OBU_i},\boldsymbol{m}_i,T_i)$.

OBU 提供自身私钥$\boldsymbol{sk}_{OBU_i}$、消息$\boldsymbol{m}_i$和系统时间戳T_i作为算法的输入条件，详细操作步骤如下描述.

① 车辆获取车联网相关服务前，需要进行身份的合法性认证. 车辆将身份信息RID^*和登录校验密码PWD^*提供给 OBU，车辆发送的校验信息被 OBU 接收到后检验等式$RID^*=RID$和$PWD^*=PWD$是否同时成立，来判断登录车辆身份的合法性，只有以上 2 个等式同时成立，OBU 才为车辆提供后续服务，否则 OBU 将拒绝车辆之后所有的服务请求.

② 对于给定的大小合适的高斯参数$\sigma_3\geqslant 12\kappa\times\sqrt{m(b^2+3)(s_1(\boldsymbol{R})^2+1)}\times\omega(\sqrt{n\lg n})$，OBU 依照参数为$\sigma_3$的离散正态高斯分布$\mathcal{D}^{2+k}_{\mathcal{R},\sigma_3}$随机采样多项式环向量$\boldsymbol{w}_i\leftarrow_{\$}\mathcal{D}^{2+k}_{\mathcal{R},\sigma_3}$. 令$ANS_{i,1}=\boldsymbol{a}\odot\boldsymbol{w}_i$，并计算$ANS_{i,2}=RID\oplus H_2(\boldsymbol{\psi}_i,ANS_{i,1})$，于是获得车辆的假名身份信息$ANS_i=(ANS_{i,1},ANS_{i,2})$.

③ OBU 计算哈希值$\mu_i=H_3(ANS_i,\boldsymbol{m}_i,T_i)$，并计算$\boldsymbol{\varphi}_i=\boldsymbol{w}_i+\mu_i\times\boldsymbol{\psi}_i$，令$\boldsymbol{sk}_{V_i}=\boldsymbol{\varphi}_i$，最后以$\min(D^m_{\mathcal{R},\sigma}/MD^m_{\mathcal{R},\sigma_3,\mu_i\cdot\boldsymbol{\psi}_i},1)$的概率输出车辆的签名密钥$\boldsymbol{\varphi}_i$. 若车载单元 OBU 未能输出符合条件的签名密钥$\boldsymbol{\varphi}_i$，需要返回步骤② 重新选取环向量$\boldsymbol{w}_i$，值得注意的是，OBU 输出符合条件的签名密钥$\boldsymbol{\varphi}_i$所需中止次数为一个小常数M，其值近似等于$\boldsymbol{e}$.

④ OBU 将完整签名密钥$\boldsymbol{\varphi}_i$、哈希值μ_i以及假名身份$ANS_i=(ANS_{i,1},ANS_{i,2})$，借助安全通信信道传输给相应的车辆.

该阶段总的时间复杂度为$O(1)+O(n\lg n)+O(n\lg n)+O(1)+O(n\lg n)+O(1)=O(n\lg n)$.

4）消息签名算法$MesSig(\boldsymbol{sk}_{V_i},\boldsymbol{m}_i,\mu_i)$.

该算法被车辆调用，车辆以完整签名密钥$\boldsymbol{\varphi}_i$、消息$\boldsymbol{m}_i$及其对应系统时间戳T_i下的哈希值μ_i作为算法输入的先决条件，具体执行步骤如下细述.

① 车辆从多项式环集合V中以随机的方式独立执行m次，获取随机环向量$\boldsymbol{\vartheta}\in\mathcal{R}^m_3$，然后计算$\boldsymbol{\phi}_i=\boldsymbol{\vartheta}\cdot\mu_i$.

② 车辆计算$\theta_i=\boldsymbol{a}\odot\boldsymbol{\vartheta}$，并计算$\rho_i=\theta_i+p_i \bmod q$.

③ 车辆生成假名身份ANS_i下关于消息$\boldsymbol{m}_i$的签名$\boldsymbol{\delta}_i=\boldsymbol{\phi}_i+\boldsymbol{\varphi}_i$，并将其作为算法的有效输出，然后车辆将消息签名对$\{ANS_i,T_i,\boldsymbol{m}_i,\rho_i,\boldsymbol{\delta}_i\}$通过 DSRC 协议广播给附近的匿名车辆和 RSU.

该阶段总的时间复杂度为$O(mn\lg n)+O(n\lg n)+O(n)+O(1)=O(mn\lg n)$.

5）签名验证算法$Verify(ANS_i,T_i,\boldsymbol{\delta}_i,\boldsymbol{m}_i)$.

根据验证消息的条目不同，可将验证算法$Verify$划分成如 2.1 节所述的 2 类子验证算法，单验证算法$Single\text{-}Verify(ANS_i,T_i,\boldsymbol{\sigma}_i,\boldsymbol{m}_i)$和批量消息聚合验证算法$Batch\text{-}Verify(ANS_i,T_i,\boldsymbol{\sigma}_i,\boldsymbol{m}_i)$. 这 2 类子算法的具体操作过程如下所述.

对于单验证算法$Single\text{-}Verify$，由于 RSU 和消息接收方车辆都能够对消息进行完整性检测，不失严谨性，假设 RSU 将消息$\boldsymbol{m}_i$、当前系统时间戳T_i以及签名$\boldsymbol{\delta}_i$作为算法$Single\text{-}Verify$的输入项. RSU 依次采取以下检测步骤：

① RSU 检测当前系统时间戳T_i是否仍然有效，若时间戳T_i失去效应，RSU 将中断后续所有的验证操作.

② RSU 校验等式条件$\boldsymbol{a}\odot\boldsymbol{\delta}_i=ANS_{i,1}+\mu_i\times\rho_i \bmod q$以及相应的不等式条件$\|\boldsymbol{\delta}_i\|_\infty\leqslant(2\sigma_3+\kappa)\sqrt{nm}$是否同时成立，若同时满足 RSU 则将有效值“1”作为输出，否则将结果值“0”作为返回结果.

该阶段的总时间复杂度为$O(1)+O(n\lg n)+O(n)=O(n\lg n)$.

至于批量消息聚合验证算法$Batch\text{-}Verify$，根据前述$Single\text{-}Verify$，类似地可将来自N个不同车辆生成的消息签名对集合$\{(ANS_1,T_1,\boldsymbol{m}_1,\boldsymbol{\nu}_1,\boldsymbol{\delta}_1),\cdots,(ANS_N,T_N,\boldsymbol{m}_N,\boldsymbol{\nu}_N,\boldsymbol{\delta}_N)\}$作为算法输入，RSU 具体验证过程如下所示：

① RSU 检查当前系统时间戳列表集合$\{T_1,T_2,\cdots,T_N\}$是否仍处于有效期，只有当时间戳集合中的元素都未失去合法性效应，RSU 才会继续后续相关验证

操作, 否则直接中止算法.

② RSU 从集合V中随机选取N个环元素$\{v_1, v_2, \cdots, v_N\}$作为聚合验证系数集合, 并计算相应的聚合签名$\boldsymbol{\delta} = \sum_{i\in[N]} v_i\boldsymbol{\delta}_i$. 最后 RSU 验证等式条件$\boldsymbol{a}_i \odot \boldsymbol{\delta} = \sum_{i\in[N]} v_i(ANS_{i,1} + \mu_i \times \rho_i) \bmod q$以及不等式条件$\|\boldsymbol{\delta}\|_\infty \leqslant N(2\kappa\sigma_3 + \kappa^2)\sqrt{nm}$是否同时符合, 当且仅当以上验证条件均满足时, RSU 才会判定该聚合签名$\boldsymbol{\delta}$满足完整性, 并返回值“1”, 其他任何情况算法都会以“0”作为返回值.

该阶段总的时间复杂复为$O(N) + O(Nn\lg n) + O(Nn) = O(Nn\lg n)$.

3.2 参数设置

安全参数n在本文方案构造中设置为 2 的整数次幂.

依据引理 8, PPT 算法*GenTrap-RLWE*的高斯参数σ_1需满足$\sigma_1 \geqslant \sqrt{n} \times \omega(\sqrt{\lg(2n)})$. 由引理 1 可知非紧凑渐近下确界函数$\omega(\sqrt{\lg n})$可将其初始化为$\sqrt{\ln(2n(1+1/\epsilon))/\pi}$. 为使所设计方案达到不亚于 128 b 的安全强度, 可令常数$\epsilon \leqslant 2^{-128}$, 且需要符合条件$|V| = \binom{n}{\kappa} 2^\kappa \geqslant 2^{128}$. 同样依据引理 8, 可知算法*GenTrap-RLWE*输出关于随机多项式环公钥矩阵$\boldsymbol{a}$的$\boldsymbol{g}$陷门$\boldsymbol{R}$, 其中$\boldsymbol{R} \leftarrow_{\$} D_{\mathcal{R}^{2\times k}, \sigma_1}$. 再依据引理 4 可知, 陷门矩阵$\boldsymbol{R}$的最大奇异值以压倒性概率吻合$s_1(\boldsymbol{R}) \leqslant \sigma_1 \times O\left(\sqrt{2n} + \sqrt{nk} + \omega(\sqrt{n\lg n})\right)$, 其中隐含的常数因子约为$1/\sqrt{2\pi}$.

至于原像采样算法*SamplePre*, 根据引理 9 可知高斯参数σ_2需要满足条件$\sigma_2 \geqslant \sqrt{(b^2+3)(s_1(\boldsymbol{R})^2+1)} \times \omega(\sqrt{\lg n})$. 且 PPT 算法*SamplePre*对于任意给定的值域空间中元素$p_i = H_1(id_{OBU_i}) \in \mathcal{R}_q$, 算法*SamplePre*都会输出对应的短向量$\boldsymbol{\psi}_i \in \Lambda^{p_i}(\boldsymbol{a})$, 其中输出向量$\boldsymbol{\psi}_i$与离散高斯分布$D_{\Lambda^{p_i}(\boldsymbol{a}), \sigma_2}$的统计距离近乎可忽略不计. 类似的由引理 2 可得, 解向量$\boldsymbol{\psi}_i$的ℓ_2范数以压倒性概率满足$\|\boldsymbol{\psi}_i\| \leqslant \sigma_2\sqrt{(2+k)n}$.

依据拒绝抽样引理 7 可知, 可设置$\sigma_3 = 12\sigma_2\kappa \times \sqrt{(2+k)n}$, 进而可知方案实际输出分布$D^m_{\mathcal{R}, \sigma_3, \mu_i\cdot\boldsymbol{\psi}_i}(z)$与理想分布$D^m_{\mathcal{R}, \sigma_3}(z)$之间的统计距离严格受限在范围$2^{-100}/M$之内, 且小常数近似等于$\boldsymbol{e}$.

由格中规约理论可知, 为了确保本文依赖的$RSIS_{n,m,q,\beta}$困难假设的难解性, 模数q需符合$q \geqslant \beta\sqrt{n} \times \omega(\lg n)$. 再根据 4.2 节的不可伪造性安全性证明部分可知, 对于 RSIS 问题解向量的ℓ_2范数界限可令$\beta = (4\sigma_3 + 2\kappa)\sqrt{nm}$, 相应的模数$q$需符合$q \geqslant (4\sigma_3 + 2\kappa)n\sqrt{m} \times \omega(\lg n)$.

4 方案安全性证明及分析

4.1 正确性

定理 1. 如果本文方案中 TA、OBU、RSU 和车辆都遵循协议, 设计严格的执行各阶段的相关算法, 则验证算法*Verify*将以压倒性概率返回有效值“1”.

证明. 根据 2.1 节中的相关定义, 算法*Verify*可分类成 2 类子算法, 分别是单验证算法*Single-Verify*和聚合验证算法*Batch-Verify*, 下面将依次给出相应的合理证明.

对于单验证情况, 给定 OBU 的身份为id_{OBU_i}、系统时间戳T_i以及对应的假名身份ANS_i. 对于消息$\boldsymbol{m}_i$, 计算消息的哈希值$\mu_i = H_3(ANS_i, \boldsymbol{m}_i, T_i)$, 并计算$\boldsymbol{\phi}_i = \boldsymbol{\vartheta}\cdot\mu_i$, 最后获得消息$\boldsymbol{m}_i$的签名$\boldsymbol{\delta}_i = \boldsymbol{\phi}_i + \boldsymbol{\varphi}_i$, 其中$\boldsymbol{\varphi}_i = \boldsymbol{w}_i + \mu_i\cdot\boldsymbol{\psi}_i$. 注意到签名密钥$\boldsymbol{\varphi}_i$通过拒绝采样方式获得, 则依据引理 6 和引理 7 可知, 签名密钥$\boldsymbol{\varphi}_i$的ℓ_2范数以压倒的概率满足$\|\boldsymbol{\varphi}_i\| \leqslant 2\sigma_3\sqrt{nm}$. 则由三角不等式, 可轻易验证如下等式:

$$\|\boldsymbol{\delta}_i\|_\infty = \|\boldsymbol{\phi}_i + \boldsymbol{\varphi}_i\|_\infty \leqslant \|\boldsymbol{\phi}_i + \boldsymbol{\varphi}_i\|_2 \leqslant \|\boldsymbol{\vartheta} \times \mu_i\|_2 + \|\boldsymbol{\varphi}_i\|_2 \leqslant \|\mu_i\|_1 \times \|\boldsymbol{\vartheta}_i\|_2 + \|\boldsymbol{\varphi}_i\|_2 = (2\sigma_3 + \kappa)\sqrt{nm}.$$

故算法*Single-Verify*中的不等式验证条件成立, 同时有

$$\begin{aligned}\boldsymbol{a} \odot \boldsymbol{\delta}_i &= \boldsymbol{a} \odot (\boldsymbol{\phi}_i + \boldsymbol{\varphi}_i) = \boldsymbol{a} \odot \boldsymbol{\phi}_i + \boldsymbol{a} \odot \boldsymbol{\varphi}_i = \boldsymbol{a} \odot (\boldsymbol{\vartheta} \times \mu_i) + \\ &\quad \boldsymbol{a} \odot (\boldsymbol{w}_i + \mu_i \times \boldsymbol{\psi}_i) = (\boldsymbol{a} \odot \boldsymbol{\vartheta} + \boldsymbol{a} \odot \boldsymbol{\psi}) \times \mu_i + \boldsymbol{a} \odot \boldsymbol{w}_i = \\ &\quad (\theta_i + p_i) \times \mu_i + \boldsymbol{a} \odot \boldsymbol{w}_i = ANS_{i,1} + H_3(ANS_i, \boldsymbol{m}_i, T_i) \times \\ &\quad \rho_i \bmod q.\end{aligned}$$

因此算法*Single-Verify*中的等式验证条件亦成立.

至于聚合验证情形, 相似地, 对于批量消息可计算其相应的聚合签名$\boldsymbol{\delta} = \sum_{i\in[N]} v_i\boldsymbol{\delta}_i$, 则有

$$\|\boldsymbol{\delta}\|_\infty = \left\|\sum_{i\in[N]} v_i\boldsymbol{\delta}_i\right\|_\infty = \sum_{i\in[N]} \|v_i\boldsymbol{\delta}_i\|_\infty \leqslant \sum_{i\in[N]} \|v_i\|_1 \times \|\boldsymbol{\delta}_i\|_\infty \leqslant N\kappa \times \|\boldsymbol{\phi}_i + \boldsymbol{\varphi}_i\|_2 \leqslant N(2\kappa\sigma_3 + \kappa^2)\sqrt{nm}.$$

故吻合算法*Batch-Verify*中的不等式验证条件, 此外有

$$\begin{aligned}\boldsymbol{a} \odot \boldsymbol{\delta} &= \boldsymbol{a}_i \odot \sum_{i\in[N]} v_i\boldsymbol{\delta}_i = \sum_{i\in[N]} v_i \times (\boldsymbol{a} \odot \boldsymbol{\delta}_i) = \\ &\quad \sum_{i\in[N]} v_i \times (ANS_{i,1} + H_3(ANS_i, \boldsymbol{m}_i, T_i)\rho_i) = \\ &\quad \sum_{i\in[N]} v_i \times ANS_{i,1} + \sum_{i\in[N]} v_i \times \mu_i \times \rho_i \bmod q.\end{aligned}$$

因而，契合算法*Batch-Verify*中的等式验证条件.

证毕.

4.2 不可伪造性

定理 2. 如果 RLWE 决策问题以及 RSIS 假设均具有困难性，则在随机预言机模型中任意 PPT 的敌手$\mathcal{A}$破解本文方案对适应性选择消息、身份攻击的不可伪造性的概率可忽略不计.

证明. 由定义 8，关于车联网中条件隐私保护聚合认证的安全模型，通过模拟游戏$\mathcal{F}$来具体刻画. 相应的可据此进行如下合理假设，如果存在一个多项式时间的敌手$\mathcal{A}$，且该敌手$\mathcal{A}$能够在多项式时间内完美伪造一个全新消息的合法签名的概率ϵ是完全不可忽略的，那么接下来即可严格证明，一定存在一个计算有效的 PPT 算法$\mathcal{B}$，其攻破结构化格上公认的平均情况下 RSIS 困难假设的概率不亚于$\epsilon\varepsilon\times(Q_{H_1}-Q_{\text{Par-Ext}}-Q_{\text{Ful-Ext}})/Q_{H_1}^2$. 其中$Q_{H_1}$是关于$H_1$哈希询问次数的上界值，$Q_{\text{Par-Ext}}$是关于局部密钥提取询问次数的上限值，$\varepsilon$是敌手$\mathcal{A}$未在签名询问阶段问询过关于新消息$\boldsymbol{m}_i^*$的签名的概率，$Q_{\text{Ful-Ext}}$是关于消息签名密钥最大询问次数. 详细过程如下.

1）系统创建阶段. 给定系统安全参数n，多项式算法$\mathcal{B}$选定随机的模数$q\equiv 1(\bmod 2n)$，正整数$b\geqslant 2$、$k=\lceil\log_b q\rceil$、$m=k+2$、公开辅助环向量$\boldsymbol{g}=(1,b,\cdots,b^{k-1})\in\mathcal{R}_q^k$、合适的高斯参数$\sigma_2\geqslant\sqrt{(b^2+3)(s_1(\boldsymbol{R})^2+1)}\times\omega(\sqrt{\lg n})$和高斯参数$\sigma_3\geqslant 12\kappa\sqrt{(2+k)(b^2+3)(s_1(\boldsymbol{R})^2+1)}\times\omega(\sqrt{n\lg n})$，以及 3 个视为随机预言机的单向抗碰撞哈希函数$H_1:\{0,1\}^*\to\mathcal{R}_q$，$H_2:\{0,1\}^*\to\mathcal{R}$，和$H_3:\{0,1\}^*\to V$. 为构造系统主公钥$\boldsymbol{a}=[1,\bar{\boldsymbol{a}}]$，算法$\mathcal{B}$首先从环空间$\mathcal{R}_q^{1\times(k+1)}$中随机抽取多项式向量$\bar{\boldsymbol{a}}$作为系统主公钥$\boldsymbol{a}$中的随机化部分. 值得注意的是，算法$\mathcal{B}$虽然没有通过调用陷门生成算法*GenTrap-RLWE*来获取随机化环向量$\bar{\boldsymbol{a}}$，但是由 RLWE 决策问题可知，在满足合适参数条件的前提下，该证明中通过从线性空间$\mathcal{R}_q^{1\times(k+1)}$中随机采样多项式向量$\bar{\boldsymbol{a}}$构造系统主公钥$\boldsymbol{a}$的方式，与通过执行陷门生成算法*GenTrap-RLWE*获取系统主公钥$\boldsymbol{a}$的方式在计算意义上是近乎不可区分的. 其次，算法$\mathcal{B}$随机地从$\mathcal{R}_q$采样元素b，然后算法$\mathcal{B}$输入随机多项式向量$\boldsymbol{a}\in\mathcal{R}_q^{1\times(2+k)}$实现 RSIS 困难问题的实例化，RSIS 是一个困难问题，其中解向量的ℓ_2范数上界满足$\beta=(4\sigma_3+2\kappa)\sqrt{nm}$，则算法$\mathcal{B}$尝试搜索一个$\ell_2$范数不等于 0 的短向量$\boldsymbol{\gamma}\in\mathcal{R}_q^{w+2k+d}$，使得$\|\boldsymbol{\gamma}\|\leqslant\beta$且$\boldsymbol{a}\odot\boldsymbol{\gamma}=0 \bmod q$，算法$\mathcal{B}$然后将$\boldsymbol{mpk}=\boldsymbol{a}$作为有效值返回给敌手$\mathcal{A}$.

2）询问阶段. 敌手$\mathcal{A}$可适应性地与算法$\mathcal{B}$建立一系列询问，具体囊括各种安全哈希询问、局部私钥提取询问、完整签名密钥提取询问以及签名询问. 在此过程，算法$\mathcal{B}$将建立并维护多个记录表，其中表L_{H_1}用于记录哈希H_1询问，表L_{H_2}用于记录哈希H_2询问，表L_{H_3}用于记录哈希H_3询问，表$L_{\text{Ful-Ext}}$用来记录签名密钥提取询问，表L_{Sig}用于记录签名询问.

① H_1询问. 敌手$\mathcal{A}$根据 OBU 的身份选择性地发起哈希H_1询问. 不失一般性，假定H_1是最先询问的. 算法$\mathcal{S}$随机抽取$k\in\{1,2,\cdots,Q_{H_1}\}$. 至于敌手$\mathcal{A}$的第$j$次$H_1$询问，倘若满足$j=k$，则算法$\mathcal{B}$将$(id_{OBU_i},b,\perp)$存于表$L_{H_1}$中，并将$b$发送给敌手$\mathcal{A}$. 否则，算法$\mathcal{B}$将严格遵循分布$D_{\mathcal{R},\sigma_2}$随机地抽样$2+k$个环元素组成多项式环向量$\boldsymbol{\psi}_i\in\mathcal{R}^{1\times(2+k)}$，并计算$p_i=\boldsymbol{a}\odot\boldsymbol{\psi}_i$. 若$p_i$已存在于表$L_{H_1}$中，则需要重新独立地随机选取$\boldsymbol{\psi}_i$. 之后，算法$\mathcal{B}$将$(id_{OBU_i},p_i,\boldsymbol{\psi}_i)$存于表$L_{H_1}$中，并将$p_i$返回给敌手$\mathcal{A}$. 根据引理 5 可知，$p_i$与$\mathcal{R}_q$上的均匀分布统计距离可忽略不计.

② 局部私钥提取询问. 敌手$\mathcal{A}$为获取身份id_{OBU_i}对应的私钥，适应性地向算法$\mathcal{B}$进行局部私钥提取询问. 此时，算法$\mathcal{B}$检索表L_{H_1}寻找匹配项. 若匹配项为$(id_{OBU_i},p_i,\boldsymbol{\psi}_i)$，则算法$\mathcal{B}$将$\boldsymbol{\psi}_i$视作有效返回值；若匹配项为$(id_{OBU_i},b,\perp)$，则将终止后续所有模拟进程.

③ 完整签名密钥提取询问. 敌手$\mathcal{A}$为了获取身份id_{OBU_i}的 OBU 对应的签名密钥，可以适应性地向算法$\mathcal{B}$进行完整签名密钥提取询问. 此刻，算法$\mathcal{B}$为响应敌手$\mathcal{A}$的询问遵照离散正态高斯分布$D_{\mathcal{R},\sigma_3}^{2+k}$随机抽取多项式环向量$\boldsymbol{w}_i$，并计算$\boldsymbol{\varphi}_i=\boldsymbol{w}_i+\mu_i\cdot\boldsymbol{\psi}_i$和$ANS_{i,1}=\boldsymbol{a}\odot\boldsymbol{w}_i$，算法$\mathcal{B}$以$\min(D_{\mathcal{R},\sigma}^{2+k}/MD_{\mathcal{R},\sigma_3,\mu_i\cdot\boldsymbol{\psi}_i}^{2+k},1)$的概率输出有效值$\boldsymbol{\varphi}_i$. 注意到模拟方案与实际方案一样，输出有效值所需重复执行的次数近乎逼近小常数 e，且分布$D_{\mathcal{R},\sigma_3}^{2+k}(\boldsymbol{w}_i)$与分布$D_{\mathcal{R},\sigma_3,\mu_i\cdot\boldsymbol{\psi}_i}^{2+k}(\boldsymbol{\varphi}_i)$统计接近. 最后算法$\mathcal{B}$将$(id_{OBU_i},\boldsymbol{\psi}_i,\boldsymbol{\varphi}_i,ANS_{i,1})$存放在表$L_{\text{Ful-Ext}}$中，并将结果$\boldsymbol{\varphi}_i$返回给敌手$\mathcal{A}$.

④ H_2询问. 算法$\mathcal{B}$建立并维护一个记录表L_{H_2}用于回应敌手$\mathcal{A}$对H_2的询问. 通常地，对于敌手$\mathcal{A}$的H_2哈希询问，算法$\mathcal{B}$首先查找表L_{H_2}，假若能够直接搜索到对应项，则直接将结果返回，否则算法$\mathcal{B}$随机地选取一个环元素$\zeta_i\in\mathcal{R}$，然后将$\{id_{OBU_i},\zeta_i\}$存于表L_{H_2}中，并将ζ_i返回给敌手$\mathcal{A}$.

⑤ H_3询问. 算法$\mathcal{B}$建立并维护一个表L_{H_3}用于回应敌手$\mathcal{A}$对H_3的询问. 类似地，假定敌手$\mathcal{A}$发起一次有效H_3询问，算法$\mathcal{B}$尝试搜索表L_{H_3}，倘若搜索到查询项算法$\mathcal{B}$，选择将结果反馈给敌手$\mathcal{A}$. 否则，算法$\mathcal{B}$

随机地从$\mathcal{R}_3$中独立采样一个环元素μ_i, 然后将$\{id_{OBU_i}, \mu_i\}$存于表L_{H_3}中, 并将μ_i返回给敌手$\mathcal{A}$.

⑥ 签名询问. 敌手$\mathcal{A}$适应性地向算法$\mathcal{B}$发起签名询问, 以得到OBU身份为id_{OBU_i}的车辆关于消息$\boldsymbol{m}_i$的有效签名. 此时, 算法$\mathcal{B}$选择直接搜索查找表L_{Sig}, 倘若直接寻找到相应的匹配项$\{id_{OBU_i}, \boldsymbol{m}_i, ANS_{i,1}, \rho_i, \boldsymbol{\delta}_i\}$, 算法$\mathcal{B}$将会将询问结果$\{\rho_i, \boldsymbol{\delta}_i\}$返回给敌手$\mathcal{A}$. 否则, 算法$\mathcal{B}$例行下述执行方案: 首先随机地采样一个环向量$\boldsymbol{\vartheta} \in \mathcal{R}_3^{2+k}$, 并计算$\theta_i = \boldsymbol{a} \odot \boldsymbol{\vartheta}$, 以及计算$\rho_i = \theta_i + p_i (\bmod q)$; 其次计算$\boldsymbol{\phi}_i = \boldsymbol{\vartheta} \cdot \mu_i$, 从而可得$\boldsymbol{\delta}_i = \boldsymbol{\phi}_i + \boldsymbol{\varphi}_i$; 最终将$\{id_{OBU_i}, \boldsymbol{m}_i, ANS_{i,1}, \rho_i, \boldsymbol{\delta}_i\}$存于表$L_{\text{Sig}}$中, 并将结果$\{\rho_i, \boldsymbol{\delta}_i\}$返回给敌手$\mathcal{A}$.

3)伪造阶段. 假设敌手$\mathcal{A}$以不可忽略的概率ϵ伪造出新消息$\boldsymbol{m}_i^*$关于身份$id_{OBU_i}^*$的合法签名$\boldsymbol{\delta}_i^*$. 如果身份$id_{OBU_i}^*$不吻合条件$H_1(id_{OBU_i}^*) = b$, 则算法$\mathcal{B}$终止. 否则算法$\mathcal{B}$将查询表L_{Sig}, 搜索到契合项$\{id_{OBU_i}^*, \boldsymbol{m}_i^*, ANS_{i.1}^*, \rho_i^*, \boldsymbol{\delta}_i^*\}$, 由前述设计步骤和引理7可获悉, 算法$\mathcal{B}$输出诚实签名$\boldsymbol{\delta}_i$, 其吻合条件$\boldsymbol{a} \odot \boldsymbol{\delta}_i = ANS_{i.1}^* + \mu_i^* \times \rho_i^*$和$\|\boldsymbol{\delta}_i\|_\infty \leqslant (2\sigma_3 + \kappa)\sqrt{nm}$的概率是压倒性的. 此外, 又由于伪造签名$\boldsymbol{\delta}_i^*$亦满足验证条件, 即有$\boldsymbol{a} \odot \boldsymbol{\delta}_i^* = ANS_{i.1}^* + \mu_i^* \times \rho_i^*$和$\|\boldsymbol{\delta}_i^*\|_\infty \leqslant (2\sigma_3 + \kappa)\sqrt{nm}$, 因而$\boldsymbol{a} \odot (\boldsymbol{\delta}_i - \boldsymbol{\delta}_i^*) = 0 (\bmod q)$.

令$\boldsymbol{\gamma} = \boldsymbol{\delta}_i - \boldsymbol{\delta}_i^*$, 则可得$\boldsymbol{a} \odot \boldsymbol{\gamma} = 0 \bmod q$, 由方案设计和引理7可知, 签名密钥$\boldsymbol{\varphi}_i$的分布与离散正态高斯分布$D_{\mathcal{R},\sigma_3}^{2+k}(\boldsymbol{w}_i)$统计接近. 且$\boldsymbol{\delta}_i = \boldsymbol{\phi}_i + \boldsymbol{\varphi}_i$, 则诚实签名$\boldsymbol{\delta}_i$的分布近似为$D_{\mathcal{R},\sigma_3,\boldsymbol{\phi}_i}^{2+k}$. 依据引理6可知, 分布$D_{\mathcal{R},\sigma_3,\boldsymbol{\phi}_i}^{2+k}$具有高的最小熵, 因此伪造签名$\boldsymbol{\delta}_i^*$具有与诚实签名$\boldsymbol{\delta}_i$不同的概率是极大的. 故$\boldsymbol{\gamma} \neq \boldsymbol{0}$的概率是压倒性的. 对于$\boldsymbol{\gamma}$有

$$\|\boldsymbol{\gamma}\|_\infty = \|\boldsymbol{\delta}_i - \boldsymbol{\delta}_i^*\|_\infty \leqslant (4\sigma_3 + 2\kappa)\sqrt{nm} = \beta.$$

因此, 算法$\mathcal{B}$攻破了参数为(q,n,β)的RSIS困难问题. 以下推算算法$\mathcal{B}$成功的概率. 算法$\mathcal{B}$成功意味着敌手$\mathcal{A}$未在局部私钥提取阶段和完整签名密钥提取询问阶段询问过身份$id_{OBU_i}^*$, 且未在签名询问阶段问询过消息$\boldsymbol{m}_i^*$的签名, 同时$H_1(id_{OBU_i}^*) = b$. 假定敌手$\mathcal{A}$未在签名询问阶段问询过消息$\boldsymbol{m}_i^*$的签名的概率为ε, 以及身份$id_{OBU_i}^*$满足条件$H_1(id_{OBU_i}^*) = b$的概率不少于$1/Q_{H_1}$, 且局部私钥提取阶段和完整签名密钥提取询问阶段没有询问过身份$id_{OBU_i}^*$的概率不低于$(Q_{H_1} - Q_{\text{Par-Ext}} - Q_{\text{Ful-Ext}})/Q_{H_1}$, 因此算法$\mathcal{B}$破解RSIS困难问题的概率不低于$\epsilon\varepsilon \times (Q_{H_1} - Q_{\text{Par-Ext}} - Q_{\text{Ful-Ext}})/Q_{H_1}^2$. 证毕.

4.3 安全目标分析

依赖于前述方案不可伪造性的安全性论证, 面向2.2节所述的安全性目标, 本节给出具体的安全目标分析, 全面剖析了本文所设计方案吻合对应的安全性需求.

1)支持消息认证. 依据定理2的安全性证明可知, 基于RLWE决策问题和RSIS求解问题的难解性, 对于任何一个PPT敌手$\mathcal{A}$而言都无法以不可忽略的概率ϵ伪造一个有效的签名$\boldsymbol{\delta}_i^*$. 因而, RSU和消息接受方车辆可以通过检查消息签名对$\{ANS_i, T_i, \boldsymbol{m}_i'', \rho_i, \boldsymbol{\delta}_i''\}$是否契合验证条件$\boldsymbol{a} \odot \boldsymbol{\delta}_i'' = ANS_{i,1} + H_3(ANS_i, \boldsymbol{m}_i'', T_i) \times \rho_i \bmod q$和$\|\boldsymbol{\delta}_i''\|_\infty \leqslant (2\sigma_3 + \kappa)\sqrt{nm}$来判定签名$\boldsymbol{\delta}_i''$是否存在伪造的行径, 同时也可判断消息的完整性是否受到破坏. 故本文所提方案支持消息完整性认证.

2)支持身份隐私保护和可追溯性. 任意车辆为实现匿名化通信, 通过使用其匿名身份ANS_i信息来广播实时道路交通安全状况消息, 且由上述方案具体描述可获悉: $ANS_i = \{ANS_{i,1}, ANS_{i,2}\}$, 假名身份由随机化值和固定化值2部分构成, 其中$ANS_{i,1} = \boldsymbol{a} \odot \boldsymbol{w}_i$且$\boldsymbol{w}_i \leftarrow_{\$} D_{\mathcal{R},\sigma_3}^{2+k}$, $ANS_{i,2} = RID \oplus H_2(\boldsymbol{\psi}_i, ANS_{i,1})$. 因为对于任何一个敌手$\mathcal{A}$来说, 为了能够从假名$ANS_i$信息中得到车辆的真实身份信息$RID$, 要么必须掌握$OBU_i$的私钥$\boldsymbol{\psi}_i$, 要么搜索到哈希值$H_2(\boldsymbol{\psi}_i, ANS_{i,1})$的第二原像, 但是由前述方案构造可知$\boldsymbol{\psi}_i$与离散高斯分布$D_{\Lambda^{p_i}(\boldsymbol{a}),\sigma_2}$统计不可区分, 其中$p_i = H_1(id_{OBU_i}) \in \mathcal{R}_q$, 根据引理3, 离散高斯分布$D_{\Lambda^{p_i}(\boldsymbol{a}),\sigma_2}$具有的最小熵至少达到$nm-1$, 故敌手$\mathcal{A}$能猜对$\boldsymbol{\psi}_i$的可能性近乎可忽略不计, 同时由于散列函数$H_2(\cdot)$的单向抗碰撞性, 敌手$\mathcal{A}$搜索到哈希值$H_2(\boldsymbol{\psi}_i, ANS_{i.1})$第二原像的可能性亦忽略不计. 因此, 本文所提方案满足身份隐私保护需求. 此外, 留意到TA可以通过查找OBU公私钥对照列表, 获取OBU_i的对应的私钥$\boldsymbol{\psi}_i$, TA进一步可演算$RID = H_2(\boldsymbol{\psi}_i, ANS_{i,1}) \oplus ANS_{i,2}$, 从而提取出车辆的真实身份信息$RID$, 但其他任何第三方实体包括RSU和其他车辆都无法获取消息发送方车辆的真实身份. 故所提方案支持车辆真实身份的可追溯性.

3)支持消息的不可链接性. 由3.1节中方案的描述可知, 车辆关于任意消息$\boldsymbol{m}_i$都会随机生成一个假名ANS_i, 其中$ANS_i = (ANS_{i,1}, ANS_{i,2})$, $ANS_{i,1} = \boldsymbol{a} \odot \boldsymbol{w}_i$, $ANS_{i,2} = RID \oplus H_2(\boldsymbol{\psi}_i, ANS_{i,1})$且$\boldsymbol{w}_i \rightarrow_{\$} D_{\mathcal{R},\sigma_3}^{2+k}$. 一方面由于环向量$\boldsymbol{w}_i$的随机性, 另一方案由于哈希函数$H_2(\cdot)$的伪随机性, 所以对任意的PPT敌手$\mathcal{A}$而言, 无法以不可忽略的优势区分任意2个车辆之间的假名. 同时, 车辆关于身份id_{OBU_i}对消息$\boldsymbol{m}_i$的签名$\boldsymbol{\delta}_i$与离散正态高斯分布$D_{\mathcal{R},\sigma_3,\boldsymbol{\phi}_i}^{2+k}$统计不可区分, 其中$\boldsymbol{\phi}_i = \boldsymbol{\vartheta} \cdot \mu_i$. 所以对于任意的PPT敌手$\mathcal{A}$而言, 无法区分任意2个车辆之间

关于任意消息的签名. 故攻击者无法从来自同一车辆的 2 个假名和签名中找到关联性. 因此, 本文所提方案支持消息的不可链接性.

4)抵御各种类型攻击. 所提方案能够抵御中间人攻击、篡改攻击、重放攻击、假冒攻击和量子计算机攻击.

① 中间人攻击. 由前述消息认证安全目标分析可知, 本文所提方案能够实现车联网中任意 2 个车辆间消息的安全认证. 因此, 本文所提消息认证方案能够有效抵抗中间人攻击.

② 篡改攻击. 由 4.2 节的安全性证明可知, RSU 或者消息接受方车辆可以通过验证条件$\boldsymbol{a}\odot\boldsymbol{\delta}_i = ANS_{i,1}+H_3(ANS_i,\boldsymbol{m}_i,T_i)\times\rho_i \bmod q$和$\|\boldsymbol{\delta}_i\|_\infty \leqslant (2\sigma_3+\kappa)\sqrt{nm}$是否同时兼备, 可轻易检测出消息签名对$\{ANS_i,T_i,\boldsymbol{m}_i,\rho_i,\boldsymbol{\delta}_i\}$中是否存在任意的篡改行为.

③ 重放攻击. 恶意敌手$\mathcal{A}$试图重放道路交通状况信息, 将选择滞后发布交通信息. 由于合法消息签名对$\{ANS_i,T_i,\boldsymbol{m}_i,\rho_i,\boldsymbol{\delta}_i\}$中含有系统时间戳$T_i$, 故 RSU 或者其他车辆可以通过检查$T_i$是否在有效期内来验证消息是否遭受到重放攻击. 故而, 所提方案能够免疫重放攻击.

④ 假冒攻击. 敌手$\mathcal{A}$试图冒充合法车辆向 RSU 和其他车辆发送消息, 则敌手$\mathcal{A}$必须成功伪造一个关于消息$\boldsymbol{m}_i^*$的合法签名$\boldsymbol{\delta}_i^*$, 根据定理 2 可知, 基于 RLWE 决策问题和 RSIS 问题的困难性, 任意的 PPT 敌手$\mathcal{A}$无法以不可忽略的概率ϵ成功伪造一个有效的签名. 因此, 本文所提方案能够有效抵御假冒攻击.

⑤ 窃取验证表攻击. 由于本文所提方案中所有 OBU 的私钥仅由其自身和 TA 存储, 且没有存储任何的验证表, 故所提方案能够抵御窃取验证表攻击.

⑥ 量子计算机攻击. 根据定理 2 的安全性证明可知, 本文所提方案的存在不可伪造性依赖于 2 类格上公开的困难假设, 分别是 RLWE 判定问题和 RSIS 问题, 且 2 类平均情况下的困难问题均可规约到格上最坏情况下的 SVP 困难问题, 而即使是量子敌手亦无法在多项式时间内攻破 SVP 困难问题. 故本文所提方案能够有效抵御量子计算机的攻击.

5 性能评估

考虑到 Dharminder 等人[17]提出的方案是现阶段已知的基于格的支持消息聚合认证的方案. 此外, 该方案在目前已有的基于格的车联网认证方案中相对计算有效. 故本文选择其作为对比方案, 验证所提方案的计算有效性. 为方便起见, 不妨将该方案简记为 LCPPA[17] 方案. 相应地, LCPPA 方案安全性取决于一般格中 SIS 和 ISIS 困难假设, 而本文所提方案的安全性建立在结构化格上的 RSIS 和 RLWE 决策困难假设上. 此外, Li 等人[18]提出了一种基于 SIS 问题的硬度以及格的 VANET 的 CPPA 协议, 将它简记为 LBCPPA[18]. 上述 3 种基于格的聚合认证方案功能特征对照如表 1 所示.

Table 1 Comparison of Characteristics

表 1 特征比较

方案	适应性安全	可追溯性	匿名认证性	不可链接性	困难假设
LCPPA	✗	✓	✓	✓	SIS/ISIS
LBCPPA	✗	✓	✓	✓	SIS/ISIS
本文方案	✓	✓	✓	✓	RLWE/RSIS

5.1 实验环境描述

考虑到实验测试环境的稳定性, 本文模拟实验均部署在 Windows 系统上, 算法语言参照 C++14.0 标准, 同时相关测试代码交由配备 32 GB RAM 和 Intel i7-12700 的处理器的主机运行. 为获取更加科学化的数据, 采取多次测定取均值的方法来实现. 考虑到本文设计的方案频繁涉及结构化格上的多项式环基本代数运算, 因此可借助代数数论 NTLlib 库[30] 提供的 NTT 技术实现快速代数运算. 此外, 可通过 SHA-256 利用伪随数生成器实例化哈希函数, 同时考虑到在局部签名密钥提取阶段调用了原像采样算法*SamplePre*. 因而为了进一步提升采样计算效率, 本文采用文献 [31] 改进的算法, 具体涉及格$\Lambda^{\perp}(\boldsymbol{g})$上任意模的抽取算法和扰动向量采样算法. 注意到本文是基于计算性实例生成的陷门, 故可以利用文献 [31] 所设计的高效扰动向量生成算法.

5.2 实验参数设置

为了实现本文方案的安全级别达到不低于 128 b 的安全强度, 同时对比方案的安全强度达到近似层次强度, 下面将给出具体设置步骤. 首先考虑到本文方案的安全性与 RSIS 困难假设密切相关, 所以方案的安全强度较大程度受制于参数(n,m,q,β)的具体选定. 其次本文方案的安全性还与 RLWE 决策困难假设有联系, 故方案安全强度一定程度受限于参数(n,m,q,σ_1)的选定. 注意到方案的具体安全级别的准确界定可借助 BKZ 2.0 算法[32]. BKZ 2.0 算法是目前公认的计算有效的格密码方案安全评估算法. 为了达到近似安全级别, LCPPA 方案相关参数设定与文献 [17] 保持相同. 本文方案具体参数的设定如表 2 所示.

Table 2 Setting of the Experimental Parameters

表 2 实验参数的设定

参数符号	含义	取值
n	安全参数	2 048
$\|q\|$	模q的比特空间	62
k	辅助向量$\boldsymbol{g}$的维数	8
b	辅助向量$\boldsymbol{g}$的基	256
σ_1	陷门函数$GenTrap\text{-}RLWE$的高斯参数	254

5.3 性能评估

本文方案与对比方案 LCPPA 和 LBCPPA 主要从计算开销和通信开销 2 个角度进行对比分析, 为了性能分析的顺利进行, 本文在上述实验部署环境下对本文方案设计中所使用的基本密码操作和相关算法的运行时间进行了相应地测定, 具体测试结果如表 3 所示.

Table 3 Running Time of Basic Cryptographic Operation and Algorithm

表 3 基础密码操作及算法运行时间 ms

时间参数	运行时间
T_{Gentrap}	9 144.670
$T_{\text{Samplepre}}$	1.738 6
T_{mul}	0.120 2
T_H	0.002
T_{s}	0.942 2
T_{Dot}	0.094 1
T_{Add}	0.100 8

注: T_{Gentrap}表示调用算法$GenTrap\text{-}RLWE$所执行的时间, $T_{\text{Samplepre}}$表示执行算法$SamplePre$所耗费的时长, T_{mul}表示 2 个环元素相乘的耗时, T_H表示执行哈希函数的耗时, T_{s}表示随机抽样一个环元素的所需时间, T_{Dot}表示维度为m的 2 个环向量内积所耗费的时长, T_{Add}表示 2 个环元素相加的耗时.

1)计算开销

考虑到对比方案 LCPPA 的开销情况, 依据文献 [17] 的结果. $T_{\text{vec-smm}}$表示$\mathbb{Z}_q^m$上 2 个元素相加的耗时, $T_{\text{vec-mlm}}$表示$\mathbb{Z}_q$上的标量元素与$\mathbb{Z}_q^m$上向量乘积的耗时, $T_{\text{vm-nm}}$表示$\mathbb{Z}_q^{n\times m}$上的矩阵与$\mathbb{Z}_q^m$上向量做乘法运算的耗时, T_H表示执行哈希函数的耗时, T_{X}表示执行异或操作的耗时, T_{sp}表示从$\mathbb{Z}_q^m$中随机抽取向量元素的耗时. 对于 LBCPPA 方案, $T_{\text{sout-eq}}$表示计算对应多项式解的过程, $T_{\text{mat-mul}}$表示矩阵乘法模 q 的执行时间, T_{sp}表示从$\mathbb{Z}_q^m$中随机抽取向量元素的耗时, $T_{\text{vm-nm}}$表示$\mathbb{Z}_q^{nm}$中的矩阵与向量在模 q 上的乘法运算, $T_{\text{vm-mk}}$表示$\mathbb{Z}_q^{mk}$中的矩阵与$\mathbb{Z}_q^k$中的向量的乘法运算, $T_{\text{vm-nk}}$表示$\mathbb{Z}_q^{nk}$中的矩阵与$\mathbb{Z}_q^k$中的向量的乘法运算, $T_{\text{vec-smn}}$表示$\mathbb{Z}_q^m$上 2 个维度为 n 的向量相加, $T_{\text{vec-smm}}$表示$\mathbb{Z}_q^m$上 2 个维度为 m 的向量相加, $T_{\text{vec-mln}}$表示$\mathbb{Z}_q$上的标量元素与$\mathbb{Z}_q^n$上的向量上的乘积, $T_{\text{vec-mlm}}$表示$\mathbb{Z}_q$上的标量元素与$\mathbb{Z}_q^m$上的向量上的乘积. 由于验证功能性的不同, 可将计算开销划分成单验证和聚合认证的 2 类, 具体分类分析如下所述.

①对于单验证情形 LCPPA 方案的计算开销, 根据文献 [17] 不难得出以下结果. LCPPA 方案在系统初始化阶段耗时为$T_{\text{vm-nm}}+3T_H\approx 13.569$ ms, 在签名阶段开销为$T_{\text{sp}}+3T_H+2(T_{\text{vm-nm}}+T_{\text{vec-mlm}}+T_{\text{vec-smm}})\approx 31.166$ ms, 单验证阶段耗时为$T_{\text{vm-nm}}+2(T_{\text{vec-mlm}}+T_{\text{vec-smm}})\approx 16.655$ ms. 对于 LBCPPA 方案的计算开销, 在系统初始化阶段耗时为$T_{\text{solut-eq}}+\text{T}_{\text{mat-mul}}\approx 5305.097$ ms, 在签名阶段开销为$(2e+1)T_H+e(T_{\text{sp}}+T_{\text{vm-nm}})+(e+1)(T_{\text{vec-smm}}+T_{\text{vm-mk}})+T_{\text{mat-mul}}\approx 179.382$ ms. 对于单验证阶段耗时为$T_{\text{vm-nm}}+2T_{\text{vm-nk}}+2T_{\text{vec-smn}}\approx 35.126$ ms.

本文方案在初始化阶段耗时为$T_{\text{Gentrap}}+T_{\text{Samplepre}}+T_H\approx 170.786$ ms, 在签名完整密钥提取过程和签名过程的总时耗为$(\text{e}+1)T_{\text{Dot}}+2eT_H+m(e+1)(T_{\text{s}}+T_{\text{mul}}+T_{\text{Add}})$, 其值近似为48.117 ms, 注意到该总耗时亦代表假名生成和签名的总耗时. 单验证阶段本文耗时为$T_{\text{Dot}}+T_{\text{mul}}+T_{\text{Add}}\approx 0.315$ ms. 相关结果见表 4 所示.

Table 4 Comparison of Computational Overhead for Single Verification

表 4 单验证下计算开销比较 ms

方案	初始化阶段	签名阶段	验证阶段
LCPPA	13.569	31.166	16.655
LBCPPA	5 305.097	179.382	35.126
本文方案	170.786	48.117	0.315

通过对表 4 中相关数据合理分析后可知, 本文方案相较于 LBCPPA 方案在初始化阶段、签名阶段以及验证阶段均有显著的优势, 这主要归因于本文利用结构化格及其上新陷门中计算有效算法, 同时利用 NTT 技术实现结构化格上多项式环任意操作下的快速实现以及运用高效的无抽样技术生成签名. 具体地, 在初始化阶段, 本文方案计算效率相较于 LBCPPA 方案提升近 2.20 倍, 签名阶段本文方案的计算效率提升幅度达到近 31 倍, 在验证阶段本文方案的计算速率提高约 111 倍.

②考虑聚合验证情况, 假定消息签名对数量为N, 则 LCPPA 方案和本文方案在前述 2 个阶段分别与对应的单验证情形完全相同, 故不在重复赘述. 下面具体讨论聚合验证情况, 首先对于 LCPPA 方案聚合验证

阶段耗时为 $T_{\text{vm-nm}}+2N\times T_{\text{vec-smm}}+(3N+1)T_{\text{vec-mlm}}$，其简化结果为 $(2.861N+48.697)$ ms. 对于 LBCPPA 方案，聚合验证阶段耗时为 $2NT_{\text{vm-nk}}+3NT_{\text{vec-mln}}+NT_{\text{vec-mlm}}+T_{\text{vm-nm}}+(3N+2)T_{\text{vec-smn}}+NT_{\text{vec-smm}}$，其简化结果为 $(4.130\,4N+13.284)$ ms. 其次本文方案开销为 $T_{\text{Dot}}+(m+3)N\times T_{\text{mul}}+[(m+2)(N-1)+1]T_{\text{Add}}$，其对应简化结果是 $(1.05N+7.490)$ ms. 具体相应结果见表 5.

Table 5 Comparison of Theoretical Computational Overhead for Batch Verification

表 5 批量验证下的理论计算开销比较 ms

方案	聚合验证阶段耗时
LCPPA	$2.861N+48.697$
LBCPPA	$4.130\,4N+13.284$
本文方案	$1.05N-7.490$

为了更直观地了解本文方案相较于 LCPPA，LBCPPA 方案在聚合验证情景下展现的优越性. 图 2 展示了具体的相关测定结果.

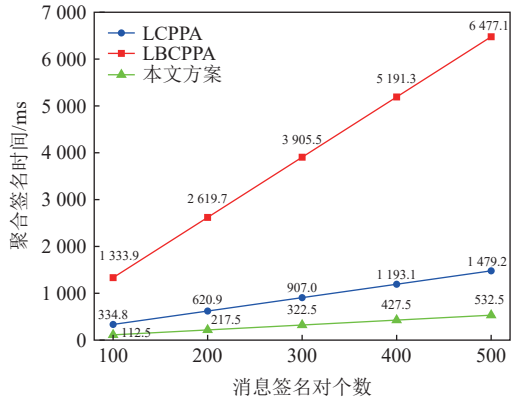


Fig. 2 Comparison of aggregate verification overhead under different numbers of message-signature pairs

图 2 不同消息签名对数量下聚合验证开销对比

由图 2 可知，相较于基于一般格构造的方案，本文方案在计算效率上有明显的优势. 具体地，对于聚合验证情形，将消息签名对的数量从 100 扩增至 500 时，相较于 LCPPA 和 LBCPPA 方案计算效率提升幅度达到近似 1.785~1.917 倍.

2）通信开销

对与单验证情形，根据文献 [17−18] 的参数设计可知，LCPPA 方案通信计算复杂度近似为 $O(n\lg q)$，LBCPPA 方案通信计算复杂度近似为 $O(2n\lg(q-1))$. 注意到本文通信开销与消息签名对 $\{ANS_i,T_i,\boldsymbol{\delta}_i\}$ 关联，不难算出其通信复杂度为 $O(n\lg q+n(\lg q)^2)$. 类似易得批量认证通信复杂度，详细结果见表 6.

Table 6 Comparison of Communication Overhead for Batch Authentication

表 6 批量认证下通信开销比较

方案	单个消息签名对	N 个消息签名对
LCPPA	$O(n\lg q)$	$O(Nn\lg q)$
LBCPPA	$O(2n\lg(q-1))$	$O(2Nn\lg(q-1))$
本文方案	$O(n\lg q+n(\lg q)^2)$	$O(Nn\lg q+Nn(\lg q)^2)$

6 总结与展望

本文基于结构化格上的 RLWE 决策困难假设和 RSIS 困难假设，并结合无抽样技术，设计了一种车联网中基于格的无抽样条件隐私保护聚合认证方案. 具体来说，首先利用计算性实例下的 *GenTrap-RLWE* 算法构造陷门生成，从而有效提高局部签名密钥提取算法的计算效率；其次利用格密码中的无抽样技术进一步提高签名算法的计算效率；然后利用多项式环特殊的可交换性质，取代之前普遍从指定域 $\mathbb{Z}_q$ 中随机抽取元素构成验证系数的方法，进而有效降低了聚合签名的 ℓ_2 范数；再者在随机预言机模型下论证方案满足适应性安全；最后通过模拟实验结果证实了所提方案相较于同类基于格的聚合认证方案在计算效率层面上更加有效，但通信开销复杂度较高. 因此，接下来将尝试考虑使用紧凑的 NTRU 格设计公私钥、签名尺寸更优的车联网中基于格的聚合认证方案.

作者贡献声明：张静、杨志负责方案整体设计并撰写论文；许艳负责实验内容的设计；崔杰、仲红提出指导意见并修改论文.

参 考 文 献

[1] Cui Jie, Wei Lu, Zhang Jing, et al. An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 20(5): 1621−1632

[2] Zhong Hong, Zhang Shuo, Cui Jie, et al. Broadcast encryption scheme for V2I communication in VANETs[J]. IEEE Transactions on Vehicular Technology, 2021, 71(3): 2749−2760

[3] Kuang Boyu, Li Yuze, Gu Fangming, et al. Review of Internet of vehicle security research: Threats, countermeasures, and future prospects[J]. Journal of Computer Research and Development, 2023, 60(10): 2304−2321 (in Chinese)
(况博裕，李雨泽，顾芳铭，等. 车联网安全研究综述：威胁、对策与未来展望[J]. 计算机研究与发展，2023，60(10)：2304−2321)

[4] Hubaux J P, Capkun S, Luo Jun. The security and privacy of smart vehicles[J]. IEEE Security & Privacy, 2004, 2(3): 49−55

[5] Raya M, Hubaux J P. Securing vehicular ad hoc networks[J]. Journal of Computer Security, 2007, 15(1): 39−68

[6] Lu Rongxing, Lin Xiaodong, Zhu Haojin, et al. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications[C]//Proc of the 27th Conf on Computer Communications(INFOCOM' 2008). Piscataway, NJ: IEEE, 2008: 1229−1237

[7] Zhang Chenxi, Lin Xiaodong, Lu Rongxing, et al. RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks[C]//Proc of the 2008 IEEE Int Conf on Communications. Piscataway, NJ : IEEE, 2008: 1451−1457

[8] Shao Jun, Lin Xiaodong, Lu Rongxing, et al. A threshold anonymous authentication protocol for VANETs[J]. IEEE Transactions on Vehicular Technology, 2015, 65(3): 1711−1720

[9] Li Jie, Lu Huang, Guizani M. ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 26(4): 938−948

[10] Shamir A. Identity-based cryptosystems and signature schemes[C]// Proc of the CRYPTO 1984. Berlin: Springer, 1984: 47−53

[11] He Debiao, Zeadally S, Xu Baowen, et al. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(12): 2681−2691

[12] Ogundoyin S O. An autonomous lightweight conditional privacy-preserving authentication scheme with provable security for vehicular ad-hoc networks[J]. International Journal of Computers and Applications, 2020, 42(2): 196−211

[13] Horng S J, Tzeng S F, Huang P H, et al. An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks[J]. Information Sciences, 2015, 317: 48−66

[14] Mei Qian, Xiong Hu, Chen Jinhao, et al. Efficient certificateless aggregate signature with conditional privacy preservation in IoV[J]. IEEE Systems Journal, 2020, 15(1): 245−256

[15] Gupta M, Gera P, Mishra B. CPAAS: An efficient conditional privacy-preservation anonymous authentication scheme using signcryption in VANET[J]. International Journal of Vehicle Information and Communication Systems, 2021, 6(1): 88−105

[16] Mukherjee S, Gupta D S, Biswas G P. An efficient and batch verifiable conditional privacy-preserving authentication scheme for vanets using lattice[J]. Computing, 2019, 101(12): 1763−1788

[17] Dharminder D, Mishra D. LCPPA: Lattice-based conditional privacy preserving authentication in vehicular communication[J]. Transactions on Emerging Telecommunications Technologies, 2020, 31(2): e3810

[18] Li Quanru, He Debiao, Yang Zhichao, et al. Lattice-based conditional privacy-preserving authentication protocol for the vehicular ad hoc network[J]. IEEE Transactions on Vehicular Technology, 2022, 71(4): 4336−4347

[19] Ajtai M. Generating hard instances of lattice problems[C]//Proc of the 28th Annual ACM Symp on Theory of Computing. New York: ACM, 1996: 99−108

[20] Wen Jiaming, Bai Lu, Yang Zhichao, et al. LaRRS: Lattice-based revocable ring signature and its application for VANETs[J]. IEEE Transactions on Vehicular Technology, 2023, 73(1): 739−753

[21] Bai Shi, Ducas L, Kiltz E, et al. CRYSTALS-Dilithium algorithm specifications and supporting documentation (version 3.1)[EB/OL]. 2021[2024-01-09]. https://pq-crystals.org /dilithium/resources.shtml

[22] Micciancio D, Regev O. Worst-case to average-case reductions based on Gaussian measures[J]. SIAM Journal on Computing, 2007, 37(1): 267−302

[23] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions[C]//Proc of the 40th Annual ACM Symp on Theory of Computing. New York: ACM, 2008: 197−206

[24] Ducas L, Micciancio D. Improved short lattice signatures in the standard model[C]//Proc of the 34th Annual Cryptology Conf. Berlin: Springer, 2014: 335−352

[25] Lyubashevsky V. Lattice signatures without trapdoors[C]//Proc of the Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2012: 738−755

[26] Peikert C, Rosen A. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices[C]//Proc of the 3rd Theory of Cryptography Conf (TCC 2006). Berlin: Springer, 2006: 145−166

[27] Ducas L, Durmus A. Ring-LWE in polynomial rings[C]//Proc of the 15th Int Conf on Practice and Theory in Public Key Cryptography. Berlin: Springer, 2012: 34−51

[28] Micciancio D, Peikert C. Trapdoors for lattices: Simpler, tighter, faster, smaller[C]//Proc of the Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2012: 700−718

[29] Choon J C, Hee Cheon J. An identity-based signature from gap Diffie-Hellman groups[C]//Proc of the 6th Int Workshop on Practice and Theory in Public Key Cryptography Miami. Berlin: Springer, 2002: 18−30

[30] Victor Shoup. NTL: A library for doing number theory[EB/OL]. [2024-01-09]. http://www.shoup.net/ntl/

[31] Genise N, Micciancio D. Faster Gaussian sampling for trapdoor lattices with arbitrary modulus[C]//Proc of the 37th Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2018: 174−203

[32] Chen Yuanmi, Nguyen P Q. BKZ2.0: Better lattice security estimates[C]//Proc of the Int Conf on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2011: 1−2



Zhang Jing, born in 1990. PhD, professor. Her main research interests include VANETs and the Internet of things.

张　静, 1990 年生. 博士, 教授. 主要研究方向为车联网、物联网.



Yang Zhi, born in 1997. Master candidate. His main research interests include lattice-based cryptography and VANETs.

杨　志, 1997 年生. 硕士研究生. 主要研究方向为格密码学、车联网.



Cui Jie, born in 1980. PhD, professor, PhD supervisor. His main research interests include Internet of vehicles security and Internet of things security.

崔　杰, 1980 年生. 博士, 教授, 博士生导师. 主要研究方向为车联网安全、物联网安全.



Xu Yan, born in 1982. PhD, associated professor. Her main research interests include cryptography and Internet of vehicles security. (xuyan@ahu.edu.cn)

许　艳, 1982 年生. 博士, 副教授. 主要研究方向为密码学、车联网安全.



Zhong Hong, born in 1965. PhD, professor, PhD supervisor. Her main research interest includes network and information security.

仲　红, 1965 年生. 博士, 教授, 博士生导师. 主要研究方向为网络与信息安全.