# 格基环签名的车联网隐私保护

崔永泉[1) ] 曹 玲[1)] 张小宇[1)] 曾功贤[2)]

[1)](华中科技大学计算机科学与技术学院 武汉 430074)

[2)](香港大学计算机科学系 香港)

**摘 要** 现今,车联网在学术以及智能交通等领域已经成为一个研究热点.车联网有一些显著的优点:(1)为驾驶者和交通管理员提供了便利(如实时交通信息系统);(2)提高了车辆行驶的安全程度(如追尾提前警告系统).这样一种应用需要车辆用户之间共享信息.然而在实际应用中,车辆之间的通讯可以被恶意攻击者用来定位和跟踪车辆,因此隐私保护在车联网中至关重要.虽然之前已经提出了一些解决方案,但是这些方案都存在各类缺点.该文提出了一个新的基于格困难问题的环签名方案来解决这个问题.相比于其他方案,格基环签名方案实现了无条件的匿名性,在必要的时候还可以为授权方提供可追踪性.另外,该文方案不同于采用传统公钥密码进行隐私保护的方案,而是基于格的环上错误学习问题而设计的,这样可以确保其在量子算法攻击下的安全性.

**关键词** 车联网;隐私保护;格签名;环签名;可追踪性

**中图法分类号** TP309 **DOI 号** 10.11897/SP.J.1016.2019.00980

# Ring Signature Based on Lattice and VANET Privacy Preservation

CUI Yong-Quan[1)] CAO Ling[1)] ZHANG Xiao-Yu[1)] ZENG Gong-Xian[2)]

[1)](*School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan* 430074)

[2)](*Department of Computer Science, University of Hong Kong, Hong Kong*)

**Abstract** In contemporary society, Vehicular Ad-hoc Network (VANET) has been a hot research topic in academic as well as other fields, such as intelligent transportation field. The application, VANET, has some charming strengths: (1) it can provide more convenient service for drivers and traffic managers (e.g. real time traffic information system); (2) it also increases the safety of vehicle traffic (e.g. rear-end early warning system). Such kind of service or convenience is based on shared information from participant users. The information includes the time, the location and other information about the roads and traffic. Usually, the message is broadcasted among many vehicles or temporary networks. Thus, communications between vehicles can be easily eavesdropped by some malicious attackers, who may be one of the normal users among the networks. And the message can be used by malicious attackers to locate and track the vehicles in practice. Therefore, it is essential to preserve the privacy in VANET. To our knowledge, there are many scheme proposed to solve this problem and they can be classified into as follows: anonymous certification, pseudo ID, group signature and ring signature. And currently, the most accepted schemes are based on pseudo ID, where users need to change their identities regularly and which is easy to be implemented. However, if the identity is changed in a not appropriate time, then the solution may not be effective. As for the anonymous certification schemes, though

收稿日期:2016-06-27;在线出版日期:2017-12-05.本课题得到国家"九七三"重点基础研究发展规划项目基金(2014CB340600)、国家自然科学基金(61173050)资助.**崔永泉**,博士,讲师,中国计算机学会(CCF)会员,主要研究方向为访问控制、数据库安全、格基密码学.E-mail:yqcui1977@hust.edu.cn.**曹 玲**(通信作者),硕士研究生,主要研究方向为格基密码学、网络安全.E-mail:1350128743@qq.com.**张小宇**,博士研究生,主要研究方向为格基密码学.**曾功贤**,博士研究生,研究方向为格基密码学、ORAM.

they offer conditional traceability with high computational efficiency, the distribution, the revocation and the huge storage of these certifications become the thorny problems. And the group signature based schemes are convenient to form a temporary network automatically and also have the property of traceability and anonymity. However, a role in these scheme, named group administrator, becomes the bottleneck of security, who is powerful and is needed to be trusted by others. In this paper, we will focus on the ring signature scheme which is paid less attention than others. The reasons why we choose ring signature are the following: (1) in ring signature based schemes, ring members are equal when compared to that of group signature based scheme, since it has no administrator role, so it is better to preserve the privacy; (2) compared to the anonymous certificate scheme, it does not need to communicate with certificate authorities, ring signature scheme is more flexible and automatic; (3) although it is not as simple as pseudo ID based schemes, ring signature scheme can achieve a higher security level. The main contributions of this paper include the following. First, we try to put forward a lattice-based ring signature scheme to deal with the privacy problem in VANET for a higher security level. In recent years, it is a concern to the attacks of quantum algorithms and lattice-based encryption schemes attracts a lot of attention. Second, to achieve the goal of anonymity and traceability, we apply the non-interactive zero knowledge proof technology to our construction. As a result, when the authorities want to know the true identity of some senders or malicious attackers who broadcast incorrect message, it can be achieved under the cooperation of all ring members.

**Keywords**　VANET; privacy preservation; lattice signature; ring signature; traceability



## 1　引　言

车联网(Vehicular Ad-Hoc Network, VANET)是一种移动自组织网络,它可以对交通全过程进行智能化控制,提高交通效率和交通安全性. 目前VANET遇到最大的挑战在于如何保持安全性和私密性之间的合理平衡:对接收者来说,从源头接收可靠的信息是至关重要的,然而这种可靠信息违背了发送者的隐私需求.

目前很多研究学者提出的实现车联网隐私保护的方案基本可归类如下:匿名证书[1-4]、群签名[5-9]、假名[10-17]、环签名[18]. 现在被VANET社区广泛接受的是假名授权方案. 为了提高效率,Jiang等人提出了一种支持批量处理的使用假名的车联网匿名认证方案[11],该方案中使用了基于身份的签名,同时通过计算HMAC(Hash-based Message Authentication Code,哈希消息认证码)来避免检查CRL(Certificate Revocation List,证书吊销列表)带来的开销. 另外,Artail等人提出了一种基于假名的车联网环境下的匿名通信框架[12],该框架包括假名的生成、分发、重生成等几个过程,并使用了一种分布式优化算法来改变假名. Vijayalakshmi等人提出了一种基于ID(IDentifier,身份标识符)的车联网身份认证方案[17],该方案使用基于公钥加密的假名方案. 在位置隐私保护方面,研究者也提出了许多基于假名的方案. Rabieh等人提出了一种用来对抗合谋攻击的车联网位置隐私保护方案[13],该方案在使用假名和匿名认证的基础上,更进一步的防止敌手获取车辆的行车路线. Huang等人提出了一种基于软件定义网络的车联网位置隐私保护方案[14],该方案中使用双线性映射理论来解决假名的分发问题. 在前人的研究基础上,人们甚至开始考虑在基础设施较缺乏的环境下车联网的工作,Sucasas等人就提出了这样一种假名方案[15],方案中的假名分发、消息验证、假名撤销等过程可以不需要持续性连接CA(Certificate Authority,数字证书认证机构).

虽然假名方案广泛地受到关注,许多研究者也投入了许多的精力,但是为了实现隐私保护,假名方案需要不断的更改假名. 这样一个瓶颈会束缚着车联网的发展,尤其是如果在一个不恰当的时间段或者位置上修改了假名,那么所提出的解决方案将可能无效.

匿名证书方向也有一些方案. Vijayakumar等

人提出了一种基于匿名证书的车联网匿名认证方案[2],该方案能够实现有条件的身份追踪,同时具有较高的计算效率. Forster 等人提出了一种车联网环境下针对匿名证书的隐私保护方案[3],该方案提出了匿名证书的一种撤销方法. Feiri 等人提出了一种车联网匿名证书管理方案[4],该方案针对车联网环境拓扑变化频繁、隐私保护等需求,提出了证书撤销、证书分发的方法. 匿名证书虽也能达到保护隐私的目的,其不足在于证书的分发、撤销以及大量证书的存储等问题,这些都需要进一步深入研究.

与本文较为接近的是群签名方案,它具备匿名性和可追踪的特点,并被一些学者用于构建匿名认证方案. Tiwari 等人提出了车联网环境下一种结合群签名和基于身份签名的安全的身份认证方案[7],该方案能够适应高交通密度的地区. Shao 等人提出了一种使用群签名的车联网匿名认证方案[9]. 该方案具有可追踪性和可撤销性,并且可以进行批量处理. 不过,在所有的群签名方案中,都涉及到一个重要的问题,那就是如何选出群管理者. 因为管理员角色权限过大,对于群签名方案来说,一般都是假设群管理员是安全可信的,但是在实际过程中,这种假设或许不能成立,因而将会对方案的安全性造成威胁.

值得一提的是,还有一部分方案使用椭圆曲线密码学、基于身份的密码学等方法来达到隐私保护的目的,例如,Liu 等人提出了一种基于随机双线性配对盲签名的车联网身份隐私保护方案[19],Guo 等人提出了一种基于椭圆曲线的车联网匿名认证方案[20],该方案具备可追踪性. 也有一些混合方案: Buttner 等人提出了一种能够进行匿名认证的车联网密钥协商协议[21],该协议结合使用了椭圆曲线加密方案和环签名方案; Mathews 等人提出了一种基于双线性配对的车联网假名生成方案[22]; Li 等人提出了一种有条件隐私安全的车联网认证框架[23],该框架使用基于 ID 的公钥加密方案,具备可追踪性; Zhang 等人提出了一种使用基于身份签名的车联网匿名认证方案[24],在该方案中,即使 RSU(Road Side Unit,路边节点)被控制,敌手也很难对车辆进行跟踪. 在位置隐私保护方面,Ying 等人提出了一种基于候选位置列表的车联网位置隐私保护方案[25],该方案动态改变 mix-zone 以提升匿名性. 这些方案充分体现了车联网社区的活跃,以及人们对该领域的热切关注程度.

在这篇文章中,我们将重点介绍的是关注较少的环签名方案. 选择环签名的理由有以下几点: (1)在环签名中,环成员的地位均等,相比于群签名方案,环签名没有群管理员角色,能够更好的保护隐私; (2)相比于匿名证书方案,它不需要时刻与证书分发中心保持联系,环签名方案更加灵活; (3)虽然不及假名方案的简便性,但环签名方案具有更高的安全性.

主要贡献及创新点. 由于车联网社区在隐私保护方面保持着高度的关注,本文将在这个问题上尝试提出新的解决办法,具体的研究内容包括: (1)更高的安全性; (2)在保障匿名性的同时实现部分特殊角色具有可追踪性. 简单来说,本文以城市车辆密集区域为背景,提出了一种基于格困难问题的环签名方案,来解决车联网中隐私保护问题. 在近十几年的密码学领域,格密码作为抵抗量子算法攻击的主要方案,一直受到广泛的关注. 此外,环签名具有良好的匿名性和不可伪造性,所以我们相信基于格困难问题的环签名方案,能够提供有效解决车联网中的隐私保护问题的能力. 方案的细节以及正式的安全性证明将在后续的章节介绍. 第二个研究内容在某些特殊情况下具有非常重要的现实意义,例如交通事故现场再现来追踪肇事者时,权威部门需要知道车联网消息交换过程中发送者的真实身份,本文在环签名中环成员的相互配合下,采用非交互的零知识证明技术,确保仅有权威部门能够辨别消息发送者,实现可追踪性.

## 2 预备知识

### 2.1 车联网

典型的 VANET 由路边节点(Road Side Unit, RSU)、信任机构(Trust Authority, TA)和装备有车载单元(On Board Unit, OBU)的交通工具组成,如图 1 所示.

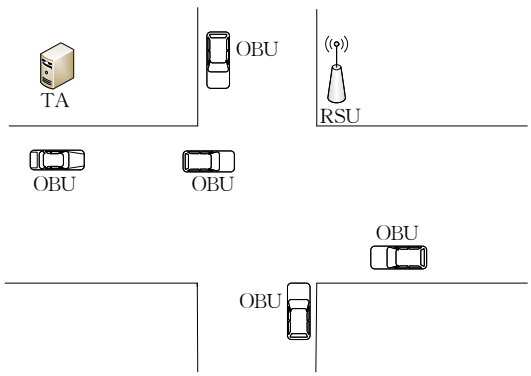


图 1 VANET 结构

VANET 基础设施 RSU 通过有线连接的方式进入 VANET，并被交通部门通过可信授权的方式管理，RSU 可以广播类似撤消车辆身份的一些常规信息. 在 VANET 中车辆需要定期向附近车辆广播车辆状态信息(包括位置、速度、方向、消息产生时的时间戳等)，这些信息对周围的所有车辆都是公开的. 一个熟练而且知识丰富的攻击者可以利用某些发送/接收装置截获来往车辆间传送的无线电波中的信息，并从这些信息中获取驾乘人员身份、车辆过往未来行驶路线、与某一特定车辆的联系等隐私. 本文主要讨论车联网中用户身份的匿名性解决方案.

本文中我们提出了一个新的车联网身份隐私保护方案，加入车联网的车辆会和附近车辆形成共同的环. 在我们的网络模型中，大部分信息如车辆周期性广播的信标消息和 RSU 广播的公共信息等是不需要保密的，但是这些消息是和责任相关联的，使用消息之前必须验证该消息来自一个合法的网络成员，并验证消息的真实性，所以需要使用签名技术. 车辆会用环签发后续的消息，从而在保证消息真实性的前提下有效地将自己的真实身份隐藏起来，实现车联网中匿名通信. 我们应用基于环的密码技术，通过路边设施帮助车辆快速地和附近的车辆形成环. 我们还提出了有效的可追踪机制，在需要的时候(如交通事故处理时)根据签名的消息可以识别出签名者的真实身份，从而实现了车辆在车联网中无条件匿名的隐私通信.

### 2.2　格理论

**定义 1.**　整数格.

$\boldsymbol{b}_i$ 为 $m$ 维的整数向量，取 $m$ 个线性无关的向量 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$，$B=(\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m)\in Z^{m\times m}$，我们称 $B$ 为一组格的基. 由 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 整系数线性组合形成的向量集合即为由基 $B$ 生成的整数格：$L(B)=\{Bc:c\in Z^m\}$.

**定义 2.**　$q$ 模格.

对于正整数 $q$、$m$、$n$ 和矩阵 $\boldsymbol{A}\in Z^{m\times n}$，可以定义下面的 $q$ 模格：

$L_q(\boldsymbol{A})=\{x\in Z^m:\exists s\in Z_q^n$，其中 $\boldsymbol{A}^{\mathrm{T}}s=x(\mathrm{mod}\,q)\}$，

$L^{\perp}(\boldsymbol{A})=\{x\in Z^m:\boldsymbol{A}x=0\,\mathrm{mod}\,q\}$.

**定义 3.**　格上的高斯分布.

任意实数 $s>0$ 和维数 $m>1$ 的格记为 $\Lambda$；高斯函数 $\rho_s$ 定义为：$\rho_s(x)=\exp(-\pi\|x\|^2/s)$. 则格上的离散高斯分布定义为 $\forall x\in\Lambda$，$D_{\Lambda,s}=\rho_s(x)/\rho_s(\Lambda)$.

**定义 4.**　错误学习问题(Learning with Errors Problem，LWE).

给定整数 $n\geq1$，$x$ 是模数 $q\geq2$，$Z_q$ 上的一个错误分布. 按下面的方式得到 $A_{s,x}\in Z_q^n\times Z$：随机选择向量 $\boldsymbol{a}\in Z_q^n$，$s\in Z_q^n$，$\boldsymbol{e}$ 服从分布 $x$，输出 $\boldsymbol{a},b=(\boldsymbol{a},s)/q+\boldsymbol{e}$，LWE 包含两个具体问题. Search 问题：已知 $A_{s,x}$ 和 $(\boldsymbol{a},b)$ 来求解 $s$ 的计算问题；Decision 问题：$s\in Z_q^n$ 服从均匀分布，区分 $(\boldsymbol{a},b)$ 的均匀分布的问题.

**定义 5.**　环上错误学习问题(Learning with Errors Problem over ring，R-LWE).

R-LWE 问题是在 LWE 问题的基础上改进的算法. 给定多项式环 $R$ 以及整数 $n$、$k$、$q$，$R=Z_q[x]/(x^n+1)$，$n=2^k$，$k\geq1$，$q=1\,\mathrm{mod}\,2n$，$\boldsymbol{a}\in R^m$，$m\in Z$，$\boldsymbol{a}$ 服从均匀分布，$\psi_\alpha$ 为正态分布，$\boldsymbol{e}\in R$，$\boldsymbol{e}\sim\psi_\alpha$，$\boldsymbol{e}$ 为服从正态分布的差错向量. R-LWE 包含两个具体问题. Search 问题：已知 $b\in R^m$，$b=\boldsymbol{a}\cdot s+\boldsymbol{e}$，由 $(\boldsymbol{a},b)$ 求解 $s$ 的问题；Decision 问题：$s\in R^m$ 服从均匀分布，$b\in R$，计算 $b=\boldsymbol{a}\cdot s+\boldsymbol{e}$，记 $A_{s,\psi}$ 为 $(\boldsymbol{a},b)$ 的分布，区分 $A_{s,\psi}$ 与 $R\times R$ 上的均匀分布的问题. 如果 Decision 问题是困难的，那么 $A_{s,\psi}$ 是伪随机的.

**定义 6.**　小整数解问题[26](Small Integer Solution Problem，SIS)

$m,n\in Z$，$q$ 是素数，矩阵 $\boldsymbol{A}\in Z_q^{n\times m}$ 服从随机均匀分布. 求解一个向量 $\boldsymbol{v}\in\Lambda_q^{\perp}(\boldsymbol{A})$，且范式满足 $\|\boldsymbol{v}\|\leq\beta$，其中 $\beta$ 为选定的小实数，称为该问题门限.

## 3　相关工作

### 3.1　基于格的数字签名

(1) 系统初始化 Initialization$(n,k,r)$：

选择安全参数 $n$($n$ 为 2 的幂次方，大于 512)以及模数 $q=2^k$，$m=n\cdot(k+2)$，$c>\sqrt{n}\omega(\sqrt{\log(2n)})$，$r\geq2\sqrt{\ln\left(2n\left(1+\frac{1}{\varepsilon}\right)\right)/\pi}$(一般 $r$ 取 3 即可)，$C=1/\sqrt{2\pi}$，$s\approx C\cdot(\sqrt{n\cdot k}+\sqrt{2n})\cdot c\cdot r$. 然后，选择一个多项式 $\phi(X)$，为了方便计算，我们可以选择 $\phi(X)=x^n+1$，那么系统中使用的环记为 $R_q=Z_q[X]/\phi(X)$.

(2) 密钥产生 KeyGen$(1^n)\rightarrow(A,R)$：

随机选择一个多项式 $a$，选择多项式集合 $R$ 作为私钥，

$$R=[r_1,r_2,\cdots,r_k]\in R_q^k,$$

以及多项式误差集合 $e$，

$$e=[e_1,e_2,\cdots,e_k]\in R_q^k,$$

最后我们计算出公钥 $A$：

$$A=[1,a,g_1-(a\cdot r_1+e_1),\cdots,g_k-(a\cdot r_k+e_k)] \tag{1}$$

其中，$g_i$ 是 $G=[1,2,\cdots,2^{k-1}]\in R_q^k$ 里的第 $i$ 项，每一项都是一个常数多项式.

于是我们返回$(A,R)$，完成初始化. 通过这种方式我们得到的公钥是伪随机的，保持着 R-LWE 问题的困难度.

(3) 签名算法 $\mathrm{Sign}(M,R,A)\rightarrow x$：

**算法 1.** $\mathrm{Sign}(M,R,A)$.

输入：要签名的信息 $M$，私钥 $R$ 和公钥 $A$

输出：签名 $x$

1. 计算哈希值 $\mu=H(M)\in R_q$，相当于将消息映射到某一个多项式上；

2. 抽样出多项式 $p=[p_1,p_2,\cdots,p_{k+2}]\in R_q^{k+2}$，使得满足 $\nu=\mu-A\cdot p\in R_q$；

3. 抽样出 $Z\in R_q$，使得 $G\cdot Z=\nu$ 成立；

4. 签名

$$x=\left[\sum_{i=1}^{k}e_i z_i,\sum_{i=1}^{k}r_i z_i,z_1,z_2,\cdots,z_k\right]+p \tag{2}$$

(4) 验证算法 $\mathrm{Verify}(\mu,x,(H,A))\rightarrow\{0,1\}$：

**算法 2.** $\mathrm{Verify}(x,A,M)$.

输入：签名值 $x$，公钥 $A$，消息 $M$

输出：1/0

验证 $A\cdot x\equiv H(M)$ 与二范式 $\|x\|_2\leq s\sqrt{m}$ 是否成立. 如果成立，那么接受，输出 1；否则拒绝，输出 0.

### 3.2 环签名的可追踪性

环签名机制拥有自发性、无条件匿名性等特点，能够用来隐藏签名者的身份信息. 在某些特殊情况下，例如发生交通事故时，需要追踪消息发送者的真实身份，因此具有可追踪性的环签名方案更具有实用价值. 环签名的可追踪性并不是近期才有的研究方向，早有学者提出了具有可追踪性的环签名方案，如孙庆英等人提出的可追踪的环签名方案[27]. 环签名实现的前提是所有环节点都积极配合，追踪签名者身份信息之前必须检查环签名是否正确有效，若有效，再接着追踪到签名者的身份.

为实现可追踪性安全要求，环签名方案三步过程中将增加下列内容.

(1) 在初始化的过程中，增加追踪密钥：

$$TP=\left(\sum_{i=1}^{k}e_i,\sum_{i=1}^{k}r_i,1\right)\in R_q^{k+2} \tag{3}$$

(2) 消息签名过程中增加 $TK$ 和 $T$ 的计算. 随机抽样出一组随机数 $t_1,t_2,\cdots,t_{usr\_num}$，计算：

$$T=\left(\sum_{i=1}^{usr\_num}t_i G\right)\cdot A_s\ (A_s\text{为签名者公钥}) \tag{4}$$

$$TK_i=t_i A_i\ (i=1,2,\cdots,usr\_num) \tag{5}$$

(3) 发布签名内容时，将 $T$ 与 $TK_i$ 一起作为签名内容发布. 消息签名验证的过程不变.

(4) 增加追踪步骤. 需要追踪签名者时，环中所有节点协作，来找到真正的签名者.

追踪过程分为以下几步：

① 检验拿到的环签名是否正确.

② 若有效，将 $TK_i$ 发送给所有环成员，环成员计算 $T_i=TK_i\cdot TP_i$，再对 $T_i$ 做签名，显然 $T_i\in R_q^k$，成员使用私钥计算得出 $x_i$，满足 $A_i x_i\equiv T_i$ 并且 $\|x_i\|_2\leq s\sqrt{m}$，返回 $x_i$ 和 $T_i$ 的值.

③ 验证 $x_i$ 值的有效性. 即 $A_i x_i\equiv T_i$ 和 $\|x_i\|_2\leq s\sqrt{m}$ 是否都成立. 计算 $T_i A_i$ 与 $G\cdot TK_i$，若环成员积极配合，返回值有效，两个值相等.

④ 计算 $T'=\left(\sum_{i=1}^{usr\_num}T_i\right)\cdot A_i$，若当 $i=s$ 时，$T'=T$ 成立，则签名者为 $s$.

### 3.3 NIZK 证明系统

本节中设计了一个非交互式零知识证明系统(Non-interactive Zero-knowledge Proof，NIZK)用来实现基于 R-LWE 环签名的验证. 环签名有两个关键算法：一个安全性好的单向陷门函数和一个可以在隐藏签名者前提下验证签名的环方程. 本文方案选择的是格困难问题中 R-LWE 问题的单向陷门函数，使用 NIZK 系统证明所验证的签名来自一个真实的签名者，即环签名是非伪造的.

依据 3.1 节内容，基于 R-LWE 的格签名为真需要两个条件都成立：

$$A\cdot x\equiv H(M) \tag{6}$$

$$\|x\|_2\leq s\sqrt{m} \tag{7}$$

由环签名的有效性可以得知，验证式(6)成立较为容易，但是验证式(7)成立可能暴露签名者的身份. 为了解决这个难题，我们借鉴 Tian 等人基于 SIS 的环签名方案[28]. 在完成其他成员的签名时，将原本的随机抽样替换成 Gentry 等人提出的格点筛选算法中的抽样算法[29]，使抽样得到的 $\sigma_i(i=1,2,\cdots,n,i\neq s)$ 全部都满足 $\|\sigma_i\|_2\leq s\sqrt{m}$ 不等式条件，验证时仅需要验证所有签名 $\|x\|_2\leq s\sqrt{n\cdot m}$($n$ 为环成员数).

NIZK 系统中，证明者将需要验证的消息摘要作为挑战值，验证者只需要验证挑战值的正确性. 如上述，我们验证只需要满足 $A\cdot\boldsymbol{x}\equiv y$. 因而我们设计了基于格的 NIZK 证明系统，用来证明环签名中确实

存在一个向量 $\boldsymbol{x}$，满足 $A\cdot\boldsymbol{x}\equiv y$. 实质是将 $A\cdot\boldsymbol{x}\equiv y$ 作为消息隐藏，却并不阻碍验证者验证等式是否成立. 我们利用的是求解 R-LWE 问题的单向性，一般由 $\boldsymbol{x}$ 求 $y$ 容易，由 $y$ 求 $\boldsymbol{x}$ 困难，但是签名者知道私钥，由 $y$ 求 $\boldsymbol{x}$ 也容易. 实现流程如下：

证明者 Prove，验证者 Verify.

首先 Prove 使用双方都知道的不同的公钥 $A$ 值，使用基于格点筛选算法的抽样算法，抽样构造 $x_1,x_2,\cdots,x_{usr\_num}$，满足 $\|x_i\|_2\leq s\sqrt{m}$，计算出对应的 $y_1,y_2,\cdots,y_{usr\_num}$. 计算消息的摘要 $\mu=H(M)$，$y_1$，$y_2,\cdots,y_{usr\_num}$ 与 $\mu$ 满足等式 $f(y_1,y_2,\cdots,y_{usr\_num},\mu,y)=0$. 得到 $y$ 值，由于函数的单向性，Prove 拥有私钥，所以能够求出对应的 $\boldsymbol{x}$. Prove 向 Verify 发出挑战值 $(x_1,x_2,\cdots,x_{usr\_num},\boldsymbol{x})$.

然后 Verify 验证挑战值的正确性. 由挑战值和公钥信息计算出 $y_1,y_2,\cdots,y_{usr\_num}$，由哈希函数计算出消息的摘要 $\mu=H(M)$. 然后验证

$$f(y_1,y_2,\cdots,y_{usr\_num},\mu,y)=0 \tag{8}$$

和

$$\|x,x_1,x_2,\cdots,x_{usr\_num}\|_2\leq s\sqrt{(usr\_num+1)\cdot m} \tag{9}$$

是否成立，若两者都成立则证明者 Prove 通过验证. 任何一个不成立，则证明者没有通过验证.

本文中设计的 NIZK 系统一方面隐藏环签名的签名者，一方面又可以验证是否存在有效签名. 证明签名中要求的式(6)与(7)同时成立，显然其安全性完全依赖于单向陷门函数的计算困难性. 本文采用的单向陷门函数基于格上 R-LWE 问题，它能够抵抗量子攻击，也是计算存储效率较好的格困难问题，因此本文的 NIZK 系统也就较为安全高效.

## 4　车联网环境下的环签名方案

(1) 系统初始化 Initialization Ring( )

**算法 3.**　Initialization Ring( ).

输入：安全参数 $n,k$，多项式 $a=x^n+1$

输出：$A,R,TP$

1. $TA$ 首先选择安全参数，获得公私钥，如上文中初始化算法 Initialization$(n,k,r)$ 和公私钥生成算法 KeyGen$(n,k)$ 所示.

2. 由可追踪性方案式(3)计算得出 $TP$，于是我们得到 $(A,R,TP)$，完成初始化. 通过这种方式我们得到的公钥是伪随机的，保持着 R-LWE 问题的困难度.

(2) 用户注册

我们方案中有两种类型的用户，即 OBU 和 RSU，不同用户具有不同的注册流程. OBU 用户身份验证注册使用与 $TA$ 相同的方法：生成公私钥，将追踪密钥和身份消息发送给 $TA$，$TA$ 验证身份，把身份与公钥绑定，用户保管 $R$ 作为私钥来签署签名，$TP$ 来完成可追踪性实现的协作.

RSU 作为一种公共基础设施，它的建设者是可信的，故可以由它的建设者为其注册，并为其分配公私钥对. 它的身份必须对所有用户公开，因此很容易成为黑客攻击的目标. 因而 RSU 把自己的 ID 作为公钥(ID 到多项式的转换)，并向所有车联网用户公开.

(3) 产生环

我们设计的环生成机制描述如下：当车辆进入 RSU 覆盖的区域时，车辆向 RSU 提出组环申请(传输过程中可以使用 RSU 的公钥加密，但是这不是本文讨论的重点，不赘述). RSU 从车辆接收到请求信息后，验证消息的时效性和有效性，将公钥存储到环集中，当环集中公钥数目达到预设值时，RSU 将环集广播出去. 所有包含在这个环集中的车辆可以使用这个环来签署各自的消息.

(4) 消息签名

当车辆向其他车辆广播消息时，它首先构造包含时间戳的消息 $M$，然后选取环 ring，ring 中包含了环中成员的公钥，利用算法 RingSign$(M,\text{ring},A,R,TP)$ 产生签名 $\sigma$.

**算法 4.**　RingSign$(M,\text{ring},A,R,TP)$.

输入：消息 $M$，其他环成员的公钥 $A_i$，自己的公私钥 $A_s,R_s$

输出：$(M\|A_1,A_2,\cdots,A_{usr\_num}\|\sigma_1,\sigma_2,\cdots,\sigma_{usr\_num}\|TK_1,TK_2,\cdots,TK_{usr\_num}\|T\|\text{rand}\|v\|s)$

1. 签名者模拟其他环成员的签名：

假设用户 $s$ 想要发送消息，环中的成员数为 $usr\_num$. 随机选择 $\{\sigma_j\}_{j\neq s}\in R_q^{usr\_num}$，计算出 $y_j\equiv A_j\sigma_j$.

2. $v=H(M)=C_{k,v}(y_1,y_2,\cdots,y_{usr\_mm})$ 计算环方程. 环方程有如下计算方式：

$$\begin{array}{ccccccc} v\rightarrow & \oplus & \rightarrow E\cdots & & E\leftarrow & \oplus & \leftarrow z(z=v) \\ & \uparrow & & & & \uparrow & \\ & y_j\equiv A_j\sigma_j & & & & y_{usr\_num}\equiv A_{usr\_num}\sigma_{usr\_num} & \end{array}$$

其中，$\oplus$ 表示异或运算，$E$ 是对称加密(对称加密可以自定义，这里的主要作用是达到混乱的效果).

3. 计算出满足环方程的 $y_s$.

4. 对 $y_s$ 做签名，如算法 1 Sign( ) 求得 $\sigma_s$ 并且满足于 $y_s\equiv A_s\sigma_s$.

5. 计算 $TK$ 与 $T$. 随机抽样出一组随机数 $t_1,t_2,\cdots,t_{usr\_num}$，分别计算 $T=\left(\sum_{i=1}^{usr\_num}t_iG\right)\cdot A_s$，$TK_i=t_iA_i$ $(i=1,2,\cdots,usr\_num)$.

6. 最后输出环签名消息.

(5)消息验证

**算法 5.** RingVerify($\mu,x,H,A$).

输入:消息的摘要 $\mu$,签名值 $x$,公钥 $A$,哈希函数 $H$

输出:1/0

一旦从邻近车辆收到消息,每个人可以通过 RingVerify($\mu,x,H,A$)算法验证消息的有效性.

1. 验证环的有效性,即验证 ring 中没有重复的元素和撤销的公钥,否则拒绝消息.

2. 验证环方程的有效性,由 $y_j \equiv A_j \sigma_j$ 计算出 $y_1, y_2, \cdots, y_{usr\_num}$,验证环方程是否成立.如果成立,那么接受;否则拒绝.

3. NIZK 系统证明 $\sigma_1, \sigma_2, \cdots, \sigma_{usr\_num}$ 中存在一个真实签名,如上文 3.3 节所述.

上面 3 个条件都满足,则验证通过,环签名正确有效.

(6)消息追踪 Trace($M$, ring, $\sigma$, rand)

如上文 3.2 节所述,必要时,通过环中所有节点的协作,来找到真正的签名者,并且假设所有的环节点都积极配合协作.

**算法 6.** Trace($M$,ring,$\sigma$,rand).

输入:环签名消息

输出:$i$

1. 检验签名的有效性,详细过程参考消息验证算法 5 RingVerify( ).若检验环签名是合法有效的签名,则继续下面的步骤.

2. 将 $TK_i$ 发送给所有环成员,要求返回 $T_i = TK_i \cdot TP_i$ 和对 $T_i$ 的签名 $x_i$,$x_i$ 显然满足 $A_i x_i \equiv T_i$ 并且 $\|x_i\|_2 \le s\sqrt{m}$.

3. 验证 $T_i$ 值的有效性.验证 $x_i$ 是否满足 $A_i x_i \equiv T_i$ 和 $\|x_i\|_2 \le s\sqrt{m}$,若 $x_i$ 满足条件再验证 $T_i$ 值的有效性.计算 $T_i A_i$ 与 $G \cdot TK_i$,若环成员积极配合,返回值有效,两个值相等.

4. 计算 $T' = \left(\sum_{i=1}^{usr\_num} T_i\right) \cdot A_i$,若当 $s=i$ 时,$T'=T$ 成立,则签名者为 $s$.

影响我们方案正常运行效率的主要是签名和验证签名两部分.消息追踪算法仅在特殊情况下需要追踪时才运行,因此我们的方案效率不考虑追踪步骤.所以在分析该方案性能时,追踪部分的运算和成员之间的交互时间都不在考虑范围内.

# 5 安全性分析与证明

## 5.1 理论分析

我们提出的基于格的环签名方案不仅可以抵抗量子算法的攻击,还具有以下属性.

匿名性:假设接收到的是一个正确的签名,我们知道签名中的每一个 $\sigma$ 值都是在对应值域内合理的取值,因此成员之外的人猜出环签名者的概率为 $1/n$(假设环中有 $n$ 名成员),而除真正的签名者外,环成员猜测成功的概率为 $1/(n-1)$.

自发性:由上述方案可知,每个成员在没有其他成员的参与下可以独自完成签名,因此有良好的自发性,能够较好地隐藏自我身份.

不可伪造性:攻击者要伪造签名,关键是要伪造方案中的 $\sigma_i$.在我们的方案中,签名者本人以外的其他人想要伪造环签名是困难的.

## 5.2 安全性证明

下面,我们将对方案的安全性进行详细的探讨.

**引理 1.** 如果 3.1 节基于格的数字签名方案中 $A \cdot x \equiv \mu$ 和 $\|x\|_2 \le s\sqrt{m}$ 都成立,则格签名是真实的.

证明. 验证 $A \cdot x \equiv \mu$ 成立,而 $\mu$ 在签名过程中满足 $G \cdot Z = \mu - A \cdot p$,即 $G \cdot Z = A \cdot x - A \cdot p$ 等式成立.具体计算过程如下:

$$\begin{aligned} G \cdot Z &= A \cdot x - A \cdot p \\ &= A(x-p) \\ &= A\left(\sum_{i=1}^{k} e_i z_i, \sum_{i=1}^{k} r_i z_i, z_1, z_2, \cdots, z_k\right) \\ &= A\left(\sum_{i=1}^{k} e_i z_i, \sum_{i=1}^{k} r_i z_i, Z\right) \\ &= (1, a, G - aR - e)(eZ, RZ, Z) \\ &= eZ + aRZ + Z(G - aR - e) \\ &= G \cdot Z \end{aligned} \tag{10}$$

验证 $\|x\|_2 \le s\sqrt{m}$ 不等式成立,说明这就是我们寻找的"小"的解.该不等式与上述 $A \cdot x \equiv \mu$ 等式同时成立,则说明该签名 $x$ 满足 R-LWE 的困难条件.由定义 5 可知,R-LWE 的 Search 问题是困难的,即已知 $\mu$ 和 $A$ 求得 $x$,并且满足不等式 $\|x\|_2 \le s\sqrt{m}$ 是困难的.因此,我们认为满足上述两个条件的签名就是真实有效的签名. 证毕.

**定理 1.** 本文提出的环签名方案具有匿名性.

证明. 假设接收到的是一个正确的签名,我们知道签名中的每一个 $\sigma$ 值都是在对应值域内合理的取值,是依据格点筛选算法抽样得到的,并且所服从的分布是不可区分的,都满足 $\|\sigma\|_2 \le s\sqrt{m}$ 不等式条件.因此环之外的人猜中真实签名的概率为 $1/n$(假设环中有 $n$ 名成员),除签名者之外的成员猜中的概率为 $1/(n-1)$.

环签名在被隐藏起来的同时还要可以被验证真伪,这是一般环签名方案都具有的安全属性.不同的是一般环签名只需要保证签名的环方程等式成立,但本文中设计的环签名方案是基于格 R-LWE 问题

的，如 3.1 节所示，需要验证等式与不等式同时成立. 我们设计了一个 NIZK 证明系统来实现，详细说明见 3.2 节. 因而本文方案签名满足环方程成立的同时，也满足确实存在一个签名者的条件. 继而本文的方案也是达到无条件匿名性的.　　证毕.

**引理 2.**　如果 R-LWE 问题是困难的，那么在我们的方案中，伪造签名是困难的.

证明.　如果敌手要伪造一个签名，关键是要构造方案中所有的 $\sigma_i$. 在此我们给出一个简单的证明思路. 假设存在攻击者 $A$ 能够伪造正确的环签名，即对于一个环，环外的 $A$ 能够构造出正确的环签名. 更进一步地分析，这个假设是表明在环方程得出 $y_i$ 后，$A$ 能够计算出对应的 $\sigma_i$.

我们假设用户 $i$ 的公钥为

$$A_i=[1,a_i,g_1-(a_i\cdot r_{i1}+e_{i1}),\cdots,g_k-(a_i\cdot r_{ik}+e_{ik})]$$

$A$ 给出的签名为

$$x=\left[\sum_{i=1}^{k}e_iz_i,\sum_{i=1}^{k}r_iz_i,z_1,z_2,\cdots,z_k\right]+p \quad (11)$$

那么我们说 $A$ 可以破解 R-LWE 问题.

我们知道公钥中存在 $k$ 组 $(a_i,a_i\cdot r_i+e_i)$，即 $k$ 个 R-LWE 问题. 从方程的角度来看，我们需要求解 $2k$ 个未知数，而现在我们仅有 $k$ 个等式. 那么我们调用 $[k/2]$ 次 $A$，即进行 $[k/2]$ 次不同的签名，就会得到另外 $k$ 个不同的等式，最终就可以求解出所有的未知数，即求解 R-LWE 问题.

但是当前计算机的计算能力还达不到在多项式时间内解决 R-LWE 问题，因此 $A$ 破解我们方案的能力在现在的条件下并不存在，故在我们的方案中，伪造签名是困难的.　　证毕.

**定理 2.**　本文的环签名方案具有可追踪性的安全属性.

环签名的密码机制中，签名者利用 $n-1$ 个他人的公钥构造签名来隐藏自己，达到匿名的目的. 但是特殊情况下需要撤销匿名性，使得有关机构可以追踪签名者的签名. 本方案通过在签名中附加信息并且得到环成员的帮助，来找到签名者.

证明.　该证明过程分为两步：第一步是证明关于上述环签名方案的可追踪性相关的追踪算法是正确有效的，第二步是证明本方案的可追踪机制能够防止签名者抵赖. 下面是详细证明过程.

(1) 可以知道追踪密钥 $TP=\left(\sum_{i=1}^{k}e_i,\sum_{i=1}^{k}r_i,1\right)\in R_q^{k+2}$，随机抽样出一组随机数 $t_1,t_2,\cdots,t_{usr\_num}$，$T=\left(\sum_{i=1}^{usr\_num}t_iG\right)\cdot A_s$（$A_s$ 为签名者公钥），$TK_i=t_iA_i$. 追踪过程分为三步：① 验证该签名是否正确有效，这一步由算法 5 RingVerify( )可以得到；② 将 $TK_i$ 发送给所有环成员，要求环成员返回 $T_i=TK_i\cdot TP_i$ 值和成员用自己私钥完成对 $T_i$ 的签名 $x$. 验证 $T_i$ 值和 $x$ 的有效性. 若 $T_iA_i$ 与 $G\cdot TK_i$ 两个值相等且 $A_ix\equiv T_i$，$\|x\|_2\le s\sqrt{m}$，返回值有效；③ 计算 $T'=\left(\sum_{i=1}^{usr\_num}T_i\right)\cdot A_i$，若当 $s=i$ 时，$T'=T$ 成立，则签名者为 $s$. 后一步是在前一步正确的基础上进行的，否则终止追踪.

该过程中有两个关键步骤：验证 $T_i$ 的有效性和证明 $T'=T$ 等式成立. 其中 $T_i$ 的有效性可验证如下：

$$\begin{aligned}T_i&=TK_i\cdot TP_i\\&=t_i(1,a,G-(aR+e))\cdot(e,R,1)\\&=t_iG\end{aligned}\quad (12)$$

则 $T_iA_i=t_iG\cdot A_i$，而 $G\cdot TK_i=G\cdot t_iA_i$，所以当环成员返回值正确时，$T_iA_i$ 与 $G\cdot TK_i$ 相等. 由 3.2 节可知当该成员对 $T_i$ 签名时，显然 $x$ 也是有效的. 此时 $T_i$ 有效.

$T'=T$ 等式成立证明如下：

$$\begin{aligned}T'&=\left(\sum_{i=1}^{usr\_num}T_i\right)\cdot A_i\\&=\left(\sum_{i=1}^{usr\_num}t_iG\right)\cdot A_i\end{aligned}\quad (13)$$

而 $T=\left(\sum_{i=1}^{usr\_num}t_iG\right)\cdot A_s$，显然，当 $i=s$ 时，$T'=T$ 成立，则签名者为 $s$. 即可追踪性机制正确可验证.

(2) 同样地，签名者 $s$ 对消息做了签名，但是在追踪签名者时不予配合.

该成员记为 $t$，公钥为 $A_t$，追踪密钥为 $TP_t$. 追踪者要求 $t$ 返回 $T_i=TK_i\cdot TP_t$ 的值和对 $T_i$ 的签名 $x$. 该成员有自己的追踪密钥，但不配合这次追踪. 也有两种情况，仅伪造 $T_i$ 或仅伪造 $x$.

伪造 $T_i$ 时，返回 $T_i'=TK_i\cdot TP_t'$ 的值. 由于 $TP_t'$ 是伪造的，因而：

$$T_i'A_i=TK_i\cdot TP_t'=t_iA_i\cdot TP_t'\ne G\cdot TK_i \quad (14)$$

即返回值 $T_i$ 无效. 下一步则验证 $\|x\|_2\le s\sqrt{m}$ 和 $Ax\equiv T_i$ 两个条件是否成立. 若成立，则可以推断该成员只是没有配合寻找真正的签名者，这样做可能的原因是签名者就是他；若不成立，则可以认为该成员完全没有配合相关机构的工作，这样一个恶意不配合的行为会被有关机构检测出来，同时也加大了该成员是真实签名者的嫌疑.

伪造 $x$ 时，验证 $\|x\|_2 \leq s\sqrt{m}$ 和 $Ax \equiv T_i$ 时不成立，而 $T_i$ 有效，可以推测 $T_i$ 的值并不是该成员计算 $T_i = TK_i \cdot TP_t$ 得到的. 验证 $T_i$ 有效性时可以知道 $T_i \cdot A_i = G \cdot TK_i$，则 $T_i = G \cdot TK_i \cdot A_i^{-1}$，此时的成员可能是伪装的，并不是真正的环成员. 验证 $T_i$ 无效时，我们可以推断该成员也可能是伪装的.

综合上述分析，只有拥有私钥的环成员可以生成有效的签名 $x$，因而伪装成环成员是无法成功的；环成员不配合追踪也不能通过 $T_i$ 验证，不配合的行为会被发现，不配合的环成员存在是真实签名者的嫌疑. 所以，确定签名者的必要条件是所有环成员都积极配合. 证毕.

**定理 3.** 本文的环签名方案满足强不可伪造性安全要求.

证明. 假设在多项式时间内，攻击者 $A$ 能够以不可忽略的概率 $p$ 破解本文的方案，成功伪造环签名，那么我们将构建模仿者 $S$ 来攻击挑战者 $C$ 声称的安全格签名算法.

我们定义一个 Game，步骤如下：

(1) 挑战者 $C$ 根据格签名算法，初始化 $n$ 个签名实例，生成 $n$ 对公私钥对 $(pk, sk)$，并将所有的 $pk$ 发送给模仿者 $S$.

(2) 模仿者 $S$ 在接收到 $pk$ 后，随机选择其他参数，完成环签名算法的初始化，并将所有 $pk$ 发送给攻击者 $A$.

(3) 查询. 攻击者 $A$ 随机选取一个消息 $M$ 发送给模仿者 $S$，$S$ 按照环签名算法，随机选择一个用户 $s$ 来产生环签名，并计算出对应的 $y_s$，将其发送给挑战者 $C$，挑战者 $C$ 计算出对应的 $\sigma_s$，并返回给模仿者 $S$. 最后模仿者 $S$ 将完整的环签名返回给攻击者 $A$.

(4) 挑战. 攻击者 $A$ 发送消息 $M$ 及其对应的之前未出现过的环签名给模拟者 $S$，并告知 $S$ 伪造的用户名，那么 $S$ 可以算出被伪造签名的用户它对应的 $y_s$，并将 $(y_s, \sigma_s)$ 发送给 $C$. 如果 $C$ 验证 $y_s$ 和对应 $\sigma_s$ 的有效，则签名 $\sigma_s$ 有效，即 $S$ 成功伪造一个格签名，输出 1；反之，$S$ 失败，输出 0.

由假设知，攻击者 $A$，能够以不可忽略的概率 $p$ 破解本文的方案，成功伪造环签名，那么 $\Pr(\text{Output}(\text{Game}) = 1) = p$，即 $S$ 将以不可忽略的概率破解挑战者 $C$ 声称的安全格签名算法. 然而现在普遍认为基于格的签名算法是安全的，因此假设不成立，即在多项式时间内，攻击者 $A$ 不能以不可忽略的概率破解本文的方案. 证毕.

## 6 性能分析

我们主要考虑的是城市中车辆密集的区域，参照 Aboobaker 文章中 VANETS 的参数设置[30]，我们使用的参数见表 1.

**表 1 车联网应用模拟参数设置**

| 参数 | 数据 |
|---|---|
| 时速 | <10 km/h |
| 基站覆盖半径范围 | 300 m |
| 车间距 | 5 m |
| 车道 | 单向 3 车道，共 6 车道 |
| 可用的带宽 | 6 Mpbs |

那么车辆通过一个基站所需时间为 300 m/10 km/h=108 s. 我们假设发送组网请求的车辆位于基站覆盖半径内的 100 m 范围内，那么在这个路段的车辆有 100/5×6=120 辆，因此有充足的车辆来组成环.

我们使用 C++ 语言，在 FLINT 库的帮助下，简单地测试了我们提出的签名方案. 其中硬件条件为 2 GB 内存，一个主频 2.53 GHz 的处理器，运行的系统为 64 位 Ubuntu 14.10.

改变安全参数 $n$、$k$、成员数三个与计算效率密切相关的因素，得到公私钥生成、签名、验证 3 个步骤的计算时间，时间精确到小数点后第六位，表 2 展示的是签名方案的实验所得数据.

**表 2 签名方案实验数据表**

| $n$ | $k$ | 成员数 | 生成密钥时间/s | 签名时间/s | 验证时间/s |
|---|---|---|---|---|---|
| 128 | 24 | 5 | 0.042707 | 0.06491 | 0.026710 |
| 256 | 24 | 5 | 0.071654 | 0.09187 | 0.069369 |
| 384 | 24 | 5 | 0.176399 | 0.11927 | 0.088405 |
| 416 | 24 | 5 | 0.137243 | 0.17518 | 0.124132 |
| 440 | 24 | 5 | 0.147013 | 0.17620 | 0.131567 |
| 448 | 24 | 5 | 0.149814 | 0.17972 | 0.127592 |
| 464 | 24 | 5 | 0.198469 | 0.18345 | 0.136139 |
| 128 | 27 | 5 | 0.047280 | 0.05689 | 0.023783 |
| 256 | 27 | 5 | 0.085054 | 0.10294 | 0.077070 |
| 384 | 27 | 5 | 0.1230155 | 0.14245 | 0.103638 |
| 416 | 27 | 5 | 0.131912 | 0.15475 | 0.118235 |
| 440 | 27 | 5 | 0.209824 | 0.22051 | 0.160457 |
| 448 | 27 | 5 | 0.219283 | 0.21907 | 0.161083 |
| 464 | 27 | 5 | 0.235437 | 0.21901 | 0.165109 |
| 128 | 24 | 10 | 0.070676 | 0.05860 | 0.039664 |
| 256 | 24 | 10 | 0.109620 | 0.13840 | 0.096559 |
| 384 | 24 | 10 | 0.184924 | 0.17640 | 0.145449 |
| 416 | 24 | 10 | 0.181447 | 0.19820 | 0.148097 |
| 440 | 24 | 10 | 0.194848 | 0.20920 | 0.157677 |
| 448 | 24 | 10 | 0.216345 | 0.21110 | 0.163102 |
| 464 | 24 | 10 | 0.207018 | 0.22540 | 0.170738 |

将表 2 中的实验数据绘制成更加直观的折线图，得到图 2、图 3、图 4. 图 2 显示了参数选择对生成密钥时间的影响，图 3 显示了参数选择对签名时间的影响，图 4 显示了参数选择对验证时间的影响，从中可以看到随着多项式公钥的度增加，生成密钥时间、签名时间、验证时间都趋向增加.

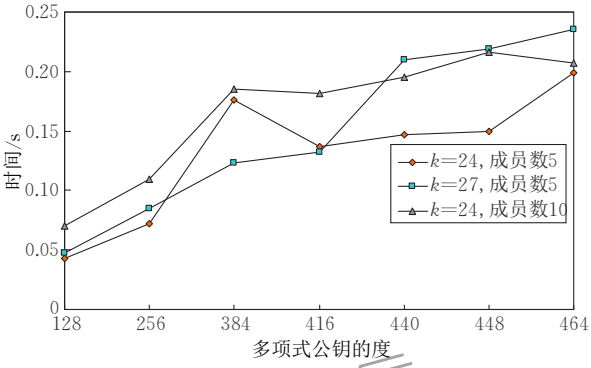


图 2　参数选择对生成密钥时间的影响

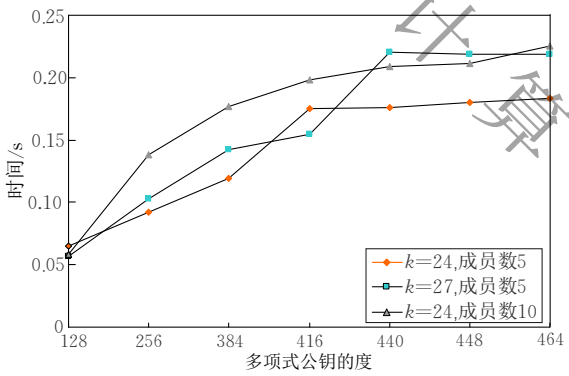


图 3　参数选择对签名时间的影响

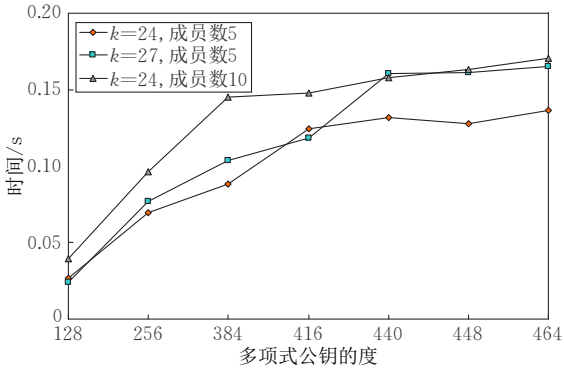


图 4　参数选择对验证时间的影响

不考虑网络中的其他问题，从表 2 数据可以看到，在城市中车辆密集的区域，有充足的车辆和宽裕的时间来组成环. 生成签名的时间相对于通过基站的时间是可接受的. 因此我们提出的方案可以初步满足组环和生成签名的需求.

在上述实验数据的基础上，我们使用网络仿真工具 NS2 的 2.35 版本来模拟实际交通环境中该车联网通信方案的运行情况. 我们模拟了一个 500 m 长的十字路口在 200 s 内的情况，车辆数目在 20～55 辆间，车速为 11 m/s，随机出现在十字路口的四个端口，通信距离是 250 m. RSU 位于十字路口中间，信号范围是 250 m. 得到的数据如图 5 所示，其中车联网延迟为实验中每个移动节点平均延迟，消息吞吐量为单位时间内环境中总吞吐量. 图 5 展示了随着车辆数目增加，车联网延迟和吞吐量都有所增加.

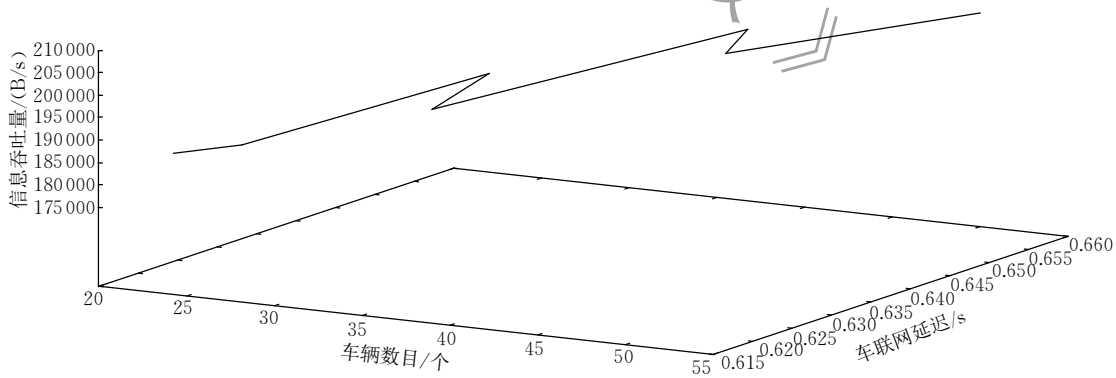


图 5　车辆密集与延迟、吞吐量

从图 5 中可以发现，车联网延迟约为 0.6 s，吞吐量约为 185 000 B/s，即 185 KB/s，显然能被用户接受.

## 7　总结及展望

随着人们对格密码这类抗量子计算攻击的密码体制关注度的提高，格签名问题也逐渐成为研究热点. 而车联网作为当前新技术的前沿，必须依靠安全技术的保障. 本文将格签名技术运用到了车联网中，主要关注车联网的隐私保护问题.

本文主要有以下的贡献，首先分析了密码学中关于格的理论、R-LWE 问题、环签名和 NIZK 非交互式零知识证明系统等理论，在前人相关研究的基

础上提出基于格上 R-LWE 问题的车联网隐私保护方案.在该方案中,采用 NIZK 证明系统实现对环签名的验证,且实现了环签名的可追踪性设计,填补了环签名相对群签名而言无法追踪签名者的不足,并改进了群签名中管理员权限过于集中的问题,也让环签名拥有更广阔的应用空间.在结合车联网的应用环境后,详细设计了基于 R-LWE 的具有可追踪性的环签名方案.然后分析并证明了格签名的可验证性、环签名的无条件匿名性、不可伪造性、强不可伪造性和可追踪性等安全属性.最后给出了模拟实验与仿真验证的结果,分别从横向和纵向两个方面考察了方案的性能.第一个实验测试基于格的环签名方案的签名效率、验证效率等签名性能参数.第二个实验在网络仿真模型下,测试了在复杂的车联网环境中,在容忍一定数据丢失率的情况下,环签名方案的有效性及吞吐量等问题.与前人的研究成果相比,本文创新主要在于:在车联网环境中引入了抗量子攻击的密码体制,并构造了基于格上 R-LWE 问题的环签名方案,实现了环签名的可追踪性设计;我们下一步优化重点在格签名的长度优化上.

总体而言,本文在提出基于格 R-LWE 问题的环签名方案的基础上,实现了车联网内用户发送消息的无条件匿名性,采用 NIZK 非交互式零知识证明系统对环签名进行验证,并设计实现了在特定条件下实现签名成员的可追踪性,同时通过模拟仿真实验测试了方案的性能.然而,本文中可追踪性是通过环成员的协作完成的,该假设比较强,值得进一步研究在现实应用环境下如何实现该假设.方案中签名内容的长度大约是环成员数量的两倍,并且与环成员数量成正比.因此进一步的环签名长度优化工作亟待解决,而且这些研究方向在之后的工作中将会是非常有价值的.

## 参 考 文 献


[1] Laurendeau C, Barbeau M. Secure anonymous broadcasting in vehicular networks//Proceedings of the IEEE Conference on Local Computer Networks 2007. Dublin, Ireland, 2007: 661-668

[2] Vijayakumar P, Azees M, Deborah L J. CPAV: Computationally efficient privacy preserving anonymous authentication scheme for vehicular ad hoc networks//Proceedings of the 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud). New York, USA, 2015: 62-67

[3] Forster D, Kargl F, Lohr H, et al. PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET)//Proceedings of the 2014 IEEE Vehicular Networking Conference (VNC). Paderborn, Germany, 2014: 25-32

[4] Feiri M, Pielage R, Petit J, et al. Pre-distribution of certificates for pseudonymous broadcast authentication in VANET//Proceedings of the 2015 IEEE 81st Vehicular Technology Conference (VTC Spring). Glasgow, UK, 2015: 1-5

[5] Wasef A, Shen X. MAAC: Message authentication acceleration protocol for vehicular ad-hoc network//Proceedings of the IEEE Global Telecommunications Conference. Hawaii, USA, 2009: 4476-4481

[6] Wasef A, Shen X. PPGCV: Privacy preserving group communications protocol for vehicular ad hoc networks//Proceedings of the IEEE International Conference on Communications. Beijing, China, 2008: 1458-1463

[7] Tiwari D, Bhushan M, Yadav A, et al. A novel secure authentication scheme for VANETs//Proceedings of the 2016 2nd International Conference on Computational Intelligence & Communication Technology (CICT). Ghaziabad, India, 2016: 287-297

[8] Yu R, Kang J, Huang X, et al. MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks. IEEE Transactions on Dependable and Secure Computing, 2016, 13(1): 93-105

[9] Shao J, Lin X, Lu R, et al. A threshold anonymous authentication protocol for VANETs. IEEE Transactions on Vehicular Technology, 2016, 65(3): 1711-1720

[10] Chaurasia B K, Verma S. Conditional privacy through ring signature in vehicular ad-hoc networks//Proceedings of the Transactions on Computational Science XIII. Berlin, Germany, 2011: 147-156

[11] Jiang S, Zhu X, Wang L, et al. An efficient anonymous batch authentication scheme based on HMAC for VANETs. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(8): 2193-2204

[12] Artail H, Abbani N. A pseudonym management system to achieve anonymity in vehicular ad hoc networks. IEEE Transactions on Dependable and Secure Computing, 2016, 13(1): 106-119

[13] Rabieh K, Mahmoud M M E A, Younis M. Privacy-preserving route reporting scheme for traffic management in VANETs//Proceedings of the 2015 IEEE International Conference on Communications (ICC). London, UK, 2015: 7286-7291

[14] Huang X, Kang J, Yu R, et al. A hierarchical pseudonyms management approach for software-defined vehicular networks//Proceedings of the 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring). Nanjing, China, 2016: 1-5

[15] Sucasas V, Saghezchi F B, Radwan A, et al. Efficient privacy preserving security protocol for VANETs with sparse infrastructure deployment//Proceedings of the International Conference on Communications. London, UK, 2015: 7047-7052

[16] Boualouache A, Moussaoui S. S2SI: A practical pseudonym changing strategy for location privacy in VANETs //Proceedings of the 2014 International Conference on Advanced Networking Distributed Systems and Applications(INDS). IEEE Computer Society, Bejaia, Algeria, 2014: 70-75

[17] Vijayalakshmi N, Sasikumar R. An ID-based privacy preservation for VANET//Proceedings of the International Conference on Computing and Communications Technologies. Chennai, India, 2015: 164-167

[18] Scheuer F, Posse K, Federrath H. Preventing profile generation in vehicular networks//Proceedings of the IEEE International Conference on Wireless and Mobile Computing. Avignon, France, 2008: 520-525

[19] Liu Z, Liu J. A study of privacy improvement using a randomized blind signature scheme in vehicular networks// Proceedings of the 2015 IEEE 12th International Conference on Ubiquitous Intelligence and Computing and 2015 IEEE 12th International Conference on Autonomic and Trusted Computing and 2015 IEEE 15th International Conference on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom). Beijing, China, 2015: 1631-1637

[20] Guo S, Zeng D, Xiang Y, et al. Chameleon hashing for secure and privacy-preserving vehicular communications. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(11): 2794-2803

[21] Buttner C, Huss S A. A novel anonymous authenticated key agreement protocol for vehicular ad hoc networks//Proceedings of the International Conference on Information Systems Security. Kolkata, India, 2015: 259-269

[22] Mathews M S, Sundhari A, Shanthi N V, et al. An efficient pseudonymous generation scheme with privacy preservation for vehicular communication//Proceedings of the International Conference on Intelligent Computing. Taiyuan, China, 2014: 109-117

[23] Li J, Lu H, Guizani M, et al. ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(4): 938-948

[24] Zhang Y, Yang L, Wang S, et al. An efficient identity-based signature scheme for vehicular communications//Proceedings of the 2015 11th International Conference on Computational Intelligence and Security (CIS). Shenzhen, China, 2015: 326-330

[25] Ying B, Makrakis D. Pseudonym changes scheme based on candidate-location-list in vehicular networks//Proceedings of the International Conference on Communications. London, UK, 2015: 7297-7297

[26] Micciancio D, Peikert C. Hardness of SIS and LWE with small parameters//Proceedings of the 33rd Annual International Cryptology Conference. Berlin, Germany, 2013: 21-39

[27] Sun Qing-Ying, Wu Ke-Li, Xu Hui-Yan. Singer-traceable ring signcryption scheme. Computer Engineering, 2011, 37(16): 129-131(in Chinese)
(孙庆英，吴克力，徐会艳. 一种可追踪签名者的环签密方案. 计算机工程，2011，37(16)：129-131)

[28] Tian Miao-Miao, Huang Liu-Sheng, Yang Wei. Efficient lattice-based ring signature scheme. Chinese Journal of Computers, 2012, 35(4): 712-718(in Chinese)
(田苗苗，黄刘生，杨威. 高效的基于格的环签名方案. 计算机学报，2012，35(4)：712-718)

[29] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. Electronic Colloquium on Computational Complexity, 2015, 2015(4): 197-206

[30] Aboobaker A. Performance analysis of authentication protocols in vehicular ad-hoc networks. Faculty of Science\Mathematics, 2010, 2010(2): 12-81

**CUI Yong-Quan**, Ph. D., lecturer. His current research interests include access control, database security, cryptogram based on lattice and VANET.

**CAO Ling**, M. S. candidate. Her current research interests include cryptogram based on lattice and Internet security.

**ZHANG Xiao-Yu**, M. S. candidate. His current research interests include cryptogram based on lattice.

**ZENG Gong-Xian**, Ph. D. candidate. His research interests include cryptogram based on lattice and Oblivious RAM.

**Background**

In this paper, the lattice cryptosystem is researched, which belongs to post quantum field. The foundation of existing lattice signatures scheme was first introduced by Ajtai's creative work, while general structure has low efficiency. Then there is two mainly research direction in lattice problem. One is designing the more efficient signature scheme in random oracle model, and the other one is researching the security in standard computation model. What's more, the above schemes are just at academic stage, far from practical application. Lattice ring signature scheme is a very incomplete piece of work, and it usually has special requirements about different applications, e. g. vehicle ad-hoc networks. Our scheme require anonymity and traceability, while the existing lattice ring signature almost don't solve the trace ability problem. This paper proposes an undeniable ring signature scheme based on lattice to resolve the problem, and modified sampling scheme is applied in signature process to improve efficiency.

This work is supported by the National Basic Research Program of China (973 Program) under Grant No. 2014CB340600, which is about Cloud Computing Security Basic Theory and Method, and under Grant No. 61173050, which is in relation to quantum searching algorithm based on adiabatic evolution. The program resolves the security of cloud computing in all aspects, to ensure it can be applied to all industries and is an important issue in improving the level of information and comprehensive strength. This research in the paper, is a crucial part for this program.