车联网中基于同态加密的兴趣点查询隐私保护协议

范馨月，周美贤
（重庆邮电大学通信与信息工程学院，重庆 400065）

摘　要：针对车联网（IoV）基于位置的服务中隐私保护不全面、计算开销高、通信开销大等问题，提出一种基于同态加密的兴趣点（PoI）查询隐私保护协议，可以同时实现车辆身份、位置、内容隐私保护以及位置服务提供商（LBSP）的PoI数据隐私保护。所提协议采用环签名和K–匿名技术实现车辆身份和位置隐私保护，并利用高级加密标准（AES）对LBSP的兴趣点进行加密。通过同态加密两方安全运算实现查询结果的盲过滤功能，并集成伪随机函数构建轻量化的条件查询模块。真实随机（ROR）安全模型和两种形式化验证工具ProVerif、scyther证明所提协议的安全性，能有效抵御身份伪造、位置追踪、会话劫持等多种安全攻击。实验评估显示，所提协议在开销和时延方面均优于现有协议。所提协议能够在保障车辆身份、位置、查询内容及位置服务提供商数据信息等多维度隐私安全的同时有效降低系统成本，更适用于资源受限的车联网场景。

关键词：车联网；基于位置的服务；盲过滤；环签名；同态加密
中图分类号：TP393.0；TN918
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025248

Homomorphic encryption based privacy protection protocol for point-of-interest queries in Internet of vehicles

FAN Xinyue, ZHOU Meixian
School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract: To address the problems of incomplete privacy protection, high computational overhead, and excessive communication overhead in the Internet of vehicles (IoV), a homomorphic encryption based privacy protection protocol for point-of-interest (PoI) queries was proposed, which could simultaneously realize the vehicle identity, location, and content privacy protection as well as the privacy protection of point-of-interest data from location based service provider (LBSP). Ring signature and K-anonymization techniques were employed in the proposed protocol to achieve privacy protection for vehicle identity and location, and an advanced encryption standard (AES) was utilized to encrypt the PoI of the LBSP. The blind filtering function of query results was realized by homomorphic encryption two-party security operation, and the pseudo-random function was integrated to build a lightweight conditional query module. The real-or-random (ROR) security model and two formal verification tools, ProVerif and Scyther, demonstrated that the proposed protocol was secure against multiple security attacks such as identity forgery, location tracking, and session hijacking. Experimental evaluation showed that it outperformed existing protocols in terms of overhead and delay. The proposed protocol can effectively reduce the system cost while guaranteeing the multi-dimensional privacy security of vehicle identity, location, query content and location service provider data information, which is highly suitable for resource-constrained IoV environments.

Keywords: Internet of vehicles, location-based services, blind filter, ring signature, homomorphic encryption

收稿日期：2025–10–10；**修回日期：**2025–12–16
通信作者：周美贤，S230101220@stu.cqupt.edu.cn
基金项目：国家自然科学基金资助项目（No.62271096）
Foundation Item：The National Natural Science Foundation of China (No.62271096)

0　引言

车联网（IoV, Internet of vehicles）作为物联网的一个重要分支，为用户提供安全、便捷的出行服务，已成为智能交通系统的重要组成部分。基于位置的服务（LBS, location based services）作为流行的位置感知应用，在IoV的背景下得到了广泛的应用。其中，基于兴趣点（PoI, point of interest）查询的LBS是应用最广泛的服务之一。位置服务提供商（LBSP, location based services provider）根据车辆的查询要求返回相应的PoI。例如通过LBS查询，车辆可以从LBSP处获得距离其当前位置r米内的加油站、餐馆或电影院等信息。

虽然LBS为日常生活提供了极大的便利，但在实际应用场景中，其查询过程中的隐私安全问题始终是亟待解决的关键安全痛点。在查询过程中，车辆需要向半可信的LBSP发送包含位置信息和查询内容的LBS查询请求，而好奇的LBSP可能会对车辆用户进行追踪，甚至为了商业利益将车辆的隐私信息泄露给第三方，造成严重的安全和隐私问题。另一方面，从LBSP的角度考虑，其拥有的PoI数据也应该被保护，不能让未经授权的车辆随意访问。因此，如何同时实现车辆的位置隐私、查询隐私以及LBSP端PoI信息隐私保护是LBS隐私保护的关键问题之一。

现有的LBS隐私保护机制根据是否依赖可信第三方（TTP, trusted third party）分为基于TTP和无TTP两类。现有基于K−匿名[1-2]的隐私保护协议大多依赖TTP架构，由TTP根据车辆的原始查询请求构建匿名集，使LBSP无法将查询车辆与匿名集中其他K−1个用户进行区分。但由于TTP不仅能获取用户的位置信息，还能掌握用户查询结果，因此容易成为攻击的目标。一旦TTP被攻破，攻击者便可能窃取用户的敏感数据。为了避免TTP引起的单点故障，文献[3-5]提出了基于加密技术的隐私保护协议，通过对查询车辆的位置和查询消息进行加密，使服务器或潜在攻击者无法获得任何明文信息。这些协议通常采用同态加密算法，该算法支持在密文状态下执行特定运算操作。尽管该技术不依赖TTP，但其会产生巨大的通信与计算开销。文献[6-7]提出的隐私保护协议同样不依赖TTP，只需要一个半可信服务器，但是这些协议通常要求用户发送虚假的LBS查询请求或接收大量冗余的PoI结果信息，导致在用户端产生较高的通信和计算开销，不适合资源受限的车辆设备。

目前已经提出了许多基于PoI查询的隐私保护协议，但有些协议不适用于资源受限的车联网环境，并且存在隐私保护不全面、时延高、通信开销大等问题。因此，本文提出了一种基于同态加密的PoI查询隐私保护协议，实现了查询车辆的身份隐私、位置隐私、查询内容隐私以及LBSP端的PoI信息隐私保护，同时还实现了较高的查询效率。本文的具体贡献如下。

1) 采用环签名和K−匿名技术，实现对查询车辆位置、身份信息和查询内容的隐私保护，同时采用高级加密标准（AES，advanced encryption standard）对称加密算法对LBSP中的数据进行加密处理。非形式化安全分析结果表明，本文协议可以确保机密性、抗身份伪造攻击等关键安全属性。

2) 基于同态加密完成两方安全运算，实现查询结果的盲过滤功能，并结合伪随机函数实现条件查询功能。在该协议中，路侧单元（RSU，road side unit）和LBSP作为2个半可信方，通过双密钥同态加密技术实现两方安全计算，有效过滤冗余的PoI记录，并结合条件查询功能确保用户能够直接获得准确的查询结果，有效减少用户端通信和计算开销。

3) 真实随机（ROR，real-or-random）模型证明本文协议的逻辑正确性及语义安全。ProVerif和Scyther两种形式化验证工具验证了协议隐私保护的有效性和安全性。通过实验仿真与性能评估，本文协议具有较低的计算开销和通信开销，更适合资源受限的车联网环境。

1　相关工作

K−匿名技术[8-10]是最常见的隐私保护技术。文献[8-9]在车辆用户和LBSP之间设置了TTP，由TTP生成K−1个虚假的位置信息，LBSP无法区分真实查询位置和虚假的位置，从而实现位置隐私保护。然而，该协议中TTP掌握用户的敏感信息，易形成单点故障风险，并且用户需自行从包含虚假信息的结果中筛选有效内容，增加了系统的通信开销。梁慧超等[10]以用户的真实路网为基础，对其进行空间划分，然后生成与用户不同位置敏感度相对应的匿名区域。但该技术对使用场景的要求相对

较高，必须在交通流量较大的地方，如城市地区和交叉路口，才能发挥其隐私保护效果。此外，还有一些基于混合区的位置隐私保护协议[11-12]，但是混合区的车辆通信需要频繁更换车辆假名，因此限制了混合区方法的实际应用。Hu等[13]提出了一种基于K–匿名和主动缓存的隐私保护协议，分析了车辆的高流动性特征，并采用混合整数非线性编程建模，基于子模态进行优化，然后用贪婪算法求解，提高了系统的缓存命中率和用户服务质量，但是该协议缺乏对轨迹隐私问题的讨论。

为解决K–匿名机制存在的单点故障问题，研究人员进一步探索基于加密的LBS隐私保护方法。Yadav等[14]提出了基于不经意传输（OT，oblivious transfer）协议与可链接环签名加密技术的隐私保护协议，该协议可以在不暴露车辆用户身份的前提下，同时保障用户的查询隐私与LBSP的数据隐私。但该协议的效率与LBSP数据库规模直接相关，并且车辆用户端需解密所有的接收信息来获得所需查询结果，增加了计算和通信开销。Qi等[3]提出了基于双密钥同态加密的K近邻查询协议，该协议中LBSP将同态加密后的PoI信息外包到云服务器进行计算，并通过与另一台云服务器协同完成双密钥同态加密运算。然而，该研究主要聚焦于合作计算过程中的计算开销分析，忽略了LBSP端因大量同态加密操作所导致的通信与计算开销问题。Wang等[15]设计了一种具有位置隐私保护的RSU辅助位置管理方法，在匿名区采用命令显示加密来保护车辆的位置隐私。Chen等[16]提出了盲过滤的高效隐私保护框架，过滤服务器通过同态加密对查询返回信息进行过滤，但该协议中过滤服务器知道车辆的查询位置，并且无法支持具体的PoI类型查询。Li等[17]在文献[16]盲过滤协议基础上针对交互轮次与计算效率进行了优化，提出了一种增强型单轮盲过滤机制，并且使用车辆端的K–匿名协议来解决过滤服务器能获得车辆位置信息的问题，但该协议无法得到准确的查询距离，只能得到所有满足条件的PoI信息。

2008年，Dwork[18]首次提出差分隐私技术，该技术能防止用户数据被泄露给攻击者。差分隐私的主要目的是在发布用户群体的聚合数据过程中保护个体的位置隐私，其核心定义是在算法的输入数据集中增加一个数据元组或删除一个数据元组，不会对算法的输出产生重大影响。隐私通常是通过添加噪声来实现的，而叠加的噪声通常必须服从拉普拉斯分布。用户位置有2个典型的属性，即地理属性和语义属性[19]。Elkhodr等[20]针对地理属性的隐私保护场景，提出了基于语义混淆生成虚假位置的协议，从而混淆攻击者。然而，这个系统既未充分考虑位置语义属性的隐私泄露风险，也没有针对地理属性与语义属性的不同特征设计分层的防护机制，导致其隐私保护能力在复杂LBS应用场景中存在局限性。目前，还有学者提出了一些基于差分隐私的车辆位置和轨迹隐私保护协议[21-22]。但当只涉及一个用户时，技术上的有效性就不能得到保证，而且泄露位置隐私的风险也更大[23]。

2 理论知识

2.1 环签名

基于椭圆曲线密码体制，选择一个素数阶为q的椭圆曲线加法群G，其生成元为P，环上用户V_i选择随机数$\mathrm{sk}_i \in {}_R\mathbb{Z}_q^*$作为私钥，环上用户数为$N$，计算公钥$\mathrm{PK}_i = x_iP$，$0 \leqslant i \leqslant N-1$。环签名算法如算法1所示。

算法1 环签名

输入 公钥集合$L = \{\mathrm{PK}_0,\cdots,\mathrm{PK}_{N-1}\}$，待签名消息$Q$

输出 环签名σ

1) 签名车辆$V_{\pi \in \{0,1,\cdots,N-1\}}$随机生成$\psi,s_i \in {}_R\mathbb{Z}_q^*$，$0 \leqslant i \neq \pi \leqslant N-1$，假设$\psi P = s_\pi P + C_\pi \mathrm{PK}_\pi$

2) V_π计算$C_{\pi+1} = h(Q,s_\pi P + C_\pi \mathrm{PK}_\pi) = h(Q,\psi P)$

3) for $j = 1{:}1{:}N-1$

4) for $i = (\pi + 1 + j) \bmod N{:}1{:}N-1$

5) 计算$C_i = h(Q,s_{i-1}P + C_{i-1}\mathrm{PK}_{i-1})$

6) end for

7) end for

8) V_π可得$(C_{\pi+2},\cdots,C_0,\cdots,C_\pi)$，用$C_\pi$根据$\psi = s_\pi + C_\pi \mathrm{sk}_\pi$求得$s_\pi$

9) V_π生成签名$\sigma = (C_0,L,s_0,s_1,\cdots,s_{N-1})$

当RSU收到请求车辆发送的消息Q和其环签名σ，执行算法2验证签名。RSU计算$C_{(i+1) \bmod N} = h(Q,s_iP + C_i\mathrm{PK}_i)$，$0 \leqslant i \leqslant N-1$，$i = N-1$时，若$C_{i+1} = C_0$成立，则验证成功接收消息，否则拒绝连接。

算法2　验证签名

输入　环签名$\sigma=(C_0,L,s_0,s_1,\cdots,s_{N-1})$

输出　验证结果

1) for $i=0{:}1{:}N-1$

2)　计算$C_{(i+1)\bmod N}=h(Q,s_iP+C_i\mathrm{PK}_i)$

3) end for

4) if $C_{i+1}=C_0$

5) 验证成功接收消息

6) else拒绝连接

7) end if

2.2　*K*–匿名

在车联网的LBS应用场景中，*K*–匿名技术通过保证发起查询的车辆位置与其他*K*–1个不同位置在可观测特征具备不可区分性，从而实现对车辆的位置隐私保护。本文采用现有的*K*–匿名技术[1]，该方法用熵来度量匿名程度，用弗雷歇距离度量轨迹相似度。该技术将匿名程度与轨迹相似度相结合，以增强位置隐私保护。同时，RSU中还集成了混合缓存策略，减少系统开销和不必要的数据暴露。

2.3　双密钥同态加密

文献[24]提出的同态加密协议中，密文可以通过2种方式进行解密，即直接解密和分布解密。双密钥同态加密具体协议如下。

1) 密钥生成（KeyGen）：随机选择2个位数相等的素数p和q，计算$N=pq$。令$\lambda=\dfrac{\mathrm{lcm}(p-1,q-1)}{2}$，再利用中国剩余定理将$\lambda$分为$\lambda'$和$\lambda''$，使其满足$\lambda'+\lambda''\equiv 1\bmod N^2$和$\lambda'+\lambda''\equiv 0\bmod N^2$。选择随机数$r\in_R\mathbb{Z}_{N^2}^*$，计算$g=-r^{2N}$。设置私钥$\mathrm{sk}_i=\theta_i\in_R[1,\dfrac{N^2}{2}]$，公钥$\mathrm{pk}_i=(N,g,h_i)$，其中$h_i=g^{\theta_i}\bmod N^2$。

2) 加密（Enc）：在收到明文$m\in\mathbb{Z}_N$后，该算法输出公钥pk_i加密的密文$[m]_{\mathrm{pk}_i}=(C_{i1},C_{i2})$，其中$C_{i1}=g^r\bmod N^2$，$C_{i2}=h_i^r(1+mN)\bmod N^2$，$r\in[1,\dfrac{N}{4}]$。

3) 解密（Dec）：密文可以通过2种方式进行解密。

①直接解密（dDec）：密文$[m]_{\mathrm{pk}_i}=(C_{i1},C_{i2})$可以通过私钥$\mathrm{sk}_i$进行直接解密。

$$m=L\left(\frac{C_{i2}}{(C_{i1})^{\theta_i}}\bmod N^2\right)\tag{1}$$

其中，$L(x)=\dfrac{x-1}{N}$。

②分步解密：第一步（pDec1）：输入密文$[m]_{\mathrm{pk}_i}$和λ'，输出密文$C_i^{(1)}=(C_{i2})^{\lambda'}=h_i^{r\lambda'}(1+mN\lambda')\bmod N^2$；

第二步（pDec2）：输入密文$[m]_{\mathrm{pk}_i}$和λ''，计算$C_i^{(2)}=(C_{i2})^{\lambda''}=h_i^{r\lambda''}(1+mN\lambda'')\bmod N^2$，最后输出明文$m=L\left(C_i^{(1)}\cdot C_i^{(2)}\right)$。

在该分步解密过程中，λ'和λ''是等价的，即解密可以通过以下方式进行：先利用λ'执行pDec1，再利用λ''执行pDec2；也可以先利用λ''执行pDec1，再利用λ'执行pDec2。

本文使用的同态加密协议满足加性同态性质。给定2个在同一公钥$\mathrm{pk}=(N,g,h)$加密下的密文$[m_0]_{\mathrm{pk}}=(g^{r_0}\bmod N^2,h^{r_0}(1+m_0N)\bmod N^2)$和$[m_1]_{\mathrm{pk}}=(g^{r_1}\bmod N^2,h^{r_1}(1+m_1N)\bmod N^2)$，可证明

$$[m_0]_{\mathrm{pk}}\cdot[m_1]_{\mathrm{pk}}=(g^{r_0+r_1}\bmod N^2,\ h^{r_0+r_1}(1+(m_0+m_1)N)\bmod N^2)=[m_0+m_1]_{\mathrm{pk}}\tag{2}$$

也可对密文进行明文负运算和标量乘法，选择随机数$k\in_R\mathbb{Z}_N^*$

$$[m]_{\mathrm{pk}}^k=[km]_{\mathrm{pk}}\tag{3}$$

$$[m]_{\mathrm{pk}}^{N-1}=[-m]_{\mathrm{pk}}\tag{4}$$

2.4　伪随机函数

伪随机函数（PRF，pseudorandom function）生成的伪随机输出与任何多项式时间对手的随机输出在计算上是不可区分的。

定义1　给定函数$F:\{0,1\}^n\times\{0,1\}^n\to\{0,1\}^n$，若对于任何概率多项式时间的攻击者$\mathcal{A}$，存在一个可忽略的函数$\epsilon$，使得$|\Pr[A^{F_\eta(\cdot)}(1^n)=1]-\Pr[A^{f_n(\cdot)}(1^n)=1]|<\epsilon(n)$。则称$F$是一个伪随机函数。其中$\eta\leftarrow\{0,1\}^n$，$f_n$是从映射$n$比特字符串到$n$比特字符串的集合中随机选择的。

性质：1)确定性，对于每个固定的密钥k和输入x，其输出$F_k(x)$始终相同。2)不可预测性，伪随机函数的输出对于外部观察者来说是不可预测的。给定输出值，攻击者无法反推密钥或者输入，并且其输出与真正的随机函数在统计上无显著区别。

3　系统模型

3.1　系统框架

本文协议涉及3个实体：车辆、RSU、LBSP。系统框架如图1所示。车辆用户负责生成查询请求

$\{(x,y),r,f\}$，(x,y)表示车辆位置，r表示查询范围，f表示查询条件。为简捷有效地描述协议，本文只设定一个查询条件f，但该协议很容易扩展为支持多个查询条件。RSU是部署在车辆用户和LBSP之间的半可信方，在接收到车辆查询请求后生成K-匿名查询区域，并与LBSP一起进行两方安全计算，完成对K-匿名查询结果的过滤操作。LBSP存储PoI数据集并为车辆用户提供位置服务，每个PoI记录表示为$\{(x_i,y_i),l_i\}$，其中(x_i,y_i)为PoI记录的位置坐标，l_i为其标签信息。如一个PoI记录为$\{(x_i,y_i)$，“餐厅”，“停车场”$\}$，其中(x_i,y_i)表示位置信息，“餐厅”“停车场”是描述该位置的辅助标签。

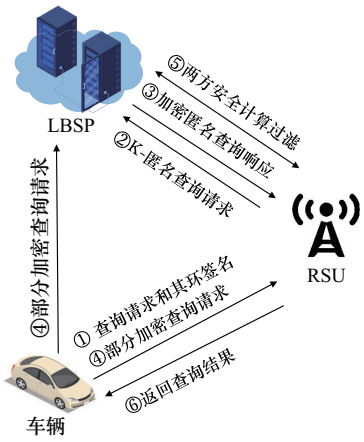

图1 系统框架

除了使用同态加密进行两方安全运算外，协议还使用对称加密AES来保护LBSP中的PoI信息。

3.2 威胁模型

本文假设LBSP和RSU都是半可信的，即诚实但好奇的。它们严格遵循设计的协议和程序，但会尝试根据在执行协议期间合法接收到的信息来推断车辆用户查询的额外信息。并假设LBSP和RSU两者不串通，两者之间的通信信道由传输层安全协议保护，外部攻击者无法从信道中了解到任何有用的信息。

本文采用的威胁模型是Dolev等[25]提出的攻击者模型，攻击者A具有以下攻击能力。

1) 通过公共通道获取、窃听、修改、删除或重发通信实体间传输的消息。

2) 对设备进行物理攻击，获取秘密数据。

3) 还可能进行假冒攻击、离线密码猜测攻击、特权内部攻击等安全攻击。

3.3 安全目标

本文协议主要研究了车辆进行LBS查询时的位置和查询隐私保护，满足以下安全目标。

1) 用户查询隐私：LBSP和RSU都无法知道车辆查询过程中任何有用的信息，包括车辆身份、位置和查询内容。

2) PoI记录隐私：在LBS查询过程中，RSU无法知道存储在LBSP中的PoI信息。

3) 查询结果隐私：准确的查询结果和距离只有车辆能解密，LBSP和RSU无法知道任何关于查询结果的信息。

4 协议设计

本节将详细介绍协议的具体设计，本文协议由5个部分组成，分别为系统初始化、生成查询请求、查询过程、响应过滤、结果解密。协议中部分符号定义如表1所示。

表1 符号定义

符号	定义
$(\mathrm{pk}',\mathrm{sk}')$	RSU同态加密公私钥对
$(\mathrm{pk}_v,\mathrm{sk}_v)$	车辆同态加密公私钥对
$(L_{\mathrm{pk}},L_{\mathrm{sk}})$	LBSP公私钥对
η	PRF密钥
λ	同态加密主私钥
$\lambda'\lambda''$	同态加密部分私钥
k	会话密钥
G,P	椭圆曲线加法循环群及其生成器
q	椭圆曲线加法群阶数
Q,σ	LBS查询请求和其环签名
$\oplus$	异或运算
$h(\cdot)$	哈希运算
$\mathrm{AEnc}(\cdot),\mathrm{ADec}(\cdot)$	AES加密和解密函数
D^*	PoI数据集
Q^*	K-匿名查询请求

4.1 系统初始化

可信中心（TA,trusted authority）选择一个素数阶为q的椭圆曲线加法群G，其生成元为P。定义哈希函数h: $\{0,1\}^* \times G \rightarrow \mathbb{Z}_q^*$。TA为LBSP生成公私钥，其中私钥$L_{\mathrm{sk}} = \delta_1 \in_R \mathbb{Z}_q^*$，公钥$L_{\mathrm{pk}} = \delta_1 P$。

RSU 在 TA 处注册，TA 通过 KeyGen 生成同态加密公私钥对 $(\mathrm{pk}',\mathrm{sk}')$。车辆在 TA 处注册，TA 通过 KeyGen 生成同态加密公私钥对 $(\mathrm{pk}_v,\mathrm{sk}_v)$ 和主私钥 λ，利用中国剩余定理将 λ 分为 λ' 和 λ''。TA 将 λ' 和 λ'' 分别发送给 RSU 和 LBSP，再为车辆生成 AES 密钥 k 作为会话密钥。公布公共参数 $\mathrm{params}=\{G,q,P,h,L_{\mathrm{pk}},\mathrm{pk}',\mathrm{pk}_v\}$。

4.2　生成查询请求

PoI 查询请求由 2 个部分组成：车辆位置 (x,y) 和查询内容 (r,f)，其中 r 表示查询范围，f 表示查询条件。

1) 环签名：查询车辆对查询请求 $Q=((x,y),(r,f))$ 进行算法 1 环签名生成签名 σ，将请求消息 Q 和其签名 σ 发送给 RSU。

2) 加密查询请求：车辆选择随机数 $a\in{}_R\mathbb{Z}_{N^2}^*$，加密查询请求得 $E(x)=(x-a,[a]_{\mathrm{pk}'})$、$E(y)=(y-a,[a]_{\mathrm{pk}'})$、$E(r)=(r-a,[a]_{\mathrm{pk}'})$，其中 $[a]_{\mathrm{pk}'}=\mathrm{Enc}(a,\mathrm{pk}')$。为了保护查询条件 f，车辆为 PRF 初始化一个随机密钥 η，计算得 $F_\eta(f)$。最后加密会话密钥 k 和 PRF 密钥 η：随机选取 $r_1,r_2\in{}_R\mathbb{Z}_q^*$，计算 $R=r_1P$，$Q=r_2P$，$C_1=r_1L_{\mathrm{pk}}$，$C_2=r_2L_{\mathrm{pk}}$，$C_3=k\oplus h(R)$，$C_4=\eta\oplus h(Q)$ 得密文 $c_k=(C_1,C_2,C_3,C_4)$。车辆将 $([a]_{\mathrm{pk}'},F_\eta(f))$ 发给 RSU，将 $(c_k,(x-a),(y-a),(r-a))$ 发给 LBSP。

4.3　查询过程

RSU 根据算法 2 验证环签名 σ，验证成功后接收查询请求 Q，根据文献[1]为请求位置构造 K−匿名查询请求 Q^*，RSU 将查询请求 Q^* 发送到 LBSP。LBSP 搜索 PoI 记录，得到 PoI 数据集 $D^*=\{(x_i,y_i),l_i\}_{1\leqslant i\leqslant n}$，并用会话密钥 k 对其中的 PoI 进行加密，然后将所有加密的 PoI 记录发送给 RSU。LBSP 处理每个 PoI 记录步骤如下。

1) LBSP 用 LBSP 公钥 L_{pk} 解密密文 c_k 得会话密钥 k 和 PRF 密钥 η：$R=C_1L_{\mathrm{pk}}$，$Q=C_2L_{\mathrm{pk}}$，$k=C_3\oplus h(R)$，$\eta=C_4\oplus h(Q)$。

2) 用会话密钥 k 对 PoI 数据集 D^* 中 PoI 记录进行加密：$E_{\mathrm{AES}}(D^*)=\mathrm{AEnc}((x_i,y_i),l_i)_{1\leqslant i\leqslant n}$。

3) 用 PRF 密钥 η 加密标签 l_i：$F_\eta(l_i)_{1\leqslant i\leqslant n}=(F_\eta(l_{i1}),F_\eta(l_{i2}),\cdots,F_\eta(l_{id}))_{1\leqslant i\leqslant n}$。

LBSP 将 $E_{\mathrm{AES}}(D^*)$ 和 $F_\eta(l_i)_{1\leqslant i\leqslant n}$ 发送给 RSU。

4.4　响应过滤

RSU 收到 LBSP 加密的 PoI 数据集 $E_{\mathrm{AES}}(D^*)$ 和加密标签 $F_\eta(l_i)_{1\leqslant i\leqslant n}$ 后，首先检查每个 PoI 记录的加密标签 $F_\eta(l_i)=(F_\eta(l_{i1}),F_\eta(l_{i2}),\cdots,F_\eta(l_{id}))$ 中是否有 $F_\eta(f)$，如果没有则直接忽略该 PoI 记录；否则进行查询范围判断，即查询位置 (x,y) 和 PoI 记录所在位置 (x_i,y_i) 之间的距离是否小于查询范围 r，将满足条件的 PoI 记录 $\mathrm{AEnc}((x_i,y_i),l_i)$ 添加到结果集合 D 中。

查询范围判断在 RSU 和 LBSP 之间执行，首先说明 2 个利用同态加密的两方安全计算协议：距离计算协议和安全比较协议。协议流程如图 2 和图 3 所示。

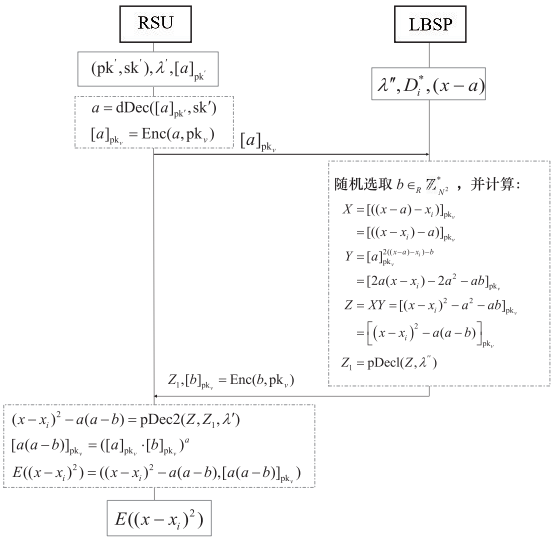

图 2　距离计算协议

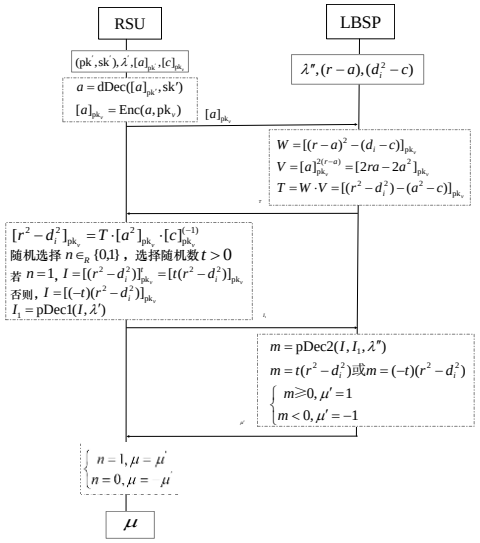

图 3　安全比较协议

1) 距离计算协议：该协议能得到$E((x-x_i)^2)$，RSU持有$((\mathrm{pk}',\mathrm{sk}'),\lambda',[a]_{\mathrm{pk}'})$，LBSP持有$(\lambda'',D_i^*,(x-a))$。协议的步骤如下。

步骤1：RSU用私钥sk'解密$[a]_{\mathrm{pk}'}$得$a=\mathrm{dDec}([a]_{\mathrm{pk}'},\mathrm{sk}')$，再用公钥$\mathrm{pk}_v$加密$a$得$[a]_{\mathrm{pk}_v}=\mathrm{Enc}(a,\mathrm{pk}_v)$，将$[a]_{\mathrm{pk}_v}$发送给LBSP。

步骤2：LBSP随机选取随机数$b\in_R\mathbb{Z}_{N^2}^*$，计算$X=[((x-a)-x_i)]_{\mathrm{pk}_v}=[((x-x_i)-a)]_{\mathrm{pk}_v}$、$Y=[a]_{\mathrm{pk}_v}^{2((x-a)-x_i)-b}=[2a(x-x_i)-2a^2-ab]_{\mathrm{pk}_v}$、$Z=XY=[(x-x_i)^2-a(a-b)]_{\mathrm{pk}_v}$、$Z_1=\mathrm{pDec1}(Z,\lambda'')$。之后LBSP将$Z_1$和$[b]_{\mathrm{pk}_v}=\mathrm{Enc}(b,\mathrm{pk}_v)$发送给RSU。

步骤3：RSU收到Z_1和$[b]_{\mathrm{pk}_v}=\mathrm{Enc}(b,\mathrm{pk}_v)$后，进行第二步解密得$(x-x_i)^2-a(a-b)=\mathrm{pDec2}(Z,Z_1,\lambda')$，计算$[a(a-b)]_{\mathrm{pk}_v}=([a]_{\mathrm{pk}_v}\cdot[b]_{\mathrm{pk}_v})^a$，最终RSU可以得到$E((x-x_i)^2)=((x-x_i)^2-a(a-b),[a(a-b)]_{\mathrm{pk}_v})$。

同理可得$E((y-y_i)^2)=((y-y_i)^2-a(a-b),[a(a-b)]_{\mathrm{pk}_v})$，得$(x,y)$和$(x_i,y_i)$之间距离平方的密文为$E(d^2)=(d^2-c,[c]_{\mathrm{pk}_v})$，其中$d^2=(x-x_i)^2+(y-y_i)^2$，$c=2a(a-b)$，$[2a(s-b)]_{\mathrm{pk}_v}=[a(a-b)]_{\mathrm{pk}_v}^2$。

2) 安全比较协议：给定2个密文$E(d^2)=(d^2-c,[c]_{\mathrm{pk}_v})$和$E(r)=(r-a,[a]_{\mathrm{pk}'})$，该协议在不解密密文的情况下比较明文距离的平方$d^2$和查询范围$r$的大小。RSU持有$((\mathrm{pk}',\mathrm{sk}'),\lambda',[a]_{\mathrm{pk}'},[c]_{\mathrm{pk}_v})$，LBSP持有$(\lambda'',(r-a),(d_i^2-c))$。协议的步骤如下。

步骤1：RSU用私钥sk'解密$[a]_{\mathrm{pk}'}$得$a=\mathrm{dDec}([a]_{\mathrm{pk}'},\mathrm{sk}')$，再用公钥$\mathrm{pk}_v$加密$a$得$[a]_{\mathrm{pk}_v}=\mathrm{Enc}(a,\mathrm{pk}_v)$，将$[a]_{\mathrm{pk}_v}$发送给LBSP。

步骤2：收到$[a]_{\mathrm{pk}_v}$后，LBSP计算$W=[(r-a)^2-(d_i^2-c)]_{\mathrm{pk}_v}$、$V=[a]_{\mathrm{pk}_v}^{2(r-a)}=[2ra-2a^2]_{\mathrm{pk}_v}$、$T=WV=[(r^2-d_i^2)-(a^2-c)]_{\mathrm{pk}_v}$，LBSP将$T$发送给RSU。

步骤3：RSU收到T后，计算$[r^2-d_i^2]_{\mathrm{pk}_v}=T\cdot[a^2]_{\mathrm{pk}_v}\cdot[c]_{\mathrm{pk}_v}^{(-1)}$。随机选择$n\in_R\{0,1\}$，$t>0$。当$n=1$时，令$I=[(r^2-d_i^2)]_{\mathrm{pk}_v}^t=[t(r^2-d_i^2)]_{\mathrm{pk}_v}$；否则$I=[(-t)(r^2-d_i^2)]_{\mathrm{pk}_v}$。使用$\lambda'$进行第一步解密得到$I_1=\mathrm{pDecl}(I,\lambda')$，再将$I_1$发送给LBSP。

步骤4：LBSP收到I_1后，利用λ''进行第二步解密得$m=\mathrm{pDec2}(I,I_1,\lambda'')$，其中$m=t(r^2-d_i^2)$或$m=(-t)(r^2-d_i^2)$。当$m\geqslant 0$时，令$\mu'=1$；当$m<0$时，令$\mu'=-1$。将$\mu'$发送给RSU。

步骤5：RSU收到μ'后，根据n的选值进行第二次判断。当$n=1$时，令$\mu=\mu'$；否则$\mu=-\mu'$。最后输出μ，若$\mu=1$，$r^2\geqslant d_i^2$；若$\mu=-1$则$r^2<d_i^2$。

根据距离计算协议计算出查询位置(x,y)和PoI记录所在位置(x_i,y_i)之间的距离平方的密文$E(d^2)=(d^2-c,[c]_{\mathrm{pk}_v})$后，再根据安全比较协议判断$d^2$和$r$的大小，当$\mu=1$时满足查询范围条件。最终结果集合$D=\{\mathrm{AEnc}((x_i,y_i),l_i)\}$满足$\mathrm{AEnc}((x_i,y_i),l_i)\in D^*$、$F_\eta(f)\in(F_\eta(l_{i1}),F_\eta(l_{i2}),\cdots,F_\eta(l_{id}))$和$\left(x-x_i\right)^2+\left(y-y_i\right)^2<r^2$。RSU将$D=\{\mathrm{AEnc}((x_i,y_i),l_i)\}$和相应的加密距离$E(d_i^2)=(d_i^2-c,[c]_{\mathrm{pk}_v})$返回给查询车辆。

4.5 结果解密

车辆收到加密后的查询结果$D=\{\mathrm{AEnc}(x_i,y_i),l_i\}$和相应的加密距离$E(d_i^2)=(d_i^2-c,[c]_{\mathrm{pk}_v})$后，使用会话密钥$k$解密得$((x_i,y_i),l_i)=ADec(D)$，使用同态加密私钥$\mathrm{sk}_v$解密得$c=\mathrm{dDec}_{\mathrm{sk}_v}([c]_{\mathrm{pk}_v})$，最终求得$d_i^2$。本文协议流程如图4所示。

5 安全分析

5.1 基于ROR的形式化证明

Abdalla等[26]提出的ROR模型是可证明安全性分析领域广泛采用的形式化安全模型，敌手A可以在多项式时间t内对目标协议进行攻击。本文协议有3个实体：V_i、RSU_j和LBSP，每类实体都包含若干个实例。$\prod_{V_i}^{s_1}$、$\prod_{\mathrm{RSU}_j}^{s_2}$和$\prod_{\mathrm{LBSP}}^{s_3}$分别表示$V_i$、$\mathrm{RSU}_j$和LBSP的第$s_1$、$s_2$和$s_3$个实例，敌手$A$可以进行以下查询。

1) Execute（$\prod_{V_i}^{s_1},\prod_{\mathrm{RSU}_j}^{s_2},\prod_{\mathrm{LBSP}}^{s_3}$）。执行该查询，$A$进行窃听模拟攻击，获得实体间交换的所有信息。

2) Send（$\prod_X^s,m$）。执行该查询，A模拟主动攻

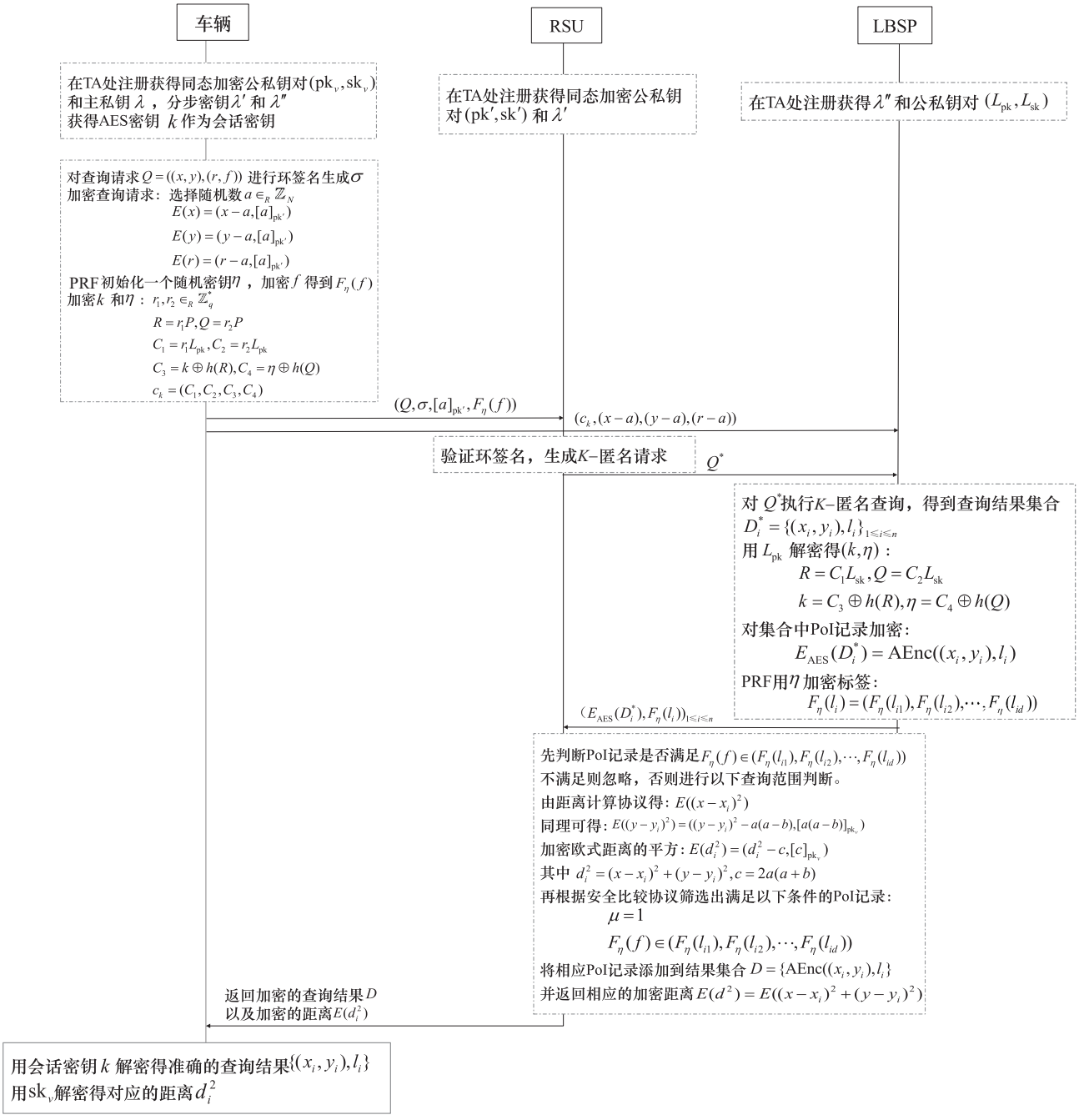

图 4　本文协议流程

击，向指定实体$\prod_X^{s}$发送伪造消息m，并接收反馈响应。

3) CorruptV（$\prod_{V_i}^{s_1}$）。执行该查询，A能获取存储在V_i中所有的秘密信息。

4) CorruptRSU（$\prod_{RSU_j}^{s_2}$）。执行该查询，A能获取存储在RSU_j中所有的秘密信息。

5) CorruptLBSP（$\prod_{LBSP}^{s_3}$）。执行该查询，A能获取存储在LBSP中所有的秘密信息。

6) Hash（i）。本文协议使用的哈希函数均被建模为随机预言机，A模拟哈希函数的查询行为验证是否存在哈希冲突，避免碰撞影响安全性。

7) Homomorphic Encrypt($\prod_X^{s}$)。执行该查询，A向指定实体$\prod_X^{s}$提交明文或密文，获取同态加密结果或密文运算结果，以测试同态加密的语义安全。

8) Test（$\prod_X^{s}$）。该查询是模拟实体间会话密钥

语义安全的模型，模拟器随机生成一个比特B，输出结果对A保密。A执行该查询，若B=1，则返回真实会话密钥；若B=0，则返回与会话密钥等长的随机数。

定理1 设A为本文协议的多项式时间敌手，其运行时间上限为t，若A无法以不可忽略的优势对本文协议发起有效攻击，则判定本文协议是安全的。假设A破坏本文协议查询内容机密性的优势为

$$\mathrm{Adv}_A^P \leqslant \frac{q_h^2}{2^{l_h}} + \frac{q_s^2}{2^{l_s-1}} + \frac{2(q_e+q_{\mathrm{he}})^2}{N} + \frac{q_c}{2^{|D|-1}} \quad (5)$$

其中，q_h、q_s、q_e、q_{he}和q_c分别表示执行Hash查询、Send查询、Execute查询、Homomorphic Encrypt查询和Corrupt查询的次数，N表示随机数的空间范围，l_h表示哈希函数的输出长度，l_s表示环签名的输出长度，$|D|$表示密码字典的空间范围。

证明 下面定义了5个游戏$\mathrm{GM}_i(i\in[0,4])$来证明本文协议的安全性，$\Pr[\mathrm{Succ}_i]$表示敌手A在游戏GM_i中获胜的概率。

1) GM_0。该游戏模拟A对本文协议P的实际攻击，包含所有查询。$\Pr[\mathrm{Succ}_0]$表示A猜对比特B的概率，A破坏协议P的优势为

$$\mathrm{Adv}_A^P \leqslant |2\Pr[\mathrm{Succ}_0]-1| \quad (6)$$

2) GM_1。在GM_1中，将哈希函数严格建模为随机预言机，通过Hash查询模拟查询内容加密和密钥派生阶段的哈希碰撞，本文协议的密文加密和密钥派生采用了哈希函数，根据生日悖论，哈希碰撞的概率为$\frac{q_h^2}{2^{l_h+1}}$，移除哈希碰撞风险后的概率差为

$$|\Pr[\mathrm{Succ}_0]-\Pr[\mathrm{Succ}_1]| \leqslant \frac{q_h^2}{2^{l_h+1}} \quad (7)$$

3) GM_2。在GM_2中，A通过Send查询向RSU发送伪造的环签名，试图冒充合法车辆提交恶意查询。q_s次尝试中，伪造出符合验证规则的合法签名的概率上界为$\frac{q_s^2}{2^{l_s}}$，移除环签名伪造风险后的概率差为

$$|\Pr[\mathrm{Succ}_1]-\Pr[\mathrm{Succ}_2]| \leqslant \frac{q_s^2}{2^{l_s}} \quad (8)$$

4) GM_3。在GM_3中，A执行Execute查询和Homomorphic Encrypt查询，模拟查询阶段的随机数碰撞，q_e+q_{he}次查询的随机数碰撞概率上界为$\frac{(q_e+q_{\mathrm{he}})^2}{N}$。协议采用随机数混淆位置，移除这一风险后的概率差为

$$|\Pr[\mathrm{Succ}_2]-\Pr[\mathrm{Succ}_3]| \leqslant \frac{(q_e+q_{\mathrm{he}})^2}{N} \quad (9)$$

5) GM_4。在GM_4中，A执行CorruptV、CorruptRSU和CorruptLBSP查询，A可分别得到目标实体的秘密参数，本文协议不同实体的秘密参数是独立生成且通过同态加密、哈希函数、随机偏移等方式，让秘密参数不会以明文形式暴露。将Corrupt查询返回的真实秘密参数替换为等长的随机串，敌手无法直接获取有效密钥，消除了Corrupt查询给敌手带来的额外攻击优势，可得

$$|\Pr[\mathrm{Succ}_3]-\Pr[\mathrm{Succ}_4]| \leqslant \frac{q_c}{2^{|D|}} \quad (10)$$

在所有核心隐私信息均被隐藏后，A无法获取有效信息，只能随机猜测比特B，因此

$$\Pr[\mathrm{Succ}_4] = \frac{1}{2} \quad (11)$$

根据式(6)~式(11)可得

$$\frac{1}{2}Adv_A^P = |\Pr[\mathrm{Succ}_0]-\frac{1}{2}| = |\Pr[\mathrm{Succ}_0]-\Pr[\mathrm{Succ}_4]| \leqslant \frac{q_h^2}{2^{l_h+1}} + \frac{q_s^2}{2^{l_s}} + \frac{(q_e+q_{\mathrm{he}})^2}{N} + \frac{q_c}{2^{|D|}} \quad (12)$$

进一步推导可知，敌手A获胜的优势为

$$\mathrm{Adv}_A^P \leqslant \frac{q_h^2}{2^{l_h}} + \frac{q_s^2}{2^{l_s-1}} + \frac{2(q_e+q_{\mathrm{he}})^2}{N} + \frac{q_c}{2^{|D|-1}} \quad (13)$$

证毕。

5.2 基于ProVerif的安全证明

ProVerif是一种基于Dolev-Yao模型[25]的自动化分析工具，用于验证密码协议的安全性。假设攻击者具备Dolev-Yao攻击能力，即能够完全控制通信信道，任意截获、篡改、重放和伪造消息，但无法破解安全的密码原语。本节主要对利用同态加密的两方安全计算协议进行建模并得到形式化的验证结果。

建模：设定2个基于同态加密的实体：RSU和LBSP，本文协议目标是通过同态加密确保RSU和LBSP在没有泄露私密信息的前提下通过密文共同

计算一个结果，此次形式化验证主要针对距离计算协议。设定查询车辆有私密查询信息x和a，LBSP有私密PoI信息x_i。定义了加解密函数，其中解密包括直接解密和分步解密。在LBSP对Z完成第一步解密得到Z_1后触发LBSP_step1事件，在RSU对Z_1进行第二步解密得到$(x-x_i)^2-a(a-b)$后触发rsu_decrypt事件。

安全性要求：通过指令query attacker<变量>来检查攻击者是否能获取到某个变量；通过指令query event<事件1> ==> event<事件2>来证明若事件1发生，则事件2也必须发生的逻辑关系。图5为两方安全计算ProVerif的验证结果，攻击者无法根据两方安全计算的过程推测出私密信息x和a，也无法推测出LBSP的私密PoI信息x_i。保护了车辆的查询信息隐私和LBSP的PoI信息隐私。并且RSU要想解密获得$(x-x_i)^2-a(a-b)$，也必须先由LBSP进行第一步解密获得Z_1，RSU无法伪造。说明RSU和LBSP都不能单独对最后的$[a(a-b)]_{\mathrm{pk}_v}$解密，除了查询车辆都无法解密最后的计算结果，实现了查询结果的隐私保护。

```
------------------------------------------------------------
Verification summary:

Query not attacker(x[]) is true.

Query not attacker(xi[]) is true.

Query not attacker(a[]) is true.

Query event(rsu_decrypt(Ex_xi[])) ==> event(LBSP_step1(Z1[])) is true.

------------------------------------------------------------
```

图5　两方安全计算ProVerif的验证结果

5.3　基于Scyther的安全证明

为进一步验证本文协议在实际执行过程中的抗攻击能力，本文使用协议验证工具Scyther进行了仿真验证。Scyther同样基于Dolev-Yao攻击模型，能够自动搜索在有限轮数内的所有可能攻击路径，并检查协议是否满足弱同步性、强同步性、存活性、协商一致性等安全属性。指定车辆V、RSU、LBSP作为协议安全验证的角色，设置高级选项运行本文协议100次，以便为每个请求查找潜在攻击的多种模式。Scyther运行结果如图6所示，结果表明未能找到任何有效攻击路径。表明本文协议可以有效抵御中间人攻击、重放攻击、会话劫持、身份伪造、会话不同步攻击等威胁，进一步增强了协议的安全性与可信度。

Scyther results : verify

Claim				Status		Commen
BlindFilter	V	BlindFilter,wagree	Weakagree	Ok	Verified	No attacks.
		BlindFilter,Valive	Alive	Ok	Verified	No attacks.
		BlindFilter,Vagree	Niagree	Ok	Verified	No attacks.
		BlindFilter,Vsync	Nisynch	Ok	Verified	No attacks.
	LBSP	BlindFilter,LBSP1	Weakagree	Ok	Verified	No attacks.
		BlindFilter,LBSP2	Alive	Ok	Verified	No attacks.
		BlindFilter,LBSP3	Niagree	Ok	Verified	No attacks.
		BlindFilter,LBSP4	Nisynch	Ok	Verified	No attacks.
	RSU	BlindFilter,RSU1	Weakagree	Ok	Verified	No attacks.
		BlindFilter,Ralive	Alive	Ok	Verified	No attacks.
		BlindFilter,Ragree	Niagree	Ok	Verified	No attacks.
		BlindFilter,Rsync	Nisynch	Ok	Verified	No attacks.

Done.

图6　Scyther运行结果

5.4　非形式化安全证明

1) 在LBS查询过程中，RSU无法知道车辆的查询内容、查询位置、最终查询结果以及LBSP的PoI数据集等有效信息。当RSU收到车辆的查询请求和环签名时，由于环签名机制具有匿名性，确保了RSU无法将查询消息与具体车辆身份关联，从而保护了查询内容和位置的隐私。虽然RSU可以访问加密数据$F_\eta(f)$、$E(x-x_i)^2$（其中$F_\eta(f)$是由车辆用密钥η通过PRF加密的查询条件，$E(x-x_i)^2$是由pk_v加密的查询结果），但由于RSU不持有密钥η，因此无法获取查询条件。同时，RSU只有部分私钥λ'，无法单独解密$E(x-x_i)^2$，所以无法获得最终的查询结果。在盲过滤阶段，LBSP向RSU发送的是$\mathrm{AEnc}((x_i,y_i),l_i)_{1\leqslant i\leqslant n}$，每个PoI记录都经过AES对称加密，由于RSU没有会话密钥k，因此即使拦截到这些记录，也无法解密并获取PoI数据集的具体内容。

2)在LBS查询过程中，LBSP无法知道车辆任何有价值的信息，包括查询内容、位置和结果。RSU向LBSP发送的是经过K–匿名化处理的查询请求Q^*，确保了LBSP无法从Q^*中识别出具体查询车辆的查询内容和位置信息。在盲过滤阶段，LBSP与RSU通过两方安全计算协作处理加密数据。LBSP同样不能单独对pk_v加密的结果进行解密，因此也无法得知最终的查询结果。

6　性能分析

本节从安全特性、计算开销和通信开销3个方面对协议进行性能分析，将本文协议与文献[3]和

文献[16-17]进行比较，以分析其有效性和实用性。

6.1 安全特性

将本文协议与对比协议的安全特性进行对比，对比结果如表 2 所示，表中√表示具有此功能，×表示不具备该功能。文献[3]采用 2 个云服务器，基于同态加密实现两方安全计算来进行 LBS 查询。该协议能返回准确的查询结果，并能实现查询位置、内容和查询结果的隐私保护。但该协议在 LBSP 端需要使用同态加密对整个 PoI 数据集进行加密，计算量巨大，并且该协议仅支持按距离查找，无法实现具体类型的 PoI 查询。文献[16-17]均采用盲过滤方法，利用同态加密过滤 K−匿名查询产生的冗余 PoI 信息，但文献[16]中，RSU 知道车辆的查询位置，并且同样无法支持具体的 PoI 类型查询。文献[17]无法得到准确的查询距离，只能得到 PoI 的坐标信息。

表 2 安全特性对比

协议	位置隐私	查询内容隐私	查询结果隐私	PoI 数据集隐私	准确的查询结果	PoI 类型查询
文献[3]	√	√	√	√	√	×
文献[16]	×	√	√	√	√	×
文献[17]	√	√	√	√	×	√
本文协议	√	√	√	√	√	√

6.2 计算开销

设置安全级别为 80 位，$\bar{p}$、p、q 是 3 个大素数。选择对称双线性配对 $\tilde{e}:G_1 \times G_1 \rightarrow G_2$，$G_1$ 是椭圆曲线 $\bar{E} \equiv (x^3 + x) \bmod \bar{p}$ 上点 $\bar{p}$ 生成的阶为 q 的加法群，其中 $\bar{p}$=512 bit，q=160 bit。选择加法循环群为 G 的 q 阶椭圆曲线 $E:y^2 \equiv x^3 + ax + b \bmod p$，其中 p=160 bit。

利用上述设置，基于 Linux 操作系统 Ubuntu2 0.04.6LTS，搭载 Intel(R) Core(TM) i5-8265U CPU @ 1.60 GHz 处理器和 8.0 GB 内存的计算平台，采用 MIRACL 密码库对相关加密操作进行运算。进行了 10 000 次测试，并计算了它们的平均值来确定执行时间。加密操作中异或运算处理时间可忽略不计。加密操作符号定义及平均执行时间如表 3 所示。

表 3 加密操作执行时间

运算操作	定义	执行时间/ms
T_{EX}	幂运算	4.400 0
T_{AES}	AES 加密/解密	0.056 5
T_{BP}	双线性映射	4.211 0
$T_{PM\text{-}BP}$	双线性映射点乘运算	1.709 2
$T_{PM\text{-}ECC}$	椭圆曲线点乘运算	0.050 0
$T_{PA\text{-}ECC}$	椭圆曲线点加运算	0.001 4

设定环上用户数 N 为 100[14]，设满足车辆查询要求的 PoI 信息有 x 条，满足 K−匿名查询的 PoI 信息有 n 条。本文协议车辆端需要的计算开销约为 $(N-1)T_{PA\text{-}ECC}+(2N+3)T_{PM\text{-}ECC}+xT_{AES}+xT_{EX} \approx 10.288\ 6+5.565x$ ms，盲过滤计算开销约为 $11nT_{EX} \approx 4.84n$ s。本文协议与其他协议的计算开销对比如表 4 所示。

将 x 和 n 分别设置为 1,2,…,5 和 50,100,150,…,1 000，得到如图 7 和图 8 所示的计算开销对比。由图 7 可知，文献[3]在车辆端完全依赖同态加密实现隐私保护，因此计算开销始终最高；文献[16-17]车辆端计算开销较为稳定，本文协议在 $n \leqslant 3$ 时计算开销最低，n=4、5 时计算开销略高于文献[16-17]。但文献[16-17]只能返回符合要求的 PoI 信息，无法在盲过滤阶段计算车辆位置与目标 PoI 的距离，车辆端也无法获取该距离值。本文协议和文献[3]能在车辆端同态解密得到距离值，因此随着 n 的增加，车辆端解密数量的增加计算开销也会增加，但在车联网 LBS 场景中，一般符合查询要求的 PoI 个数仅在个位数范围内。因此，本文协议在实际应用中额外引入的解密计算开销是可接受的，整体性能仍能保持较优水平。如图 8 所示，在盲过滤阶段，本文协

表 4 计算开销对比

协议	车辆端	盲过滤
文献[3]	$(4+2x)T_{EX}$	—
文献[16]	$5T_{BP}+(1+x)T_{AES}+2T_{PM\text{-}BP}$	$15nT_{EX}+nT_{AES}$
文献[17]	$6T_{BP}+(3+x)T_{AES}$	$9nT_{EX}+3nT_{BP}+nT_{AES}$
本文协议	$(N-1)T_{PA\text{-}ECC}+(2N+3)T_{PM\text{-}ECC}+xT_{AES}+xT_{EX}$	$11nT_{EX}$

议在计算开销方面始终优于对比协议，表现出最低的计算负担。

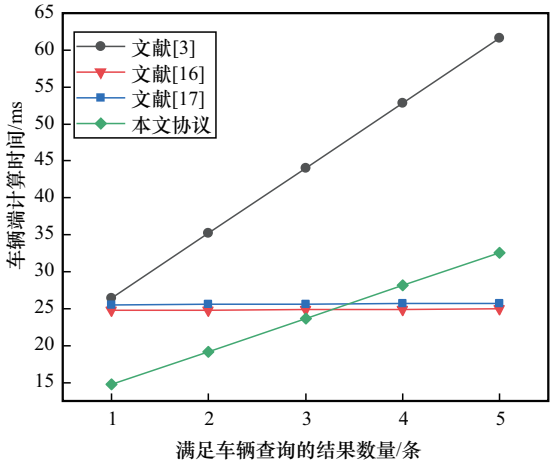

图 7　车辆端计算时间

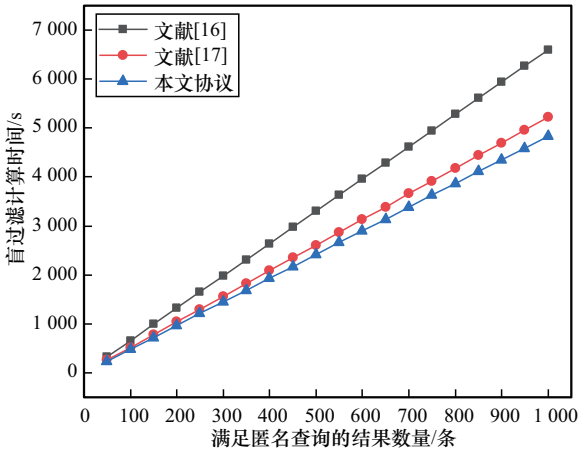

图 8　盲过滤计算时间

6.3　通信开销

根据实验配置计算本文协议和对比协议的通信开销，各协议的通信开销对比如表 5 所示。密文长度是影响通信性能的主要原因。根据设置，$\bar{p}$ 和 p 分别为64 B和20 B，G_1、G_2中的元素为64×2=128 B，G 中元素为20×2=40 B。Z_q^* 中元素、AES 密文 C_{AES} 分别为20 B、16 B。

表 5　　通信开销对比

协议	通信开销
文献[3]	$7n\lvert Z_q^*\rvert$
文献[16]	$\lvert G\rvert + 3\lvert G_2\rvert + (n+2)\lvert Z_q^*\rvert + n\lvert C_{\mathrm{AES}}\rvert$
文献[17]	$4\lvert G_1\rvert + (n+3)\lvert Z_q^*\rvert + n\lvert C_{\mathrm{AES}}\rvert$
本文协议	$2\lvert G\rvert + (n+2)\lvert Z_q^*\rvert + n\lvert C_{\mathrm{AES}}\rvert$

由图 9 可知，本文协议随着满足匿名查询的 PoI 数量增加，各协议的通信开销均呈线性增长，文献[3]通信开销始终远高于其他协议。文献[16-17]在整体增长趋势上较为接近，但其通信量仍明显高于本文协议。相比之下，本文协议能以较低的通信开销实现更多的隐私保护要求，体现出更好的通信性能和可扩展性。

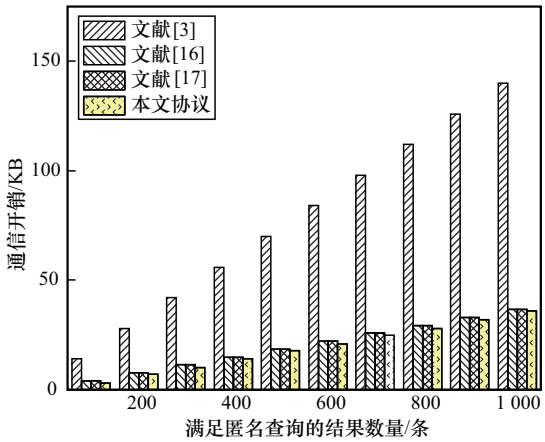

图 9　通信开销对比

7　结束语

本文针对车联网环境下 LBS 查询隐私保护以及通信与计算开销优化的问题，提出了一种基于同态加密的 PoI 查询隐私保护协议。本文协议融合 K–匿名、伪随机函数、环签名及同态加密技术，实现了车辆查询身份、位置和内容的隐私保护，并同时实现了 LBSP 端数据的隐私保护。RSU 与 LBSP 作为半可信方，通过双密钥同态加密实现盲过滤功能，有效过滤查询冗余数据，减少查询车辆的通信与计算负担。通过 ROR 模型和 ProVerif、Scyther2 种形式化验证工具，证明了协议在身份、位置与内容隐私保护方面的安全性。实验结果表明，本文协议在计算与通信开销上均优于现有协议，能够在保证隐私保护的同时显著降低系统成本。

参考文献：

[1] LI Y F, WANG B, LIU Q, et al. LPPS-IKHC: location privacy-preserving scheme using improved k-anonymity and hybrid cache for IoV[J]. IEEE Transactions on Vehicular Technology, 2025, 74(8): 12864-12878.

[2] ZHANG S W, HU B, LIANG W, et al. A caching-based dual K-anonymous location privacy-preserving scheme for edge computing[J]. IEEE Internet of Things Journal, 2023, 10(11): 9768-9781.

[3] QI J Q, JIA X Y, LUO M, et al. A privacy-aware K-nearest neighbor query scheme for location-based services[J]. IEEE Internet of Things Journal, 2024, 11(6): 10831-10842.

[4] ZHOU J, CAO Z F, QIN Z, et al. LPPA: lightweight privacy-preserving authentication from efficient multi-key secure outsourced computation for location-based services in VANETs[J]. 2020, 15: 420-434.

[5] LI S C, ZHAO S S, MIN G Y, et al. Lightweight privacy-preserving scheme using homomorphic encryption in industrial Internet of Things[J]. IEEE Internet of Things Journal, 2022, 9(16): 14542-14550.

[6] KANG J W, YU R, HUANG X M, et al. Location privacy attacks and defenses in cloud-enabled Internet of vehicles[J]. IEEE Wireless Communications, 2016, 23(5): 52-59.

[7] KHAZBAK Y, FAN J Y, ZHU S C, et al. Preserving location privacy in ride-hailing service[C]//Proceedings of the 2018 IEEE Conference on Communications and Network Security (CNS). Piscataway: IEEE Press, 2018: 1-9.

[8] GUPTA R, RAO U P. Achieving location privacy through CAST in location based services[J]. Journal of Communications and Networks, 2017, 19(3): 239-249.

[9] CABALLERO-GIL C, MOLINA-GIL J, HERNÁNDEZ-SERRANO J, et al. Providing *k*-anonymity and revocation in ubiquitous VANETs[J]. Ad Hoc Networks, 2016, 36: 482-494.

[10] 梁慧超, 王斌, 崔宁宁, 等. 路网环境下兴趣点查询的隐私保护方法[J]. 软件学报, 2018, 29(3): 703-720.
LIANG H C, WANG B, CUI N N, et al. Privacy preserving method for point-of-interest query on road network[J]. Journal of Software, 2018, 29(3): 703-720.

[11] GUO N, MA L Y, GAO T H. Independent mix zone for location privacy in vehicular networks[J]. IEEE Access, 2018, 6: 16842-16850.

[12] KHODAEI M, PAPADIMITRATOS P. Cooperative location privacy in vehicular networks: why simple mix zones are not enough[J]. IEEE Internet of Things Journal, 2021, 8(10): 7985-8004.

[13] HU L, QIAN Y F, CHEN M, et al. Proactive cache-based location privacy preserving for vehicle networks[J]. 2018, 25(6): 77-83.

[14] YADAV V K, ANDOLA N, VERMA S, et al. Anonymous and linkable location-based services[J]. IEEE Transactions on Vehicular Technology, 2022, 71(9): 9397-9409.

[15] WANG Y W, LI X H, ZHANG X H, et al. ARPLR: an all-round and highly privacy-preserving location-based routing scheme for VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(9): 16558-16575.

[16] CHEN J, HE K, YUAN Q, et al. Blind filtering at third parties: an efficient privacy-preserving framework for location-based services[J]. 2018, 17(11): 2524-2535.

[17] LI X X, ZHU Y W, WANG J. Highly efficient privacy preserving location-based services with enhanced one-round blind filter[J]. IEEE Transactions on Emerging Topics in Computing, 2021, 9(4): 1803-1814.

[18] DWORK C. Differential privacy: a survey of results[C]//Theory and Applications of Models of Computation. Berlin: Springer, 2008: 1-19.

[19] DU X X, ZHU H, ZHENG Y D, et al. A semantic-preserving scheme to trajectory synthesis using differential privacy[J]. IEEE Internet of Things Journal, 2023, 10(15): 13784-13797.

[20] ELKHODR M, SHAHRESTANI S, CHEUNG H. A semantic obfuscation technique for the Internet of Things[C]//Proceedings of the 2014 IEEE International Conference on Communications Workshops (ICC). Piscataway: IEEE Press, 2014: 448-453.

[21] ZHAO P, ZHANG G L, WAN S H, et al. A survey of local differential privacy for securing Internet of vehicles[J]. The Journal of Supercomputing, 2020, 76(11): 8391-8412.

[22] JIANG H L, PEI J, YU D X, et al. Applications of differential privacy in social network analysis: a survey[J]. IEEE Transactions on Knowledge and Data Engineering, 2023, 35(1): 108-127.

[23] GUPTA R, RAO U P. An exploration to location based service and its privacy preserving techniques: a survey[J]. Wireless Personal Communications, 2017, 96(2): 1973-2007.

[24] LIU X M, DENG R H, CHOO K R, et al. An efficient privacy-preserving outsourced calculation toolkit with multiple keys[J]. 2016, 11(11): 2401-2414.

[25] DOLEV D, YAO A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2): 198-208.

[26] ABDALLA M, FOUQUE P A, POINTCHEVAL D. Password-based authenticated key exchange in the three-party setting[J]. IEE Proceedings-Information Security, 2006, 153(1): 27-39.

[作者简介]

范馨月（1979– ），女，四川犍为人，重庆邮电大学副教授、硕士生导师，主要研究方向为信息安全、通信信号处理、图像视频处理等。

周美贤（2000– ），女，重庆人，重庆邮电大学硕士生，主要研究方向为车联网安全、认证协议等。