北京航空航天大學

BEIHANG UNIVERSITY

基于零知识证明的位置隐私保护方案

摘要

近年来，移动端用户数量迅猛增长，对基于手机定位的位置服务需求也不断增加。位置服务的广泛使用虽然让生活更加便利，但也带来了用户位置隐私泄露的安全问题。泄露的位置隐私不仅会保护用户具体位置，更可能会间接暴露用户的行为习惯、具体身份、社交信息等敏感信息，甚至影响到用户的实际生活。在当前网络环境中，用户对位置隐私的保护意识不足或缺少有效保护手段，并且手机应用软件对用户位置信息的滥用现象屡禁不止；随着大数据、深度学习等分析技术的发展，保护位置隐私的难度也随之增大，位置隐私保护方法急需进步与革新。

本作品立足于用户个体的位置隐私保护，提出了一种全新的位置范围定位技术。利用零知识范围证明技术，在隐藏个人位置的前提下，向服务方证明用户处于一定精度的空间范围内，从而使服务方不再需要用户的具体位置而能够提供一些范围性的服务。由于证明技术的零知识特性，服务方无法通过证明过程和结果来获取用户的具体位置，从而将用户位置与服务方隔绝，有效保护了用户的位置隐私。本作品所用技术被证明是后量子安全的，具有高安全性。

本作品的零知识证明技术还能简化用户范围模糊的过程，利用所设计协议的高效性平衡了安全性与便利性，贴合现实位置服务的频繁与突发等特点。在具体通信复杂度、具体证明复杂度和具体验证复杂度三项主要指标上，本文零知识范围证明均有不错的表现。在数据量较大时，本作品设计的零知识证明大小将优于网络安全和系统安全旗舰会议 ACM CCS 2020 中 Lyubashevsky 等人的基于格的零知识证明方案。在批处理设置实验中，本作评设计的零知识证明大小远远优于公钥密码学顶级会议 EUROCRYPT 2021 中 Couteau 等人的零知识证明方案，同数据规模下空间占用率减小约 90 %。

本作品将有助于解决位置服务现有痛点，重塑“互联网 + 位置隐私保护”的服务理念和完善服务质量。随着市场规模日益增长，应用前景非常广阔。

关键词：位置隐私保护，零知识范围证明，向量内积论证，交互式谕示证明

Abstract

In recent years, the number of mobile users has grown rapidly, with the increasing demand for location services based on GPS location . Although the widespread use of location services makes life more convenient, it also brings the security problem of user location privacy leakage. For malicious attackers, the leaked location privacy may indirectly lead to the disclosure of sensitive information such as users' behavior habits, specific identities, and social information, which in turn affects the actual life of users. In the current network environment, first of all, users have insufficient awareness of location privacy protection or lack of effective protection means. Secondly, there are many abuse of location services in the use of software such as apps. And finally, with the development of big data, artificial intelligence and other technologies, the difficulty of protecting location privacy has also increased. A new location privacy technology is needed to solve these problems.

Based on the privacy protection of personal location, this work proposes a new range positioning technology. Using zero-knowledge range proof technology, under the premise of hiding personal location, it proves to the service that the user is within a certain accuracy of the space, allowing the service party no longer needs the user's specific location and can provide some range services. Due to the zero-knowledge nature of the proof technology, the service provider cannot obtain the specific location of the user through the proof process and result, thereby isolating the user's location from the service party and effectively protecting the user's location privacy. At the same time, because the zero-knowledge range proof in the work is post-quantum safe, the new range positioning technology has high security, which can effectively resist quantum computing-level attacks and greatly reduces the possibility of malicious attackers cracking the range proof system.

The core technology of this work lies in the efficiency of zero-knowledge protocols. In order to fit the frequency of real-world location services, a more efficient inner product argument and range proof protocol in zero-knowledge system is designed. In the three main indicators of specific communication complexity, specific proof complexity and specific verification complexity, the zero-knowledge range proof in this paper has good performance, which is sufficient to meet the actual needs. When the data volume reaches more than 48KB, the proof size of this design will be better than

the lattice-based zero-knowledge proof scheme of Lyubashevsky et al. in ACM CCS 2020, the flagship conference on cybersecurity and system security. Among the 1000 instances in the batch setting, the zero-knowledge range proof size in this paper is far better than the zero-knowledge proof scheme of Couteau et al. in EUROCRYPT 2021, the top conference on public key cryptography, and the space occupancy rate is reduced by about 90% under the same data scale.

This work will help solve the existing pain points of location services, reshape the service concept of ”Internet + location privacy protection” and improve service quality. With the growing market size, the application prospects are very broad.

Keywords: GPS positioning, zero-knowledge range proof,Inner Product Argument, Interactive Oracle Proof

目录

一、作品概述

本章首先介绍基于位置信息隐私保护的研究背景和研究意义，接着介绍国内外相关领域的研究现状，然后引出本文研究的主要内容，最后给出本文各章节的内容安排。

（一）研究背景与研究意义

近年来，移动用户数量迅猛增长，越来越多的用户选择使用移动设备来满足他们的日常活动需求，而不是依靠电脑。[1]在此背景下，基于位置的服务（Location Based Services, LBS）成为了一种趋势。基于位置的服务是指服务提供商根据用户提交的位置信息，返还给用户对应的基于位置信息的相应服务。大多数现代服务系统都会要求用户发送他们的位置信息，以提供更具适应性、符合用户实际需求和偏好的服务，例如关于天气、交通的警报服务或者提供出行的最佳路线。[2]

在用户提交的位置信息中，最常用、便于服务提供商进行处理的位置信息是用户直接的地理位置信息，这也和用户个人隐私安全有着密切关系。但是，当移动应用频繁询问用户所在位置信息时，用户的位置信息面临着暴露的风险，甚至用户的其他隐私也不再安全。比如不可信的服务提供商可以利用用户的位置信息和上传时间，结合大数据分析手段绘制出用户的时间活动轨迹和活动热点图，进一步分析出用户的行为习惯、具体身份、社交信息等敏感隐私。在更极端的情况下，服务提供商还可以分析出用户的隐私画像，对匿名用户进行去匿名化，严重威胁用户隐私安全。

事实上相当多的移动应用都会询问用户的位置信息，这也带来了泄露位置信息、侵犯隐私的隐患。以 Google 应用市场为例，根据 2017 年的统计数据，在最受欢迎的 2800 个移动应用（aplication, 简称 app）中，4 成以上的 app 要求用户提供访问位置信息的权限，其中包括在后台可以直接访问位置的 app,[3]这在当时引起了用户群体一定的抗议。然而遗憾的是，当前大多数服务提供商对位置信息的保护力度远远不够。用户通常只能简单选择“是”或“否”给予服务提供商具体位置，而不能选择被上传的用户位置的精度，也没有对位置数据后续使用情况的追溯权限。服务提供商以使用用户地理位置提供精准服务的名义，将可能侵犯隐私的数据条款隐藏在繁杂的用户条款中，将用户摆在了无法反制的弱势地位上。现行的大多数隐私保护方案都基于通信渠道的安全性和授权，在获取位置信息后，服务提供方并没有对这些敏感信息给予应有的保护,[4]在这样的环境下，如何保护位置信息的隐私安全成为了一个新的问题。

需要注意的是，在保护位置信息隐私安全的同时，我们还应该保证位置信息的真实性以及用户获得的服务质量。如果忽略了位置信息的真实性，那么在一些特殊情景下，用户可能会向系统提供错误的位置信息来达成某些目的。比如攻击者可以向系统发送虚假的位置信息，以寻求系统的漏洞；或者用户可以在发生交通事故肇事逃逸后提交错误的位置信息，以逃避追责[5]。位置隐私系统还需要在安全匿名性与服务质量之间取得平

衡。当前保护位置隐私信息的一种重要方式是模糊用户的实际位置，将用户位置信息隐藏在虚假的位置或者一个模糊的范围中。这样固然对位置隐私起到一定的保护作用，却可能降低用户获得的服务质量，影响用户的服务体验。这两个需求也对现有位置隐私保护方案提出了更高的要求。

而现有的大多数位置隐私保护方案要么在在保护用户位置信息安全上存在漏洞，要么在满足上述两种诉求时系统复杂度和计算开销代价过高。在这样的背景下，如果可以探索出一种新的位置隐私保护方案，这将为保护用户位置信息安全提供极大助力，并进一步促进隐私保护领域相关技术的发展。同时，如果将新的方案技术移植应用到其他领域，那将会为各行业的数据信息安全提供更可靠的保障。

（二）研究现状

随着移动终端数量逐年增加和定位技术的发展，基于位置服务（LBS）被广泛应用在日常生活中。而在用户享受服务的同时，用户的位置信息可能会被服务提供商或攻击者采集进而造成隐私泄露。为了解决用户位置隐私的安全，国内外研究人员对位置信息保护模型进行了广泛的研究，迄今为止已经初步形成了若干成熟的位置隐私保护模型和相关的保护技术。本节将对其中比较成熟、应用比较广泛的位置隐私保护系统结构以及相关技术技术进行介绍。

1. 位置隐私保护系统结构

现行的基于位置的隐私保护系统主要有 3 种结构，分别是集中式结构、分布式结构以及混合式结构。这三种结构各有优缺点，分别适用不同的应用场景。

（1）集中式结构

集中式结构在客户端和服务提供商之间加入位置匿名服务器，帮助用户进行位置匿名处理，并帮助用户从模糊的服务集合中筛选出用户实际需要的服务。[6]引入位置匿名服务器后，移动用户端的计算、存储负担大为减小，一些复杂的算法、功能也有了实现的可能。但是引入第三方服务器也带来了一些问题。一旦服务器受到攻击并泄露信息，或者服务器不再可信，用户的位置隐私将被泄露。

（2）分布式结构

鉴于集中结构位置匿名服务器带来的安全问题和性能瓶颈问题，分布式结构去除了位置匿名服务器，并通过多台移动设备之间的协作来实现位置匿名效果。用户发起查询请求后，多个移动设备相互协作形成一个匿名区域，从而将用户真实的位置信息隐藏在这个区域中。这种结构与集中式结构相比无疑更加安全，但是却也对用户移动设备的计算能力提出了一定的要求。

（3）混合结构

基于集中式结构和分布式结构的优点，混合结构同时使用了两种结构。用户既可以通过位置匿名服务器完成匿名，也可以通过多台移动设备协助来形成一个匿名区域。虽然混合式结构集中了之前两种结构的优点，但是这种结构也存在一定的缺点。在构建和维持混合式系统结构时需要不断设置、调整参数[7]，以决定系统在不同条件下选择哪种方式来完成用户和服务提供商之间的通信，这也束缚了混合结构的进一步发展。

表 1 位置隐私保护系统 3 种结构对比

结构名称	优点	缺点
集中式结构	计算、存储性能提高	有泄露隐私的风险
分布式结构	提高安全性	对移动设备性能要求较高
混合结构	兼具安全性和性能	系统参数限制了应用

2. 位置隐私保护技术

位置隐私保护方法主要从位置数据加密、匿名位置区域和差分隐私等方面考虑，其中匿名位置区域、差分隐私两个方向近年来不断发展，应用前景相对可观，本部分也将着重介绍这两个方向的研究进展。

（1）位置数据加密

位置数据加密方法通过加密算法对位置信息进行加密，从而达到保护位置隐私的效果。如 Zhu 等人基于加密算法提出一个隐私保护框架，将 LBS 外包到云中，并允许用户动态控制精度，从而在服务和隐私之间进行权衡。[8] 但密码学方法有较为统一的缺陷就是计算开销大，如同态加密一类能对加密数据进行处理的算法，具体应用场景下实用性较低。

（2）匿名位置区域

在基于匿名位置区域的位置隐私保护技术中，比较成熟的是 K-匿名技术。Pierangela 等人基于用虚拟用户位置代替真实位置的想法，首次提出 K-匿名隐私保护技术，通过泛化的方式保护数据隐私。[9] 在此基础上，Gruteser 等[10]提出一种假位置数据隐私保护模型，将产生的 K 个虚假位置混淆在用户真实位置中，生成一个模糊范围达到匿名效果 1。K-匿名隐私保护技术和当前分布式系统结构有较高的相容性，使用时也比较灵活，但是其匿名效果依赖于 K 值的选取。K 值太小时匿名效果难以保持，但是当 K 值较大时，系统将会承担很多不必要的计算开销。另外，K-匿名隐私保护技术也依赖于分布式系统结构，用户需要在类似 P2P 网络中与其他用户进行通讯，这增加了潜在安全风险，

并增加了较大通讯与时间开销。

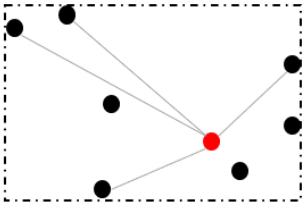

图 1 K-匿名模糊范围

（3）差分隐私

差分隐私技术通过向用户精确位置添加随机噪声，生成一系列模糊位置，从而确定一个模糊范围。其有较强统计学基础作为支撑，具有可靠的安全下限。在 2006 年，Cynthia Dwork 等[11]基于不可区分性运用拉普拉斯分布，首次提出差分隐私。在此基础上，Frank 等[12]提出差分隐私指数机制，并基于各种差分隐私机制将其运用到数据查询、数据挖掘等领域的差分隐私保护。经过众多研究者的迭代研究，Wei 等[13]提出一种基于差分隐私的位置保护方案，将用户准确位置信息拆分成多级网格，通过控制网格粒度控制位置隐私保护的安全性。差分隐私对加扰噪声选取考究，算法、系统整体复杂度较高，生成很多个模糊位置（以确定模糊范围）时计算开销较大，并且容易保留数据统计学特点。

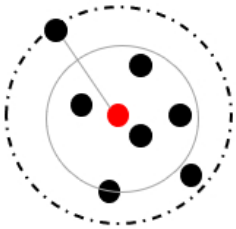

图 2 差分隐私模糊范围

（三）作品概述与创新点说明

现有的位置隐私保护技术主要依靠添加虚假或者无关的位置信息，从而形成一个相对匿名的区域。用户实际位置信息隐藏在这个区域内，服务提供方和攻击者都难以从这个区域中采集用户的位置隐私。考虑到用户还是提交了位置信息，本文希望借鉴现有技术，提供一个用户在不暴露位置的同时获取服务的方法。

注意到区块链中的零知识证明技术具有正确性（证明结果可信）和零知识性（不会暴露关键信息）的优秀性质，并且这两个性质满足了位置隐私保护的需求，本文希望将

零知识证明技术引入位置隐私保护，以改善现有模型。

零知识证明技术源于区块链中的 Zcash 货币应用体系。在用户之间进行交易前，付款的一方（prover）需要向另一方（verifier）证明自己的账户下有充足的余额。而零知识证明技术允许 prover 在证明自己账户余额足以完成交易的同时，保护 prover 自己的账户信息，防止敌手通过暴露的账户信息牟取利益。同时，零知识证明技术保证了 verifier 得到的证明结果是正确的，即 verifier 不会受到 prover 的欺骗。

本文借鉴了区块链中的零知识范围证明技术，对现有位置隐私保护系统进行改进优化，并提供一种在不提交用户位置信息的同时获取服务提供方服务的方法。具体创新成果如下。

1. 隐私保护性

地理位置隐私保护并非一个新领域，现行已经有许多加密技术可以为地理位置信息提供隐私保护服务。与其他传统加密技术一样，零知识证明技术满足了隐私保护的需求。同时，零知识证明还允许用户无需透露自己具体的位置信息，就可以达到提供精准位置的服务效果。这一特性使得零知识证明技术与其他传统加密手段有本质区别，即地理位置信息泄露的源头被切断，用户的隐私信息（地理位置）从未直接或间接（以密文的形式）出现在系统的通信信道中，这大大提高了隐私保护性。

2. 可验证性

除了隐私保护性的大大提高之外，零知识证明范围技术相比与其他位置信息保护技术有着独特的有点————绝对可信的可验证性。使用零知识证明技术，用户的地理位置在完全不暴露的前提下，会对其他用户和服务提供商保持真实性。其他用户和服务提供商可以验证用户提供的范围信息证明的正确性，提高服务交易的可信度。同时，这种信任关系的加强也避免了非法分子由于恶意竞争或者谋取私利等原因，通过服务交易的信任漏洞非法盗取服务提供商的信息，或是对其展开安全攻击的情况。

3. 自主可控性

引入零知识范围证明技术后，保护用户位置隐私不再需要第三方位置匿名服务器的参与，也不需要在多个用户端之间进行协作通信以达到匿名效果。使用零知识证明技术，用户可以自主决定地理位置信息的精确度，以及地理位置认证的过程。一方面，这一改以往被动地进行位置认证过程，提供了自主性；另一方面，这项技术允许用户控制地理位置范围的精度，增强了用户对于位置隐私的可控性。

4. 高效性

我们所提出的零知识范围证明位置隐私保护机制，相比其他现有机制，摆脱了冗长的系统建立与通信过程。本机制只保留必要的通信需求（如发送位置证明与返回服务），减少了用户端与服务端直接的通信量，提高了通信效率。与此同时，在不失安全性的前提下，我们的证明生成过程相比于其他传统加密技术也有着显著的简化特点，这使我们的系统具有更高的承载能力。

（四）论文组织结构

本文共有七章，其中最后一章是本文引用的参考文献具体结构见下图。

第一章是作品概述，主要从本文的研究背景与意义、研究现状和作品概述与创新点说明三部分构成。

第二章是本文需要使用到的定理、算法的一些预备知识，包括安全的随机数生成和零知识范围证明的理论基础内容，后者包括默克尔树、里得·所罗门编码、向量内积论证等 7 个预备知识。

第三章是本文作品设计与实现的过程，包括需求分析、作品系统概述、问题转化和关键技术 4 部分。在分析隐私保护行业需求的基础上，我们设计出具有广阔应用前景的位置隐私保护系统，并呈现出在实际解决问题时我们如何将应用问题转化为原理性问题，并罗列出在解决问题过程中我们使用的一些关键技术。

第四章是作品成果展示与分析。在理论上将问题解决后，我们设计出了具有前端对接能力的作品，并展示它的具体功能。在这之后，我们从性能和安全性两方面对我们的作品进行分析、评估。

第五章是前景展望。在完成作品初步设计以后，我们对作品的应用前景进行初步分析，判断出作品具有较大潜力，在应用市场上有较大的实现可能。

第六章是结论。基于本文工作，我们得出结论，论证了作品的可行性。

第七章是参考文献，罗列了本文所引用的参考文献。

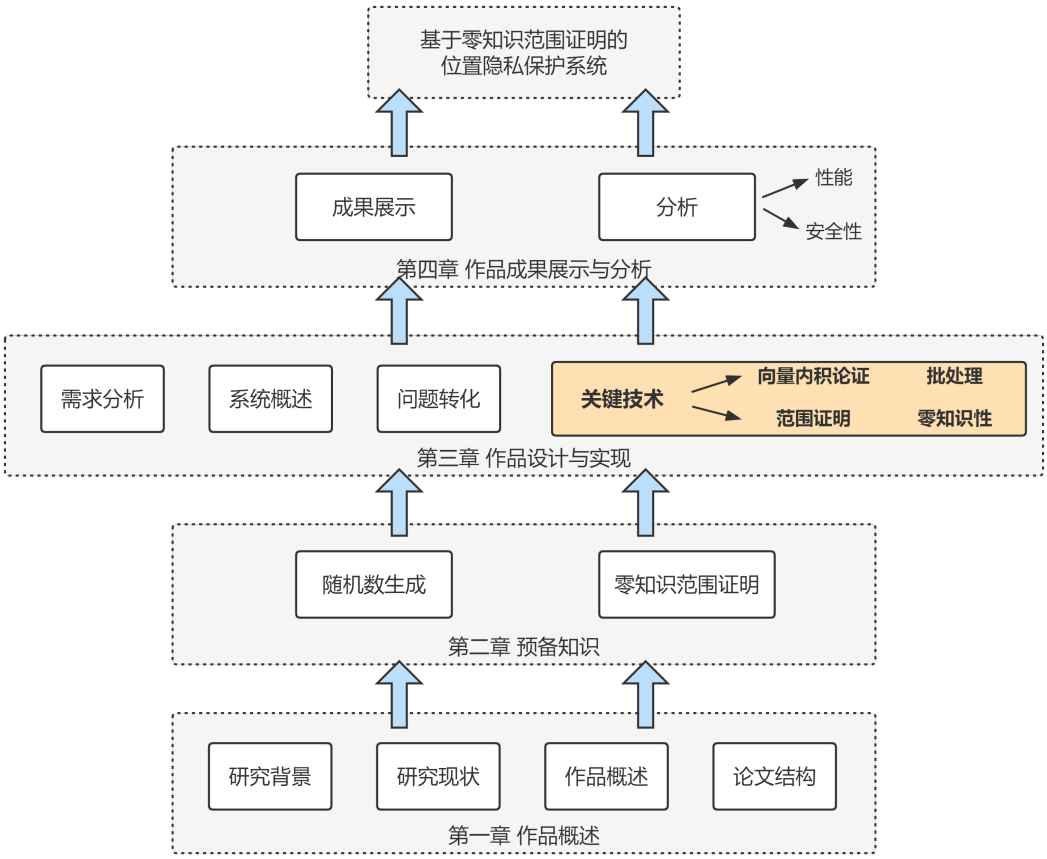

图 3 论文组织结构

二、预备知识

本部分主要介绍零知识范围证明涉及的基础知识，包括八个部分，依次为基于椭圆曲线密码的伪随机数生成算法、默克尔树、里德 · 所罗门编码、零知识证明 ZKAoK，交互式谕示机证明 IOP, 单变量和校验协议、FRI 低度检测和向量内积论证。其中，伪随机数算法用于随机数 R 的生成, 默克尔树用于对秘密向量的承诺和实现谕示机的问询，里德 · 所罗门编码用于编码向量，零知识证明 ZKAoK 阐述零知识证明的性质，IOP 用于证明和验证双方之间 k 轮的交互证明，单变量和校验协议用于验证集合上多项式值的和，FRI 低度检测用于判断多项式的阶数，最后的向量内积证明则用于向量的承诺。对以上知识的基本理解，将有助于进一步认识零知识范围证明及其对应的构造过程。

（一）基于椭圆曲线密码的随机数生成算法

我们选取位置模糊点时使用了基于椭圆曲线密码（Elliptic Curve Cryptography, ECC ）的随机数生成算法，我们在 Lap-Piu Lee 提出的模型基础上[25]，针对我们的问题进行优化。该算法具有较小的密钥尺寸与较高的安全性，是一种轻量级伪随机数算

法，Lap-Piu Lee 在论文中证明了其基本模型能够通过 FIPS 140-2 标准中对伪随机数生成器的统计测试。[25] 该算法选取一个定义在 F_p 上的椭圆曲线 $E(F_p)$ ，其中 p 是素数。为了生成公私钥，首先选择椭圆曲线上的基点 $G(x,y)$，其阶数为 n ；接着选取私钥 d ，$1 < d < n$ ；最终公钥为 $Q = dG$，$Q(x,y)$ 也是椭圆曲线上的点。为了生成伪随机数，该算法某一参数 y 的哈希值作为种子初始化伪随机数生成器，随机数生成的迭代公式为 $x_n = k_n Q,\ k_n = k_{n-1} + n - 1,\ k_1 = H(y)$ 。

具体实现中选择的椭圆曲线参数为 SECG（Standards for Efficient Cryptography Group）提出的 SECP128r1 标准；选择的哈希函数是 BLAKE3 ，同样具有轻量化的特点。

（二）范围证明的理论基础

1. 默克尔树

默克尔树[15]（Merkle Tree or Hash Tree）是一棵用哈希值搭建起来的树，树的所有节点都存储了哈希值。整棵树包含根节点、中间节点和叶节点。树采取自下而上的生成方式，叶节点经哈希运算得到哈希值，而其余节点的哈希值均由其子节点的哈希值经哈希计算得到。默克尔树的具体结构见图 4。

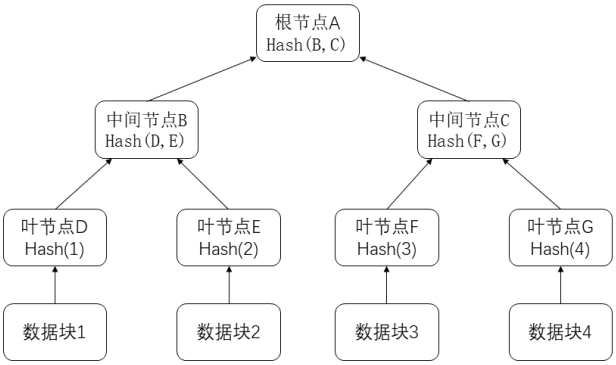

图 4 默克尔树结构图

基于哈希函数的防碰撞特性（Collision resistance）、隐藏性 (Hiding) 和谜题友好性（Puzzle friendly），对默克尔树的任意局部修改，都会对根节点和路径上的中间节点产生影响。默克尔树的这个特性提供了一种很好的检测数据是否被篡改的方法。在本文中，我们使用具有抗碰撞特性和不可逆特性的哈希函数来构造默克尔树，进而利用构造的树来完成对向量的承诺，并通过次线性尺度的证明来开放树的多处索引。对向量 v 的承

诺包含以下三种算法，即承诺操作（Commit）、开放操作（Open）、验证操作（Verify）：

- $\text{root}_v \leftarrow \text{MT.Commit}(v)$
- $(\{v_i\}_{i\in\mathcal{I}}, \pi_{\mathcal{I}}^v) \leftarrow \text{MT.Open}(\mathcal{I}, v)$
- $\{1,0\} \leftarrow \text{MT.Verify}(\text{root}_v, \mathcal{I}, \{v_i\}_{i\in\mathcal{I}}, \pi_{\mathcal{I}}^v)$

2. 里得·所罗门编码

里得·所罗门编码[16][17]（Reed-Solomon Code, RS Code）是一种编码方式，用其编码的码字是域上某个特定单变量多项式的一组函数值，表示成向量的形式。因此，在本文中我们使用 RS Code 来编码向量。

用抽象代数的模型来定义，选择一个 q 阶的有限域 $\mathbb{F}$，作为编码的字母表。再选择 $\mathbb{F}$ 的一个陪集 L，所选择的特定单变量多项式成为编码多项式（encoding polynomial），且度小于 $\rho \cdot |L|$，其中 $\rho \in (0,1)$ 称为编码率，用这样的多项式编码出的向量表示为 $\text{RS}[L,\rho] \in \mathbb{F}^{|L|}$。

具体而言，编码的过程如下：设插值集 $H = \{\xi_1, \cdots, \xi_{|H|}\}$，估值集 $L = \{\eta_1, \cdots, \eta_{|L|}\}$，且 $|L| > |H|$，被编码的向量设为 $v \in \mathbb{F}^{|H|}$。首先，找到预设的度的编码多项式 $\hat{p}$，使得 $\hat{p}|_H = \{\hat{p}(\xi_1), \cdots, \hat{p}(\xi_{|H|})\} = v$。然后计算 $\hat{p}$ 在 L 上的估值（Evaluation），得到码字 $\hat{p}|_L$。计算估值和插值的算法使用快速傅里叶变换（Fast Fourier Transform, FFT）和其逆变换（Inverse FFT, IFFT）。

3. 诚实验证方前提的零知识证明

零知识证明（Zero-Knowledge Argument of Knowledge, ZKAoK）是一种验证协议，在其中证明方（Prover）不提供任何有关某个论断的有用信息，而能使验证方（Verifier）验证该论断为正确的。这项协议技术在信息安全及密码学等领域应用广泛。“诚实验证方前提（Honest Verifier）”意为验证方是正确遵循协议进行验证的。

用计算复杂度理论（Computational Complexity Theory）的模型定义，零知识证明是一个用于证明 NP（Non-deterministic Polynomial）二元关系 $\mathcal{R}$ 的算法三元组 $(\mathcal{G}, \mathcal{P}, \mathcal{V})$。其中 $\mathcal{G}$ 表示公共参数生成算法，设其输出为 pp；$\mathcal{P}$ 和 $\mathcal{V}$ 分别表示非确定多项式时间（Probabilistic Polynomial Time, PPT）的证明算法和验证算法。

诚实验证方前提的零知识证明[16]具有以下条件需要满足：

- **完备性（*Completeness*）**：即正确的论断都可以被证明为正确。假设 λ 为私有参数，对于每个 $\mathcal{G}$ 的输出 $\text{pp} \leftarrow \mathcal{G}(1^\lambda)$，每个 $\mathcal{R}$ 中的元素 (x,ω)，以及字母表上任意字符

串 $z \in \{0,1\}^*$，有：

$$\Pr[\langle \mathcal{P}(\omega), \mathcal{V}(z)(\text{pp}, x) = 1\rangle] = 1 - \text{negl}(\lambda)$$

其中 Pr 表示概率，negl(λ) 表示当 λ 足够大时，可以忽略不计的量。

- **正确性（*Soundness*）**：即被证明的论断大都是正确的，只有极小的可能出错。对于每个 $\mathcal{G}$ 的输出 $\text{pp} \leftarrow \mathcal{G}(1^\lambda)$，每个不在 $\mathcal{R}$ 中的元素 (x, ω)，以及字母表上任意字符串 $z \in \{0,1\}^*$，有：

$$\Pr[\langle \mathcal{P}^*(\omega), \mathcal{V}(z)(\text{pp}, x) = 1\rangle] \leq \text{negl}(\lambda)$$

其中 $\mathcal{P}^*$ 表示任意的 PPT 证明方。

- **零知识性（*Zero-knowledge*）**：即 $\mathcal{P}$ 和 $\mathcal{V}$ 之间的对话可以只依据公开信息被完全模拟。对于每个 $\mathcal{G}$ 的输出 $\text{pp} \leftarrow \mathcal{G}(1^\lambda)$，任意的诚实的 PPT 验证方 $\mathcal{V}$，每个 $\mathcal{R}$ 中的元素 (x, ω) 和任意字母表上的字符串 $z \in \{0,1\}^*$，存在一个 PPT 模拟机 $\mathcal{S}$，使得：

$$\{\langle \mathcal{P}(\omega), \mathcal{V}(z)\rangle(\text{pp}, x)\} \overset{c}{\approx} \{\mathcal{S}^{\mathcal{V}}(\text{pp}, x, z)\}$$

其中 $\mathcal{S}^{\mathcal{V}}$ 表示多项式空间下给定 $\mathcal{V}$ 的模拟机，$\overset{c}{\approx}$ 表示两者在计算上不可区分（Computationally indistinguishable）。

- **知识论证性（*Argument of knowledge*）**：即所有论证的证明都不会是不合法的。对于每个 $\mathcal{G}$ 的输出 $\text{pp} \leftarrow \mathcal{G}(1^\lambda)$，任意的 $x, z \in \{0,1\}^*$，对于所有恶意的 PPT 证明方 $\mathcal{P}^*$，存在一个可预期多项式时间的抽取机 $\mathcal{E}$，使得：

$$\Pr[\langle \mathcal{P}^*(\omega), \mathcal{V}(z)\rangle(\text{pp}, x) = 1 \wedge ((x, \omega) \notin \mathcal{R})|_{\omega \leftarrow \mathcal{E}^{\mathcal{P}^*}(\text{pp}, x)}] \leq \text{negl}(\lambda)$$

其中 $\mathcal{E}^{\mathcal{P}^*}$ 表示抽取机对 $\mathcal{P}^*$ 的任意性及整个运行过程都具有访问权限。

4. 交互式谕示机证明

交互式谕示机证明[18] [19]（Interactive Oracle Proof, IOP）是一种证明系统模型，在其中验证方可以通过谕示机概率性地问询证明方所持有的关于被证明的论断的有效信息，但由于是概率性地问询，所以验证方并不能得到证明方的全部信息。

同样，使用计算复杂度理论的模型来定义，IOP 是证明 k 轮 NP 二元关系的算法三元组 $(\mathcal{G}, \mathcal{P}, \mathcal{V})$，其中 $\mathcal{G}$ 表示公共参数生成算法，设其输出为 pp；$\mathcal{P}$ 和 $\mathcal{V}$ 分别表示 PPT

证明算法和验证算法。具体而言，一个 k 轮的 IOP 包含 k 轮的交互（interaction）。在第 i 轮（$0 < i \leq k$），验证方向证明方均匀且随机地发送消息 m_i，且验证方能够通过谕示机得到以 m_i 为输入的输出，证明方需返回 π_i 给验证方。在最后一轮，验证方得到了证明方返回的 k 个位置的信息 $\pi = (\pi_1, \cdots, \pi_k)$，并且需决定接受或拒绝证明方的证明（Proof）。

交互式谕示机证明[20]具有以下条件需要满足：

- **完备性（*Completeness*）**：对于每个 pp$\leftarrow \mathcal{G}(1^\lambda)$ 以及 $(x, \omega) \in \mathcal{R}$，有：

$$\Pr[\langle \mathcal{P}(\omega), \mathcal{V}^\pi \rangle(\text{pp}, x) = 1] = 1$$

其中 $\mathcal{V}^\pi$ 表示 $\mathcal{V}$ 可以访问谕示 π。

- **正确性（*Soundness*）**：对于每个 pp$\leftarrow \mathcal{G}(1^\lambda)$，每个 PPT 的 $\mathcal{P}^*$ 以及 $(x, \omega) \notin \mathcal{R}$，有：

$$\Pr[\langle \mathcal{P}^*(\omega), \mathcal{V}^\pi \rangle(\text{pp}, x) = 1] \leq \text{negl}(\lambda)$$

在本文中，主要涉及两种类型的 IOP，分别是 *RS-IOP* 和 *IOP of proximity*，前者即使用里德-所罗门码（Reed-Solomon code）的 IOP，后者指对于正确性的条件，允许证明方的秘密和合法证据之间具有微小的差距（proximity）。

5. 单变量求和校验协议

单变量求和校验协议（Univariate Sum-check Protocol）主要应用于有限域上的多项式求和问题。首先，假设有两个乘法群 $H, L \subset \mathbb{F}$ ($|L| > |H|$)，一个小于 $k(k > |H|)$ 阶的单变量多项式 $f(\cdot)$，以及一个被声明（claimed）的和 μ。在已有假设上，单变量求和校验协议的作用就是证明 $\sum_{a \in H} f(a) = \mu$。

在实际操作中，证明方需要将 $f(x)$ 利用带余除法唯一地转化为 $x \cdot \hat{p}(x) + \zeta + \hat{Z_H}(x)\hat{h}(x)$，其中除式为 $\hat{Z_H}(x)$，代表 H 上的“消失”多项式（Vanishing polynomial），满足 $\forall a \in H,\ \hat{Z_H}(a) = 0$。接着，基于对 $\hat{f}|_L$ 和 $\hat{h}|_L$ 的谕示机访问，验证方可以验证是否有 $\hat{p}|_L \in \text{RS}(L, \frac{|H|-1}{|L|})$ 以及 $\hat{h}|_L \in \text{RS}(L, \frac{|L|-|H|}{|L|})$，其中：

$$\hat{p}(x) = \frac{|H| \cdot \hat{f}(x) - \mu - |H| \cdot \hat{Z_H}(x)\hat{h}(x)}{x} \tag{1}$$

以上采用 RS 编码的 IOP 满足正确性和完备性[20]，当我们将它转换为一个标准 IOP 时，它仍然是在检验谕示 $\hat{f}|_L, \hat{h}|_L, \hat{p}|_L$ 是否为具有相应度的界限的 RS 码。而这个过程可以通

过下面的低度检测协议来完成。

6. 低度检测和 FRI

给定度 $k_1,\cdots,k_t$，码字 $\hat{v}_1|_L,\cdots,\hat{v}_t|_L$，其中 L 为一个乘法陪集，低度检测协议允许验证方借助对这些码字的谕示机访问来检验以下语句是否成立：

$$\forall j\in\{0,\cdots,t\},\ \hat{v}_j|_L\in \mathbf{RS}[L,\frac{k_j}{|L|}] \tag{2}$$

公式（2）用于检测编码给定码字的编码多项式的度是否低于给定的度。

在本文中，我们的低度检测协议选取快速 Reed-Solomon 交互式谕示机邻近证明[21]（Fast Reed-Solomon Interactive Oracle Proof of Proximity, Fast RS IOPP, FRI）。给定对证明方消息 l 处取值的谕示机访问，该 FRI 是具有完整性（Completeness）和正确性（Soundness）容错率为 $O(\frac{L}{\mathbb{F}})+\text{negl}(l,k)$ 的 IOPP，其中 $l=O(\lambda),k=\max\{k_1,\cdots,k_t\}$。

总的来说，用于实现单变量求和校验的 FRI 协议可以表示为：

$$\langle \text{FRI}.\mathcal{P}(\hat{f},\hat{h},\hat{p},\text{FRI}.\mathcal{V}^{\hat{f}|_L,\hat{h}|_L,\hat{p}|_L})\rangle(k,k-|H|,|H|-1) \tag{3}$$

7. 向量内积论证

向量内积论证（Inner Product Arguments, IPA），是一证明手段，即给出两个向量 $\vec{a},\vec{b}$ 的承诺（commitment），其中 $\vec{a},\vec{b}$ 属于 $\mathbb{F}^n$，$\mathbb{F}$ 为域，可以证明这两个被承诺的向量的内积等于某一公开的标量，而不需要揭示这两个向量的具体取值。

在信息安全领域，常见的承诺方式有皮特森哈希值（Pedersen hash）或者 RS 编码，在本文中采用后者。

向量内积论证可以用于证明单变量多项式在某点处的值。首先将多项式 $\hat{f}=f_0+f_1x+\cdots+f_nx^n$ 表示为向量 $\vec{f}=(f_0,f_1,\cdots,f_n)$ 注意到：

$$\hat{f}(s)=(\vec{f},(1,s,\cdots,s^n)) \tag{4}$$

公式（4）表明计算等价于两个向量的内积，因此可转化为向量内积论证。

三、作品设计与实现

（一）需求分析

为了使改进后的位置隐私保护系统更符合当前应用市场的需要，本文设计出的作品应满足一定的功能和性能的需求。本节将对位置隐私保护系统在功能上、性能上的需求进行分析，从而为本文作品指引改进方向。

1. 功能需求

位置隐私保护系统涉及用户、服务提供商乃至第三方应用，具有广泛的应用场景。因此，改进后的位置隐私保护系统应满足一定的功能需求，以满足各方需要。

（1）保护用户位置隐私安全

位置隐私保护系统的出发点是保护用户隐私安全，不管如何改进，这一点应当始终保持。当前位置隐私保护技术主要通过添加虚假或者无关的位置信息，以此混淆用户真实的位置信息。改进后的位置信息保护系统虽然是基于零知识范围证明技术，但也应该达到这一效果。

我们的系统通过两方面来保证这一点，第一是随机选点时的随机性，第二是零知识证明对被证明信息的隐蔽性，第二点是对第一点的进一步补充和保护。**（2）保证用户返回的位置信息可信**

虽然在现阶段的“用户-服务提供商”模式下，保证用户提交的位置信息的真实性似乎没有很大的必要，但是可以看到，攻击者可以通过向服务提供商或者系统提交错误的位置信息，窃取系统信息，从而达到某种攻击系统的目的。所以改进后的位置隐私保护系统也应该保证位置信息的真实性，防止攻击者通过提交错误的位置信息攻击系统这一漏洞。我们的零知识证明天然可以保障这一点。

（3）保障用户得到的服务质量

用户的位置隐私固然重要，但是保护用户隐私应该在不明显影响用户得到的服务质量这一前提下。现有的 K-匿名技术、虚假位置技术等位置隐私保护技术都能大致满足这一需求。因此，改进后的位置隐私保护系统应谨慎选择模糊位置的边界和精度，平衡好服务质量与隐私保护。

2. 性能需求

考虑到用户所在的移动用户端性能有限，以及系统的计算开销应该限制在一定范围内，实际应用中位置隐私保护系统应该满足一定的性能需求。

（1）计算复杂度

通常用户发起查询请求后，服务提供商应该在较短时间内返回查询结果和对应服务。同时，用户所在的移动用户端计算、存储能力通常比较有限，难以支撑复杂的计算过程。所以改进后的位置隐私保护系统应该具有较低的计算时间、空间复杂度，从而保证系统实际运行的效果。

（2）可拓展性

近年来我国位置服务产业快速发展，截至 2021 年卫星导航与位置服务产业总体产值已经达到 4690 亿元[14]，产业前景不可估量。在此背景下，位置隐私保护系统将会面向多种应用场景，这也对位置隐私保护系统的可拓展性提出了比较高的要求。所以改进后的系统在设计和实现上需要有一定程度的解耦、分层设计，以适应随时变化的业务场景。所以在设计系统时应有意识地将系统模块化开发，并留下优化、拓展的空间，便于新功能的拓展。

（3）健壮性

位置信息涉及用户隐私，应该防止泄露的可能。所以系统应该具有一定的防卫或者恢复能力，在受到攻击或者发生错误时能采取措施减少损失。具体而言，当局部系统出错或受到攻击时，这部分系统应该能在较短时间内恢复并继续运行，而不会造成大范围影响，从而在最大程度上减少系统运行的风险。这也是应用场景对位置隐私保护系统在健壮性上的要求。

（二）系统概述

本作品系统主要涉及两个主体：服务请求方和服务提供商。服务请求方一端由**手机网页端交互界面、定位与生成零知识范围证明系统**构成，具体技术涉及 Vue.js 、C++ 和 Python。服务提供商一端由**数据库、（零知识范围证明）验证系统**构成，开发技术使用 Shell 和 MySQL 。

系统工作总体流程图如图 5所示。首先，请求方选择以何种精度 r 模糊自己的位置，接着本地系统自动采集用户的精确经纬度地理位置 (x, y) 。本地系统获得参数 (x, y, r) 后，在以 $\frac{r}{2}$ 为半径的圆内，生成一个模糊位置 (x', y') 。具体模糊位置生成过程为，使用基于椭圆曲线的轻量随机数生成算法（见预备知识第一节），生成一个伪随机极坐标 (R, α) ，极坐标原点为 (x, y) 。然后基于该相对极坐标计算出模糊位置 (x', y') 。

本地系统基于该模糊位置 $(x',\ y',\ R)$ ，生成一个对范围的零知识证明：$Proof : R < \frac{r}{2}$ ，并将 $(x,\ y,\ Proof)$ 打包发送至服务提供商数据库。服务提供商验证证明，确认用户在该模糊范围内，提供相应的服务。最终效果是服务提供商只知道请求方在 $(x', y', \frac{r}{2})$ 这一个圆形范围内，服务请求方保护了自身位置隐私，同时其接受的服务精度偏差不超过 r。

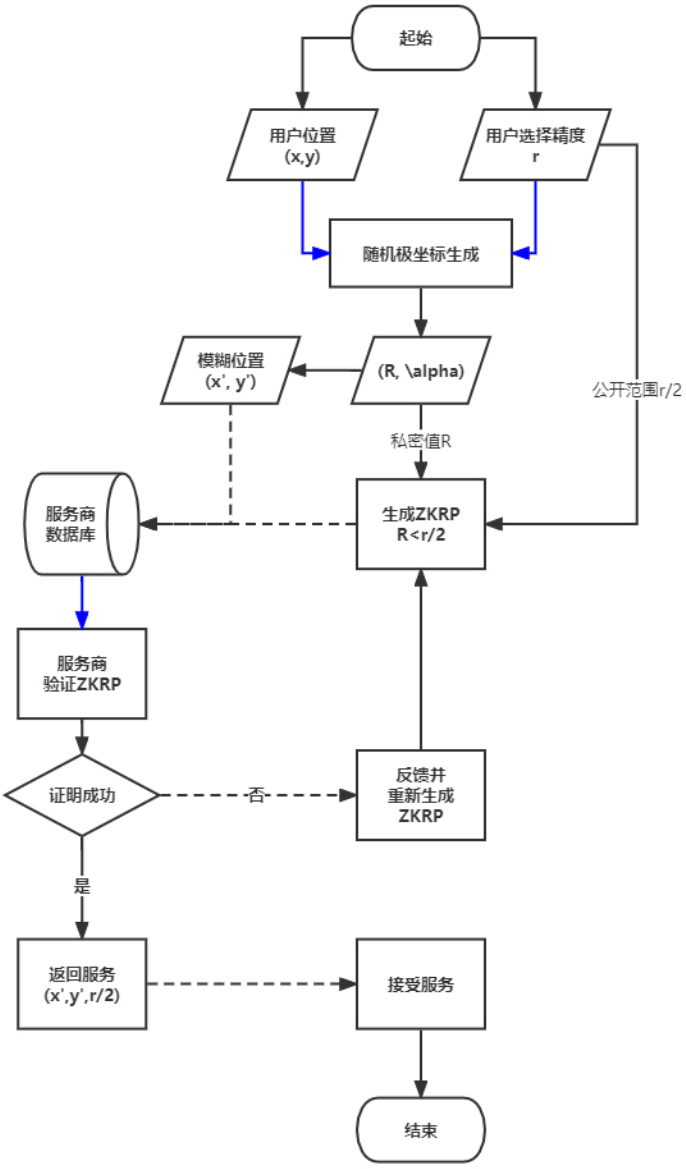

图 5 系统工作总体流程图

（三）问题转化

1. 基于哈达玛积的问题转化

基于零知识范围证明的的位置隐私保护系统改进实际上是围绕精确位置经纬度上的零知识范围证明展开的。这是改进的新系统的技术核心。为了使系统的针对目标更加清晰，我们定义如下问题场景: 证明方在拥有一个隐藏的用户位置坐标和一个公开的参考点位置坐标的基础上，向验证方证明用户位置坐标在参考点位置坐标的一定范围内，但这个过程不会透露用户位置坐标的具体信息。在以下两章中，我们将介绍该问题的解决方案和相应的技术原理。

观察问题场景，我们发现其中涉及两个位置坐标：隐藏的用户位置坐标和公开的参考点位置坐标，分别记作 $S(x_1, y_1)$ 和 $P(x_2, y_2)$。考虑到实际生活场景中的位置坐标往往是经纬度形式，因此这两个坐标同样采用经纬度形式。同时为了兼顾一定的准确性，在经纬度精度上，本文选取 4 位小数作为参考样例, 即 x_1,x_2,y_1,y_2 均为五位小数。此时最大误差大概是在 5 米左右。当然，如果需要让结果进一步精确，仍可以进一步调整精度。

要判断坐标 S 是否在坐标 P 的一定范围内，我们可以参考平面中心圆模型。通过判断两者间的距离 R 是否处于一定数值范围内，即可检验坐标间关系是否满足要求。为了使问题更加明确，本文中用符号 l_{min},l_{max} 分别来表示距离的下界和上界，且均为整数。在本文中，l_{min} 默认取 0，因为取 0 已经可以满足应用场景的需求。至于整数的选取则是为了将问题迁移到零知识范围证明上时更加简单、易实现。实际应用中，$l_{\min}$,$l_{\max}$ 应根据具体需求进行一定的变化。基于以上定义，我们将问题转化为：用户 GPS 坐标在参考点 GPS 坐标的一定范围内等价于检验以下公式：

$$l_{\min} < d_{SP} \leq l_{\max} \tag{5}$$

其中 d_{SP} 代表坐标 S 和 P 之间的距离，数值选取小数点后 5 位。而要得出 d_{SP} 的具体数值，我们需要利用坐标 $S(x_1, y_1)$ 和 $P(x_2, y_2)$ 进行如下公式计算:

$$\begin{cases} S' = (R\cos x_1 \cos y_1, R\sin x_1 \cos y_1, R\sin y_1), \\ P' = (R\cos x_2 \cos y_2, R\sin x_2 \cos y_2, R\sin y_2), \\ d_{SP} = R\arccos[\cos(x_1 - x_2)\cos y_1 \cos y_2 + \sin y_1 \sin y_2]. \end{cases} \tag{6}$$

其中 S' 和 P' 分别代表经纬度坐标 $S(x_1, y_1)$ 和 $P(x_2, y_2)$ 在三维直角坐标系下对应坐标，R 代表地球的半径。这样就可以进行 d_{SP} 和 L 的比较了。

但是，我们采用的零知识范围证明适用于任意整数范围，而非任意实数范围。并且零知识范围证明主要是对向量进行操作，而非直接的数值。因此我们不仅需要将 d_{SP} 进行整数化处理，还要进一步将其转化为进制形式来形成对应向量。下面介绍解决方案。

首先，将 d_{SP},$l_{\min}$,$l_{\max}$ 乘以 10^5, 进一步得到 D_{SP},$L_{\min}$,$L_{\max}$ 这样我们不仅保留了小数部分，避免了直接去除小数部分带来的误差，同时完成了取整。不过值得注意，乘以 10 的几次方主要取决于应用需求和相关参数的精度选取。

接着，取满足 $u^{n-1} < L_{\max} \leq u^n$ 的 u 和 n, 对 D_{SP},$L_{\min}$,$L_{\max}$,$D_{SP} - L_{\min}$,$D_{SP} - L_{\max} + u^n$ 分别进行进制转化，得到向量 v,a,b,c,d。本文中以二进制作为参考样例。进一步计算

以下内积关系，以证明 $L_{\min} < D_{SP} \leq L_{\max}$:

$$\begin{cases} \langle v \odot (v - 1^m), r \rangle = 0 \\ \langle c \odot (c - 1^m), r \rangle = 0 \\ \langle d \odot (d - 1^m), r \rangle = 0 \\ \langle c, r_{[:m-n]} || 0^n \rangle = 0 \\ \langle d, r_{[:m-n]} || 0^n \rangle = 0 \\ \langle v - a - c, 2^m \rangle = 0 \\ \langle v - b + bi(2^n) - d, 2^m \rangle = 0 \end{cases} \tag{7}$$

以上运算基于一个足够大的有限域 $\mathbb{F}$ 的。参数 m 大小为 $|\mathbb{F}|$, 参数 r 是验证方随机选取的一个挑战值。$\odot$ 表示哈达玛积，即 $a \odot b = (a_1, \ldots, a_k) \odot (b_1, \ldots, b_k) = (a_1 b_1, \ldots, a_k b_k)$。$bi()$ 表示将数转化为二进制的向量。以上的七个公式就是零知识范围证明实际上的证明对象，至此问题已经转化完成，接下去的流程就是零知识范围证明了。其中的具体原理，详见下一章关于零知识范围证明的介绍。

2. 基于椭圆曲线密码的随机数算法问题转化

系统中需要根据精确位置信息 (x, y) 与用户要求的精度 r 生成伪随机数坐标。为了保证随机性，参数中还需要引入时间戳，即需要随机数算法 $F(x,\ y,\ r,\ t) = R,\ R \in (0, \frac{r}{2})$ 。我们需要对原有基于 ECC 的随机数算法做出适应性改进，具体函数 F(x,y,r,t) 的生成过程如下：

- 使用 BLAKE3 中哈希函数计算参数 t（时间戳）和参数 y 的哈希值 $H(t,\ y)$，转化为整数并记为 s。应保证 $1 < s < n$，若不满足，则反复迭代使用哈希函数（例如计算 $H(H(t,\ y))$。
- 使用 s 作为伪随机数生成器的初始化种子，计算 $R = s \cdot Q$ 。
- 分别使用 BLAKE3 中哈希函数计算 $H(y),\ H(x)$
- 异或计算 $Z = R \oplus H(x) \oplus H(y)$，并取余 r，即 $R = Z\ mod\ r$，得到结果。

（四）关键技术

基于已介绍的基础知识，此部分将正式阐述基于交互式谕示机证明的零知识范围证明的原理和构造过程。这一部分将逐步递进，依次介绍批处理向量内积证明、任意基底 u 的范围证明、批处理范围证明、对于任意范围的范围证明和补充零知识性。从而阐释

本文 ZKRP 中的批处理实现、任意基底原理、任意范围证明的转化、零知识性质的由来，以及如何借助这些理论来完成零知识范围证明的构造。在以上过程中，我们将理解零知识范围证明的重要部分，形成对零知识范围证明基本原理与框架的认识，进而掌握零知识范围证明的核心所在。

1. 批处理向量内积论证

为了实现批处理 IPA（Batch Inner Product Argument, B-IPA），我们考虑单变量求和校验协议的一个性质：无论多个多项式的阶数是否相同，单变量求和校验协议都支持校验每一个一元多项式的和[20]。此性质为构造一个校验编码向量间内积关系的 IPA 提供了一种可能，其中编码向量来自于不同阶数的编码多项式。

特别地，将阶数分别为 $k_1, ..., k_t$ 的秘密编码多项式设为 $\hat{v}_1, ..., \hat{v}_t$。再将阶数分别为 $k_{t+1}, ..., k_{2t}$ 的公开多项式设为 $\hat{r}_1, ..., \hat{r}_t$。假定证明方 $\mathcal{P}$ 想要证明对于任意 $j \in \{1, \cdots, t\}$，都满足 $\sum_{a\in H} \hat{v}_j(a) \cdot \hat{r}_j(a) = y_j$。实现过程中，证明方 $\mathcal{P}$ 首先需要用默克尔树生成对 $(\hat{v}_1|_L, ..., \hat{v}_t|_L)$ 的承诺，并将其发送给验证方 $\mathcal{V}$。接着，验证方选择随机 t 个元素 $\beta_1, ..., \beta_t$，设 $\hat{q} = \sum_{j=1}^{t} \beta_j \hat{v}_j \cdot \hat{r}_j$。最后证明方 $\mathcal{P}$ 和验证方 $\mathcal{V}$ 使用单变量求和校验协议来证明以下等式成立：

$$\sum_{a\in H} \hat{q}(a) = \sum_{a\in H} \sum_{j=1}^{t} \beta_j \hat{v}_j(a) \cdot \hat{r}_j(a) = \sum_{j=1}^{t} \beta_j y_j \tag{8}$$

除此之外，批处理 IPA 的正确性容错率（Soundness error）仅取决于 t 个项中最大的阶数 $k_{\max}$，$k_{\max} = \max\{k_i + k_{t+i}\}_{1\le i\le t}$。

基于此，我们给出**批处理内积关系（*Batch inner product relation*）**的定义：设二元关系 $\mathcal{R}_{\text{B-IPA}}$ 为所有 (x, ω) 的集合，其中：

$$x = (\mathbb{F}, H, L, \{k_j\}_{1\le j\le 2t}, \{\hat{r}_j\}_{1\le j\le t}, \{y_j\}_{1\le j\le t})$$
$$\omega = \{\hat{v}_j\}_{1\le j\le t}$$

且有公式（8）成立。

接下来验证该批处理 IPA 的正确性、完备性以及知识论证性：

- **批处理 IPA 的完备性（*B-IPA Completeness*）**：考虑 $\hat{q}$ 的变换，设对 $j \in \{1, \cdots, t\}$，有 $\sum_{a\in H} \beta_j v_j(a) r_j(a) = \beta_j y_j$，那么公式（8）成立。这符合单变量和校验的二元关系形式。因此，批处理 IPA 有着与单变量和校验协议相同的完备性。
- **批处理 IPA 的正确性（*B-IPA Soundness)*）**：可以考虑以下两种发生错误的情形：

情形一. 假设由于随机的线性选择组合，非法的单变量和校验关系恰好成立。我们假设 $\forall j \in \{1,\cdots,t\}, \sum_{a\in H} \hat{v}_j(a)\cdot \hat{r}_j(a) = y'_j$，且对于 $\{1,\cdots,t\}$ 的某个子集 Q，有 $\forall q \in Q, y_q \neq y'_q$。简便起见，不妨设 $t \in Q$。验证方随机选择 t-1 个元素 $\beta_1,\cdots,\beta_{t-1}$，则 $\sum_{j=1}^{t}\beta_j y_j = \sum_{j=1}^{t}\beta_j y'_j$ 当且仅当：

$$\beta_t = \frac{\beta_1(y'_1 - y_1) + \cdots + \beta_{t-1}(y'_{t-1} - y_{t-1})}{y_t - y'_t} \tag{9}$$

公式（9）发生的可能性仅为 $1/|\mathbb{F}|$，而实际选用的有限域大小往往很大，因此概率可忽略不计。

情形二. 假设变量和校验关系是非法的，即公式（8）不成立。那么批处理 IPA 正确性的错误有以下三种可能：

（1）若 RS 编码的 IOP 非法，则正确性取决于单变量和校验协议，故具有正确性。

（2）若 FRI 非法，则正确性错误的上界为 $\epsilon_{FRI} = \mathcal{O}(|L|/|\mathbb{F}|) + negl(\ell, k_{max}/|L|)$。

（3）若默克尔树的根不正确或任意验证路径不正确，由于哈希函数的防碰撞性质，正确性错误的上界为 $negl(\lambda)$。

- **批处理 IPA 的知识论证性（*B-IPA Knowledge Argument)*：**批处理 IPA 是基于随机谕示机模型的一种知识论证。对于任意 PPT 对手 $\mathcal{P}^*$，总存在一个 PPT 抽取机 $\mathcal{E}$ 使得：给定 $\mathcal{P}^*$ 的随机访问带，对每个由 $\mathcal{P}^*$ 生成的陈述：

$$x = (\mathbb{F}, H, L, \{k_j\}_{j\in[2t]}, \{\hat{r_j}\}_{j\in[t]}, \{y_j\}_{j\in[t]}) \tag{10}$$

有以下的概率为 negl(λ)：

$$\Pr\left[\begin{array}{c} \text{root}^* \leftarrow \mathcal{P}^*(1^\lambda, x), \langle \mathcal{P}^*, \mathcal{V}\rangle(\text{pp,x}) = 1, \{\hat{v}_j\}_{1\le j\le t} \leftarrow \mathcal{E}(1^\lambda, x) : \\ \text{MT.Commit}(\mathbb{V}|_L) \neq \text{root}^* \vee (x, \{\hat{v}_j\}_{1\le j\le t}) \notin \mathcal{R}_{\text{B-IPA}} \end{array}\right] \tag{11}$$

批处理 IPA 的知识论证属性来源于默克尔树的可抽取性。给定默克尔树树根和足够多的验证通路，总存在一个高效的方法能够抽取默克尔树上所有被承诺的叶节点。一旦这些叶节点被成功提取，就能通过 IFFT 算法获取满足 $|L| > k_{\max}$ 的秘密多项式，进而实现知识论证的属性[18] [16]。

图 6 展示了在批处理 IPA 中，证明方与验证方进行交互、证明方向验证方证明 $(x,\omega) \in \mathcal{R}_{\text{B-IPA}}$ 的流程。

其中 $\mathbb{V}|_L \in \mathbb{F}^{t\times|L|}$ 表示矩阵 $(a_{ij})_{t\times|L|} = (\hat{v}_i|_L[j])$。**MT.Commit**$(\mathbb{V}|_L)$ 表示将矩阵 $\mathbb{V}|_L$ 的每一列放入默克尔树的叶节点。

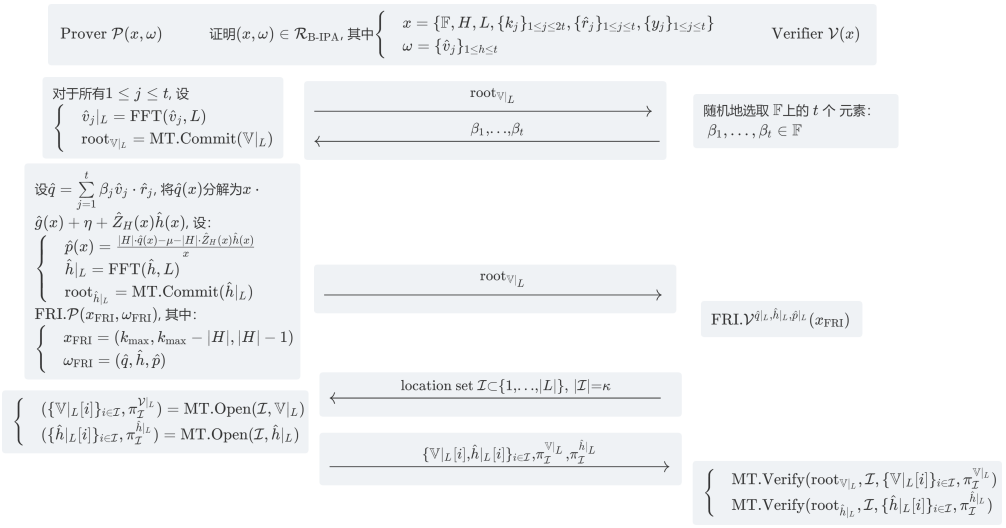

图 6：批处理向量内积论证（Batch IPA）$\langle\mathbf{IPA}_B.\mathcal{P}(\omega),\mathbf{IPA}_B.\mathcal{V}\rangle(x)$

2. 对于 $[0,u^{n-1}]$ 的范围证明

为了证明上界为 u^m（即 u 进制展开为 m 位）的秘密值 V 在范围 $[0,2^n-1]$ 中（$n<m$），只需要满足以下等式：

$$\begin{aligned} &v\odot(v-1^m)\odot\cdots\odot(v-u^m)=0^m,\\ &v\odot(1^{m-n}||0^n)=0^m. \end{aligned} \tag{12}$$

其中 $v=(v_0,v_1,\ldots,v_{m-1}), V=\sum_{j=0}^{m}v_ju^j$。进一步地，相当于证明：

$$\begin{aligned} &\langle v\odot(v-1^m)\odot\cdots\odot(v-u^m),r\rangle=0,\\ &\langle v,r_{[:m-n]}||0^n\rangle=0. \end{aligned} \tag{13}$$

经理论计算，对于验证方选取的任意 $r\in\mathbb{F}$，公式（13）非法成立，即出现正确性错误的概率为 $1/\mathbb{F}$。

对于公式（13），可以利用批处理 IPA 来证明，即输入设为：

$$\begin{aligned} &x = (\mathbb{F}, H, L, (u|H| - (u-1)), |H|, |H|, |H|, (\hat{r}, \hat{s}), (0,0)), \\ &\omega = (\hat{w}, \hat{v}) \end{aligned} \tag{14}$$

基于此，我们给出**范围关系（*Range relation*）**的定义：设二元关系 $\mathcal{R}_{\mathrm{RP}}$ 为所有 (x, ω) 的集合，其中：

$$x = (\mathbb{F}, H, L, m, n, [0, u^n - 1]),\ \omega = V.$$

且有秘密值 V 满足 $V \in [0, u^n - 1]$ 成立。

图（7）展示了在 RP 中，证明方与验证方进行交互、证明方向验证方证明 $(x, \omega) \in \mathcal{R}_{\mathrm{RP}}$ 的流程。其中 $\mathbb{F}$ 是一个有限域，L, H 是 $\mathbb{F}$ 的乘法陪集。秘密值 V 满足 $V \in [0, u^n - 1]$。

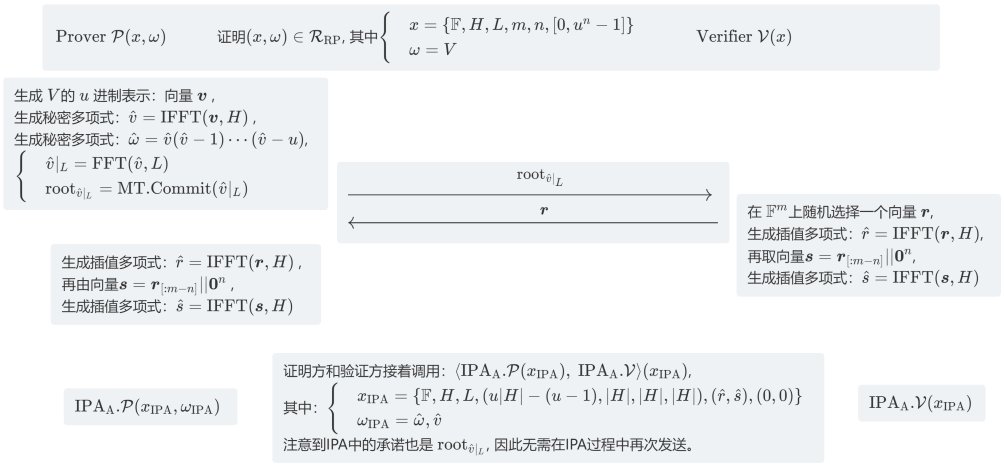

图 7 ：范围证明（Range Proof）$\langle \mathbf{RP}.\mathcal{P}(\omega), \mathbf{RP}.\mathcal{V}\rangle(x)$

3. 批处理范围证明

基于前述的批处理 IPA，我们可以构建一个证明多个秘密值在各自对应范围内的证明。假设我们要证明秘密值 $V_1, ..., V_t$ 分别处于对应范围 $[0, u_1^{n_1} - 1], ..., [0, u_t^{n_t} - 1]$，那么对于任意 $j \in \{1, \ldots, t\}$, 都有如下公式：

$$\begin{aligned} &v_j \odot (v_j - 1^m) \odot \cdots \odot (v_j - u_j^m) = 0^m, \\ &v_j \odot (1^{m-n_j} || 0^{n_j}) = 0^m \end{aligned} \tag{15}$$

其中 $m \geq \max\{n_1, ..., n_t\}$。进一步转换上述公式，可以推出：对于任意 $j \in \{1, \cdots, t\}$,

都有如下公式：

$$\begin{aligned}&\langle v_j \odot (v_j - 1^m) \odot ... \odot (v_j - u_j^m), r\rangle = 0,\\&\langle v_j, (r^{m-n_j}||0^{n_j})\rangle = 0\end{aligned} \tag{16}$$

对于公式（16），可以利用批处理 IPA 来证明，即输入设为：

$$\begin{aligned}&x = (\mathbb{F}, H, L, \{k_j\}_{j\in[4t]}, \{\hat{r}_j\}_{j\in[2t]}, \{y_j\}_{j\in[2t]}),\\&w = \hat{w}_1, ..., \hat{w}_t, \hat{v}_1, ..., \hat{v}_t,\end{aligned} \tag{17}$$

其中一些变量满足如下关系:

$$\begin{aligned}&\{k_j\}_{j\in[t]} = \underbrace{u_1|H| - (u_1 - 1), ..., t_t|H| - (u_t - 1)}_{t},\\&\{k_j\}_{j\in[t+1,4t]} = \underbrace{|H|, ..., |H|}_{3t},\\&\{\hat{r}_j\}_{j\in[2t]} = \underbrace{\hat{r}, ..., \hat{r}}_{t}, \underbrace{\hat{s}_1, ..., \hat{s}_t}_{t},\\&\{y_j\}_{j\in[2t]} = \underbrace{0, ..., 0}_{2t}.\end{aligned} \tag{18}$$

其中对任意 $j \in \{1, \cdots, t\}, \hat{s}_j$ 和 $\hat{v}_j$ 是 $r^{m-n_j}||0^{n_j}, v_j$ 的编码多项式，以及 $\hat{w}_j = \hat{v}_j(\hat{v}_j - 1) \cdots (\hat{v}_j - u_j)$。

4. 对于任意范围的范围证明

考虑到实际整数范围证明往往是任意整数，我们需要进一步拓宽前述范围证明的通用性。为了实现这一点，我们需要利用前述的对范围 $[0, u^n - 1]$ 的范围证明。假设要验证秘密值 $V \in [A, B - 1]$, 其中 A, B 均为任意整数。收到 Camenisch[22]等人的启发，我们首先将这个问题进行如下转化：

$$V - A \in [0, u^n - 1] \wedge V - B + u^n \in [0, u^n - 1] \tag{19}$$

其中 $u^{n-1} < B < u^n$。基于新的公式，我们成功将任意整数范围的证明转化到了范围 $[0, u^n - 1]$ 的证明上，从而我们可以利用前述的对范围 $[0, u^n - 1]$ 的范围证明来实现任意范围的范围证明。

在任意范围的证明流程中，验证方不采用基于秘密值 V 的向量 v 的询问，而是直接

让证明方通过 IPA 证明 $V - A = C$ 和 $V - B + u^n = D$。由于此处 IPA 不止一个，因此我们可以引入批处理 IPA 来加快处理过程。实际上，任意范围的范围证明可以简单看作基于批处理 IPA 的多个任意基底范围证明的有效融合。

5. 补充零知识性

前述的范围证明实际上并不是零知识性的，它存在两个层面的知识泄露：

- 问询环节：在验证者打开默克尔树的承诺时，其可见 l 个 $\mathbb{V}|_L$ 的估值。而这些估值与秘密向量 $\{v_j\}_{1\leq j\leq t}$ 相关，因而会泄露 $\{V_j\}_{1\leq j\leq t}$ 的部分信息。
- PRI 协议环节：在验证方借助 $O(\log|L|)$ 轮对码字 $\hat{v}_1|_L, \cdots, \hat{v}_L|_L$ 的谕示机访问时，验证方可以根据这些已得的信息获取额外的其他信息。

因此，我们采取与张、谢等人[16]相似的处理。

对于第一个知识泄露，我们使证明者采取以下措施：选择一个度为 l 的随机多项式 $\hat{\delta}_j$，利用其掩盖 $\hat{v}_j$，即 $\hat{v}'_j = \hat{v}_j + \hat{Z}_H \cdot \hat{\delta}_j$，其中 $\hat{Z}_H$ 是陪集 H 上的“消失”多项式，即对 $\forall h \in H, \hat{Z}_H(h) = 0.$

对于第二个知识泄露，我们使证明者采取同样的措施，即使用随机多项式 $\hat{\gamma}$ 来掩盖秘密多项式 $\hat{v}$，并控制 $\hat{\gamma}$ 的度在 $(u_{\max}+1)|H| + u_{\max}(l-1)$。基于以上处理，我们给出批处理的零知识范围证明的流程，如图（8）所示。

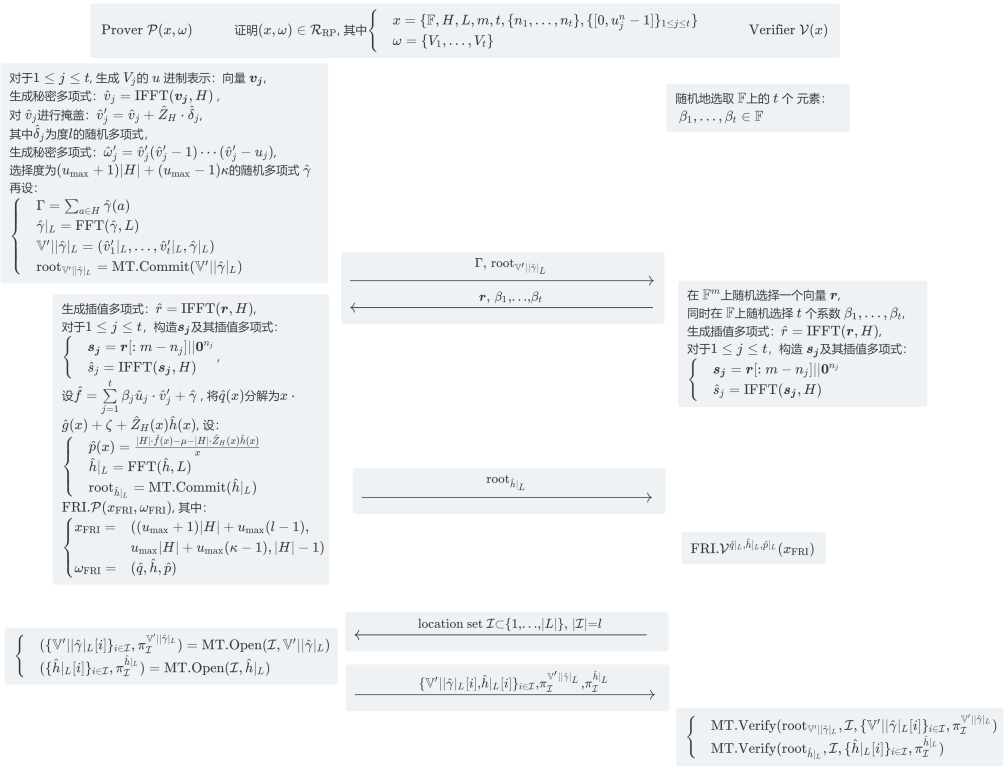

图 8：零知识范围证明（Zero-Knowledge Range Proof）$\langle\mathbf{RP_{zk}}.\mathcal{P}(\omega),\mathbf{RP_{zk}}.\mathcal{V}\rangle(x)$

可以证明，以上流程具有完备性（Completeness）、正确性（Soundness）、知识论证性（Argument of knowledge）、诚实验证者前提的零知识性（Honest-verifier zero knowledge）。

四、作品成果展示与安全性分析

（一）作品前端功能展示

1. 设置界面

本作品最终形式是手机“设置”应用中全新设计的隐私选项界面以及效果展示界面，后续可以封装为 SDK 软件工具包供第三方应用调用使用。

根界面如图 9所示，用户可以选择不同应用，进入针对不同应用的设置选项界面，符合一般“设置”应用组织逻辑。

图 9 设置界面

举例而言，用户点击进入“地图”应用的具体设置界面，如下图 10所示。界面中用户可以选择是否开启我们的基于零知识范围证明技术的位置隐私保护服务，并在下方通过滚轮组件选择用户希望的用户精度。选择好后，用户可以进入演示界面。一般情境下，用户在此即可退出，在具体应用请求位置时我们的系统能够自动开始工作，为了作品演示需求，我们在此提供虚拟演示界面。

(a) 界面示意图 **(b) 交互演示**

图 10 “地图”应用设置界面

2. 实际效果演示界面

实际效果界面主体由一张虚拟地图构成，如图 11所示，用户有一个退出键和三个主要选项，分别是“定位”，“模糊”以及“生成证明”。

“定位”选项，系统请求当前用户精确位置，并在虚拟地图上显示相对坐标；“模糊”选项，系统生成用户模糊位置范围，并在虚拟地图上用红色突出显示；“生成证明”选项，系统更具用户模糊范围生成零知识范围证明，并发送给服务器，进行验证。“生成证明按钮”会同时弹出文字提示，用户上滑界面即可进入认证界面。

(a) 定位操作示意图 **(b) 模糊操作示意图** **(c) 生成证明操作示意图**

图 11 “演示”界面

3. 认证界面

用户向服务提供商服务器发送证明后，服务器会对证明进行验证，过程中用户和服务器会反复通信验证。认证界面 12的进度条会显示当前认证进度，并且会提示用户当前证明的范围具体值。当认证成功后，会跳出文字提示，至此系统完成一次模糊位置情况下的服务请求。

(a) 示意图　　**(b)** 交互

图 12 “认证”界面

（二）ZKRP 性能分析

1. 空间复杂度

本篇论文所使用的 ZKRP 具有较小的空间复杂度。在实际零知识范围证明中，证明的大小是处于可接受范围的。以上将从两方面进行分析：

从理论层面分析，证明的空间占用主要来自于以下几个方面：1.RS 编码中的插值集和估值集。2. 默克尔树。3. 批量 IPA 开销。进而可以推出整个理论证明大小，相关公式表示如下：

$$\begin{aligned} 1|H| \ +1|H| + 2 \cdot Tree(|L|/2^{\eta_1}, \ell)|H| \ + \ 2 \cdot Tree(|L|/2^{\eta_1+\eta_2}, \ell)|H| \ + \\ 3 \cdot \ell \cdot 2^{\eta_1}|\mathbb{F}| \ + \ \ell \cdot 2^{\eta_2}|\mathbb{F}| \ + \ 2^{k_{max}-\eta_1-\eta_2}|\mathbb{F}| \end{aligned} \tag{20}$$

表 2 范围证明空间性能测试结果

维数 n	证明次数 t	范围证明大小		
		π	π in [23]	π in[24]]
32	1	22.4KB	11.8KB	-
64	1	28.7KB	-	-
128	1	28.3KB	26.4KB	-
256	1	34.8KB	-	-
512	1	40.7KB	51.3KB	-
固定 64	180	0.11MB	-	4.52MB
	500	0.27MB	-	4.87MB
	1000	0.52MB	-	5.36MB

注：其中前四行数据涉及参数 $\ell = 41$,$\rho = 2^{-3}$,$e = 3$,$\lambda = 120$,$\eta = \{2, 2\}$。第五行参数 $\ell = 41$,$\rho = 2^{-3}$,$e = 3$,$\lambda = 120$,$\eta = \{2, 3\}$。后三行参数 $\ell = 33$,$\rho = 2^{-3}$,$e = 3$,$\lambda = 128$,$\eta = \{1, 2\}$。

从实际需求出发，GPS 范围证明的距离边界可选范围 $[l_{\min}, l_{\max}] \subseteq [0, 10^6]$。经整数化处理，范围扩展到 $L_{\min}, L_{\max} \subseteq [0, 10^{11}]$。而对于本文的 ZKRP，即使范围扩大到 $[0, 2^{512} - 1]$, 在其它参数选取合理的情况下，其证明大小也仅有 $40.7KB$。这意味着，在 GPS 范围证明的应用场景下，ZKRP 证明大小可以保持在一个很小的值，不会占用太多的空间。而这符合 GPS 范围证明对轻量化的需求。

以二进制向量为基准，本文 ZKRP 与其它后量子安全 ZKRP 的空间性能测试结果如表 2所示。从表格可以看出，当维数 n 不断增大时，本文 ZKRP 的证明大小增长幅度明显小于 Lyubashevsky 的 ZKRP[23]，在 $n = 512$ 时，前者证明大小已经小于后者，缩减幅度达到了 20.6%。这充分说明，无论维数是高还是低，本文 ZKRP 均有不错的证明大小。除此之外，本文 ZKRP 由于引入了批量处理操作，其在多次证明时具有相当优异的表现。与 Couteau 等人[24]的 ZKRP 相比，当 $n = 1000$ 时，本文 ZKRP 证明大小远小于后者，仅为后者的 9.7%。批量处理操作的引入，可以说是大幅度优化了范围证明在多次证明中的表现，这有利于有效解决实际应用中的多证明处理问题。

2. 时间复杂度

本篇论文采用的 ZKRP 在运行时间上同样具有不错的表现，尤其是面对 GPS 范围证明这种输入数值相对较小的应用场景。

从理论层面分析，双方交互的时间为 $\mathcal{O}(\log n)|\mathbb{F}|$, 证明时间为 $\mathcal{O}(n\log n)$FFT+$\mathcal{O}(\log n)|\mathbb{F}|$, 验证时间为 $\mathcal{O}(n\log n)$FFT+$\mathcal{O}(logn)|\mathbb{F}|$，其中 n 代表向量维数。这些理论数值表明本文采用的 ZKRP 具有良好的时间性能。

表 3 本文 ZKRP 时间性能测试结果

向量维数	范围维数	证明时间（s）	验证时间（s）
32	32	0.0207	0.0041
	128	0.0456	0.0077
	512	0.1855	0.0243
64	32	0.0354	0.0069
	128	0.0755	0.0123
	512	0.2907	0.0400
128	32	0.0638	0.0103
	128	0.1401	0.0197
	512	0.5242	0.0624

本文 ZKRP 的性能测试结果如表 3所示。由表 3可知，当维数 $n=32$，范围维数为 32 时，证明时间为 $0.0207s$，验证时间为 $0.0041s$，处于一个很小的数量级。当维数 n 变为 128，范围维数变为 512 时，证明时间为 $0.5242s$，验证时间为 $0.0624s$, 两者时间明显增大。不过，类似于空间复杂度，由于应用场景中的证明范围并不是很大，范围证明的时间开销也是相对较小的。而在 GPS 范围证明这个应用场景，$[l_{\min},l_{\max}]\subseteq[0,10^6]\Rightarrow L_{\min},L_{\max}\subseteq[0,10^{11}]$，此时证明时间仍处于 10^{-2} 数量级，验证时间仍处于 10^{-3} 数量级。甚至在一般情况，范围可能进一步缩小到 $[l_{\min},l_{\max}]\subseteq[0,10^3]\Rightarrow L_{\min},L_{\max}\subseteq[0,10^8]$，证明时间将进一步减少。而这种数量级的时间显然是可接受的。

（三）安全性分析

考虑系统框架和工作流程，整体系统的安全性主要取决于两个因素：随机距离 R 和用户隐藏的坐标 (x,y)。以下将具体论述这两者的安全性。

随机距离 R 的安全性 考虑随机距离 R 的安全性等效于考虑根据公开参数 x', y', r 能否推出随机距离 R。因为一旦确定 R，那么就可以确定用户坐标 (x, y) 在以公开坐标 (x', y') 为中心，半径为 R 的环上，此时用户的可能坐标范围大幅度缩小，用户坐标的隐私性受到严重威胁。但在本文介绍的系统中，攻击者很难获得随机数 R。原因如下：

在随机距离 R 的生成上，系统选择使用基于椭圆曲线密码的随机数算法。具体生成流程为：首先将时间戳等变化的信息作为算法的种子输入，进而生成一个对应的随机数 R_0。接着根据算法随机数生成范围与系统所需的 R 范围 $[0, \frac{r}{2}]$ 的倍数差 q，进行一次整除的范围缩小处理，得到所需的 R，即 $R = R_0//q$。观察流程，我们可以发现，随机距离 R 的生成实际上仅在最后的范围缩小处理过程中与 r 有关，而生成过程则完全独立与 r。这表明 R 的安全性依靠于伪随机数生成算法的安全性，与公开参数无关。后续证明中 R 作为私密值，安全性再次被零知识证明技术提高。

用户坐标的安全性 在系统中, 用户坐标的隐私性是由零知识范围证明技术保证的。在零知识范围证明中，通过对公开输入 x', y', r 和隐藏输入 (x, y) 进行一系列的数学运算，从而得到 (x, y) 在 (x', y') 一定范围内的零知识证明。由于证明过程是零知识的，即没有透露给验证方任何有效信息，验证方在知晓公开参数 x', y', r 的前提下也不会得到任何关于 (x, y) 的信息，即无法从证明的公开参数、过程和结果中推出隐藏输入 (x, y)。而且本文中的 ZKRP 是后量子安全的，即使面对量子攻击，也拥有一定的抵抗攻击能力。ZKRP 的使用充分保证了用户坐标的安全性，且强度很高。

五、结论与展望

（一）全文总结

随着移动用户数量的增加，基于位置的服务成为一种趋势，用户的位置信息也被频繁地获取。在这一背景下，保护用户位置信息安全的需要变得更加迫切。如何在减少对用户服务质量的影响、保证用户在某些特定情景下不会提交虚假信息的同时，切实保护用户的位置隐私，成为了隐私保护领域研究的一个重要课题。

首先本文对现有位置隐私保护系统的系统结构和应用技术进行了广泛调研，并对现行的 K-匿名隐私保护技术和差分隐私相关技术进行了充分研究。在此基础上，本文认识到现有技术局限性，并希望借助其他技术来弥补这一安全漏洞或是性能瓶颈。

接着本文对区块链中的零知识证明技术、零知识范围证明技术进行了研究，对相关知识、原理进行了充分学习，最终发掘出零知识证明技术在位置隐私保护领域的应用潜力。在此基础上，我们提出将零知识范围证明技术应用到现有的位置隐私保护系统之中，在保护隐私的同时也满足前文所提到的其他服务需求。

在确定这一方向后，本文分别从技术原理上、作品实现上和应用前景上对本文思路进行可行性验证分析。经过多重检验，本文中将零知识范围证明技术应用到位置隐私保护领域的想法具有较高的可行性，应用前景广阔。

本文的成果与贡献主要有以下几方面：

对现有位置隐私保护系统进行多方面改进。使用零知识范围证明技术后，用户不再发送自己的真实位置，这在源头上解决了用户位置隐私泄露的一个隐患，在很大程度上消除了攻击者或者不可信第三方采集用户位置信息的可能。同时，改进后的系统不再需要位置匿名服务器，也不再需要多个移动设备互相协作才能实现匿名效果，这进一步简化了系统结构，减少了当前位置隐私保护系统的很大一部分开销。

拓宽了零知识证明技术的应用场景。虽然零知识证明技术以其零知识性、正确性出名，但在区块链以外的领域，零知识证明技术的应用可谓十分有限。但是经过本文多方面的严谨验证，零知识证明技术的应用场景有望开拓到位置隐私保护领域，乃至其他类型隐私保护、其他行业的各种场景之中。这为零知识证明技术的应用和扩展提供了更多可能。

（二）展望

随着 5G 万物互联的时代到来，智能家居物联网、可穿戴可移动设备的普及会将位置隐私问题泛化到生活的各个角落，用户将越来越享受到位置服务带来的福利，但也一并承担着愈多的泄露个人位置隐私的风险。

可以预见，在目光可及的未来，位置隐私保护仍将是一个经久不衰的课题。在这样的背景下，本文所提及的——将零知识证明技术应用到位置隐私保护领域——或能为解决该问题提供全新的思路。

也需要承认，由于能力有限，本文所构建的位置隐私保护模型仍有进一步提高的空间。但是，我们已经论述和尝试证明了我们的系统的发展潜力和潜在价值，我们的系统有较强的启发性与扩展性，这将是其内在的最大价值。

参考文献

[1] Adepu S, Adler R F. A comparison of performance and preference on mobile devices vs. desktop computers[C]//2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). IEEE, 2016: 1-7.

[2] Bettini C. Privacy protection in location-based services: a survey[J]. Handbook of mobile data privacy, 2018: 73-96.

[3] Liu D, Gao X, Wang H. Location privacy breach: Apps are watching you in background[C]//2017 IEEE 37th international conference on distributed computing systems (ICDCS). IEEE, 2017: 2423-2429.

[4] Jayaraman P P, Yang X, Yavari A, et al. Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation[J]. Future Generation Computer Systems, 2017, 76: 540-549.

[5] Song J H, Wong V W S, Leung V C M. Secure location verification for vehicular ad-hoc networks[C]//IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference. IEEE, 2008: 1-5.

[6] Gruteser M, Grunwald D. Anonymous usage of location-based services through spatial and temporal cloaking[C]//Proceedings of the 1st international conference on Mobile systems, applications and services. 2003: 31-42.

[7] 李梦涵, 钟小宇, 李丽红. 基于位置服务的隐私保护研究 [J]. 信息与电脑 (理论版),2022,34(15):248-250.

[8] Zhu X, Ayday E, Vitenberg R. A privacy-preserving framework for outsourcing location-based services to the cloud[J]. IEEE Transactions on Dependable and Secure Computing, 2019, 18(1): 384-399.

[9] Samarati P, Sweeney L. Generalizing data to provide anonymity when disclosing information[C]//PODS. 1998, 98(188): 10-1145.

[10] Gruteser M, Grunwald D. Anonymous usage of location-based services through spatial and temporal cloaking[C]//Proceedings of the 1st international conference on Mobile systems, applications and services. 2003: 31-42.

[11] McSherry F, Talwar K. Mechanism design via differential privacy[C]//48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07). IEEE, 2007: 94-103.

[12] 张琳, 刘彦, 王汝传. 位置大数据服务中立足于差分隐私的数据发布技术 [J]. 通信学报，2016, 37(9): 46-54.

[13] Wei J, Lin Y, Yao X, et al. Differential privacy-based location protection in spatial crowdsourcing[J]. IEEE Transactions on Services Computing, 2019, 15(1): 45-58.

[14] 张梦凡等.《2022 中国卫星导航与位置服务产业发展白皮书》发布北斗进入规模应用发展新阶段 [EB/OL] . 光明网.（2022—02—19）[2023—04—09].https://tech.gmw.cn/2022-05/19/content_35746711.htm

[15] Merkle R C. A certified digital signature[C]//Advances in cryptology—CRYPTO’89 proceedings. New York, NY: Springer New York, 2001: 218-238.

[16] Zhang J, Xie T, Zhang Y, et al. Transparent polynomial delegation and its applications to zero knowledge proof[C]//2020 IEEE Symposium on Security and Privacy (SP). IEEE, 2020: 859-876.

[17] Bhadauria R, Fang Z, Hazay C, et al. Ligero++: A new optimized sublinear IOP[C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. 2020: 2025-2038.

[18] Ben-Sasson E, Chiesa A, Spooner N. Interactive oracle proofs[C]//Theory of Cryptography: 14th International Conference, TCC 2016-B, Beijing, China, October 31-November 3, 2016, Proceedings, Part II 14. Springer Berlin Heidelberg, 2016: 31-60.

[19] Reingold O, Rothblum G N, Rothblum R D. Constant-round interactive proofs for delegating computation[C]//Proceedings of the forty-eighth annual ACM symposium on Theory of Computing. 2016: 49-62.

[20] Ben-Sasson E, Chiesa A, Riabzev M, et al. Aurora: Transparent succinct arguments for R1CS[C]//Advances in Cryptology–EUROCRYPT 2019: 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19–23, 2019, Proceedings, Part I 38. Springer International Publishing, 2019: 103-128.

[21] Ben-Sasson E, Bentov I, Horesh Y, et al. Fast reed-solomon interactive oracle proofs of proximity[C]//45th international colloquium on automata, languages, and programming (icalp 2018). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.

[22] Camenisch J, Chaabouni R, Shelat A. Efficient protocols for set membership and range proofs[C]//Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2008 (CONF): 234-252.

[23] Lyubashevsky V, Nguyen N K, Seiler G. Practical lattice-based zero-knowledge proofs for integer relations[C]//Proceedings of the 2020 ACM SIGSAC conference on computer and communications security. 2020: 1051-1070.

[24] Couteau G, Klooβ M, Lin H, et al. Efficient range proofs with transparent setup from bounded integer commitments[C]//Advances in Cryptology – EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17 – 21, 2021, Proceedings, Part III. Cham: Springer International Publishing, 2021: 247-277.

[25] Lee, Lap-Piu, and Kwok-Wo Wong. A random number generator based on elliptic curve operations[C]//Computers and Mathematics with Applications 47, no. 2-3 (2004): 217-226.