密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2019, 6(4): 443–454

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

隐私保护的点与任意多边形位置关系判定*

张明武[1,2,3], 冷文韬[1], 沈 华[1]

1. 湖北工业大学 计算机学院, 武汉 430068
2. 桂林电子科技大学 计算机与信息安全学院, 桂林 541004
3. 智能地学信息处理湖北省重点实验室, 武汉 430074

通信作者: 张明武, E-mail: csmwzhang@gmail.com

摘 要: 点与多边形位置关系判定的保密计算是一种非常有用的安全多方计算几何应用, 目前已有的方案仅支持凸多边形的关系判定. 本文提出一种有效隐私保护的点与任意多边形位置关系判定方案. 该方案使用模拟射线的判定法将点与任意多边形位置关系的判定问题转化为任意一条过点的射线与多边形相交点数的奇偶性判定问题. 设计中首先提出一种精简高效的叉积协议, 该协议利用符号位编码将明文空间划分为两个不相交的子空间, 分别用于点的正负坐标到明文空间的映射空间从而实现了支持负数的叉积运算, 然后基于该叉积协议并利用同态加密方案设计一种隐私保护下的点与多边形位置关系的判定协议, 以计算射线与多边形的相交点数, 最后利用模拟范例证明该协议的安全性. 现有点与多边形位置关系判定方案通常只适用于凸多边形的情况, 本文方案不仅能支持对凸多边形的判定且能支持对凹多边形的判定. 模拟实验显示本文提出的叉积协议的运行效率相对于已有的叉积协议提高了 67.5%. 由于避免使用了复杂的密码原语, 本文提出的判断方案获得了线性的计算复杂度和通信开销.

关键词: 安全多方计算; 叉积协议; 点与多边形关系; 同态加密

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000313

中文引用格式: 张明武, 冷文韬, 沈华. 隐私保护的点与任意多边形位置关系判定[J]. 密码学报, 2019, 6(4): 443–454.

英文引用格式: ZHANG M W, LENG W T, SHEN H. Privacy preservation protocol to determine position relation between points and arbitrary-polygons[J]. Journal of Cryptologic Research, 2019, 6(4): 443–454.

Privacy Preservation Protocol to Determine Position Relation Between Points and Arbitrary-polygons

ZHANG Ming-Wu[1,2,3], LENG Wen-Tao[1], SHEN Hua[1]

1. School of Computer Science, Hubei University of Technology, Wuhan 430068, China
2. School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin 541004, China

* 基金项目: 国家自然科学基金 (61672010, 61702168, 61701173); 湖北省自然科学基金面上项目 (2017CFB596); 湖北省教育厅重点项目 (D20181402); 交通物联网技术湖北省重点实验室 (武汉理工大学)(WHUTIOT-2017B001); 广西密码学与信息安全重点实验室 (GCIS201717); 智能地学信息处理湖北省重点实验室开放课题 (KLIGIP-2017A11)

Foundation: National Natural Science Foundation of China (61672010, 61702168, 61701173); General Project of Natural Science Foundation of Hubei Province (2017CFB596); Key Project of Hubei Provincial Department of Education Key Project (D20181402); Hubei Key Laboratory of Transportation Internet of Things Technology (Wuhan University of Technology) (WHUTIOT-2017B001); Guangxi Key Laboratory of Cryptography and Information Security (GCIS201717); Open Fund of Hubei Key Laboratory of Intelligent Geo-Information Processing (KLIGIP-2017A11)

收稿日期: 2018-08-04 定稿日期: 2019-02-22

3. Hubei Key Laboratory of Intelligent Geo-Information Processing, Wuhan 430074, China
Corresponding author: ZHANG Ming-Wu, E-mail: csmwzhang@gmail.com

Abstract: Privacy-preserving evaluation of geometric position relation between points and polygons is a useful and practical tool in secure multiparty geometric evaluations. However, existing protocols only support the determination between points and concave-polygons. In this work, a privacy-preserving determining relation protocol between points and arbitrary polygons is proposed, which employs the conversion technique of points and polygons into a parity decision problem in which a ray, i.e., starting from the point and going in any fixed direction, intersects the edges of the corresponding polygon. First, a streamlined and efficient cross-product protocol is constructed, which employs the coding technique of dividing the plaintext space into two disjoint subspaces, so that it supports the mapping space from positive and negative coordinates to the plaintext space. Based on the proposed cross-product protocol and homomorphic encryption scheme, a privacy-preserving determining relationship between points and polygon positions is designed, which can calculate the intersection point between the ray and the polygon. Compared with the known results, the proposed protocol supports the determination of convex polygons and implements the determination of concave polygons. Simulation experiments show that relating to the existing cross product protocol, the operating efficiency of the proposed cross product protocol improves by 67.5%. By avoiding to use complex cryptographic primitives, the proposed scheme achieves linear computational complexity and communication overhead.

Key words: secure multi-party computation; cross-product protocol; point and concave-polygon; homomorphic encryption

1 引言

随着移动互联网和大数据相关技术的不断发展, 人类社会的信息量越来越多, 隐私问题日益突出. 例如, 为了让企业领导者了解员工是否到达指定的工作区域, 员工需要报告自己的具体坐标位置, 同时员工也被告知工作区域的具体信息. 员工的具体坐标位置属于员工的个人隐私信息, 工作区域的具体信息属于企业的隐私信息, 因此, 上述应用场景中存在隐私泄漏问题. 如何在不泄漏员工隐私信息和企业隐私信息的条件下企业领导者可以了解掌握员工到达指定工作区域的情况, 是一个亟待解决的问题. 在另外一个应用场景中, 某个调查机构需要调查统计指定区域的车流量情况, 为了保证调查的有效性该调查机构必须保密被调查区域的信息同时利用车辆的位置信息得到统计结果. 车辆的位置信息属于车辆使用者的隐私信息, 因此, 该应用场景中也存在隐私泄漏问题. 如何在不泄漏车辆位置信息和被调查区域信息的条件下调查机构获得该区域的车流量情况, 也是一个值得研究的问题. 上述这些问题可以被抽象为具有具有隐私保护的点与多边形关系判定问题, 该问题主要涉及到具有隐私保护的多方几何计算. 具有隐私保护的多方几何计算属于安全多方计算 (secure multi-party computation, SMC) [1–3] 研究领域. SMC 实现了在分布式环境下, 多个互不信任的参与者在不泄漏自己输入的前提下协作完成指定的计算. SMC 的具体应用领域主要有: 数据挖掘 [4]、计算几何 [5]、比特币交易 [6] 等.

点与多边形的位置关系判定 [7](point-in-polygon problem, PIPP) 是计算几何中的常见问题. 解决该问题的方法有射线法 [8] 和面积法以及夹角法 [9] 等. 其中射线法是指, 通过判定点引出一条射线, 计算该射线与多边形的交点数, 若交点的数为奇数, 则坐标点在多边形内部, 否则坐标点在多边形外 [8]. 在具有隐私保护的点与多边形关系判定问题中, 参与双方中的一方拥有一个点另一方拥有一个构成多边形的顶点集合, 在不泄漏各自输入信息的前提下, 双方协作完成点与多边形的位置关系判定, 并且双方也无法从判定结果中推测出对方的输入. 文献 [2] 基于 Monte Carlo 方法和 Cantor 编码设计了点包含与图形包含问题的近似解决方案, 该方案将问题转化为集合包含问题, 利用了可交换加密, 是一种近似求解问题的方法, 其精度与复杂度成正比, 存在一定误差. 点包含问题是指, 判断判定点是否位于指定区域内. 点包含问题

是点与多边形位置关系中的一种. 文献 [5] 基于安全两方点积协议和向量控制协议, 首次解决了安全两方点包含问题, 该方案调用了数次百万富翁协议, 导致协议的复杂度较高. 文献 [10] 将点包含问题转化为三角形面积问题, 并基于内积协议给出解决三角形面积问题的方案. 该方案受制于问题转化方法的局限性并不适用于凹多边形的情况. 文献 [11] 提出了一种茫然安全点线位置关系判断协议, 并利用该协议解决了点包含问题, 该方法基于茫然传输和百万富翁协议, 其效率不高, 并且无法适用于复杂的任意多边形. 文献 [12] 基于内积协议设计了一种具有隐私保护的点与直线距离的计算协议, 解决了隐私保护的直线与圆圈的相交问题. 文献 [13] 提出了安全的两方向量叉积协议以及安全的点与线叉积协议, 协议必须调用百万富翁协议, 其复杂度与多边形的边数有关, 且仅支持普通凸多边形. 文献 [14] 在云外包环境下将点与面的位置关系等转化为夹角问题, 并设计了基于云外包条件的内积协议, 但该协议无法适用于任意多边形情况. 文献 [15] 使用角度旋转法解决了点与多边形的关系判定问题, 该方案虽然解决了点与任意多边形的关系判定, 然而其计算复杂度较高. 由于实际应用中人们往往面临的是点与凹凸多边形结合的复杂图形的位置关系判定, 因此, 研究和设计点与任意多边形的位置关系判定协议具有很重要的应用价值. 但目前缺少高效安全地求解点与任意多边形关系判定问题的方案.

针对上述问题, 本文首先基于文献 [12] 提出的编码方式设计了一种精简高效的叉积协议, 该协议实现了具有隐私保护的点与直线相对位置的判定, 然后在该叉积协议的基础之上本文结合射线法提出了一种具有隐私保护的点与任意多边形关系判定方案.

本文的主要贡献有: (1) 提出了一种具有隐私保护的点与任意多边形关系判定的方案, 该方案同时适用于凸多边形与凹多边形的情况. (2) 设计了一种高效的叉积协议, 该协议基于明文空间数域划分的思想实现了支持负数的叉积运算, 提升了判定方案的效率. (3) 提出了一种高效的转化方法, 将点与任意多边形位置关系的判定问题转化为任意一条过点的射线与多边形相交的点数奇偶性的判定问题.

2 设计目标及安全性定义

2.1 安全性定义

本文的安全目标是, 参与计算的两方均无法获得对方的输入信息. 本文在半诚实参与者安全模型下达到该安全目标. 半诚实参与者是指能够严格遵守协议的执行指令, 在协议的执行过程中记录所有得到的中间结果并企图根据自己获得的信息推测出额外信息的参与者. 基于该安全模型, 如果参与者可以利用自己的输入和协议的输出单独模拟整个协议的执行过程并且在此过程中得不到任何额外的信息, 那么该协议就能保证参与者输入的安全性. 上述安全性的形式化定义如下:

假设两个参与者要计算函数 $f:\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^*\times\{0,1\}^*$, 其中 $f_1(x,y)$ 和 $f_2(x,y)$ 分别代表 f 的第一个元素和第二个元素; π 表示计算 f 的协议; S_1 和 S_2 是两个多项式时间算法, 它们作为模拟器模拟协议的执行过程. $S_i(x,f(x,y))$ 表示模拟器以第 i 个参与者的输入和协议的输出作为参数模拟协议的执行过程, $\mathrm{view}_i^{\pi}(x,y)$ 表示第 i 个参与者的视图, $\mathrm{output}_i^{\pi}(x,y)$ 表示第 i 个参与者执行协议得到的结果, 其中 $i=1,2$. 对于确定性功能函数 f, 我们称协议 π 在半诚实模型下秘密的计算 f 当且仅当 S_1 和 S_2 是使得

$$\{S_1(x,f(x,y))\}_{x,y\in\{0,1\}^*}\overset{c}{\equiv}\{\mathrm{view}_1^{\pi}(x,y)\}_{x,y\in\{0,1\}^*} \tag{1}$$

$$\{S_2(y,f(x,y))\}_{x,y\in\{0,1\}^*}\overset{c}{\equiv}\{\mathrm{view}_2^{\pi}(x,y)\}_{x,y\in\{0,1\}^*} \tag{2}$$

其中 $|x|=|y|$.

2.2 设计目标

基于上述安全模型, 本文设计目标是提出一种具有隐私保护的、高效的点与任意多边形关系判定方案. 具体来说, 提出的方案需要达到下述设计目标:

(1) 安全性. 通过执行方案, 双方在不知道对方输入信息的情况下协作完成点与多边形的位置关系判定, 并且双方也无法从判定结果中推测出对方的输入, 即方案必须满足2.1节提出的安全性要求.

(2) 正确性. 对在凸多边形内或外的任何点, 方案都能得到正确的判定结果; 对在凹多边形内或外的任何点, 方案都能得到正确的判定结果. 即, 针对任意多边形, 方案都能够正确判定点和多边形的位置关系.

(3) 高效性. 为更具实用性, 方案应有效减少参与双方之间的通信开销和每个参与方的计算开销.

3 预备知识

3.1 叉积

设 $\overrightarrow{oa}$ 和 $\overrightarrow{ob}$ 是如图1所示的两向量, 其中点 $a=(x_a,y_a)$, $b=(x_b,y_b)$, $o=(0,0)$. $\overrightarrow{oa}$ 和 $\overrightarrow{ob}$ 的叉积 [16] 记为 $\overrightarrow{oa}\times\overrightarrow{ob}$, 定义为:

$$\overrightarrow{oa}\times\overrightarrow{ob}=\begin{vmatrix} x_a-0 & y_a-0 \\ x_b-0 & y_b-0 \end{vmatrix}=x_ay_b-x_by_a$$

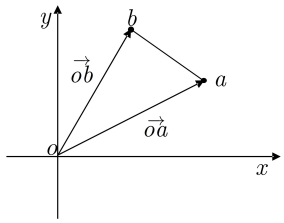

图 1 叉积定义

Figure 1 Definition of cross product

3.2 同态加密

同态加密是一种允许对密文进行计算的一类加密算法. 在将明文加密后, 对密文进行有限的加法或乘法运算后仍可以解密, 解密后的结果与对明文的操作是一致的, 从而达到对密文数据计算的目的. Paillier 公钥密码系统 [17] 是一种常见的同态加密算法, 其主要包括三个算法: 密钥产生算法 (Gen)、加密算法 (Enc) 和解密算法 (Dec). 该加密算法的同态性主要体现在以下方面:

$$\mathrm{Dec}\left(\mathrm{Enc}\left(m_1,r_1\right)\cdot\mathrm{Enc}\left(m_2,r_2\right)\right)=m_1+m_2 \tag{3}$$

$$\mathrm{Dec}\left(\mathrm{Enc}\left(m_1,r_1\right)^{m_2}\right)=m_1m_2 \tag{4}$$

其中 m_1 和 m_2 是消息空间中的两个消息, r_1 和 r_2 是两个随机数.

3.3 点与直线位置关系

文献 [16] 已证明点与直线的位置关系等价于求点与直线的叉积, 可以通过求点与直线的叉积来判断点与直线的位置关系. 点 $p_0=(x_0,y_0)$ 与直线 $\overline{p_1p_2}$ 的关系 (其中 $p_1=(x_1,y_1)$, $p_2=(x_2,y_2)$) 定义如下.

定义 1 (点与直线的关系) 计算点 p_0 与直线 $\overline{p_1p_2}$ 的叉积

$$\begin{aligned}\overline{p_1p_2}\times\overline{p_1p_0}&=\begin{pmatrix} x_0-x_1 & x_1-x_2 \\ y_0-y_1 & y_1-y_2 \end{pmatrix}\\ &=(x_0-x_1)(y_1-y_2)-(x_1-x_2)(y_0-y_1)\\ &=x_0y_1-x_0y_2-y_0x_1+y_0x_2+x_1y_2-x_2y_1\end{aligned} \tag{5}$$

如果 $\overline{p_1p_2}\times\overline{p_1p_0}>0$, 那么点 p_0 在直线 $\overline{p_1p_2}$ 的下方; 如果 $\overline{p_1p_2}\times\overline{p_1p_0}=0$, 那么点 p_0 与直线 $\overline{p_1p_2}$ 共线; 如果 $\overline{p_1p_2}\times\overline{p_1p_0}<0$, 那么点 p_0 在直线 $\overline{p_1p_2}$ 的上方. 利用符号函数:

$$\mathrm{Sgn}(x)=\begin{cases}1, & x>0\\ 0, & x=0\\ -1, & x<0\end{cases} \tag{6}$$

将点与直线的位置关系表示为:

$$H_{p_0\in\overline{p_1p_2}}=\mathrm{Sgn}\left(\overrightarrow{p_1p_2}\times\overrightarrow{p_1p_0}\right)=\begin{cases}1, & p_0\text{在}\overline{p_1p_2}\text{下方}\\ 0, & p_0\text{与}\overline{p_1p_2}\text{共线}\\ -1, & p_0\text{在}\overline{p_1p_2}\text{下方}\end{cases} \tag{7}$$

3.4 点与任意多边形的位置关系

文献 [18] 给出并证明了关于点与任意多边形位置关系的如下定理.

定理 1 点与任意多边形的位置关系等价于过判定点的任意射线与任意多边形相交的点数, 若相交点数为奇数则判定点在多边形内, 否则在多边形外.

4 隐私保护的点与多边形关系判定

4.1 问题描述和转化

4.1.1 问题描述

设 Alice 拥有一个点 $p_0=(x_0,y_0)$, Bob 拥有一个由 n 个顶点 $\{p_1=(x_1,y_1),p_2=(x_2,y_2),\cdots,p_n=(x_n,y_n)\}$ 构成的任意多边形 P, 在不泄漏双方各自信息的情况下, Alice 和 Bob 协作判断 Alice 拥有的点 p_0 是否在 Bob 的任意多边形 P 内.

4.1.2 问题转化

本文基于模拟射线法的思路将点与任意多边形位置关系的判定问题转化为任意一条过点的射线与多边形相交点数的奇偶性判定问题. 为了便于描述, 本文提出了同侧点的概念, 其定义如下.

定义 2 (同侧点) 经过点的直线等价于两条以该点为顶点并且方向相反的射线, 其中同一条射线上的点称作该点的同侧点.

基于同侧点的概念, 本文给出了实现问题转化的定理.

定理 2 过判定点作直线, 直线与多边形的交点中同侧点的数量等价于过判定点射线与多边形的交点数, 若交点数为奇数则判定点在多边形内, 否则判定点在多边形外.

证明: 已知一条直线可被判定点划分为两条方向相反的射线, 若直线与多边形相交, 显然这些交点分别存在于两条方向相反的射线上, 因此可统计得到判定点的同侧点数, 由定理1结论可知定理2成立. □

定理 3 若多边形的顶点全部位于直线的同一侧, 则直线与多边形不相交.

证明: 假设直线与多边形相交, 那么必定存在一个顶点在直线上或在直线的另一侧, 命题得证. □

定理 4 过判定点做任意一条直线, 若直线与多边形不相交, 则判定点必定在多边形外.

证明: 假设判定点在多边形内, 过判定点任意做一条直线, 由于直线的性质其必定会与多边形相交, 因此假设不成立, 命题得证. □

基于定理2–4, 点与任意多边形位置关系的判定被转化为任意一条过点的射线与多边形相交点数的奇偶性判定. 例如, 图2和图3中的点 p_0 和任意多边形的相对位置可以通过统计点 p_0 的同侧点数并根据同侧点的奇偶性得到.

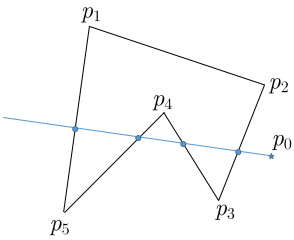

图 2 点 p_0 在多边形外

Figure 2 Example of a point outside a polygon

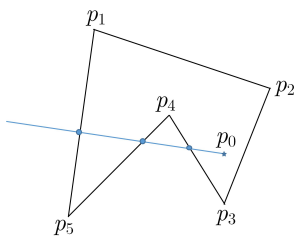

图 3 点 p_0 在多边形内

Figure 3 Example of a point inside a polygon

为了方便表达, 定义如下谓词:

$$f(p_0,P)=\begin{cases}1, & 点p_0在多边形P内部\\ 0, & 点p_0在多边形P外部\end{cases} \tag{8}$$

根据定义1可知叉积协议是一种用来解决点与直线位置关系判定的工具, 文献 [16] 中提出的具有隐私保护的叉积协议虽然能保密的判定点与直线的位置关系, 但是其需要调用复杂度较高的密码学原语. 本文设计了一个轻量级的叉积协议用于判定点与直线的位置关系. 针对任意一条过点的射线与多边形相交点数的奇偶性判定问题, 基于该轻量级叉积协议, 本文给出的判定方案包括 3 个步骤.

步骤 1: 首先任取一点 p' 与判定点 p_0 组成一条直线 $\overline{p_0p'}$;

步骤 2: 根据叉积协议, 计算得到多边形 P 的顶点与直线 $\overline{p_0p'}$ 的相对位置关系, 从而找出多边形与直线 $\overline{p_0p'}$ 相交的所有边;

步骤 3: 根据叉积协议, 计算得到判定点 p_0 与相交边的相对位置关系, 从而获得以判定点为顶点的同侧点数, 若同侧点数为奇数则判定点 p_0 在多边形 P 的内部, 若为偶数则判定点 p_0 在多边形 P 的外部.

4.2 具体方案

本文提出的具有隐私保护的点与任意多边形位置关系的判定方案包括两个协议: 具有隐私保护的点与直线位置关系判定协议和具有隐私保护的点与任意多边形位置关系的判定协议. 首先由 Alice 和 Bob 分别根据安全参数生成各自的 Paillier 加密算法的公私钥对 $(\mathrm{PK}_A,\mathrm{SK}_A)$ 和 $\mathrm{PK}_B,\mathrm{SK}_B$, 然后 Alice 和 Bob 执行具有隐私保护的点与任意多边形位置关系的判定协议, 使得 Alice 和 Bob 在保证自己的输入信息不被泄漏的情况下均知道点 p_0 是否在多边形 P 中. 在执行点与任意多边形位置关系的判定协议的过程中, 具有隐私保护的点与直线位置关系判定协议将被调用以协助完成点与任意多边形位置关系的判定. 本文使用文献 [12] 中支持符号位的编码方式, 对于明文空间 $\{0,1,\cdots,T\}$, 设 $L=\lfloor\log T\rfloor+1$, 将明文空间中的元素表示成长度为 L 的二进制数, 将其中的第 L 位视为符号位. 根据符号位的值, 本文将明文空间分成正负两个部分. L 为 1 的元素构成明文空间的负数空间, L 为 0 的元素构成明文空间的正数空间. 点的坐标范围为 $[-T/2,T/2]$. 当点坐标落在范围 $[0,T/2]$ 内时, 将该坐标映射到明文空间的正数空间, 此时只需直接映射即可; 当点坐标落在范围 $[-T/2,0)$ 内时, 将该坐标映射到明文空间的负数空间, 此时通过将坐标值加上 T 进行映射. 协议的具体内容描述如下.

协议 1 隐私保护的点与直线位置关系判定

输入: 点 $p_0'(x_0',y_0')$, 直线 $\overline{p_1'p_2'}$, 其中直线经过点 $p_1'(x_1',y_1')$, $p_2'(x_2',y_2')$.

输出: 执行协议双方得到 p_0' 点与直线 $\overline{p_1'p_2'}$ 的位置关系.

为了叙述的方便, 将点 p_0' 的拥有者的公私钥分别记为 $\mathrm{PK}_{p_0'}$ 和 $\mathrm{SK}_{p_0'}$.

步骤 1. 点 p_0' 的拥有者基于自己公钥 $\mathrm{PK}_{p_0'}$ 利用加密算法 Enc 对点 p_0' 进行加密, 得密文集合 $C_{p_0'}$:

$$\begin{gathered}C_{p_0'}=(C_1,C_2,C_3,C_4),C_1=\mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(x_0'\right),C_2=\mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(T-x_0'\right),\\ C_3=\mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(T-y_0'\right),C_4=\mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(y_0'\right)\end{gathered} \tag{9}$$

步骤 2. 点 p_0' 的拥有者将 $C_{p_0'}$ 发送给直线 $\overline{p_1'p_2'}$ 的拥有者, 直线 $\overline{p_1'p_2'}$ 的拥有者选取随机数 r 并做如下计算:

$$\begin{aligned}
M &= C_1^{y_1'} \cdot C_2^{y_2'} \cdot C_3^{x_1'} \cdot C_4^{x_2'} \cdot \mathrm{Enc}_{\mathrm{PK}_{p_0'}}(r) \\
&= \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(x_0'\right)^{y_1'} \cdot \mathrm{Enc}_{\mathrm{pK}_{p_0'}}\left(T-x_0'\right)^{y_2'} \cdot \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(T-y_0'\right)^{x_1'} \cdot \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(y_0'\right)^{x_2'} \cdot \mathrm{Enc}_{\mathrm{pK}_{p_0'}}(r) \\
&= \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(x_0'y_1' + \left(T-x_0'\right)y_2' + \left(T-y_0'\right)x_1' + x_2'y_0' + r\right) \\
W &= \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(x_1'y_2'\right) \\
K &= \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(T\left(y_2'+x_1'\right) + x_2'y_1' + r\right)
\end{aligned} \tag{10}$$

并将计算结果 (M, W, K) 发送给点 p_0' 的拥有者.

步骤 3. 点 p_0' 的拥有者接收到 (M, W, K) 后做如下计算.

$$H_{p_0'\&\overline{p_1'p_2'}} = \mathrm{Sgn}\left(\mathrm{Dec}_{\mathrm{SK}_{p_0'}}(M) + \mathrm{Dec}_{\mathrm{SK}_{p_0'}}(W) - \mathrm{Dec}_{\mathrm{SK}_{p_0'}}(K)\right) \tag{11}$$

步骤 4. 点 p_0' 的拥有者将结果 $H_{p_0'\&\overline{p_1'p_2'}}$ 告诉直线 $\overline{p_1'p_2'}$ 的拥有者.

将上述协议1的执行记为 $H_{p_0'\&\overline{p_1'p_2'}} = g\left(p_0', \overline{p_1p_2}\right)$.

协议 2 隐私保护的点与任意多边形位置关系判定

输入: Alice 拥有点 $p_0\left(x_0, y_0\right)$, Bob 拥有多边形 $P = \{p_j\left(x_j, y_j\right), j \in (1, \cdots, n)\}$.

输出: Alice 和 Bob 均得到点 $p_0\left(x_0, y_0\right)$ 与多边形 P 的位置关系.

步骤 1. Alice 随机选取点 $p'\left(x', y'\right)$, 构造直线 $\overline{p_0p'}$.

步骤 2. 以直线 $\overline{p_0p'}$ 和多边形的顶点 $p_j\left(x_j, y_j\right)$ 作为输入, 使用 Bob 的公钥执行协议1, 即 $H_{p_j'\&\overline{p_0p'}} = g\left(p_j', \overline{p_0p'}\right)$, 其中 $j = 1, 2, \cdots, n$, 协议被执行了 n 次, 将 n 次执行得到的结果记为 $R = \{H_{p_1\&\overline{p_0p'}}, H_{p_2\&\overline{p_0p'}}, \cdots, H_{p_n\&\overline{p_0p'}}\}$.

步骤 3. Bob 在 R 中筛选出满足下述 Cross 条件的元素组 $\left(H_{p_j\&\overline{p_0p'}}, H_{p_{j+1}\&\overline{p_0p'}}\right)$, 其中 $1 \leqslant j < n$.

$$\mathrm{Cross} = \{(-1,1), (1,-1), (0,1), (0,-1), (-1,0), (1,0), (0,0)\} \tag{12}$$

如果 $\left(H_{p_j\&\overline{p_0p'}}, H_{p_{j+1}\&\overline{p_0p'}}\right)$ 等于 (–1, 1) 或 (1, –1), 则意味着点 p_j 和 p_{j+1} 点位于直线 $\overline{p_0p'}$ 的两侧;

如果 $\left(H_{p_j\&\overline{p_0p'}}, H_{p_{j+1}\&\overline{p_0p'}}\right)$ 等于 (0, 1) 或 (0, –1), 则意味着点 p_j 位于直线 $\overline{p_0p'}$ 上同时点位于直线 $\overline{p_0p'}$ 的一侧;

如果 $\left(H_{p_j\&\overline{p_0p'}}, H_{p_{j+1}\&\overline{p_0p'}}\right)$ 等于 (–1, 0) 或 (1, 0), 则意味着点 p_{j+1} 位于直线 $\overline{p_0p'}$ 上同时点 p_j 位于直线 $\overline{p_0p'}$ 的一侧;

如果 $\left(H_{p_j\&\overline{p_0p'}}, H_{p_{j+1}\&\overline{p_0p'}}\right)$ 等于 (0, 0), 则意味着点 p_j 和 p_{j+1} 点位于直线 $\overline{p_0p'}$ 上.

将所有满足 Cross 条件的元素组对应点构成的直线构成的集合记为 I_{Cross}, 即 $I_{\mathrm{Cross}} = \{\overline{p_lp_{l+1}} | (H_l, H_{l+1}) \in \mathrm{Cross}\}$, 其中 $1 \leqslant j < n$. 注意, 如果 $\left(H_{p_n\&\overline{p_0p'}}, H_{p_1\&\overline{p_0p'}}\right) \in \mathrm{Cross}$, 那么 $\overline{p_np_1} \in I_{\mathrm{Cross}}$. 显然有 $|I_{\mathrm{Cross}}| = k < n$. 若 $|I_{\mathrm{Cross}}| = 0$, 则 $\overline{p_0p'}$ 与多边形 P 不相交, 点 p_0 在多边形 P 外, 协议结束, 否则继续下面的步骤.

步骤 4. 以点 p_0 和线段 $\overline{p_lp_{l+1}} \in I_{\mathrm{Cross}}$ 作为输入, 使用 Alice 的公钥执行协议1, 即 $H_{p_0\&\overline{p_lp_{l+1}}} = g\left(p_0, \overline{p_lp_{l+1}}\right)$. 协议被执行了 $|I_{\mathrm{Cross}}|$ 次, 将 $|I_{\mathrm{Cross}}|$ 次执行得到的结果记为 $R' = \left\{H_{p_0\&\overline{p}_lp_{l+1}} | \overline{p_lp_{l+1}} \in \mathrm{Cross}\right\}$. 若 $\exists 0 \in R'$, 则点 p_0 在多边形 P 内, 即 $f\left(p_0, P\right) = 1$; 若 R' 中 –1 或 1 的个数为奇数, 则 p_0 点在多边形 P 内, 即 $f\left(p_0, P\right) = 1$; 若 R' 中 –1 或 1 的个数为偶数, 则 p_0 点在多边形 P 外, 即 $f\left(p_0, P\right) = 0$.

步骤 5. Alice 将结果 $f(p_0, P)$ 发送给 Bob.

5 正确性及安全性证明

5.1 正确性

5.1.1 协议1正确性分析

协议1的目标是安全计算如下公式:

$$\overline{p_1p_2} \times \overline{p_1p_0} = x_0y_1 - x_0y_2 - y_0x_1 + y_0x_2 + x_1y_2 - x_2y_1 \tag{13}$$

由加密同态性可得:

$$\mathrm{Enc}(-x_0)^{y_0} = \mathrm{Enc}(T - x_0)^{y_0} = \mathrm{Enc}(Ty_0 - x_0y_0) \tag{14}$$

显然, 当把负值映射到明文空间的负值空间后, 对其进行同态运算会导致明文数值上的偏移. 协议1将公式(13)中的减法运算均安排在解密之后进行, 保证加密过程中的明文为正数.

$$\begin{aligned}\overline{p_1p_2} \times \overline{p_1p_0} &= \mathrm{Dec}(M) + \mathrm{Dec}(W) - \mathrm{Dec}(K)\\ &= (x_0y_1 + (T - x_0)y_2 + (T - y_0)x_1 + x_2y_0 + r) + (x_1y_2) - (T(y_2 + x_1) + x_2y_1 + r)\\ &= x_0y_1 - x_0y_2 - y_0x_1 + y_0x_2 + x_1y_2 - x_2y_1\end{aligned} \tag{15}$$

因此, 协议1能够得到正确的计算结果.

5.1.2 协议2正确性分析

将点 p_0 与随机选取的点 p' 确定的直线 $\overline{p_0p'}$ 与多边形 P 的顶点作为输入, 执行协议1得到多边形 P 的各个顶点与直线 $\overline{p_0p'}$ 的位置关系, 即集合 R. 基于5.1.1的证明可以保证集合 R 的正确性. 若 R 中的元素全部为 1 或 –1, 则意味着多边形 P 的全部顶点均位于直线 $\overline{p_0p'}$ 的同一侧, 说明直线 $\overline{p_0p'}$ 与多边形 P 不相交, p_0 在多边形 P 的外部, 协议结束. 若 R 中的元素不全部为 1 或 –1, 则说明直线与多边形相交, 即 $|I_{\text{Cross}}| \neq 0$. I_{Cross} 中的直线与直线 $\overline{p_0p'}$ 相交, 以点 p_0 和 I_{Cross} 中的直线作为输入执行协议1, 根据执行结果可以推测出直线 $\overline{p_0p'}$ 与多边形 P 相交的点数, 即点 p_0 的同侧点的个数. 基于5.1.1的证明可以保证该同侧点的个数的正确性. 根据获得的同侧点的个数, 基于定理1可以推断出点 p_0 是在多边形 P 的内部还是外部. 同侧点个数的正确性及文献 [18] 对定理1的证明可以保证推断结论的正确性.

下面讨论点在多边形上的特殊情况, 点在多边形任意一条边上被认定为点在多边形内. 不妨假设点 p_0 位于直线 $\overline{p_lp_{l+1}} \in I_{\text{Cross}}$ 上, 根据定义1可知 $H_{p_0\varepsilon\overline{p_lp_{l+1}}} = 0$, 以点 p_0 与直线 $\overline{p_lp_{l+1}}$ 为输入执行协议1, 基于5.1.1的证明可知协议1的输出结果为 0, 根据协议2, 因为 $\exists 0 \in R'$, 所以点 p_0 在多边形 P 内, 协议2的输出结果是正确的.

5.2 安全性证明

5.2.1 协议1安全性证明

$g_1\left(p_0', \overline{p_1'p_2'}\right)$ 表示执行协议1后点 p_0' 的拥有者的结果, $g_2\left(p_0', \overline{p_1'p_2'}\right)$ 表示执行协议1后直线 $\overline{p_1'p_2'}$ 的拥有者的结果.

$$H_{p_0', \&\overline{p_1'p_2'}} = g_1\left(p_0', \overline{p_1'p_2'}\right) = g_2\left(p_0', \overline{p_1'p_2'}\right) \tag{16}$$

构造模拟器 S_1 模拟直线 $\overline{p_1'p_2'}$ 的拥有者的协议执行过程, 构造模拟器 S_1 随机选取 $p_0^*(x_0^*, y_0^*)$, 使得

$$H_{p_0', \&\overline{p_1'p_2'}} = g_1^*\left(p_0^*, \overline{p_1'p_2'}\right) = g_2\left(p_0', \overline{p_1'p_2'}\right) \tag{17}$$

构造模拟器 S_1 使用自己的公钥 $\mathrm{PK}_{p_0'}$ 进行如下加密操作:

$$C_{p_0^*} = (C_1^*, C_2^*, C_3^*, C_4^*) = \left(\mathrm{Enc}_{\mathrm{PK}_{p_0'}}(x_0^*), \mathrm{Enc}_{\mathrm{PK}_{p_0'}}(T - x_0^*), \mathrm{Enc}_{\mathrm{PK}_{p_0'}}(T - y_0^*), \mathrm{Enc}_{\mathrm{PK}_{p_0'}}(y_0^*)\right) \tag{18}$$

构造模拟器 S_1 选择随机数 $r'\,(r'\neq 0,1)$, 进行如下计算:

$$\begin{aligned}M^* &= C_1^{*y_1}\cdot C_2^{*y_2}\cdot C_3^{*x_1}\cdot C_4^{*x_2}\cdot \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(r'\right)\\ &= \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(x_0^*\right)^{y_1}\cdot \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(T-x_0^*\right)^{y_2}\cdot \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(T-y_0^*\right)^{x_1}\cdot \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(y_0^*\right)^{x_2}\cdot \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(r'\right)\\ &= \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(x_0^*y_1+\left(T-x_0^*\right)y_2+\left(T-y_0^*\right)x_1+x_2y_0^*+r'\right)\\ W &= \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(x_1y_2\right)\\ K &= \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(T(y_2+x_1)+x_2y_1+r'\right)\end{aligned}\tag{19}$$

模拟结束.

显然, 我们可以得到:

$$S_1\left(p_0',\overline{p_1'p_2'}\right)=\left\{p_1',p_2',C_{p_0^*},M^*,W,K,H\right\},\quad \mathrm{view}_1\left(p_0',\overline{p_1'p_2'}\right)=\left\{p_1',p_2',C_{p_0'},M,W,K,H\right\}\tag{20}$$

因为 $H_{p_0'\&\overline{p_1'p_2'}}=g_1^*\left(p_0^*,\overline{p_1'p_2'}\right)=g_2\left(p_0',\overline{p_1'p_2'}\right)$, 所以 $C_{p_0'}$ 与 $C_{p_0^*}$ 不可区分、M^* 和 M 不可区分, 故 S_1 与 view_1 不可区分.

构造模拟器 S_2 模拟点 p_0' 的拥有者的执行过程. 构造模拟器 S_2 随机选取 $\overline{p_1^*p_2^*}$, 其中 $p_1^*\left(x_1^*,y_1^*\right)$, $p_2^*\left(x_2^*,y_2^*\right)$ 使得

$$H_{p_0'\&\overline{p_1'p_2'}}=g_2^*\left(p_0',\overline{p_1^*p_2^*}\right)=g_1\left(p_0',\overline{p_1'p_2'}\right)\tag{21}$$

构造模拟器 S_2 使用公钥 $\mathrm{PK}_{p_0'}$ 进行如下加密操作:

$$C_{p_0'}=\left(\mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(y_0'\right),\mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(-x_0'\right),\mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(-y_0'\right),\mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(x_0'\right)\right)\tag{22}$$

构造模拟器 S_2 选择随机数 $r^*\,(r^*\neq 0,1)$, 计算:

$$\begin{aligned}M^* &= C_1^{y_1^*}\cdot C_2^{y_2^*}\cdot C_3^{x_1^*}\cdot C_4^{x_2^*}\cdot \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(r^*\right)\\ &= \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(x_0'\right)^{y_1^*}\cdot \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(T-x_0'\right)^{y_2^*}\cdot \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(T-y_0'\right)^{x_1^*}\cdot \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(y_0'\right)^{x_2^*}\cdot \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(r^*\right)\\ &= \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(x_0'y_1^*+(T-x_0')y_2^*+(T-y_0')x_1^*+x_2^*y_0'+r^*\right)\\ W^* &= \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(x_1^*y_2^*\right)\\ K^* &= \mathrm{Enc}_{\mathrm{PK}_{p_0'}}\left(T(y_2^*+x_1^*)+x_2^*y_1^*+r^*\right)\\ H_{p_0'\&\overline{p_1'p_2'}} &= \mathrm{Sgn}\left(\mathrm{Dec}_{\mathrm{SK}_{p_0'}}(M^*)+\mathrm{Dec}_{\mathrm{SK}_{p_0'}}(K^*)-\mathrm{Dec}_{\mathrm{SK}_{p_0'}}(W^*)\right)\end{aligned}\tag{23}$$

模拟结束.

显然, 可以得到

$$S_2\left(p_0',\overline{p_1'p_2'}\right)=\left\{p_0',C_{p_0'},M^*,W^*,K^*,H\right\},\quad \mathrm{view}_2\left(p_0',\overline{p_1'p_2'}\right)=\left\{p_0',C_{p_0'},M,W,K,H\right\}\tag{24}$$

因为 $H_{p_0'\&\overline{p_1'p_2'}}=g_2^*\left(p_0',\overline{p_1^*p_2^*}\right)=g_1\left(p_0',\overline{p_1'p_2'}\right)$, 所以 M^* 和 M 不可区分, W^* 和 W 不可区分, K^* 和 K 不可区分, 故 S_2 与 view_2 不可区分.

上述证明过程说明协议1是隐私保护安全的.

5.2.2 协议2的安全性证明

协议2安全性要求, Alice 和 Bob 执行完协议2后, Alice 在不泄漏自己拥有的点 p_0 信息和 Bob 在不泄漏自己拥有多边形 P 的信息的情况下, Alice 和 Bob 均知道点 p_0 与多边形 P 的相对位置关系. 协议2的安全性依赖协议1. 协议2的输出结果为 $f(p_0,P)=f_1(p_0,P)=f_2(p_0,P)$, 其中 $f_1(p_0,P)$ 表示执行协议2后 Alice 得到的结果, $f_2(p_0,P)$ 表示执行协议2后 Bob 得到的结果. 构造模拟器 S_3 模拟 Bob 执行协议2的过程, 模拟器 S_3 随机选取一个点 p_0^* 使得 $f_2^*(p_0^*,P)=f_2(p_0,P)=f(p_0,P)$. 依次以直线 $\overline{p_0^*p'}$ 和多边形 P 的每个顶点为输入执行协议1, 得到 P 的每个顶点与直线 $\overline{p_0^*p'}$ 的位置关系集合 R^*. 根据 R^* 中的结果计算出 I^*_{Cross}, 使用 I^*_{Cross} 中的线段 $\overline{p_l^*p_{l+1}^*}$ 和 p_0^* 执行协议1, 得到结果 $f_2^*(p_0^*,P)$.

$$S_3(p_0^*,P)=\{P,R^*,I^*_{\text{Cross}},f_2^*(p_0^*,P)\},\quad \text{view}_3(p_0,P)=\{P,R,I_{\text{Cross}},f(p_0,P)\} \tag{25}$$

由于 $f_2^*(p_0^*,P)=f_2(p_0,P)=f(p_0,P)$, 所以 R 与 R^* 不可区分, I_{Cross} 与 I^*_{Cross} 不可区分, 故 $\text{view}_3(p_0,P)$ 与 $S_3(p_0^*,P)$ 不可区分.

同理对 Alice 也可以构造模拟器 S_4 证明 $\text{view}_4(p_0,P)$ 与 $S_4(p_0^*,P)$ 不可区分. 上述证明过程说明协议保证了双方输入信息的安全.

6 性能分析

6.1 协议1性能分析

制约安全多方计算协议性能的主要因素是协议的通信复杂度和计算复杂度. 本文将从上述两个方面对协议1和文献 [14] 提出的协议进行分析比较. 为了便于叙述, 本文分别用符号 T_{enc}、T_{dec}、T_{mult} 和 T_{pow} 表示 1 次加密操作、1 次解密操作、1 次密文乘法运算和 1 次模幂运算的时间.

执行 1 次协议1需要进行 7 次加密操作、3 次解密操作、3 次密文乘法运算和 4 次模幂运算, 故执行 1 次协议1的计算开销为: $7T_{\text{enc}}+3T_{\text{dec}}+3T_{\text{mult}}+4T_{\text{pow}}$.

执行 1 次协议1, 需要传递 7 个密文和一个计算结果 $H_{p_0'\&\overline{p_1'p_2'}}$. 假设安全参数为 τ, Paillier 的密文长度为 2τ, 因为 $H_{p_0'\&\overline{p_1'p_2'}}$ 的比特长度相对于 τ 来说很小, 所以 $H_{p_0'\&\overline{p_1'p_2'}}$ 的长度可以忽略不计. 因此, 执行 1 次协议1所需要的通信开销为 $7\cdot(2\tau)=14\tau$.

文献 [14] 利用云环境中的点积协议设计了一种点与直线关系的判定协议, 在计算内积时文献 [14] 利用了 BGN 的乘法同态, 需要执行多次双线性对运算, 因此本文提出的协议在计算性能方面优于文献 [14] 提出的协议. 为了证实这一分析结果, 我们给出了仿真实验. 实验环境为 Windows 7 64 位操作系统、内存 4 G、Intel(R) Pentium(R) CPU G3220 @ 3.00 GHz, 基于 JPBC [19] 的库函数, 实验模拟了协议1的执行, 在模拟的过程中我们忽略了通信消耗的时间并取 τ 为 160 bit, 实验数据如表 1 所示.

表 1 协议1计算性能比较的实验数据 (单位: ms)

Table 1 Experimental data of computation performance comparison of Protocol 1 (ms)

方案	加密时间 T_{enc}	解密时间 T_{dec}	模幂运算 T_{pow}	密文乘法 T_{mult}	双线性运算	总时间
协议1	0.668 63	0. 570 65	1.260 35	1.386 25	-	10.567 917
文献 [14]	2.714 03	2.381 08	0.621 1535	0.063 5648	4.505 8532	32.436 56

上述实验仿真数据说明本文提出的协议1的计算性能优于文献 [14] 提出的协议. 值得注意的是, 文献 [20] 使用的是仰角比较协议, 文献 [13] 使用的是安全叉积协议, 文献 [21] 使用的是极角比较协议, 文献 [22] 使用的是角度旋转协议. 协议1对比其他文献, 协议1在设计上避免使用复杂的密码原语从而降低了计算开销, 更加精简.

6.2 协议2性能分析

协议2的计算开销依赖于协议1的计算开销、多边形 P 的顶点数 n 以及多边形 P 与直线 $\overline{p_0p'}$ 相交的边数 $|I_{\text{Cross}}|<n$. 在最坏情况下, 执行 1 次协议2仅仅需要执行 $n+|I_{\text{Cross}}|$ 次协议1, 因此其计算复杂度和通信复杂度为 $O(n+|I_{\text{Cross}}|)=O(n)$. 文献 [11] 提出的点包含协议需要调用了叉积协议和百万富翁协

议以及不经意传输协议 OT_1^n, 其计算复杂度和通信复杂度都为 $O(n\log n)$. 协议2使用了模拟射线法的问题转化方式, 避免了复杂的基本密码协议的使用, 既适用于凸多边形的情况也适用于凹多边形的情况. 文献 [11,13,20–22] 使用了复杂的基本密码协议, 并且其提出的协议不适用于凹多边形的情况 [10,23]. 上述比较结果如表2所示.

表 **2** 协议2的性能比较

Table 2 Performance analysis of Protocol 2

方案	支持凹多边形判定	支持凸多边形判定	通信复杂度	计算复杂度
协议2	是	是	$O(n)$	$O(n)$
文献 [11]	否	是	$O(n\log n)$	$O(n\log n)$
文献 [13]	否	是	$O(n^2)$	$O(n^2)$
文献 [20]	否	是	$O(n\log n)$	$O(n)$
文献 [21]	否	是	$O(n\log n)$	$O(n\log n)$
文献 [22]	否	是	$O(n^2)$	$O(n^2)$

7 结论

隐私保护的点与任意多边形关系的判定问题, 具有较高的研究意义. 解决该问题的方法一般从问题本身出发寻找突破口, 然后结合隐私保护相关技术设计具体的解决方案. 本文基于支持符号位的编码和同态加密算法设计了高效的点与直线关系判定协议, 然后利用模拟射线法的转化方法将点与任意多边形位置关系的判定问题转化为任意一条过点的射线与多边形相交点数的奇偶性判定问题, 最后给出了具有隐私保护的点与任意多边形关系判定方案. 本文研究的问题是基于半诚实模型下两个参与者的二维空间安全几何计算问题. 但是如何实现三维空间下多个参与者以及恶意模型下的具有隐私保护的几何计算问题还有待进一步的研究.

References

[1] DU W L, ZHAN Z J. A practical approach to solve secure multi-party computation problems[C]. In: Proceedings of the 2002 Workshop on New Security Paradigms. ACM, 2002: 127–135. [DOI: 10.1145/844102.844125]

[2] LI S D, SI T G, DAI Y Q. Secure multi-party computation of set-inclusion and graph-inclusion[J]. Journal of Computer Research and Development, 2005, 42(10): 1647–1653.
李顺东, 司天歌, 戴一奇. 集合包含与几何包含的多方保密计算 [J]. 计算机研究与发展, 2005, 42(10): 1647–1653.

[3] MOHASSEL P, ROSULEK M, ZHANG Y. Fast and secure three-party computation: The garbled circuit approach[C]. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015: 591–602. [DOI: 10.1145/2810103.2813705]

[4] BOGDANOV D, NIITSOO M, TOFT T, et al. High-performance secure multi-party computation for data mining applications[J]. International Journal of Information Security, 2012, 11(6): 403–418. [DOI: 10.1007/s10207-012-0177-2]

[5] ATALLAH M J, DU W L. Secure multi-party computational geometry[C]. In: Algorithms and Data Structures—WADS 2001. Springer Berlin Heidelberg, 2001: 165–179. [DOI: 10.1007/3-540-44634-6_16]

[6] ANDRYCHOWICZ M, DZIEMBOWSKI S, MALINOWSKI D. Secure multiparty computations on Bitcoin[J]. Communications of the ACM, 2016, 59(4): 76–84. [DOI: 10.1145/2896386]

[7] LI S D, WU C Y, WANG D S, et al. Secure multiparty computation of solid geometric problems and their applications[J]. Information Sciences, 2014, 282: 401–413. [DOI: 10.1016/j.ins.2014.04.004]

[8] GALETZKA M, GLAUNER P O. A simple and correct even-odd algorithm for the point-in-polygon problem for complex polygons[C]. In: Proceedings of the 12th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP 2017). Porto, Portugal, 2017: 175–178.

[9] HORMANN K, AGATHOS A. The point in polygon problem for arbitrary polygons[J]. Computational Geometry: Theory and Applications, 2001, 20(3): 131–144. [DOI: 10.1016/S0925-7721(01)00012-8]

[10] CHEN Z H, LI S D, HUANG Q, et al. New solutions to two privacy-preserving location-relation determining

problems[J]. Chinese Journal of Computers, 2018, 41(2): 336–348. [DOI: 10.11897/SP.J.1016.2018.00336]
陈振华, 李顺东, 黄琼, 等. 两个保密位置判断问题的新解法 [J]. 计算机学报, 2018, 41(2): 336–348. [DOI: 10.11897/SP.J.1016.2018.00336]

[11] ZHANG J, LUO S S, YANG Y X, et al. Research on the privacy-preserving point-in-polygon protocol[J]. Journal on Communications, 2016, 37(4): 87–95. [DOI: 10.11959/j.issn.1000-436x.2016075]
张静, 罗守山, 杨义先, 辛阳. 保护私有信息的点包含协议研究 [J]. 通信学报, 2016, 37(4): 87–95. [DOI: 10.11959/j.issn.1000-436x.2016075]

[12] YANG B, SUN A D, ZHANG M W. Secure two-party protocols on planar circles[J]. Journal of Information & Computational Science, 2011, 8(1): 29–40.

[13] LUO Y L, HUANG L S, ZHONG H, et al. A secure protocol for determining whether a point is inside a convex polygon[J]. Chinese Journal of Electronics, 2006, 15(4): 578–582.

[14] CHEN Z H, LI S D, HUANG Q, et al. Privacy-preserving determination of spatial location-relation in cloud computing[J]. Chinese Journal of Computers, 2017, 40(2): 351–363. [DOI: 10.11897/SP.J.1016.2017.00351]
陈振华, 李顺东, 黄琼, 等. 云外包计算中空间位置关系的保密判定 [J]. 计算机学报, 2017, 40(2): 351–363. [DOI: 10.11897/SP.J.1016.2017.00351]

[15] CHEN L, LIN B. Privacy-preserving point-inclusion two-party computation protocol[C]. In: Proceedings of the 2013 International Conference on Computational and Information Sciences, IEEE, 2013: 257–260. [DOI: 10.1109/ICCIS.2013.75]

[16] LUO Y L, HUANG L S, JING W W, et al. Privacy-preserving cross product protocol and its applications[J]. Chinese Journal of Computers, 2007, 30(2): 248–254.
罗永龙, 黄刘生, 荆巍巍, 等. 保护私有信息的叉积协议及其应用 [J]. 计算机学报, 2007, 30(2): 248–254.

[17] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]. In: Advances in Cryptology—EUROCRYPT '99. Springer Berlin Heidelberg, 1999: 223–238. [DOI: 10.1007/3-540-48910-X_16]

[18] GALETZKA M, GLAUNER P O. A correct even-odd algorithm for the point-in-polygon (PIP) problem for complex polygons[OL]. arXiv: Computational Geometry. https://arxiv.org/abs/1207.3502, 2017.

[19] LYNN B. The pairing-based cryptography library[OL]. http://crypto.stanford.edu/pbc/. 2007.

[20] YANG B, SHAO Z Y, ZHANG W Z. Secure two-party protocols on planar convex hulls[J]. Journal of Information & Computational Science, 2012, 9(4): 915–929.

[21] THOMAS T. Secure two-party protocols for point inclusion problem[J]. International Journal of Network Security, 2009, 9(1): 1–7.

[22] LI S D, DAO S W, DAI Y Q. Efficient secure multiparty computational geometry[J]. Chinese Journal of Electronics, 2010, 19(2): 324–328.

[23] GONG L M, LI S D, DOU J W, et al. Homomorphic encryption scheme and a protocol on secure computing a line by two private points[J]. Journal of Software, 2017, 28(12): 3274–3292. [DOI: 10.13328/j.cnki.jos.005239]
巩林明, 李顺东, 窦家维, 等. 同态加密方案及安全两点直线计算协议 [J], 软件学报, 2017, 28(12): 3274–3292. [DOI: 10.13328/j.cnki.jos.005239]

作者信息

张明武 (1972–), 湖北仙桃人, 博士, 教授. 主要研究领域为密码学、信息安全与隐私保护.
csmwzhang@gmail.com

冷文韬 (1993–), 湖北武汉人, 硕士研究生, 主要研究领域为信息安全.
12395405654@qq.com

沈华 (1978–), 江苏兴化人, 博士, 副教授. 主要研究领域为信息安全与隐私保护.
cshshen@hbut.edu.cn