空间位置关系的安全多方计算及其应用

张卫国 孙 嫚* 陈振华 陈 娓
(西安科技大学 西安 710054)

摘 要： 空间位置关系的保密计算属于安全多方计算中的空间几何问题，在机密性商业、工程、军事等方面有着重要的意义。但目前大多数空间几何问题都是通过转化为距离或数据对应成比例问题解决的，计算复杂性较高，且应用范围受限。针对这些问题，该文先将原问题转化为一个点是否为一个方程的解，再利用一种简单高效的内积协议一次性解决了点线、点面、线线、线面、面面等 5 种空间位置关系的判定，并利用模拟范例证明了协议的安全性。该文方案并没有利用任何公钥加密算法，取得了信息论安全；并且由于问题的巧妙转化，使得能解决的问题更加广泛，效率也相对较高。

关键词： 安全多方计算；位置关系；空间几何；内积协议
中图分类号： TP309 **文献标识码：** A **文章编号：** 1009-5896(2016)09-2294-07
DOI: 10.11999/JEIT160102

Secure Multi-party Computation of Spatial Relationship and Its Application

ZHANG Weiguo SUN Man CHEN Zhenhua CHEN Wei
(*Xi'an University of Science and Technology*, *Xi'an* 710054, *China*)

Abstract: Privacy-preserving determination of spatial relationship belongs to spatial geometry problem in secure multiparty computation, which is significant to confidential business, engineering, military, *etc*. However, most existing schemes transform the original problem into the distance problem or the correspondingly proportional data problem, which makes the computation complexity high and the application range being limited. To deal with these problems, first, the original problem is transformed into whether a point is the solution of equation. Based on the technique, a simple and efficient scalar product protocol is adopted to determine five spatial relationships all at once: point and line, point and plane, line and line, line and plane, and plane and plane. In addition, the security of the proposed protocol is proved with simulation paradigm. The proposed scheme does not employ any public key encryption algorithm so as to achieve the information security. The analysis indicates the trick transformation makes the proposed scheme higher efficient and more applicable than the known schemes.

Key words: Secure multi-party computation; Position relationship; Spatial geometry; Scalar product protocol

1 引言

安全多方计算最早由文献[1]提出，是指在不泄漏各方的输入数据(隐私性)的条件下，能正确完成输入数据的函数计算(正确性)。安全多方计算的特点使得人们能够最大限度地利用私有数据完成所需的计算任务而不破坏数据的隐私性。因此它在统计分析[2]、保密关联规则挖掘[3]、隐私保护聚类挖掘[4,5]、保密的几何问题[6–8]等方面有着广泛的应用。

文献[9]曾预言安全多方计算所处的地位就如同公钥密码学 10 年前所处的地位一样重要，它是计算科学一个极其重要的工具，而实际应用才刚起步。因此丰富其理论将使它成为计算科学和现实应用中一个必不可少的工具。1987 年，文献[10]提出了一个通用方案来解决所有的安全多方计算问题。该文献还指出，在大多数参与者是诚实的情况下，所有的安全多方计算问题均存在解决方案。这一完备性结论为以后的安全多方计算协议的研究提供了动力，也为安全多方计算的应用指出了乐观的前景。后来，在文献[11]中系统地总结了安全多方计算的研究成果，包括安全性定义、敌手模型的定义以及通用解决方案的描述。文献[11]的工作成为大部分安全多方计算问题解决方案的理论基础，其贡献对整个密码学领域都具有重大的影响。

收稿日期：2016-01-21；改回日期：2016-06-15；网络出版：2016-08-09
*通信作者： 孙嫚 sunman_xust@163.com
基金项目：国家自然科学基金(U1261114)
Foundation Item: The National Natural Science Foundation of China (U1261114)

文献[12]在前人工作的基础上，进一步研究了一些具体的安全多方计算问题及其应用，包括科学计算、几何计算、统计分析等问题。空间几何问题的保密计算也是安全多方计算中一个很重要的组成部分。针对于此，文献[13]研究了安全两方多边形相交等问题。文献[14]研究了点与平行线位置关系等问题。而位置关系问题的安全计算是空间几何中的一个重要分支，在现实生活中应用广泛。比如以下的场景：

为了摧毁一颗老化的气象卫星，A, B 两国想合作在太空发射两颗导弹来击毁，但是在发射的过程中就有可能进行干扰或碰撞。但是为了各自利益都不愿意告诉对方自己所在的位置信息，那么 A, B 两国如何在不泄露各自私有信息的前提下完成合作？

以上场景属于保密军事问题，转化成数学模型就是判断空间两条直线是否相交，属于安全多方计算中的空间保密位置判定问题，但目前这方面的研究文献并不多。由于现实中很多问题都可以归结为此问题。因此研究其理论意义对现实问题有着重要的应用价值。

针对点、线、面等空间位置关系的安全计算问题，以往的学者们提出了一些解决方案。文献[15]利用四面体的体积将问题转化为距离来判定点面、线面、面面的位置关系，但是若用该方法研究点线、线线的位置关系，我们无法在该条线上取 3 个不共线的点，继而也不能构造一个四面体，那么就无法把四面体的体积转化为距离来判定点线、线线的位置关系。因此该方法研究范围受限。2006 年，文献[16]利用法向量与方向向量的关系，解决了线线、线面、面面位置关系的问题。该方案用到了多种基本协议：比较相等协议、点积协议，又利用了数据对应成比例协议；此外，又利用求距离的方法研究了点线、点面的位置关系。因此计算十分繁琐。

以上方案由于转化方法的问题，要不所解决的空间位置关系较少，研究范围受限；要不，计算十分繁琐，复杂性较高。针对此问题，本文首先将空间位置关系问题转化为一个点是否为一个方程的解。避免了多次求距离或数据对应成比例的方法，从而提高了应用范围和效率；其次，在将原问题转化成该问题的基础上，共设计了 5 个协议：(1)利用内积设计了点线位置关系的协议 1、点面位置关系的协议 2。(2)在协议 1 和协议 2 的基础上，又设计了线与线位置关系的协议 3、线与面位置关系的协议 4、面与面位置关系的协议 5；最后，文中 5 个协议都没有利用任何公钥加密算法，安全性级别较高，取得了信息论安全。

2　预备知识

2.1 安全多方计算的安全性定义

(1)半诚实参与者：安全多方计算的协议运行环境分为半诚实参与者模型和恶意攻击者模型[10, 17]，半诚实参与者指协议方将诚实地执行协议，不会篡改输入和输出信息，但可能会保留计算的中间结果，试图推导出协议之外的信息或者他人的信息。

(2)半诚实模型下的安全性定义：文献[10,17]利用比特承诺和零知识证明理论设计了一个编译器，这个编译器可以将在半诚实参与者条件下保密计算函数 f 的协议 π 自动生成在恶意参与者条件下也能保密计算 f 的协议 π'。新的协议 π' 可以迫使恶意参与者以半诚实方式参与协议的执行，否则就会被发现。因此大多数情况下，我们只设计半诚实模型下的协议。当我们设计出所需要的半诚实模型下的安全多方协议时，只要按照文献[10,17]的通用转化方法就可以将原协议转化为恶意模型下的新协议。基于这一结论，本文也只给出半诚实模型下的协议和相应的安全性模拟范例。

设 $f(x,y)$ 为概率多项式函数，π 是计算 f 的协议，设 Alice 拥有 x，Bob 拥有 y，他们要在不暴露 x,y 的前提下，合作计算函数 $f(x,y)=(f_1(x,y), f_2(x,y))$。计算的目的是为了让 Alice 和 Bob 分别得到函数 f 的两个分量 $f_1(x,y), f_2(x,y)$。Alice 在执行协议 π 的过程中所得到的视图记为 $\mathrm{view}_1(x,y)$，输出记作 $\mathrm{output}_1(x,y)$；同理，Bob 的视图记为 $\mathrm{view}_2(x,y)$，输出记作 $\mathrm{output}_2(x,y)$。文献[11]中给出计算不可区分性的半诚实参与者的安全两方计算的定义，表述如下：

定义 1　协议 π 保密地计算了 $m<N$，如果存在概率多项式时间模拟器 S_1 与 S_2 使得式(1)，式(2)同时成立：

$$\begin{aligned}&\{(S_1(x,f_1(x,y),f_1(x,y))\}\\&\quad\stackrel{c}{\equiv}\{(\mathrm{view}_1(x,y),\mathrm{output}_2(x,y))\}\end{aligned}\tag{1}$$

$$\begin{aligned}&\{(f_1(x,y),S_2(y,f_2(x,y)))\}\\&\quad\stackrel{c}{\equiv}\{(\mathrm{output}_2(x,y),\mathrm{view}_2(x,y))\}\end{aligned}\tag{2}$$

其中，$\stackrel{c}{\equiv}$ 表示计算不可区分。

此定义说明了任何一方参与者视图中的信息只能从自己输入和所获得的输出中得到，即说明任何一方参与者视图中不包含额外的信息，这样就保证了在协议执行过程中，任何一方得不到其他方的私有信息。因此要证明一个两方计算协议是保密的，就必须构造使得式(1)和式(2)成立的模拟器 S_1 与 S_2。

2.2 一个基本的保密内积协议

假设有两个参与者，Alice 拥有秘密输入向量 $\boldsymbol{X}=(x_1,x_2,\cdots,x_n)$，Bob 拥有秘密输入向量 $\boldsymbol{Y}=(y_1,y_2,\cdots,y_n)$，他们希望进行协作计算 $\boldsymbol{X}\cdot\boldsymbol{Y}$，但是都不想泄露彼此的信息。

下面给出文献[18]设计的一个信息论安全的保密内积协议(表 1)。

表 1 信息安全保密内积协议

输入 Alice 秘密输入向量 $\boldsymbol{X}=(x_1,x_2,\cdots,x_n)$，Bob 秘密输入向量 $\boldsymbol{Y}=(y_1,y_2,\cdots,y_n)$。

输出 Alice 和 Bob 都知道 $\boldsymbol{X}\times\boldsymbol{Y}$ 的值。

(1) Alice 和 Bob 共同生成一个 $n\times n/2$ 的矩阵 $\boldsymbol{C}$。

(2) Alice 该做的：

(a)Alice 随机生成一个维数为 $n/2$ 的向量 $\boldsymbol{R}$，($\boldsymbol{R}=R_1,\cdots,R_{n/2}$)。

(b) Alice 继而又生成 $n\times1$ 阶矩阵 $\boldsymbol{X}'$，即 $\boldsymbol{X}'=\boldsymbol{C}\times\boldsymbol{R}$，计算 $\boldsymbol{X}''=\boldsymbol{X}+\boldsymbol{X}'$ 。

(c) Alice 发送 $\boldsymbol{X}''$ 给 Bob。

(3) Bob 该做的：

(a) Bob 生成一个内积 S' ,即 $S'=\sum_{i=1}^{n}x_i'\cdot y_i$。

(b) Bob 继而生成 $n/2\times1$ 阶矩阵 $\boldsymbol{Y}'$，即 $\boldsymbol{Y}'=\boldsymbol{C}^{\mathrm{T}}\times\boldsymbol{Y}$ 。

(c) Bob 发送 S' 和 $\boldsymbol{Y}'$ 给 Alice。

(4) Alice 该做的：

(a) Alice 生成一个减法因子 S'' ,即 $S''=\sum_{i=1}^{n}Y_i'\cdot R_i$。

(b) Alice 最终生成所需的内积 $S,S=S'-S''$。

(c) Alice 发送内积 $S=\boldsymbol{X}\bullet\boldsymbol{Y}$ 给 Bob。

结束！

该协议通过构造一个不可逆的矩阵进行计算，由于没有利用任何公钥加密算法取得隐私保护，因此安全性级别较高，达到了信息论安全。

2.3 本文研究的问题

本文研究以下 5 个问题：

问题 1 安全计算空间点与空间直线的位置关系：Alice 有一个秘密的空间点 $p_0(x_0,y_0,z_0)$，Bob 有一条秘密的空间直线 $L:\begin{cases}A_1x+B_1y+C_1z+D_1=0\\A_2x+B_2y+C_2z+D_2=0\end{cases}$。Alice 和 Bob 两人想在不泄露给对方信息的条件下来判定点 p_0 和直线 L 的位置关系。

问题 2 安全计算空间点与空间平面的位置关系：Alice 有一个秘密的空间点 $p_0(x_0,y_0,z_0)$，Bob 有一个秘密的空间平面 $\Pi:Ax+By+Cz+D=0$。Alice 和 Bob 两人想在不泄露给对方信息的条件下来判定点 p_0 和平面 Π 的位置关系。

问题 3 安全计算空间直线与空间直线的位置关系：Alice 有一条秘密的空间直线 $L_1:\begin{cases}A_1x+B_1y+C_1z+D_1=0\\A_2x+B_2y+C_2z+D_2=0\end{cases}$，Bob 也有一条秘密的空间直线 $L_2:\begin{cases}A_3x+B_3y+C_3z+D_3=0\\A_4x+B_4y+C_4z+D_4=0\end{cases}$。Alice 和 Bob 两人想在不泄露给对方信息的条件下来判定直线 L_1 与直线 L_2 的位置关系。

问题 4 安全计算空间直线与空间平面的位置关系：Alice 有一条秘密的空间直线 $L:\begin{cases}A_1x+B_1y+C_1z+D_1=0\\A_2x+B_2y+C_2z+D_2=0\end{cases}$，Bob 有一个秘密的空间平面 $\Pi:Ax+By+Cz+D=0$。Alice 和 Bob 两人想在不泄露给对方信息的条件下来判定直线 L 与平面 Π 的位置关系。

问题 5 安全计算空间平面与空间平面的位置关系：Alice 有一个秘密的空间平面 $\Pi_1:Ax+By+Cz+D=0$，Bob 也有一个秘密的空间平面 $\Pi_2:A_1x+B_1y+C_1z+D=0$。Alice 和 Bob 两人想在不泄露给对方信息的条件下来判定平面 Π_1 与平面 Π_2 的位置关系。

3 解决方案

3.1 问题的转化和解决

本文把点与线、点与面的位置关系转化为一个点是否为一个方程的解，进而提出一种高效的方法来保密判定点与线、点与面的位置关系。

以下协议假设所有的参与者都是在半诚实模型下，网络之间传输都是公开信道。

3.2 两个具体的协议

协议 1 安全计算点与线的位置关系

输入：Alice 保密输入点 $p_0(x_0,y_0,z_0)$，Bob 保密输入直线 $L:\begin{cases}A_1x+B_1y+C_1z+D_1=0\\A_2x+B_2y+C_2z+D_2=0\end{cases}$。

输出：Alice 和 Bob 都知道点 p_0 在直线 L 上或者点 p_0 在直线 L 外。

(1)Alice 计算向量 $\boldsymbol{a}=(x_0,y_0,z_0,1)$，Bob 计算向量 $\boldsymbol{b}=(A_1,B_1,C_1,D_1)$，$\boldsymbol{c}=(A_2,B_2,C_2,D_2)$。

(2)Alice 和 Bob 执行两次 2.2 节的保密内积协议，可计算出向量 $\boldsymbol{a}$ 与向量 $\boldsymbol{b}$ 的内积和向量 $\boldsymbol{a}$ 与向量 $\boldsymbol{c}$ 的内积。

(3)如果两次保密求内积的值都为零，则点在线上，否则其他情况都在线外。

分析：在协议 1 中，调用 2.2 节的内积协议。首先 Alice 和 Bob 一起生成不可逆矩阵 $\boldsymbol{C}$，接着由于 Alice 随机生成一个 $n/2$ 维的向量 $\boldsymbol{R}$，所以即使

Alice 发送 $\boldsymbol{X}''=\boldsymbol{X}+\boldsymbol{X}', \boldsymbol{X}'=\boldsymbol{C}\times\boldsymbol{R}$ 给 Bob, Bob 也得不到 Alice 的任何信息。其次，Bob 用 Alice 发来的 $\boldsymbol{X}''$ 和向量 $\boldsymbol{Y}$ 计算内积 $S'=\sum_{i=1}^{n}x_i''\cdot y_i$，然后再生成 $n\times1$ 阶矩阵 $\boldsymbol{Y}'=\boldsymbol{C}^{\mathrm{T}}\times\boldsymbol{Y}$。由于矩阵 $\boldsymbol{C}$ 是不可逆的，所以 Bob 把 $S'=\sum_{i=1}^{n}x_i''\cdot y_i$ 和 $\boldsymbol{Y}'=\boldsymbol{C}^{\mathrm{T}}\times\boldsymbol{Y}$ 发送给 Alice, Alice 也得不到 Bob 的任何信息。最后，Alice 生成一个减法因子 $S''=\sum_{i=1}^{n}Y_i'\cdot R_i$，进而求出所需的内积 $S=S'-S''$。因此，在整个协议中即保护了 Alice 的隐私性又保护了 Bob 的隐私性。

协议 2　安全计算点与面的位置关系

输入：Alice 保密输入点 $p_0(x_0,y_0,z_0)$, Bob 保密输入平面 $\Pi: Ax+By+Cz+D=0$。

输出：Alice 和 Bob 都知道点 p_0 在平面 Π 上或者点 p_0 在平面 Π 外。

(1) Alice 计算向量 $\boldsymbol{a}=(x_0,y_0,z_0,1)$, Bob 计算向量 $b=(A,B,C,D)$。

(2) Alice 和 Bob 执行一次 2.2 节的保密内积协议，可计算出向量 $\boldsymbol{a}$ 与向量 $\boldsymbol{b}$ 的内积。

(3) 如果保密求内积的值为零，则点在面上，否则点在面外。

分析：在协议 2 中，隐私安全性和协议 1 相同，不同的是在协议 2 中我们只进行一次保密内积协议，比协议 1 更简洁更高效。

4　应用

本节将协议 1 和协议 2 作为基础子协议，进一步判定了线与线、线与面、面与面的位置关系。

4.1 问题的转化

有别于前人方案利用距离的解决方法，本文是在其中一条直线上任取两个点，然后把原问题转化为这两个点是否都属于一个方程的解。进而保密判定了线与线、线与面、面与面的位置关系。

以下协议假设所有的参与者都是在半诚实模型下，网络之间传输都是公开信道。

4.2 具体协议

协议 3　安全计算线与线的位置关系

输入：Alice 保密输入直线 $L_1:\begin{cases}A_1x+B_1y+C_1z+D_1=0\\A_2x+B_2y+C_2z+D_2=0\end{cases}$, Bob 保密输入直线 $L_2:\begin{cases}A_3x+B_3y+C_3z+D_3=0\\A_4x+B_4y+C_4z+D_4=0\end{cases}$。

输出：Alice 和 Bob 都知道直线 L_1 与直线 L_2 是平行、相交或重合。

步骤 1　Alice 在 L_1 上任意选取两个确定的点 $p_1(x_1,y_1,z_1)$，$p_2(x_2,y_2,z_2)$。

步骤 2　Alice 计算向量 $\boldsymbol{a}=(x_1,y_1,z_1,1), \boldsymbol{b}=(x_2,y_2,z_2,1)$，Bob 计算向量 $\boldsymbol{c}=(A_3,B_3,C_3,D_3)$，$\boldsymbol{d}=(A_4,B_4,C_4,D_4)$。

步骤 3　Alice 和 Bob 执行 4 次 2.2 节的保密内积协议，即向量 $\boldsymbol{a}$ 与向量 $\boldsymbol{c}$ 的内积，向量 $\boldsymbol{a}$ 与向量 $\boldsymbol{d}$ 的内积，向量 $\boldsymbol{b}$ 与向量 $\boldsymbol{c}$ 的内积，向量 $\boldsymbol{b}$ 与向量 $\boldsymbol{d}$ 的内积。

步骤 4　如果向量 $\boldsymbol{a}$ 分别与向量 $\boldsymbol{c}$、向量 $\boldsymbol{d}$ 做内积的结果都为零，则说明点 p_1 在直线 L_2 上，否则在直线 L_2 外；同样，如果向量 $\boldsymbol{b}$ 分别与向量 $\boldsymbol{c}$、向量 $\boldsymbol{d}$ 做内积的结果都为零，则说明点 p_2 在直线 L_2 上，否则在直线 L_2 外。最后的结果分为两种：如果两个点都在直线 L_2 上，则直线 L_1 与直线 L_2 重合，否则就是相交或者平行。如果是后者，转为第 5 步。

步骤 5　Alice 用自己任意选取的这两点表示这条直线所在方向向量 $\boldsymbol{d}$，Bob 取直线 L_2 上的方向向量 $\boldsymbol{e}$，根据 2.2 节的的保密内积协议，Alice 可以得到 $<\boldsymbol{d},\boldsymbol{e}>/|\boldsymbol{d}|$，记该数的绝对值为 x。Bob 可以得知 $|\boldsymbol{e}|$，记该数的绝对值为 y。根据夹角公式 $<\boldsymbol{d},\boldsymbol{e}>/|\boldsymbol{d}|=|\boldsymbol{e}|\cos\theta$，利用 Hash 函数判断 $h(x)$ 与 $h(y)$ 是否相等，若 $h(x)=h(y)$，则 $x=y$，说明 $\cos\theta=\pm1$，即直线 L_1 与直线 L_2 平行，否则相交。

分析：在协议 3 中，我们首先用的是内积协议，隐私安全性和以上协议完全相同。不同的是在步骤 5 我们引进夹角公式和 Hash 函数。由内积协议我们可以知道，最终是 Alice 计算 $<\boldsymbol{d},\boldsymbol{e}>$ 的值，只要 Alice 不告诉 Bob $<\boldsymbol{d},\boldsymbol{e}>/|\boldsymbol{d}|$ 的值，那么 Alice 的隐私性就可以保证。Bob 也是如此。Hash 函数是一个单向陷门函数，所以即使最后两人知道 $h(x)=h(y)$ 的值，也不可能得知 x, y 的值。因此各自的隐私性都得到保护，所以协议安全。

协议 4 安全计算线与面的位置关系

输入：Alice 保密输入直线 $L:\begin{cases}A_1x+B_1y+C_1z+D_1=0\\A_2x+B_2y+C_2z+D_2=0\end{cases}$, Bob 保密输入平面 $\Pi: Ax+By+Cz+D=0$。

输出：Alice 和 Bob 都知道直线 L 与平面 Π 是相交、平行或重合。

步骤 1　Alice 在 L 上任意选取两个点 $p_1(x_1,y_1,z_1)$，$p_2(x_2,y_2,z_2)$。

步骤 2　Alice 计算向量 $\boldsymbol{a}=(x_1,y_1,z_1,1)$, $\boldsymbol{b}=(x_2,y_2,z_2,1)$, Bob 计算向量 $\boldsymbol{c}=(A,B,C,D)$。

步骤 3　Alice 和 Bob 执行两次 2.2 节保密内积协议，即计算向量 $\boldsymbol{a}$ 与向量 $\boldsymbol{c}$ 的内积、向量 $\boldsymbol{b}$ 与向量

$\boldsymbol{c}$ 的内积。如果向量 $\boldsymbol{a}$ 与向量 $\boldsymbol{c}$ 和向量 $\boldsymbol{b}$ 与向量 $\boldsymbol{c}$ 的内积结果都为零，则直线 L 在平面 Π 上，即重合；否则就是相交或者平行。如果是后者，转入第 4 步。

步骤 4 Alice 用自己任意选取的这两点表示这条直线所在方向向量 $\boldsymbol{d}$，Bob 取平面 Π 上任取一个向量 $\boldsymbol{e}$，根据 2.2 节的的保密内积协议，Alice 可以得到 $<\boldsymbol{d},\boldsymbol{e}>/|\boldsymbol{d}|$，记该数的绝对值为 x。Bob 可以得知 $|\boldsymbol{e}|$，记该数的绝对值为 y。根据夹角公式 $<\boldsymbol{d},\boldsymbol{e}>/|\boldsymbol{d}|=|\boldsymbol{e}|\cos\theta$，利用 Hash 函数判断 $h(x)$ 与 $h(y)$ 是否相等，若 $h(x)=h(y)$，则 $x=y$，说明 $\cos\theta=\pm1$，即直线 L 与平面 Π 平行，否则相交。

分析：在协议 4 中，隐私安全性和协议 3 相同。

协议 5 安全计算面与面的位置关系

输入：Alice 保密输入平面 $\Pi: Ax+By+Cz+D=0$，Bob 保密输入平面 $\Pi_1: A_1x+B_1y+C_1z+D_1=0$。

输出：Alice 和 Bob 都知道平面 Π 与平面 Π_1 是平行、相交或重合。

步骤 1 Alice 在平面 Π 上任意选取 3 个点 $p_1(x_1,y_1,z_1)$，$p_2(x_2,y_2,z_2)$，$p_3(x_3,y_3,z_3)$(3 点不在一条直线上)。

步骤 2 Alice 计算向量 $\boldsymbol{a}=(x_1,y_1,z_1,1),\boldsymbol{b}=(x_2,y_2,z_2,1),\boldsymbol{c}=(x_3,y_3,z_3,1)$。Bob 计算向量 $\boldsymbol{d}=(A_1,B_1,C_1,D_1)$。

步骤 3 Alice 和 Bob 执行 3 次保密内积协议，即计算向量 $\boldsymbol{a}$ 与向量 $\boldsymbol{d}$ 的内积，向量 $\boldsymbol{b}$ 与向量 $\boldsymbol{d}$ 的内积，向量 $\boldsymbol{c}$ 与向量 $\boldsymbol{d}$ 的内积。

步骤 4 如果 3 次保密求内积的结果都为零，那么平面 Π 与平面 Π_1 重合；如果有其中一个或两个不为零，那么平面 Π 与平面 Π_1 相交；如果都不为零，则转为步骤 5。

步骤 5 Alice 在平面 Π 上任取向量 $\boldsymbol{e}$，Bob 在平面 Π_1 上任取向量 $\boldsymbol{f}$。根据 2.2 节的的保密内积协议，Alice 可以得到 $<\boldsymbol{e},\boldsymbol{f}>/|\boldsymbol{e}|$，记该数的绝对值为 x。Bob 可以得知 $\boldsymbol{f}$，记该数的绝对值为 y。根据夹角公式 $<\boldsymbol{e},\boldsymbol{f}>/|\boldsymbol{e}|=|\boldsymbol{f}|\cos\theta$，利用 Hash 函数判断 $h(x)$ 与 $h(y)$ 是否相等，若 $h(x)=h(y)$，则 $x=y$，说明 $\cos\theta=\pm1$，即平面 Π 与平面 Π_1 平行，否则相交。

分析：在协议 5 中，隐私安全性和协议 3、协议 4 相同。

5 安全性分析

在本节，应用 2.1 节的安全性模拟范例给出本文 5 个协议的安全性证明，由于协议 1~协议 5 证明过程相似，而且协议 2~协议 5 都是以协议 1 为基础协议设计得到。安全性依赖于协议 1 保障。为了节省篇幅，我们以证明协议 1 安全性为主，而对于协议 2~协议 5，只给出安全性结论。

定理 1 协议 1 保密判定点与线的位置关系。

证明 通过构造满足式(1)和式(2)的模拟器 S_1,S_2 来证明本定理。在本协议中 $f_1(p_0,L)=f_2(p_0,L)=p_0\in L$ 或 $f_1(p_0,L)=f_2(p_0,L)=p_0\notin L$。

假设 $f_1(p_0,L)=f_2(p_0,L)=p_0\in L$ 来构造模拟器 S_1，S_1 接受 $\big(p_0,f_1(p_0,L)\big)$ 作为输入，按如下方式工作：

(1) S_1 接受输入 $(p_0,p_0\in L)$ 后，首先随机的选取一个集合 L'，使得 $f_1(p_0,L)=f_1(p_0,L')$，然后用 (p_0,L') 来模拟。按照协议，给定的输入 $p_0(x_0,y_0,z_0)$ 即向量 $\boldsymbol{a}=(x_0,y_0,z_0,1)$，$S_1$ 随机选取的集合 L' 即为两个向量 $\boldsymbol{b}'=\big(A_1',B_1',C_1',D_1'\big)$，$\boldsymbol{c}'=\big(A_2',B_2',C_2',D_2'\big)$ 使得 $\boldsymbol{a}\cdot\boldsymbol{b}'=\boldsymbol{a}\cdot\boldsymbol{b}$，$\boldsymbol{a}\cdot\boldsymbol{c}'=\boldsymbol{a}\cdot\boldsymbol{c}$。

(2) 利用文献[18]进行保密内积计算 $\boldsymbol{a}\cdot\boldsymbol{b}'$ 和 $\boldsymbol{a}\cdot\boldsymbol{c}'$ 的值。

(3) 判断得到最终的结果 C'。

在本协议中，$\text{view}_1(p_0,p_0\in L,p_0\notin L)=\{\boldsymbol{a},\boldsymbol{a}\cdot\boldsymbol{b},\boldsymbol{a}\cdot\boldsymbol{c}\}$，$S_1(p_0,p_0\in L,p_0\notin L)=\{\boldsymbol{a},\boldsymbol{a}\cdot\boldsymbol{b}',\boldsymbol{a}\cdot\boldsymbol{c}'\}$。由于 $\boldsymbol{b}$，$\boldsymbol{b}'$，$\boldsymbol{c}$，$\boldsymbol{c}'$ 都是随机概率性选取，因而这些量在计算上不可区分。又由于 $C=f_1(p_0,L)=p_0\in L$，$f_1(p_0,L)=f_1(p_0,L')$，因此 $C'=f_1(p_0,L')=p_0\in L'$ 所以 $C=C'$。

又因为 $\text{output}_2(p_0,L)=f_2(p_0,L)=p_0\in L$，所以 $\{(S_1(x,f_1(x,y)),f_2(x,y))\}\underline{\underline{c}}\{(\text{view}_1(x,y),\text{output}_2(x,y))\}$

同理，用类似的方法可构造模拟器 S_2 使得：$\{(f_1(x,y),S_2(y,f_2(x,y)))\}\underline{\underline{c}}\{(\text{output}_1(x,y),\text{view}_2(x,y))\}$

用类似的方法可以证明协议 2~协议 5 的安全性，这里不再一一赘述。

6 效率分析与比较

本节将本文的方案和文献[15]、文献[16]的方案在效率以及性能方面做一个分析和比较。

(1)计算复杂度：由于这些方案有的使用公钥加密算法，有的未使用公钥加密算法，而且在运算过程中都使用了多项式数乘运算，因此，把方案的加解密次数与数乘运算的个数作为衡量计算复杂性的指标。除了点线、线线外，本文与参考文献共同研究的是点面、线面、面面 3 种空间位置关系。因此为了给出一个横向比较，统一用本文方案(协议 2、协议 4、协议 5)与文献[15]文献[16]中同类点面、线面、面面 3 种协议进行比较。

点面协议：文献[15]进行数乘计算 18 次，加解密次数 0 次；文献[16]进行数乘运算 16 次，加解密次数 12 次；而本文的协议 2 进行数乘运算 4 次，加

解密次数 0 次。

线面协议：文献[15]进行数乘计算 9 次，加解密次数 0 次；文献[16]进行数乘运算 21 次，加解密次数 21 次；而本文的协议 4 进行数乘运算 12 次，加解密次数 0 次。

面面协议：文献[15]进行数乘计算 12 次；加解密次数 0 次；文献[16]进行数乘计算 20 次，加解密次数 63 次，而本文的协议 5 进行数乘计算 16 次，加解密次数 0 次。

(2)通信复杂度：衡量通信复杂度的指标用协议交换信息的比特数，或者用通信轮数，在多方保密计算研究中通常用轮数(round)。

(3)性能：以方案所能解决的问题以及安全性级别作为衡量性能的指标。

综合以上分析，本文与现有文献[15]文献[16]在点面、线面、面面的效率对比如表2；本文与现有文献[15]文献[16]的性能对比如表3。

从表 2 可以看出，无论是从数乘个数、加解密次数还是通信复杂度方面做比较，本文所设计的 3 个协议都比文献[16]中同类的各个协议的计算量少；而对于文献[15]而言，虽然本文的协议 4、协议 5 在数乘个数方面比其多，但是相差不大，且加解密次数相同，同时本文的协议 2 在各个方面都比其同类协议计算量少，因此，本文的效率相对较高。

从表 3 可以看出，文献[15]解决空间中的点面、线面、面面 3 种位置关系；文献[16]虽然研究了空间中的点线、点面、线面等 5 种位置关系，但是空间中的点线、点面协议并未使用作者新提出的方法，而是另外一种方法。而本文用同一种方法一次性解决了空间中的点线、点面、线面等 5 种位置关系。因此，本文的方法能解决的问题范围更广。

综合以上，以往的方案或者计算复杂性较高，或者研究问题的范围受限。而本文的方案在和信息论安全的参考文献相比，在保持同样安全性级别的情况下，我们能判断的位置关系更多，即解决的问题范围更广；在和计算性安全的参考文献相比，我们的方法具有通用性，可以一次性判断空间多种位置关系，效率更高。

7　结论

空间位置关系的保密计算属于安全多方计算中的空间几何问题，现实中很多问题都能归结于此。而已存在的方案大多把原问题转化为距离或数据对应成比例问题来解决，计算复杂性较高，且应用范围受限。本文首先将原问题转化成一个点是否属于一个方程的解，然后基于密码学和数学中的知识解决了此问题。本文设计的 5 个协议，并没有利用任何公钥加密算法，取得了信息论安全；并且由于问题的巧妙转化，使得本文方案能解决的问题更广，效率也相对较高。

表 2 本文方案与现有方案的效率比较

问题	方案	计算复杂性		通信复杂度
		数乘个数	加解密次数	
点面关系	文献[15]	18	0	3
	文献[16]	16	12	5
	本文方法(协议2)	4	0	3
线面关系	文献[15]	9	0	2
	文献[16]	21	12	5
	本文方法(协议4)	12	0	3
面面关系	文献[15]	12	0	3
	文献[16]	20	63	4
	本文方法(协议5)	16	0	3

表 3 本文方案与现有方案的性能比较

方案	安全性	解决问题				
		点线	点面	线线	线面	面面
文献[15]	信息论安全	否	是	否	是	是
文献[16]	计算性安全	是	是	是	是	是
本文方法	信息论安全	是	是	是	是	是

参 考 文 献

[1] YAO A C. Protocols for secure computations[C]. Proceedings of 23rd IEEE Symposiumon Foundations of Computer Science, Chicago, IL, USA, 1982: 160–164. doi: 10.1109/SFCS.1982.38.

[2] KAMM L. Privacy-preserving statistical analysis using secure multi-party computation[D]. [Ph.D. dissertation], University of TARTU, 2015: 50–54.

[3] 刘峰, 薛安荣, 王伟. 一种隐私保护关联规则挖掘的混合算法[J]. 计算机应用研究, 2012, 29(3): 1108–1109. doi: 10.3969/j.issn.1001-3695.2012.03.084.
LIU Feng, XUE Anrong, and WANG Wei. Hybrid algorithm for privacy preserving association rules mining[J]. *Application Research of Computers*, 2012, 29(3): 1108–1109. doi: 10.3969/j.issn.1001-3695.2012.03.084.

[4] ROY B. Performance analysis of clustering in privacy preserving data mining[J]. *International Journal of Computer Applications & Information Technology*, 2014, 5(4): 35–39.

[5] 崇志宏, 倪巍伟, 刘腾腾, 等. 一种面向聚类的隐私保护数据发布方法[J]. 计算机研究与发展, 2010, 47(12): 2083–2089.
CHONG Zhihong, NI Weiwei, LIU Tengteng, *et al*. A privacy-preserving data publishing algorithm for clustering application[J]. *Journal of Computer Research and Development*, 2010, 47(12): 2083–2089.

[6] LI C and LIN B G. Privacy-preserving point-inclusion two-party computation protocol [C]. 2013 IEEE Fifth International Conferenceon on Computational and Information Sciences (ICCIS), Hubei, China, 2013: 257–260. doi: 10.1109/ICCIS.2013.75.

[7] 王斑, 罗文俊. 安全多方计算在空间几何问题中的应用[J]. 计算机系统应用, 2015, 24(1): 156–160. doi: 10.3969/j.issn.1003-3254.2015.01.029.
WANG Ting and LUO Wenjun. Applications of secure multi-party computation in spacegeometry problems[J]. *Computer Systems & Applications*, 2015, 24(1): 156–160. doi: 10.3969/j.issn.1003-3254.2015.01.029.

[8] QIN Jing, DUAN Hongwei, ZHAO Huawei, *et al*. A new lagrange solution to the privacy-preserving general geometric intersection problem[J]. *Journal of Network and Computer Applications*, 2014, 46(1): 94–99. doi:10.1016/j.jnca.2014. 08.004.

[9] GOLDWASSER S. Multi-party computations: Past and present[C]. Proceedings of the 16th Annual ACM Symposium on Principles of Distributed Computing, New York, USA, 1997: 1–6. doi: 10.1145/259380.259405.

[10] GOLDRE O, MICALI S, and WIGDERSON A. How to play any mental game[C]. Proceedings of the 19th Annual ACM Conference on Theory of Computing, New York, USA, 1987: 218–229.

[11] GOLDREICH O. Secure multi-party computation(draft)[OL]. http://www.wisdow.weizmann.ac.il/~oded/pp.html,1998.

[12] DU W L and ATALLAH M J. Secure multi-party computation problems and their applications: A review and open problems[C]. Proceedings of the 2001 Workshop on New Security Paradigms, New York, USA, 2001: 11–22.

[13] 荆巍巍. 安全多方计算中若干基础协议及应用的研究[D]. [博士论文], 中国科学技术大学, 2008. doi: 10.7666/d.y1270516.
JING Weiwei. Research on several basic protocols and application of secure multi-party, computation[D]. [Ph.D. dissertation], University of Science and Technology of China, 2008. doi: 10.7666/d.y1270516.

[14] 王斑, 罗文俊. 基于阈值的点线距离与位置关系保密判定协议[J]. 计算机工程与应用, 2010, 46(13): 87–89. doi: 10.3778/j.issn.1002-8331/.2010.13.026.
WANG Ting and LUO Wenjun. Privacy-preserving determination protocol for point-line distance and position relation based on threshold[J]. *Computer Engineering and Applications*, 2010, 46(13): 87–89. doi: 10.3778/j.issn.1002-8331/.2010.13.026.

[15] LI Shundong, WU Chunying, WANG Daoshun, *et al*. Secure multiparty computation of solid geometric problems and their applications[J]. *Information Sciences*, 2014, 282(10): 401–413. doi: 10.1016/j.ins.2014.04.004.

[16] 罗永龙, 黄刘生, 荆巍巍, 等. 空间几何对象相对位置判定中的私有信息保护[J]. 计算机研究与发展, 2006, 43(3): 410–416.
LUO Yonglong, HUANG Liusheng, JING Weiwei, *et al*. Privacy protection in the relative position determination for two spatial geometric objects[J]. *Journal of Computer Research and Development*, 2006, 43(3): 410–416.

[17] GOLDREICH O. Foundations of Cryptography: Basic Applications[M]. London: Cambridge University Press, 2004: 599–729.

[18] CLIFTON C, KANTARCIOGLU M, VAIDYA J, *et al*. Tools for privacy preserving distributed data mining[J]. *ACM SIGKDD Explorations Newsletter*, 2002, 4(2): 28–34.

张卫国： 男，1964年生， 教授， 研究方向为信息安全与安全多方计算.

孙 嫚： 女，1990年生， 硕士生， 研究方向为安全多方计算.

陈振华： 女，1976年生，副教授， 研究方向为秘密共享与安全多方计算.

陈 娓： 女，1992 年生， 硕士生， 研究方向为安全多方计算.