两个保密位置判断问题的新解法

陈振华[1),2),3)] 李顺东[4)] 黄 琼[5)] 董立红[1)] 陈 娓[1)]

[1)](西安科技大学计算机科学与技术学院 西安 710054)

[2)](中国科学院信息工程研究所信息安全国家重点实验室 北京 100093)

[3)](桂林电子科技大学广西可信软件重点实验室 广西 桂林 541004)

[4)](陕西师范大学计算机科学学院 西安 710062)

[5)](华南农业大学数学与信息学院 广州 510642)

摘 要 保护隐私的位置判断是一种具体的安全多方计算几何问题,这种问题是指各个参与者位于平面或者空间中的一个位置,在保持各自输入隐私的条件下,判断他们之间的相对位置.点包含问题是保密判断一个点是否落在一个凸多边形的内部;两组数据对应成比例问题可保密判断空间中两个平面或直线是否平行,这两个问题同属于安全多方几何计算中保护隐私的位置判断问题.目前该两个问题的已存方案由于转化方法的问题,并不太高效,因此研究如何构造高效协议有着重要的意义.针对这个问题,该文首先将点包含问题转化为三角形面积问题;将两组数据对应成比例问题转化为向量共线问题,然后基于内积协议解决了这两个问题.最后,将该文的两个协议作为基础协议,分别给出了三个应用:保密判断凸多边形包含、三角形相似、空间几何对象的相对位置.最后的分析显示,相比以往的方案,作者的转化技巧是全新的,避免了以往方案中多个基础协议的使用和循环语句的不断调用的缺陷,这使得方案更加简洁,效率得到了提高.

关键词 安全多方计算;点包含;数据对应成比例;内积;位置关系判断

中图法分类号 TP309 **DOI号** 10.11897/SP.J.1016.2018.00336

New Solutions to Two Privacy-Preserving Location-Relation Determining Problems

CHEN Zhen-Hua[1),2),3)] LI Shun-Dong[4)] HUANG Qiong[5)] DONG Li-Hong[1)] CHEN Wei[1)]

[1)](*School of Computer Science and Technology, Xi'an University of Science and Technology, Xi'an* 710054)

[2)](*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093)

[3)](*Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin, Guangxi* 541004)

[4)](*School of Computer Science, Shaanxi Normal University, Xi'an* 710062)

[5)](*College of Mathematics and Informatics, South China Agricultural University, Guangzhou* 510642)

Abstract Privacy-preserving location-relation determination as a specific secure computation geometry issue refers to that each participant locates at a certain position in the plane or the space, who can determine the relative location among them, while keeping individual private inputs. Privacy-preserving location-relation determination as an essential field in secure computation geometry has many applications in real world and location-based services meanwhile protecting user's location privacy such as location monitoring services in wireless sensor networks and location query service in mobile platforms. So, the study on privacy-preserving location-relation determination had an important significance in literature. As two specific problems in this issue, point-inclusion problem refers to determine whether a point is inside a convex polygon or not; two sets of data

收稿日期:2016-09-28;在线出版日期:2017-05-10.本课题得到国家自然科学基金(61472146)、陕西省自然科学基础研究计划面上项目(2017JM6069)、信息安全国家重点实验室开放课题基金(2016-MS-19)、广西可信软件重点实验室研究课题资助(kx201614)资助.
陈振华,女,1976年生,副教授,硕士生导师,研究领域为密码学与信息安全.E-mail:chenzhenhua@snnu.edu.cn.**李顺东**,男,1963年生,教授,博士生导师,主要研究领域为密码学和信息安全.**黄 琼**,男,1982年生,教授,硕士生导师,主要研究领域为密码学和信息安全.**董立红**,女,1968年生,教授,硕士生导师,主要研究领域为系统工程.**陈 娓**,女,1992年生,硕士研究生,主要研究方向为密码学和信息安全.

correspondingly proportional problem refers to determine whether two lines or two planes is parallel or not. The two problems can be classified as the privacy-preserving location-relation determination issue in secure multi-party computation. In theory, the secure multi-party computation problem is solvable by using Yao's garbled circuit protocol. While this approach is appealing in its generality, the computation complexity of the resulting protocols depends on the size of the circuit that expresses the functionality to be computed. When the size of the input domain and the complexity of the circuit are big, the general solution will be really time-consuming. So, using the solutions derived from these general results to solve specific problems can be impractical; problem-specific solutions should be developed. For efficiency reasons, there are many solutions instead of Yao's garbled circuit protocol to deal with the two problems. However, so far the existing schemes to two problems leads to a lower efficiency because of the complexity of transform method or the invoking of multiple basic protocols and loop statements. It is a non-trivial challenge to construct the efficient protocols about the two problems. To this end, making full use of mathematic properties, in this paper we tackle the two problems with the technique of novel transform. To deal with it, we first transform the point-inclusion problem into the triangle area problem, and further into the scalar product problem by taking advantage of the properties of scalar product and matrix. Eventually, we solve the original problem based on the existing scalar product protocol. Secondly, we transform the two sets of data correspondingly proportional problem into the vector collineation problem, and further into the included angle problem. Since the included angel problem can be come up with through the scalar product, we can design the protocol of the two sets of data correspondingly proportional by means of an off-the-shelf scalar product protocol. Furthermore, we give the security analysis and performance analysis. Lastly, employing our two protocols as the basic building blocks, we offer three practical applications convex polygon-inclusion problem that is to privately judge whether one convex polygon is inside the other convex polygon or not, triangle similarity problem that is to privately judge whether two triangles are similar or not, and spatial location-relation problem that is to privately judge in spatial geometry the relative position between plane and plane, line and line, line and plane, point and line, as well as point and plane, respectively. Compared with the technique in other schemes, that in ours is entirely novel and trick, which let our protocols avoid invoking multiple basic protocols and loop statements. These make our protocols more concise and efficient than others.

Keywords　secure multi-party computation; point-inclusion problem; two sets of data correspondingly proportional problem; scalar product; location-relation determination

1　引　言

在目前信息化时代，越来越多的合作计算都需要在保护参与方隐私的条件下完成，这种计算模式都可归属为安全多方计算. 该概念是由 Yao[1] 首先提出的，要求参与计算的各个参与者利用个人的私有数据合作计算一个共同函数. 其中的安全性要求是指在计算过程中保护各个参与方数据的隐私：(1) 不能得到对方的数据；(2) 也不能从计算结果中推出对方的数据. 安全多方计算问题包括：安全科学计算、安全几何计算、安全统计分析等. 它在现实的很多方面都有一些具体的应用. 比如，保真数据分享[2]、比特币交易[3]、高纬数据分类[4]、安全秘密共享[5] 及匿名认证[6].

在安全几何计算中，由于参与者的位置非常敏感，需要对位置隐私进行保护. 因此保护隐私的位置判断成为了安全多方计算中的一个重要研究热点，该问题是指参与方处在平面或立体中的某个位置，在不泄露各自信息的条件下，保密判断参与者之间的相对位置.

点包含问题是保护隐私的位置判断中重要问题之一,即保密判断一个点是否落在某区域内部.针对此问题,Li 等人[7]给出了点与圆、点与椭圆关系的判定方法;Luo 等人[8]给出了点与圆关系的判定方法;Thomas[9]对点和星形多边形的位置进行了判断;Liu 等人[10]对点和平面上任意一条曲线的位置关系进行了研究.但这些已知的方法,都是图形边界规则,且表达式单一.而实际问题中,很多图形的边界并不规则,如果图形边界为不规则的凸多边形,以上方案都已失效.

空间位置关系判断问题是保护隐私的位置判断中另外一个重要问题,即保密判断空间中立体、平面,直线的相对位置.在处理该问题时,罗永龙等人[11]需要首先判断两组数据是否对应成比例,才能得到空间点、线、面的相对位置关系.Li 等人[12]需要计算三棱椎的体积,再利用距离,从而完成对空间点、线、面相对位置的判断.在以上方案中,罗永龙等人[11]使用的两组数据对应成比例协议非常的繁琐.而 Li 等人[12]的方法由于是通过三棱椎转化成距离完成,但两条直线却无法构成三棱椎,因此该方法无法判断空间中两条直线的关系.若只仅仅判断空间中两个平面或直线是否平行,那么已存方法或者效率比较低下(罗永龙等人的方法[11])、或者就已失效(Li 等人的方法[12]).

本文正是针对以上两个具体保密位置判断问题方案中存在的不足,进行了研究,并重新设计了新颖而简洁的协议.

1.1 相关工作

针对第一个问题:即如何判断点和不规则凸多边形包含问题.最早 Du 等人[13]提出了解决方案,首先将点包含问题转化为点和凸多边形各个边之间的位置关系问题,然后基于多种基础协议:点积协议、百万富翁协议、向量优势协议,比较相等协议,判断点和线段之间的位置关系从而解决了该问题.而多种基础协议的使用,使得该问题的解决繁复而低效.后来,Luo 等人[14]将该问题转化为点和多边形各个顶点组成的向量是否都为同一个时针方向问题,利用内积协议和百万富翁问题设计了叉积协议,从而解决了该问题,相比 Du 等人[13]的方案,效率有所提高.

但以上方案[13-14]的一个共同缺点是:由于转化方法的问题,需要调用多种基础协议,且大多基础协议要用到公钥加解密算法,而公钥加解密算法的效率本身就比较低,因此造成了整个协议的效率比较低.为了提高效率,李顺东等人[15]基于 Monte Carlo 方法和 Cantor 编码,将原问题转化为集合包含问题,利用可交换加密算法解决了此问题.该方法很好的提高了效率,但存在的问题是:该协议只是近似解法,并不是精确解法,存在一定的误差.

针对第二个问题:即如何只判断空间两平面或两直线是否平行.由于平面的法向量已知,直线的方向向量已知,因此该问题可以转化为两组数据对应成比例问题.该问题首先由罗永龙等人[11]提出了解决方案,他们将此问题转化为两个对应数据的商是否相等,使用循环语句不断调用内积协议,再使用百万富翁问题,使得方案的计算成本和通信成本较高,成为了制约效率的瓶颈.虽然后来姚亦飞等人[16]对此方案进行了改进,但基本思想还是罗永龙等人[11]的思想,还是不能突破这种思维模式.

以上罗永龙等人[11]和姚亦飞等人[16]方案的共同缺点是:由于转化方法的问题,需要使用循环语句不断调用基础协议,造成了整个方案繁复而效率低下.因此本文欲寻求高效的方法解决两组数据对应成比例问题,从而可判断空间平面或者直线是否平行.

1.2 本文贡献

针对以上方案中存在的问题,我们重新设计了点包含问题的协议和两组数据对应成比例问题的协议,主要贡献如下:

(1)我们的转化方法是全新的:将点包含问题转化为面积问题;将两组数据对应成比例问题转化为向量共线问题.

(2)给出了新的应用:

①将点包含协议应用于图形包含判断;

②将两组数据对应成比例协议分别应用于图形相似判断和空间几何对象相对位置判断.

(3)提高了效率:避免了以往方案中多种基础协议的使用和循环语句的调用,仅利用了内积协议和 hash 函数就解决了本文的两个问题,较大地提高了效率.

2 预备知识

2.1 安全性定义

(1)安全多方计算中的参与者

安全多方计算中的参与者类型主要分为:半诚实者和恶意者[17-18].半诚实者是指在安全多方计算过程中,诚实的输入各自的数据和中间所得到的结果,并严格遵守协议.但出于好奇心或者被某些利益驱使,企图从中间过程和最终计算结果中推算出对方的一些信息.恶意者恰好与之相反,除了试图得到对方信息外,还可能在协议的每一步伪造虚假信息.

由于 Goldreich 在文献[17-18]中已经提出了一些通用转化方法，该方法可以将任意半诚实参与者下设计的协议转化为恶意参与者下的协议，因此我们也假设本文的协议都是在半诚实参与者下设计的. 感兴趣的读者如果想得到恶意参与者下的协议，可以利用 Goldreich 在文献[17-18]中提到的通用方法将本文协议进一步转化.

由于本文的协议都是在两方半诚实参与者下设计的，因此本文只给出两方半诚实参与者下的安全性定义.

(2) 半诚实参与者的安全性定义

设 $f(x,y)$为一个多项式时间的概率函数，Alice 的输入为 x，Bob 的输入为 y，两方合作执行 f 的协议为 π，在执行 π 的过程中，需要在保护 x,y 隐私的前提下，计算出函数 $f(x,y)=(f_1(x,y),f_2(x,y))$. 计算结束后，Alice 得到函数 f 的一个分量 $f_1(x,y)$；Bob 得到函数 f 的另外一个分量 $f_2(x,y)$. 将协议 π 的执行过程中 Alice 获得的视图记为 $view_1(x,y)$，输出记作 $output_1(x,y)$；Bob 的视图记为 $view_2(x,y)$，输出记作 $output_2(x,y)$. 按照 Goldreich 在文献[17]给出的表述，两方半诚实参与者安全性定义如下.

定义 1.　假设有两个概率多项式时间的模拟器 S_1 与 S_2，同时满足以下两式：

$$\{(S_1(x,f_1(x,y)),f_2(x,y))\}\underline{\underline{c}}\{(view_1(x,y),output_2(x,y))\} \quad (1)$$

$$\{(S_2(y,f_2(x,y)),f_1(x,y))\}\underline{\underline{c}}\{(view_2(x,y),output_1(x,y))\} \quad (2)$$

那么计算 $f(x,y)$的协议 π 具有保密性. 其中$\underline{\underline{c}}$是计算不可区分性的表示符号.

以上两式表明了在协议 π 的执行过程中，任意一方在协议中所获得的信息，都只能由自己的输入和自己的输出模拟. 即，一方所获得的信息中都不能得到对方的信息，从而说明了协议 π 是保密执行的.

2.2　hash 函数

定义 2.　若函数 $y=H(x)$同时满足：

(1) 将任一范围的 x 影射成某一特定范围的 y.

(2) 已知x，可在多项式时间内计算出$y=H(x)$；已知 y，不存在多项式时间求出 x，满足 $y=H(x)$.

(3) 不存在多项式时间求两个$x_1,x_2,x_1\neq x_2$，满足 $H(x_1)=H(x_2)$.

则称 $H(x)$为 hash 函数.

2.3　内积协议

定义 3(内积问题).　Alice 拥有向量 $\boldsymbol{X}=(x_1,x_2,\cdots,x_n)$，Bob 拥有向量 $\boldsymbol{Y}=(y_1,y_2,\cdots,y_n)$. 在不揭示双方向量隐私的条件下，两者合作计算出内积 $\langle\boldsymbol{X},\boldsymbol{Y}\rangle$的值.

内积问题是安全多方计算中的基本问题，针对该问题构造的内积协议是构建众多安全多方计算协议的基本模块. 内积协议最早由 Atallah 等人[19]提出，后来有很多文献[20-26]分别根据不同程度的复杂性和安全性提出了不同的方法.

3　点和凸多边形的包含问题

3.1　问题的描述和转化

(1) 问题的描述

Alice 有一个点 $P_0(x,y)$，Bob 有一个多边形 P，该多边形 P 有 n 个顶点 $P_i(x_i,y_i)$，$i=1,2,\cdots,n$. 在不揭示双方隐私的条件下，Alice 和 Bob 想知道 P_0是否在 P 的内部.

(2) 问题的转化

对于点和凸多边形的位置关系，为了清楚起见，我们分别给出下面两图. 其中图 1 表示点 P_0在凸多边形 P 的内部，图 2 表示点 P_0在凸多边形 P 的外部.

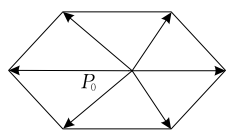

图 1　点在凸多边形内部

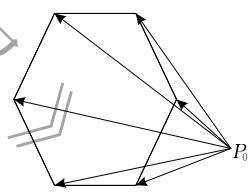

图 2　点在凸多边形外部

从图 1 可以看出，若 P_0在 P 的内部，那么 P_0和 P 各个顶点的连线组成的三角形面积之和必与凸多边形面积相等. 反之，从图 2 可以看出，若 P_0在 P 的外部，那么 P_0和 P 各个顶点的连线组成的三角形面积之和不等于凸多边形面积. 若用 S_{Δ_i}表示 P_0和 P 的任意两个相邻顶点 P_i,P_{i+1}组成的三角形面积，即必有 $S_{凸多边形}=\sum_{i=1}^{n}S_{\Delta_i}$. 而对于 P_0和 P 的两个相邻顶点 P_i,P_{i+1}组成的三角形面积 S_{Δ_i}，有

$$S_{\Delta_i}=\frac{1}{2}\begin{vmatrix}x_0 & y_0 & 1\\ x_i & y_i & 1\\ x_{i+1} & y_{i+1} & 1\end{vmatrix}$$

$$=\frac{1}{2}\left(x_0\begin{vmatrix}y_i & 1\\ y_{i+1} & 1\end{vmatrix}-y_0\begin{vmatrix}x_i & 1\\ x_{i+1} & 1\end{vmatrix}+\begin{vmatrix}x_i & y_i\\ x_{i+1} & y_{i+1}\end{vmatrix}\right)$$

若记 $\begin{vmatrix} y_i & 1 \\ y_{i+1} & 1 \end{vmatrix} = A_i$，$\begin{vmatrix} x_i & 1 \\ x_{i+1} & 1 \end{vmatrix} = B_i$，$\begin{vmatrix} x_i & y_i \\ x_{i+1} & y_{i+1} \end{vmatrix} = C_i$，则三角形面积：$S_{\Delta_i} = \frac{1}{2}(x_0 A_i - y_0 B_i + C_i)$.

通过以上转化得出，要判断点 P_0 是否在凸多边形 P 的内部，只需判断 P_0 和 P 的两个相邻顶点 P_i，P_{i+1} 组成的所有三角形面积之和是否与凸多边形面积相等即可. 而要求三角形面积 S_{Δ_i}，可看成一方持有向量 $\boldsymbol{X}=(x_0,-y_0,1)$，另一方持有向量 $\boldsymbol{Y}_i=(A_i,B_i,C_i)$，通过保密求内积$\langle \boldsymbol{X},\boldsymbol{Y}_i\rangle$可以得到. 而对于保密求内积，可以调用 2.3 节中现有内积协议之一完成. 下面给出具体的协议.

3.2 具体协议

协议 1. 安全判断点和凸多边形包含.

输入：Alice 保密输入一个点 $P_0(x,y)$，Bob 保密输入一个凸多边形 P，该凸多边形 P 有 n 个顶点 $P_i(x_i,y_i)$，$i=1,2,\cdots,n$

输出：Alice 和 Bob 都知道 P_0 是否在 P 的内部，即 $P_0 \subset P$ 或者 $P_0 \not\subset P$

1. Bob 在本地任选凸多边形 P 两个相邻的顶点 P_i，P_{i+1}，得到 $P_i(x_i,y_i)$，$P_{i+1}(x_{i+1},y_{i+1})$，计算：

$A_i = \begin{vmatrix} y_i & 1 \\ y_{i+1} & 1 \end{vmatrix}$，$B_i = \begin{vmatrix} x_i & 1 \\ x_{i+1} & 1 \end{vmatrix}$，$C_i = \begin{vmatrix} x_i & y_i \\ x_{i+1} & y_{i+1} \end{vmatrix}$

Bob 得到向量 $\boldsymbol{Y}_i=(A_i,B_i,C_i)$，$i=1,2,\cdots,n$. 进一步，得到这 n 个向量之和 $\sum_{i=1}^{n}\boldsymbol{Y}_i$.

2. Alice 得到向量 $\boldsymbol{X}=(x_0,-y_0,1)$.

3. Bob 调用内积协议得到 $\left\langle \boldsymbol{X},\sum_{i=1}^{n}\boldsymbol{Y}_i \right\rangle$，进一步，Bob 得到 n 个三角形的面积之和：

$$\sum_{i=1}^{n} S_{\Delta_i} = \frac{1}{2}\sum_{i=1}^{n}\langle \boldsymbol{X},\boldsymbol{Y}_i\rangle = \frac{1}{2}\left\langle \boldsymbol{X},\sum_{i=1}^{n}\boldsymbol{Y}_i \right\rangle$$

4. Bob 计算自己多边形的面积 $S_{凸多边形}$，并和 $\sum_{i=1}^{n} S_{\Delta_i}$ 做比较. 若 $S_{凸多边形} = \sum_{i=1}^{n} S_{\Delta_i}$，则点 P_0 在凸边形 P 的内部；否则在外部.

在我们的协议 1 中，根据 Bob 计算的最后内积结果，这样可以比较 n 个三角形的面积之和是否和自己持有的多边形面积相等. 由于内积的结果 $\left\langle \boldsymbol{X},\sum_{i=1}^{n}\boldsymbol{Y}_i \right\rangle$ 含有 2 个未知数 x_0，y_0，因此不能得到 Alice 的任何信息. 此外，我们并没有逐个计算每个小三角形的面积 S_{Δ_i}，而是充分利用内积的性质 $\langle \boldsymbol{X},\boldsymbol{Y}_1\rangle + \langle \boldsymbol{X},\boldsymbol{Y}_2\rangle = \langle \boldsymbol{X},\boldsymbol{Y}_1+\boldsymbol{Y}_2\rangle$，一次性求出了各个三角形面积之和，这样就避免了循环语句的使用.

对于点和凸多边形的包含问题，当点在凸多边形的边界上时，三角形面积之和等于凸多边形面积，因此，我们把这种情况归于点在凸多边形内部.

对于点和凹多边形的包含问题，不存在本文的规律，即，若点在凹多边形内部，则三角形面积之和不一定等于凹多边形面积(画图立刻可以得出本结论)，本文的方法不再适用. 因此，对于点和凹多边形的包含问题，需要寻求另外的解决方法.

4 两组数据对应成比例问题

4.1 问题的描述和转化

(1) 问题的描述

Alice 有一组数据 $\{x_1,x_2,\cdots,x_n\}$，Bob 有一组数据 $\{y_1,y_2,\cdots,y_n\}$，在不泄露各自信息的情况下，Alice 和 Bob 想知道两组数据是否对应成比例.

(2) 问题的转化

若两组数据 $\{x_1,x_2,\cdots,x_n\}$ 和 $\{y_1,y_2,\cdots,y_n\}$ 对应成比例，那么就有 $\frac{x_1}{y_1}=\frac{x_2}{y_2}=\cdots=\frac{x_n}{y_n}=k$，即 $\{x_1,x_2,\cdots,x_n\}=k\{y_1,y_2,\cdots,y_n\}$. 若把 $(x_1,x_2,\cdots,x_n)$ 记为向量 $\boldsymbol{X}$，$(y_1,y_2,\cdots,y_n)$ 记为向量 $\boldsymbol{Y}$，则有 $\boldsymbol{X}=k\boldsymbol{Y}$，即两个向量可线性表出，表示在几何图形上就为两个向量共线. 为了清楚起见，我们分别给出下面两图(为了便于观察，我们给出的是平面图). 其中图 3 表示两组数据对应成比例(即向量 $\boldsymbol{X}$ 和向量 $\boldsymbol{Y}$ 共线)；图 4 表示两组数据对应不成比例(即向量 $\boldsymbol{X}$ 和向量 $\boldsymbol{Y}$ 不共线).

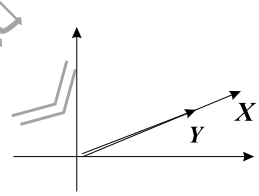

图 3 两组数组对应成比例

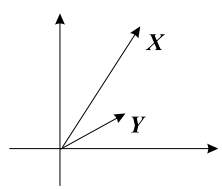

图 4 两组数组对应不成比例

从图 3 可以看出，若两组数据对应成比例，那么两组数据对应的向量必能线性表出，即两个向量必然共线，此时两向量夹角为 0 或者 π，而夹角公式 $\cos\theta = \frac{\langle \boldsymbol{X},\boldsymbol{Y}\rangle}{|\boldsymbol{X}|\,|\boldsymbol{Y}|}$，$\theta$ 为向量 $\boldsymbol{X}$ 和向量 $\boldsymbol{Y}$ 的夹角.

通过以上转化得出，要判断两组数据是否对应成比例，只需判断两个向量是否共线，即判断两个向

量的夹角是否为 0 或者 π 即可. 而要求夹角，可以借助内积协议$\langle \boldsymbol{X},\boldsymbol{Y}\rangle$完成. 下面给出具体协议.

4.2 具体协议

协议 2. 安全判断两组数据对应成比例.

输入：Alice 保密输入数组 $X=\{x_1,x_2,\cdots,x_n\}$，Bob 保密输入数组 $Y=\{y_1,y_2,\cdots,y_n\}$，$n\geq 3$

输出：Alice 和 Bob 都知道两组数据是否对应成比例，即 $X=kY$ 或者 $X\neq kY$

1. Alice 和 Bob 分别将两组数据写成两个向量 $\boldsymbol{X},\boldsymbol{Y}$，然后调用内积协议，Alice 得到$\langle \boldsymbol{X},\boldsymbol{Y}\rangle$，并计算 $\dfrac{\langle \boldsymbol{X},\boldsymbol{Y}\rangle}{|\boldsymbol{X}|}$. 进一步，Alice 计算 Hash 值 $H\left(\left|\dfrac{\langle \boldsymbol{X},\boldsymbol{Y}\rangle}{|\boldsymbol{X}|}\right|\right)=H_1$.
2. Bob 计算 Hash 值 $H(|\boldsymbol{Y}|)=H_2$.
3. Alice 和 Bob 比较 H_1 和 H_2 是否相等，若 $H_1=H_2$，则 $\left|\dfrac{\langle \boldsymbol{X},\boldsymbol{Y}\rangle}{|\boldsymbol{X}|}\right|=|\boldsymbol{Y}|$，此时 $\cos\theta=\left|\dfrac{\langle \boldsymbol{X},\boldsymbol{Y}\rangle}{|\boldsymbol{X}|\,|\boldsymbol{Y}|}\right|=1$，即 $\cos\theta=\pm 1$，则表明向量 $\boldsymbol{X}$ 和向量 $\boldsymbol{Y}$ 的夹角为 0 或者 π，即两个向量 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$ 共线，得到两组数据 X 和 Y 对应成比例；否则不成比例.

在协议 2 中，由于我们的协议是根据两向量是否共线来进行，即通过夹角完成的. 若判断出两个数组对应数据成比例，Bob 向量 $\boldsymbol{Y}$ 的模长 $|\boldsymbol{Y}|$ 会被 Alice 得到. 但 Alice 从模长 $|\boldsymbol{Y}|$ 中不能推导出 Bob 的任何信息. 不过协议 2 的安全性已经不再是完美安全性(即信息零泄露). 关于此点，Du 等人在文献[13]中进行了论述：为了协议的高效性，在不影响方案安全性的前提下，可以在设计协议时，允许信息部分泄露，达到接受性安全即可.

由于协议 2 针对的是三维以上数组，对于二维数组，可以直接利用罗永龙等人[11]的思想，化为商，调用一次内积即可完成.

5 安全性分析

应用 2.1 节的安全性定义对本文的 2 个协议进行证明.

定理 1. 协议 1 保密判断了点和凸多边形是否包含.

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

$$f_1(X,Y)=f_2(X,Y)=(P_0\subset P)$$

或者

$$f_1(X,Y)=f_2(X,Y)=(P_0\not\subset P)$$

假设 $f_1(X,Y)=f_2(X,Y)=(P_0\subset P)$，构造模拟器 S_1. S_1 接受 $(X,f_1(X,Y))$ 作为输入，按如下方式工作：

第 1 步. S_1 接受输入 $(X,f_1(X,Y))=(P_0,P_0\subset P)$ 后，首先随机选取一个凸多边形 P'，该多边形 n 个顶点为 $P_i'(x_i',y_i')$，$i=1,2,\cdots,n$，使得 $f_1(P_0,P)=f_1(P_0,P')$. 然后用 $(P_0(x_0,y_0),P')$ 进行模拟. 按照协议 1，S_1 得到向量 $\sum_{i=1}^{n}\boldsymbol{Y}_i'$.

第 2 步. S_1 得到向量 $\boldsymbol{X}=(x_0,-y_0,1)$，记为 A.

第 3 步. S_1 调用内积协议，得到三角形的面积之和 $\sum_{i=1}^{n}S_{\Delta_i}'=\dfrac{1}{2}\sum_{i=1}^{n}\langle \boldsymbol{X},\boldsymbol{Y}_i'\rangle=\dfrac{1}{2}\left\langle \boldsymbol{X},\sum_{i=1}^{n}\boldsymbol{Y}_i'\right\rangle$，记为 B'.

第 4 步. S_1 计算凸多边形 P' 的面积 $S'_{凸多边形}$，并计较 $S'_{凸多边形}$ 和 B' 是否相等. 若相等，则点 P_0 在凸边形 P' 的内部，结果记为 C'.

在本协议中：

$$view_1(X,Y)=\{X,A,C\}$$

$$S_1(X,f_1(X,Y))=\{X,A,C'\}$$

由于 $C=f_1(P_0,P)=(P_0\subset P)$，$f_1(P_0,P)=f_1(P_0,P')$，因此 $C'=f_1(P_0,P')=(P_0\subset P')$，得到 $C=C'$. 所以：

$$\{X,A,C\}\subseteq\{X,A,C'\}$$

又因为 $output_2(X,Y)=f_2(X,Y)=(P_0\subset P)$，因此有：

$$\{(S_1(x,f_1(x,y)),f_2(x,y))\}\subseteq\{(view_1(x,y),output_2(x,y))\}$$

同理，用类似的方法可构造模拟器 S_2，使得：

$$\{(S_2(y,f_2(x,y)),f_1(x,y))\}\subseteq\{(view_2(x,y),output_1(x,y))\}$$

证毕.

定理 2. 协议 2 保密判断了两组数据是否对应成比例.

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

$$f_1(X,Y)=f_2(X,Y)=(X=kY)$$

或者

$$f_1(X,Y)=f_2(X,Y)=(X\neq kY)$$

假设 $f_1(X,Y)=f_2(X,Y)=(X=kY)$，构造模拟器 S_1. 首先将 $(X,f_1(X,Y))$ 输入给 S_1，S_1 执行以下步骤：

第 1 步. S_1 选取一个随机的 n 维数组 Y'，使得 $f_1(X,Y)=f_1(X,Y')$. 然后用 (X,Y') 进行模拟. 按照协议 2，S_1 先将原来两个数组分别转化为向量 $\boldsymbol{X}$，$\boldsymbol{Y}'$，然后调用内积协议得到$\langle \boldsymbol{X},\boldsymbol{Y}'\rangle$，记为 A'. 并计算 $\dfrac{\langle \boldsymbol{X},\boldsymbol{Y}'\rangle}{|\boldsymbol{X}|}=\dfrac{A'}{|\boldsymbol{X}|}$，记为 B'. 进一步，S_1 计算

$$H\left(\left|\frac{\langle \boldsymbol{X},\boldsymbol{Y}'\rangle}{|\boldsymbol{X}|}\right|\right)=H(B')=H_1'.$$

第 2 步. S_1 计算 $H(\boldsymbol{Y}')=H_2'$.

第 3 步. 比较 H_1'和 H_2'是否相等,若 $H_1'=H_2'$,则两组数据对应成比例,将结果记为 C'.

在本协议中:

$$view_1(X,Y)=\{X,A,B,H_1,H_2,C\}$$

$$S_1(X,f_1(X,Y))=\{X,A',B',H_1',H_2',C'\}$$

由于 $C=f_1(X,Y)=(X=kY)$, $f_1(X,Y)=f_1(X,Y')$,因此 $C'=f_1(X,Y')=(X=kY')$,得到 $C=C'$. 由于 Y'为 S_1随机取的一组数据,而 S_1并不知道对方数据 Y 的任何信息,因此 $H_2\subseteq H_2'$, $A\subseteq A'$. 而由于 $B'=\frac{A'}{|X|}$, $H_1'=H(B')$; $B=\frac{A}{|X|}$, $H_1=H(B)$,因此 $B\subseteq B'$, $H_1\subseteq H_1'$. 所以:

$$\{X,A,B,H_1,H_2,C\}\subseteq\{X,A',B',H_1',H_2',C'\}$$

又因为 $output_2(X,Y)=f_2(X,Y)=(X=kY)$,因此有:

$$\{(S_1(x,f_1(x,y)),f_2(x,y))\}$$
$$\subseteq\{(view_1(x,y),output_2(x,y))\}$$

同理,用类似的方法可构造模拟器 S_2,使得:

$$\{(S_2(y,f_2(x,y)),f_1(x,y))\}$$
$$\subseteq\{(view_2(x,y),output_1(x,y))\}$$ 证毕.

6 执行分析

将本文设计的 2 个协议和引言中的相关协议进行效率和性能的分析和对比. 由于文献[15]提出的方法不是精确解法,只是一种近似解法,因此针对点包含,我们只将协议 1 和文献[13,14]这三种精确解法做出分析和对比. 针对两组数据对应成比例,我们将协议 2 和文献[11,16]进行分析和对比. 为了便于做出比较,统一凸多边形的顶点都为 n 个,两组数据的维数都为 n 维.

计算复杂度

由于以上方案利用了基础协议中的内积协议、百万富翁协议和判断相等协议. 为了方便比较,假设所有方案调用的是同一个内积协议、同一个百万富翁协议、同一个判断相等协议. 内积协议记为 M_s,百万富翁协议记为 M_m,判断相等协议记为 M_e. 由于各个文献使用的基础协议次数各不相同,因此把各个方案中需要调用的基础协议总个数作为衡量计算复杂性的指标.

(1) 点包含问题

文献[13]:使用了 n 个内积协议、$4n$ 个百万富翁协议、1 个判断相等协议. 得到总计算开销为 $nM_s+4nM_m+M_e$.

文献[14]:使用了 n 个内积协议、n 个百万富翁协议. 得到总计算开销为 nM_s+nM_m.

Ours(协议 1):使用了 1 个内积协议,得到总计算开销为 M_s.

(2) 两组数据对应成比例问题

文献[11]:使用了 n 个内积协议、1 个判断相等协议. 得到总计算开销为 nM_s+M_e.

文献[16]:最优情况下,内积协议和判断相等协议各使用 1 个;最坏情况下,内积协议和判断相等协议各使用 n 个. 得到总计算开销为 $(M_s+M_e)\sim(nM_s+nM_e)$.

Ours(协议 2):使用了 1 个内积协议、2 个 hash 运算. 得到总计算开销为 M_s+2H.

通信复杂度

通信复杂度可以利用协议传递的信息位数,或者传递轮数做为比较标准,在安全多方计算中多选用传递轮数(round). 假设所有方案中使用的内积协议和百万富翁协议各交互了 3 rounds.

(1) 点包含问题

文献[13]:使用了内积协议、向量优势协议、判断相等协议. 而向量优势协议是通过不断调用百万富翁协议完成. 内积协议交互了 $3n$ rounds、向量优势协议交互了 $12n$ rounds、判断相等协议交互了 3 rounds. 得到总通信开销为 $(3+15n)$ rounds.

文献[14]:使用了叉积协议. 而叉积协议是通过内积协议和百万富翁协议完成的. 内积协议交互了 $3n$ rounds、百万富翁协议交互了 $3n$ rounds. 得到总通信开销为 $6n$ rounds.

Ours(协议 1):使用了内积协议. 得到总通信开销为 3 rounds.

(2) 两组数据对应成比例问题

文献[11]:内积协议交互了 $3n$ rounds、判断相等协议交互了 3 rounds. 得到总通信开销为 $(3+3n)$ rounds.

文献[16]:最优情况下,内积协议和判断相等协议各交互了 3 rounds;最坏情况下,内积协议和判断相等协议各交互了 $3n$ rounds. 得到总通信开销为 6 rounds$\sim$6n rounds.

Ours(协议 2):内积协议交互了 3 rounds、hash 函数交互了 1 round. 得到总通信开销为 4 rounds.

性能

以各个方案利用的基础协议多少、循环语句调用多少作为衡量性能的指标.

综合以上分析,得到协议 1 与文献[13-14],协议 2 与文献[11,16]在效率和性能方面的比较分别如表 1、表 2.

表 1　协议 1、2 与相关协议的效率比较

问题	协议	计算成本	通信成本
点包含	文献[13]	$nM_s+4nM_m+M_e$	$(6+12n)$rounds
	文献[14]	nM_s+nM_m	$6n$ rounds
	Ours(协议 1)	M_s	3 rounds
数据对应成比例	文献[11]	nM_s+M_e	$(3+3n)$rounds
	文献[16]	$nM_s+nM_e\sim M_s+M_e$	6 rounds$\sim 6n$ rounds
	Ours(协议 2)	M_s+2H	4 rounds

表 2　协议 1、2 与相关协议的性能比较

问题	协议	基础协议		循环语句
		种类	个数	
点包含	文献[13]	内积；百万富翁 向量优势；判断相等	4	$5n$
	文献[14]	内积；叉积 百万富翁	3	$2n$
	Ours(协议 1)	内积	1	1
数据对应成比例	文献[11]	内积判断相等	2	n
	文献[16]	内积判断相等	2	$1\sim 2n$
	Ours(协议 2)	内积；Hash	2	1

7　应　用

本节以本文的两个协议作为基础模块，给出三个具体的应用. 将协议 1 应用于图形包含，解决了两个凸多边形包含问题；将协议 2 应用于图形相似，不但解决了两个三角形相似问题，而且给出了空间位置关系的高效判断方法.

7.1　应用 1：两个凸多边形包含

(1) 问题的描述

Alice 有一个凸多边形Ω_1，顶点分别为$p_i(x_i,y_i)$，$i=1,2,\cdots,n$；Bob 有另一个凸多边形 Ω_2，顶点分别为 $q_j(x_j,y_j)$，$j=1,2,\cdots,m$，在不泄露各自信息的情况下，判断凸多边形 Ω_1 是否包含凸多边形 Ω_2. 为了清楚起见，我们分别给出下面两个图形. 其中图 5 表示两个凸多边形包含，图 6 表示两个凸多边形不包含.

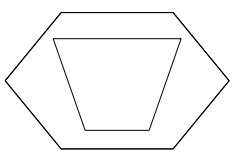

图 5　两个凸多边形包含

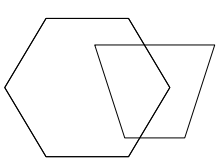

图 6　两个凸多边形不包含

(2) 问题的解决

从图 5、图 6 可以看出，要判断两个凸多边形是否有包含关系，只需判断凸多边形 Ω_1 是否包含凸多边形 Ω_2 的所有顶点即可. 如果凸多边形 Ω_1 包含凸多边形 Ω_2 的所有顶点，那么两者存在包含关系；如果有一个顶点不被包含，那么两者不存在包含关系. 即将凸多边形包含问题转化为点和凸多边形的包含问题，从而调用协议 1 解决.

(3) 具体协议

协议 3.　安全判断两个凸多边形包含.

输入：Alice 保密输入一个凸多边形 Ω_1，顶点分别为 $p_i(x_i,y_i)$，$i=1,2,\cdots,n$；Bob 保密输入另一个凸多边形 Ω_2，顶点分别为 $q_j(x_j,y_j)$，$j=1,2,\cdots,m$

输出：Alice 和 Bob 都知道凸多边形 Ω_1 是否包含凸多边形 Ω_2

1. 对于凸多边形 Ω_2 的顶点 $q_1(x_1,y_1)$，Alice 调用协议 1，判断点 q_1 是否在凸多边形 Ω_1 内部，如果不在内部，那么协议停止，得到凸多边形 Ω_1 不包含凸多边形 Ω_2；否则转入下一步.
2. For ($j=1$；$j<=m$；$j++$)，Alice 不断调用协议 1，若所有凸多边形 Ω_2 的顶点 q_j 都包含在凸多边形 Ω_1 内部，那么凸多边形 Ω_1 包含凸多边形 Ω_2.

7.2　应用 2：两个三角形相似

(1) 问题的描述

Alice 有一个三角形 Ω_1，顶点分别为 $p(x_i,y_i)$，$i=1,2,3$；Bob 有另一个三角形 Ω_2，顶点分别为 $q_j(x_j,y_j)$，$j=1,2,3$，在不泄露各自信息的情况下，判断两三角形 Ω_1 和 Ω_2 是否相似.

(2) 问题的解决

根据已有几何知识得知，要判断两三角形是否相似，只需判断两个三角形的边是否对应成比例即可. 即将两个三角形相似问题转化为两组数据对应成比例问题，从而调用协议 2 解决. 但由于 Alice 和 Bob 不知道两个三角形到底哪两条边对应，因此需要使用循环语句进行穷举. 如果存在成比例的情况，则协议结束，输出结果为两个三角形相似；否则需要执行所有可能的组合，如果所有的组合都不成比例，则两个三角形不相似. 最坏的情况下，需要调用 6 次协议 2.

(3) 具体协议

协议 4.　安全判断两个三角形相似.

输入：Alice 保密输入一个三角形 Ω_1，顶点分别为 $p_i(x_i,y_i)$，$i=1,2,3$；Bob 保密输入另一个三角形 Ω_2，顶点分别为 $q_j(x_j,y_j)$，$j=1,2,3$

输出：Alice 和 Bob 都知道两三角形 Ω_1 和 Ω_2 是否相似

1. Alice 计算三角形 Ω_1 的每个边长，记为数组 $X=\{a_1,a_2,a_3\}$；同理，Bob 计算三角形 Ω_2 的每个边长，

记为数组 $Y=\{b_1,b_2,b_3\}$.

2. 调用协议 2,Alice 和 Bob 判断两个数组 X 和 Y 是否应成比例,如果成比例,那么协议停止,得到两个三角形相似;否则转入下一步.
3. Alice 和 Bob 不断将各自数组的每个分量对换位置,调用协议 2,若所有情况下(最坏情况是调用 6 次),不存在对应成比例,那么两个三角形不相似;反之,若有一次对应成比例,则两个三角形相似.

7.3 应用 3:空间几何对象相对位置判断

罗永龙等人在文献[11]中利用内积协议和两组数据对应成比例协议,保密解决了空间线线、线面、面面这些几何对象相对位置的判断. 但罗永龙等人[11]设计的两组数据对应成比例协议,由于调用了循环语句,导致协议非常繁琐,效率不高. 本节,我们利用本文设计的数组对应成比例协议(协议 2),将罗永龙等人[11]的方案改进,以此得到高效协议.

(1) 拟解决的问题

问题 1:保密判断空间两直线的相对位置. Alice 持有直线 $L_1:\begin{cases}A_1x+B_1y+C_1z+D_1=0\\A_2x+B_2y+C_2z+D_2=0\end{cases}$,Bob 持有另一直线 $L_2:\begin{cases}A_3x+B_3y+C_3z+D_3=0\\A_4x+B_4y+C_4z+D_4=0\end{cases}$. 两者在保护各自隐私的前提下,判断两空间直线 L_1 与 L_2 的相对位置.

问题 2:保密判断空间直线与平面的相对位置. Alice 持有直线 $L:\begin{cases}A_1x+B_1y+C_1z+D_1=0\\A_2x+B_2y+C_2z+D_2=0\end{cases}$,Bob 持有平面 $\Pi:A_3x+B_3y+C_3z+D_3=0$. 两者在保护各自隐私的前提下,判断空间直线 L 与平面 Π 的相对位置.

问题 3:保密判断空间两平面的相对位置. Alice 持有平面 $\Pi_1:A_1x+B_1y+C_1z+D_1=0$,Bob 持有另一平面 $\Pi_2:A_2x+B_2y+C_2z+D_2=0$. 两者在保护各自隐私的前提下,判断两空间平面 Π_1 与 Π_2 的相对位置.

(2) 问题的转化

空间线与线、线与面、面与面的位置关系可以转化为方向向量和法向量的关系.

例如,要解决本节的问题三:面面位置判断. 等价于已知平面 Π_1 的法向量为 $\boldsymbol{a}=(A_1,B_1,C_1)$,平面 Π_2 的法向量为 $\boldsymbol{b}=(A_2,B_2,C_2)$. 若向量的内积 $\langle\boldsymbol{a},\boldsymbol{b}\rangle=A_1A_2+B_1B_2+C_1C_2=0$,表示两个法向量垂直,则平面 Π_1 与平面 Π_2 垂直. 若内积 $\langle\boldsymbol{a},\boldsymbol{b}\rangle=A_1A_2+B_1B_2+C_1C_2\neq0$,则进一步判断两组数据 $\frac{A_1}{A_2}=\frac{B_1}{B_2}=\frac{C_1}{C_2}$ 是否对应比例. 若不对应成比例,那么平面 Π_1 与平面 Π_2 相交;若对应成比例,表示两个法向量平行或者重合,则平面 Π_1 与平面 Π_2 平行或者重合. 在此基础上,进一步区分平行和重合的情况,判断两组数据 $\frac{A_1}{A_2}=\frac{B_1}{B_2}=\frac{C_1}{C_2}=\frac{D_1}{D_2}$ 是否对应成比例,若对应成比例,那么重合;否则平行.

由以上分析可知,要判断空间两个平面的相对位置,可转化为判断空间两平面法向量的关系,而要判断两个法向量的关系,可通过内积协议和数组对应成比例协议,即调用本文协议 2 完成. 下面给出本文设计的新协议.

(3) 新的协议

协议 5. 安全计算空间两直线的相对位置.

输入:Alice 以直线 L_1 作为秘密输入,

$$L_1:\begin{cases}A_1x+B_1y+C_1z+D_1=0\\A_2x+B_2y+C_2z+D_2=0\end{cases},$$

Bob 以直线 L_2 作为秘密输入,

$$L_2:\begin{cases}A_3x+B_3y+C_3z+D_3=0\\A_4x+B_4y+C_4z+D_4=0\end{cases}$$

输出:在保护空间两直线 L_1 和 L_2 隐私的前提下,Alice 和 Bob 判断两者的相对位置

1. Alice 利用行列式计算叉积,得到直线 L_1 的方向向量

$$\boldsymbol{e}_1=(m_1,n_1,l_1)=\begin{vmatrix}i&j&k\\A_1&B_1&C_1\\A_2&B_2&C_2\end{vmatrix}.$$

同理,Bob 也可以得到直线 L_2 的方向向量

$$\boldsymbol{e}_2=(m_2,n_2,l_2)=\begin{vmatrix}i&j&k\\A_3&B_3&C_3\\A_4&B_4&C_4\end{vmatrix}.$$

2. Alice 和 Bob 调用内积协议,保密计算内积 $\langle\boldsymbol{e}_1,\boldsymbol{e}_2\rangle$. 若 $\langle\boldsymbol{e}_1,\boldsymbol{e}_2\rangle=0$,则两个方向向量垂直,即两条直线 L_1 与 L_2 垂直. 若 $\langle\boldsymbol{e}_1,\boldsymbol{e}_2\rangle\neq0$,则进一步调用协议 2,判断两组数据 $\frac{m_1}{m_2}=\frac{l_1}{l_2}=\frac{n_1}{n_2}$ 是否对应比例. 若不对应成比例,则两个方向向量相交,即两条直线 L_1 与 L_2 相交;若对应成比例,那么两个方向向量平行或者重合,即两条直线 L_1 与 L_2 平行或重合,则转入下面的步骤.
3. Alice 在 L_1 上任取一点 $\{x_0,y_0,z_0\}$,得到向量 $\boldsymbol{a}=(x_0,y_0,z_0,1)$. Bob 持有向量 $\boldsymbol{b}=(A_3,B_3,C_3,D_3)$,$\boldsymbol{c}=(A_4,B_4,C_4,D_4)$. 利用内积协议,Alice 和 Bob 分别得到两向量 $\boldsymbol{a}$ 与 $\boldsymbol{b}$、两向量 $\boldsymbol{a}$ 与 $\boldsymbol{c}$ 的内积. 若 $(\langle\boldsymbol{a},\boldsymbol{b}\rangle=0)\wedge(\langle\boldsymbol{a},\boldsymbol{c}\rangle=0)$,则得到 L_1 与 L_2 的相对位置为重合;若不满足,则得到 L_1 与 L_2 的相对位置为平行.
4. Alice 将判断结果传递给 Bob.

协议 6. 安全计算空间直线与平面的相对位置.

输入:Alice 以直线 $L:\begin{cases}A_1x+B_1y+C_1z+D_1=0\\A_2x+B_2y+C_2z+D_2=0\end{cases}$ 作为秘密输入,Bob 以平面 $\Pi:A_3x+B_3y+C_3z+D_3=0$ 作为秘密输入

输出：在保护空间直线 L 和平面 Π 隐私的前提下，Alice 和 Bob 判断两者的相对位置

1. Alice 利用行列式计算叉积，得到直线 L 的方向向量 $\boldsymbol{e}=(m,n,l)=\begin{vmatrix} i & j & k \\ A_1 & B_1 & C_1 \\ A_2 & B_2 & C_2 \end{vmatrix}$，Bob 持有平面 Π 的法向量 $\boldsymbol{d}=(A_3,B_3,C_3)$.

2. Alice 和 Bob 调用内积协议，保密计算内积$\langle \boldsymbol{e},\boldsymbol{d}\rangle$. 若$\langle \boldsymbol{e},\boldsymbol{d}\rangle\neq 0$，则进一步调用协议 2，判断两组数据$\frac{m}{A_3}=\frac{l}{B_3}=\frac{n}{C_3}$是否对应比例. 若不对应成比例，那么方向向量和法向量相交，即直线 L 与平面 Π 相交；若对应成比例，那么方向向量和法向量平行，即直线 L 与平面 Π 垂直. 若内积$\langle \boldsymbol{e},\boldsymbol{d}\rangle=0$，则说明方向向量和法向量垂直，得到直线 L 与平面 Π 要么重合，要么平行. 为了得到定论，执行如下环节.

3. Alice 在直线 L 上任取点$\{x_1,y_1,z_1\}$，从而得到向量 $\boldsymbol{a}=(x_1,y_1,z_1,1)$，Bob 持有向量 $\boldsymbol{b}=(A_3,B_3,C_3,D_3)$，再次调用内积协议，可求得内积$\langle \boldsymbol{a},\boldsymbol{b}\rangle$. 若$\langle \boldsymbol{a},\boldsymbol{b}\rangle=0$，那么直线 L 与平面 Π 相对位置为重合；若不满足，得到直线 L 与平面 Π 相对位置为平行.

4. Alice 将判断结果传递给 Bob.

协议 7.　安全计算空间两平面的相对位置.

输入：Alice 以平面 $\Pi_1:A_1x+B_1y+C_1z+D_1=0$ 作为秘密输入，Bob 平面 $\Pi_2:A_2x+B_2y+C_2z+D_2=0$ 作为秘密输入

输出：在保护空间两平面 Π_1 和 Π_2 的隐私下，Alice 和 Bob 判断两者的相对位置

1. Alice 得到平面 Π_1 的法向量 $\boldsymbol{d}_1=(A_1,B_1,C_1)$，Bob 得到平面 Π_2 的法向量 $\boldsymbol{d}_2=(A_2,B_2,C_2)$.

2. Alice 和 Bob 调用内积协议，计算内积$\langle \boldsymbol{d}_1,\boldsymbol{d}_2\rangle=A_1A_2+B_1B_2+C_1C_2$. 若$\langle \boldsymbol{d}_1,\boldsymbol{d}_2\rangle=0$，表示两个法向量垂直，则平面 Π_1 与平面 Π_2 垂直. 若内积$\langle \boldsymbol{d}_1,\boldsymbol{d}_2\rangle\neq 0$，则调用协议 2，进一步判断两组数据$\frac{A_1}{A_2}=\frac{B_1}{B_2}=\frac{C_1}{C_2}$是否对应比例. 若不对应成比例，那么平面 Π_1 与平面 Π_2 相交；若对应成比例，表示两个法向量平行或者重合，则平面 Π_1 与平面 Π_2 平行或者重合，转入以下步骤.

3. Alice 再次调用协议 2，判断两组数据$\frac{A_1}{A_2}=\frac{B_1}{B_2}=\frac{C_1}{C_2}=\frac{D_1}{D_2}$是否对应成比例. 若对应成比例，那么平面 Π_1 与平面 Π_2 相对位置为重合；若不满足，得到 Π_1 与 Π_2 的相对位置为平行.

4. Alice 将判断结果传递给 Bob.

(4) 效率分析与比较

我们给出本小节的三个协议和罗永龙等人[11]在处理同样的空间几何问题时构造的协议的效率对比. 两个方案利用的基础协议中，比较复杂的是内积协议，因此把两个方案中用户需要调用的内积协议总次数，作为衡量计算复杂性的指标，其它忽略不计. 为了便于做出比较，统一本小节和文献[11]中，两组数据的规模都是 n，使用的都是同一个内积协议. 通信复杂度仍然用轮数(round). 假设内积协议每调用一次，通信轮数为 3 rounds. 用√(是)、×(否)表示位置关系的是否判断和循环语句的是否调用.

文献[11]的安全计算两直线相对位置(协议 5)：分别需要计算 1 次内积和判断 1 次数据是否对应成比例. 当判断数据是否对应成比例时，又需要反复不断计算内积，导致该协议共需要计算 n 次内积. 而本文安全计算两直线相对位置(协议 5)：内积计算了 3 次，判断数据是否对应成比例时，只需要计算 1 次内积，因此，共计算 4 次内积.

文献[11]安全计算线与面的相对位置(协议 6)：没有调用数据对应成比例协议，计算了 2 次内积. 本文安全计算线与面的相对位置(协议 6)：内积计算了 2 次，判断数据是否对应成比例时，只需要计算 1 次内积，因此，共计算 3 次内积.

文献[11]安全计算两平面相对位置(协议 4)：内积计算了 1 次，判断数据是否对应成比例进行了 2 次. 每判断 1 次数据是否对应成比例，需要计算内积 $n-1$ 次. 因此内积共需要 $2n-1$ 次. 本文的安全计算两平面相对位置(协议 7)：内积计算了 1 次，判断数据是否对应成比例进行了 2 次，但本文每判断 1 次数据是否对应成比例，内积只需要计算 1 次，因此内积共需要计算 3 次.

由上述分析，得到本小节 3 个协议与文献[11]中 3 个协议的效率比较和性能比较分别如表 3、表 4.

表 3　本节 3 个协议与文献[11]中 3 个协议的效率比较

问题	协议	计算成本	通信成本
两直线	文献[11](协议 5)	n	$3n$ rounds
	Ours(协议 5)	4	12 rounds
线与面	文献[11](协议 6)	2	6 rounds
	Ours(协议 6)	3	9 rounds
两平面	文献[11](协议 4)	$2n-1$	$(6n-3)$ rounds
	Ours(协议 7)	3	9 rounds

表 4　本节 3 个协议与文献[11]中 3 个协议的性能比较

问题	协议	位置关系				循环语句
		平行	相交	垂直	重合	
两直线	文献[11](协议 5)	√	√	×	×	√
	Ours(协议 5)	√	√	√	√	×
线与面	文献[11](协议 6)	√	√	×	×	×
	Ours(协议 6)	√	√	√	√	×
两平面	文献[11](协议 4)	√	√	√	√	√
	Ours(协议 7)	√	√	√	√	×

从表 4 可以看出,本文的三个协议能判断的空间几何位置关系多于罗永龙等人[11]设计的协议.此外,罗永龙等人[11]在判断空间几何位置时,几乎都使用了数组对应成比例协议,而此协议是通过不断调用循环语句完成的,复杂性随着数组规模 n 呈线性增长.而我们在处理同样的问题时,利用本文的数组对应成比例协议,是一次性完成的,并没有使用任何循环语句,和数组规模 n 无关,因此从表 3 可以看出,罗永龙等人[11]设计的保密判断空间几何位置关系协议的通信复杂性和计算机复杂性都较高,效率较低.相反,我们设计的协议效率较高.虽然从表 3 看到在判断空间直线与空间平面位置关系时,罗永龙等人[11]的协议 6 由于没有使用数组对应成比例协议,效率高于我们设计的协议 6,但是从表 4 可以看出,文献[11]的协议 6 能判断的位置关系却远少于我们能判断的位置关系.

从表 3、表 4,可以进一步看到,数组对应成比例协议的优良与否,直接制约着基于该协议而设计的其它安全多方计算协议的效率.因此,本文的工作对于安全多方计算的发展有着重要的意义.

7.4 安全性分析

本小节的 3 个应用主要依靠协议 1 和协议 2,安全性证明和协议 1、协议 2 的证明过程类似,为了节省篇幅,我们只对 7.3 节的协议 5 给出证明,其它这里不再一一赘述.

定理 3. 协议 5 安全计算了空间两直线的相对位置.

证明. 由 2.1 节安全性定义构造模拟器 S_1,S_2.在本协议中

在协议 5 中

$$f_1(X,Y)=f_2(X,Y)$$
$$=(L_1\perp L_2)\vee(L_1//L_2)\vee$$
$$(L_1=L_2)\vee(L_1\text{相交}\ L_2)$$

或者

$$f_1(X,Y)=f_2(X,Y)$$
$$=(\neg(L_1\perp L_2))\vee(\neg(L_1//L_2))\vee$$
$$(\neg(L_1=L_2))\vee(\neg(L_1\text{相交}\ L_2))$$

假设 $f_1(X,Y)=f_2(X,Y)=(L_1//L_2)$,构造模拟器 S_1.S_1 接受$(X,f_1(X,Y))$作为输入,按如下方式工作:

第 1 步. S_1 接受输入$(X,f_1(X,Y))=(L_1,(L_1//L_2))$后,首先随机选取一条直线 L_2':

$$\begin{cases}A_3'x+B_3'y+C_3'z+D_3'=0\\A_4'x+B_4'y+C_4'z+D_4'=0\end{cases}$$

使得 $f_1(L_1,L_2)=f_1(L_1,L_2')$,然后用$(L_1,L_2')$进行模拟.按照协议 5,$S_1$ 分别得到直线 L_1、直线 L_2'的方向向量 $\boldsymbol{e}_1=(m_1,n_1,l_1)$、$\boldsymbol{e}_2'=(m_2',n_2',l_2')$.

第 2 步. S_1 调用内积协议,计算内积$\langle\boldsymbol{e}_1,\boldsymbol{e}_2'\rangle$,记为 A'.进一步调用本文的数组对应成比例协议(协议 2)判断$\frac{m_1}{m_2'}=\frac{n_1}{n_2'}=\frac{l_1}{l_2'}$是否对应成比例,将判断结果记为 B'.

第 3 步. S_1 由直线L_1得到向量 $\boldsymbol{a}=(x_0,y_0,z_0,1)$.由直线 L_2'得到向量:

$$\boldsymbol{b}'=(A_3',B_3',C_3',D_3'),$$
$$\boldsymbol{c}'=(A_4',B_4',C_4',D_4').$$

S_1 分别计算两向量 $\boldsymbol{a},\boldsymbol{b}'$的内积,两向量 $\boldsymbol{a},\boldsymbol{c}'$的内积.将$\langle\boldsymbol{a},\boldsymbol{b}'\rangle$的结果记为 C',将$\langle\boldsymbol{a},\boldsymbol{c}'\rangle$的结果记为 D'.

第 4 步. 得到最后的判断结果,记为 E'

在本协议中:

$$view_1(X,Y)=\{X,\boldsymbol{e}_1,A,B,\boldsymbol{a},C,D,E\}$$
$$S_1(X,f_1(X,Y))=\{X,\boldsymbol{e}_1,A',B',\boldsymbol{a},C',D',E'\}$$

由于 $E=f_1(X,Y)=(L_1//L_2)$,$f_1(X,Y)=f_1(X,Y')$,因此 $E'=f_1(X,Y')=(L_1//L_2')$,得到 $E=E'$.由于 A',C',D'都是调用保密内积得到,因此由内积的安全性可以得到两者之间不可区分,即:

$$A\subseteq A',\ C\subseteq C',\ D\subseteq D'.$$

由于 B,B'是调用本文的保密判断数组对应成比例协议(协议 2)完成的,因此 $B\subseteq B'$.

于是得到:

$$\{X,\boldsymbol{e}_1,A,B,\boldsymbol{a},C,D,E\}\subseteq\{X,\boldsymbol{e}_1,A',B',\boldsymbol{a},C',D',E'\}$$

又因为 $output_2(X,Y)=f_2(X,Y)=(L_1//L_2)$,因此有:

$$\{(S_1(x,f_1(x,y)),f_2(x,y))\}$$
$$\subseteq\{(view_1(x,y),output_2(x,y))\}$$

同理,用类似的方法可构造模拟器 S_2,使得:

$$\{(S_2(y,f_2(x,y)),f_1(x,y))\}$$
$$\subseteq\{(view_2(x,y),output_1(x,y))\}$$

证毕.

8 结 语

安全多方计算中保护隐私的相对位置判断,有着重要的研究价值.本文针对位置关系的两个具体问题:点包含问题和两组数据对应成比例问题进行了研究.将点包含问题转化为三角形面积问题;将数组对应数据成比例问题转化为向量共线问题,然后利用内积协议和 hash 函数解决了这两个问题.最后,将本文的两个协议作为基础协议,分别给出了三

个应用：保密判断凸多边形包含、三角形相似、空间几何对象的相对位置.本文两个问题的解决，由于转化方法的巧妙，避免了以往方案中多个基础协议的使用和循环语句的不断调用，极大地提高了效率.

在本文的协议中，最重要的一个思想就是将原问题转化.这种思想是安全多方计算解决问题的一个关键，因具体问题转化方法的不同，直接制约着所利用的密码学工具和方案最后的效率.本文点包含问题的三角形面积转换思想，进一步推广可以解决图形包含问题(比如文中应用 1).数组对应成比例问题，进一步推广可以解决图形相似和空间几何位置问题(比如文中应用 2、应用 3).反之，将这些安全多方计算中的保密位置关系嵌入到加密算法中，可以设计出不同以往的带有关系属性的公钥加密方案.这些工作，我们都已经在陆续研究.

协议 2 由于考虑高效性，未达到完美安全性.因此，如何既能达到完美安全性又能取得高效性，可以就此问题继续研究.此外，本文给出的前两个应用(7.1 节，7.2 节)，均是基于本文两个基本协议完成，都调用了循环语句.为了提高效率，可以针对这两个应用，设计具体问题具体处理的专有协议.以上这些开放问题都将是未来进一步研究的课题.

参　考　文　献

[1] Yao A C. Protocols for secure computations//Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science. Chicago, USA, 1982: 160-164

[2] Freudiger J, Rane S, Brito A E, Uzun E. Privacy preserving data quality assessment for high-fidelity data sharing// Proceedings of the ACM Workshop on Information Sharing & Collaborative Security. Scottsdale, USA, 2014: 21-29

[3] Andrychowicz M, Dziembowski S, Malinowski D, et al. Secure multiparty computations on bitcoin//Proceedings of the 2014 IEEE Symposium on Security and Privacy. San Jose, USA, 2014: 443-458

[4] Yang Jing, Zhao Jia-Shi, Zhang Jian-Pei. A privacy preservation method for high dimensional data mining. Acta Electronica Sinica, 2013, 41(11): 2187-2192(in Chinese)
(杨静，赵家石，张健沛. 一种面向高维数据挖掘的隐私保护方法. 电子学报，2013，41(11)：2187-2192)

[5] Samanthula B K, Elmehdwi Y, Howser G, et al. A secure data sharing and query processing framework via federation of cloud computing. Information Systems, 2015, 48: 196-212

[6] Shi R, Mu Y, Zhong H, et al. Quantum private set intersection cardinality and its application to anonymous authentication. Information Sciences, 2016, 370: 147-158

[7] Li Shun-Dong, Dai Yi-Qi. Secure two-party computational geometry. Journal of Computer Science and Technology, 2005, 20(2): 258-263

[8] Luo Y L, Huang L S, Zhong H. Secure two-party point-circle inclusion problem. Journal of Computer Science and Technology, 2007, 22(1): 88-91

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

[10] Liu L, Wu C, Li S. Two privacy-preserving protocols for point-curve relation. Journal of Electronics (China), 2012, 29(5): 422-430

[11] Luo Yong-Long, Huang Liu-Sheng, Jing Wei-Wei, et al. Privacy protection in the relative position determination for two spatial geometric objects. Journal of Computer Research and Development, 2005, 43(3): 410-416(in Chinese)
(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. 计算机研究与发展，2005，43(3)：410-416)

[12] Li S, Wu C, Wang D, et al. Secure multiparty computation of solid geometric problem and their applications. Information Sciences, 2014, 282: 401-413

[13] Du W, Zhan Z. A practical approach to solve secure multi-party computation problems//Proceedings of the 2002 Workshop on New Security Paradigms. Virginia Beach, USA, 2002: 127-135

[14] Luo Yonglong, Huang Liusheng, Zhong Hong, et al. A secure protocol for determining whether a point is inside a convex polygon. Chinese Journal of Electronics, 2006, 15(4): 578-582

[15] Li Shun-Dong, Si Tian-Ge, Dai Yi-Qi. Secure multi-party computation of set-inclusion and graph-inclusion. Journal of Computer Research and Development, 2005, 42(10): 1647-1653(in Chinese)
(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. 计算机研究与发展，2005，42(10)：1647-1653)

[16] Yao Yi-Fei. A Study of Preserving-Privacy Statistic Problems [Ph. D. dissertation]. University of Science and Technology of China, Hefei, 2008(in Chinese)
(姚亦飞. 保护私有信息的统计计算问题研究[博士学位论文]. 中国科学技术大学，合肥，2008)

[17] Goldreich O. Foundations of Cryptography: Basic Applications. London: Cambridge University Press, 2004: 599-729

[18] Goldreich O, Micali S, Wigderson A. How to play any mental game//Proceedings of the 19th Annual ACM Conference on Theory of Computing. Pittsburgh, USA, 1987: 218-229

[19] Atallah M J, Du Wenliang. Secure multi-party computational geometry//Proceedings of the Workshop on Algorithms and Data Structures. LNCS 2125. Providence, USA, 2001: 1165-1179

[20] Liu F, Ng W K, Zhang W. Secure scalar product for big-data in MapReduce//Proceedings of the IEEE 1st International Conference on Big Data Computing Service and Applications. Redwood City, CA, USA, 2015: 120-129

[21] Calvino A, Ricci S, Domingo-Ferrer J. Privacy-preserving distributed statistical computation to a semi-honest multi-cloud //Proceedings of the IEEE Conference on Communications and Network Security. Rovira, Spain, 2015: 506-514

[22] Zhu Y, Takagi T. Efficient scalar product protocol and its privacy-preserving application. International Journal of Electronic Security and Digital Forensics, 2015, 7(1): 1-19

[23] Mohammed N, Alhadidi D, Fung B, et al. Secure two-party differentially private data release for vertically partitioned data. IEEE Transactions on Dependable and Secure Computing, 2014, 11(1): 59-71

[24] De I, Tripathy A. A secure two party hierarchical clustering approach for vertically partitioned data set with accuracy measure//Thampi S M, et al, eds. Recent Advances in Intelligent Informatics. Berlin Heidelberg, Germany: Springer International Publishing, 2014: 153-162

[25] Sheng G, Wen T, Guo Q, et al. Privacy preserving inner product of vectors in cloud computing. International Journal of Distributed Sensor Networks, 2014, 6: 1-6

[26] Dong C, Chen L. A fast secure dot product protocol with application to privacy preserving association rule mining// Tseng V S, et al, eds. Advances in Knowledge Discovery and Data Mining. Berlin Heidelberg, Germany: Springer International Publishing, 2014: 606-617

CHEN Zhen-Hua, born in 1976, associate professor, M. S. supervisor. Her research interests include cryptography and information security.

LI Shun-Dong, born in 1963, professor, Ph.D. supervisor. His research interests include cryptography and information security.

HUANG Qiong, born in 1982, professor, Ph. D. supervisor. His research interests include cryptography and information security.

DONG Li-Hong, born in 1968, professor, Ph. D. supervisor. Her research interest is system engineering.

CHEN Wei, born in 1992, M. S. candidate. Her research interests include information security and cryptography.

Background

The growth of the internet has triggered tremendous opportunities for cooperative computation, where people are jointly conducting computation tasks based on the private inputs they individually supply. These computations could occur between mutually entrusted parties, or even between competitors. It is referred to as secure multi-party computation, in which secure computation geometry is an essential field. Privacy-preserving location-relation determination as a specific secure computation geometry problem refers to that each participant can determine the relative location among them, while keeping individual private inputs. Point-inclusion problem is to determine whether a point is inside a convex polygon or not; two sets of data correspondingly proportional problem is to determine whether two lines or planes is parallel or not. The two problems classified as a same category-privacy-preserving location-relation determination issue in secure computation geometry-have been extensively researched by many papers. However, the existing schemes make use of multiple basic protocols and invoke loop statement, which make them intricate and efficient. So, the research on how to improve its efficiency has important significance.

This research is supported by the National Natural Science Foundation of China (61472146), the Open Foundation of State Key Laboratory of Information Security (2016-MS-19), the Natural Science Basic Research Plan in Shaanxi Province of China (2017JM6069), and the Guangxi Key Laboratory of Trusted Software (kx201614).