doi:10.3969/j.issn.1000-436x.2013.01.004

安全两方线段求交协议及其在保护隐私凸包交集中的应用

孙茂华[1,2]，罗守山[1,2,3]，辛阳[1,2]，杨义先[1,2]
(1.北京邮电大学 信息安全中心，北京 100876；2.北京邮电大学 灾备技术国家工程实验室，北京 100876；
3.北京安码科技有限公司，北京 100876)

摘 要：研究了现有安全多方计算几何协议，提出了安全多方计算几何的模型和框架，从数学模型、安全模型和通信模型 3 个维度展开描述。针对现有安全两方线段关系判定协议都忽略求解交点坐标的问题，在半诚实模型下基于 Paillier 同态加密技术提出了安全两方线段求交协议，使用 Goldreich 证明法进行了理论安全性分析，并在恶意模型下进行了推广。分析结果表明，该半诚实模型下的算法在效率上优于现有算法。作为安全两方线段求交协议的应用，结合 O'Rourke 算法提出了保护隐私的凸包求交集协议，弥补了安全计算几何领域仅实现了凸包并集算法的缺陷。

关键词：密码学；安全多方计算几何；安全两方线段求交；保护隐私；凸包交集
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1000-436X(2013)01-0030-13

Secure two-party line segments intersection scheme and its application in privacy-preserving convex hull intersection

SUN Mao-hua[1,2], LUO Shou-shan[1,2,3], XIN Yang[1,2], YANG Yi-xian[1,2]
(1. Information Security Center，Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China;
3. Beijing Safe-Code Technology Co.,Ltd. , Beijing 100876, China)

Abstract: The model and framework of secure multi-party computational geometry were presented based on the existing protocols. The new framework has three dimensions, the math model, the security model and the communication model. Using the new model and framework, a secure two-party line segments intersection protocol based on Paillier homomorphic encryption scheme is proposed. This protocol solves the problem that the existing secure two party intersect-determination schemes of line segments cannot output the exact coordinates of the intersection. The security of the protocol is demonstrated using Goldreich method. The results show that this protocol has better efficiency than the existing ones. In addition, the secure two-party line segments intersection in malicious model is also designed. As an application, a privacy-preserving convex hull intersection protocol is proposed based on the O'Rourke scheme. This application makes up for the gap in privacy-preserving convex hull intersection protocol in the area of secure multi-party computational geometry.

Key words: cryptography; secure multi-party computational geometry; secure two-party line segments intersection scheme; privacy-preserving; convex hull intersection scheme

1 引言

随着信息技术的推广，越来越多的机构采用信息技术实现办公和通信。不同机构之间利用信息技术进行合作，但是，在合作过程中，出于利益考虑，机构往往不愿意透露自己的商业信息，这就为合作的顺利进行带来了不便。考虑如下 2 个问题，问题 1：战争期间，A 国和 B 国都打算在 C 国修建铁路。在铁路完工之前，修建路线是保密的。为了防止将来发生火车相撞，A 国和 B 国希望在不泄露自己路

收稿日期：2012-07-13；**修回日期**：2012-11-20
基金项目：国家自然科学基金资助项目（61121061, 61161140320）
Foundation Item: The National Natural Science Foundation of China (61121061, 61161140320)

线的前提下，确定 2 条路线是否有交汇，并根据交汇位置进行协商谈判。问题 2：跨国公司 A 和 B 都打算在 C 国拓展新市场，两公司分别拟定了其在 C 国展开业务的新区域，并作为一级商业机密保护。现在，两公司希望在不泄露各自区域信息的前提下确定新区域是否有重合以及重合区域的信息。

上述问题本质上是在分布式环境下，不同参与方在不泄露自己私有信息的前提下共同完成某种计算。为了解决这些问题，安全多方计算(SMC, secure multi-party computation)应运而生。

安全多方计算是指在分布式网络中，多个用户在不泄露自己秘密的情况下，以自己的秘密作为输入共同计算某个函数[1]。Yao 在文献[2]中首次提出了安全两方计算协议。后来，Goldreich 对 SMC 做了比较完整的总结，并提出了 SMC 的安全性定义[3]。近几年来，安全多方计算取得了众多研究成果[4~20]。文献[4]中构造了一种安全多方计算协议用于分享公共安全网络中的秘密信息。文献[5]中利用秘密共享构造了一种安全多方排序协议，该协议可在一定程度上同时抵抗主动和被动敌手攻击。刘文等利用 ElGamal 密码体制解决了安全多方数据排序问题[6]。文献[7]中利用安全多方计算技术，针对可嵌套共谋，提出可信防共谋协议模型。2011 年，Maheshwari 和 Kiyawat 将安全多方计算和云计算结合，提出了安全多方云计算的概念、应用场景和框架结构[8]。2012 年，Dima 等利用安全多方计算实现了数据挖掘中的 $e-$differential 隐私保护[9]。2012 年，Wang 等研究了安全多方计算中的恶意模型，提出了制约性反攻击的概念，保证了恶意模型下安全多方计算协议的安全性[10]。Goldreich 等基于密码学安全模型提出了可以计算任意函数的安全多方计算协议[11]。理论上讲，任何安全多方计算问题都可以使用电路估值方案解决。但是，出于效率和复杂度的考虑，这种方案在实际应用中并不可行。针对不同应用环境，需要研究不同的解决方案。

作为安全多方计算在计算几何领域的应用，安全多方计算几何的概念首先由 Mikhail 等提出[12]。安全多方计算几何是指在分布式环境中多方共同解决计算几何问题，计算结束后，除了结果信息外各参与方不能获知额外的信息。目前，安全多方计算几何主要研究下列四类问题：点包含问题、多边形相交问题、最近点对问题以及凸包问题。文献[13]基于 Monte Carlo 方法和 Cantor 编码分别设计了判断任意几何图形点包含问题协议以及判断任意几何图形相交、包含关系的协议。文献[14]提出了安全两方向量叉积协议和安全两方三点叉积协议，并在此基础上实现了安全两方点包含协议。文献[15]基于坐标系秘密交换协议和不同坐标系下两点距离计算协议，首次解决了不同坐标系下圆是否包含点的判定问题。文献[16]基于茫然传输实现了可以判定 2 个任意多边形以及 2 个任意几何图形相交关系的协议。文献[17]设计了一个蒙特卡洛偏真算法，用于判断多边形的位置关系。文献[18]解决了安全多方最近点对问题，但是引入了茫然第三方，因此该协议的实用性不高。文献[19]基于向量差最小值协议和同态加密方案实现了安全多方最近点对协议，协议效率高于文献[18]，且不需要茫然第三方的参与。文献[20]基于 Graham 算法、安全叉积协议、姚氏百万富翁协议设计了一个安全两方凸包求解算法。文献[21]基于裹包法、姚氏百万富翁协议、叉积协议解决了安全两方凸包问题。

文献[12, 13, 16, 17, 22]虽然给出了安全多方线段求相交协议，但是只能判断线段是否有交点，无法计算交点的坐标信息。因此，不能完全解决问题 1。从文献[20]和文献[21]可以看出，目前在凸包运算的隐私保护研究中，主要解决凸包并集操作，还没有实现凸包交集操作的隐私保护。因此，无法解决问题 2。

表 1 分析了近几年来提出的安全多方多边形相交协议和安全多方凸包求解协议的原理和贡献。

本文首先研究安全多方计算几何模型和框架，从数学模型、安全模型、通信模型 3 个维度展开描述。为了解决问题 1，本文分别提出了半诚实模型和恶意模型下的安全两方线段求交协议，不仅可以确定 2 条线段是否有交点，还可以输出交点坐标信息；为了解决问题 2，本文首先利用 O'Rourke 算法将求解凸包交集问题转换为求解 2 个凸多边形相交边的交点问题，然后利用本文提出的安全两方线段求交协议给出具体的交点坐标。

2　预备知识

2.1　Goldreich 安全证明法

Goldreich 给出了半诚实模型下安全性证明方法，被广泛应用在安全多方计算几何的安全性分析中。

定义 1　（Goldreich 安全证明法）[3]

设 $f:\{0,1\}_1^*\times\cdots\times\{0,1\}_m^*\to\{0,1\}_1^*\times\cdots\times\{0,1\}_m^*$，其中，$f_i(x_1,x_2,\cdots,x_m)$ 是 $f(x_1,x_2,\cdots,x_m)$ 的第 i 个元素。

表 1 安全多方计算几何相关研究

类别	文献	原理	主要贡献
安全多方多边形相交问题	[12]	利用点积协议和向量控制协议判断 2 条线段是否相交，进而判断 2 个多边形是否相交	首次提出了安全多方计算几何问题并给出了解决方案
	[13]	基于 Monte Carlo 方法和 Cantor 编码	可以判断任意几何图形的相交、包含关系
	[16]	基于茫然传输协议	可以判定 2 个任意多边形以及 2 个任意几何图形的相交关系
	[17]	基于线段相交判定协议	文章算法是一个蒙特卡洛偏真算法；文章首次实现了安全多方计算几何领域中协议的实验分析
	[22]	基于安全两方叉积协议判断线段是否相交	文献给出了安全两方点线叉积协议，该协议是安全多方计算几何的常用协议
安全多方凸包求解问题	[20]	基于 Graham 算法、安全叉积协议、姚氏百万富翁协议	基于 Graham 算法解决了安全凸包问题
	[21]	基于裹包法、姚氏百万富翁协议、叉积协议	基于裹包法解决了安全凸包问题

定义 $f_I(x_1,x_2,\cdots,x_m)=\{f_{i_1}(x_1,x_2,\cdots,x_m),\cdots,f_{i_j}(x_1,x_2,\cdots,x_m)\}$ 其中，$I=\{i_1,i_2,\cdots,i_j\}\subseteq\{1,2,\cdots,m\}$。设 $\prod$ 为计算 f 的 m 方协议，当输入为 $\overline{x}=(x_1,x_2,\cdots,x_m)$ 时，第 i 方在执行 $\prod$ 的过程中得到信息序列 $(x_i,r_i,m_1^i,m_2^i,\cdots,m_k^i)$，记为 $view_i^{\prod}(\overline{x})$，其中 r_i 表示第 i 方独立的掷币输出；m_j^i 表示第 i 方收到第 j 次的信息。当输入为 $\overline{x}=(x_1,x_2,\cdots,x_m)$ 时，执行协议 $\prod$ 以后，第 i 方的输出结果记为 $output_i^{\prod}(\overline{x})$。对于一个函数 f，如果存在概率多项式时间算法（或者称为模拟器 S），使得对于所有的 $I\subseteq[m]$，有

$$\{S(I,(x_{i_1},x_{i_2},\cdots,x_{i_t}),f_1(\overline{x}),f(\overline{x})\}_{\overline{x}\in(\{0,1\}^*)^m}\overset{c}{\equiv}$$

$$\{view_i^{\prod}(\overline{x}),output^{\prod}(\overline{x})\}_{\overline{x}\in(\{0,1\}^*)^m}$$

则认为 $\prod$ 秘密计算了 f，其中 $\overset{c}{\equiv}$ 表示多项式电路计算不可区分。要证明一个安全多方计算协议是安全的，就必须构造满足上述条件的模拟器 S。

该定义可以直观地理解为对于一个半诚实参与者，如果可以直接利用自己的输入与协议的输出通过单独模拟整个协议的执行过程而得到在执行协议过程中所能得到的任何信息，那么协议就能保证输入的私密性。如果一个计算协议能被这样模拟，参与者就不能从协议的执行过程中得到有价值的信息，这样的协议就是安全的。

目前，在安全多方计算协议领域，Goldreich 证明法是公认的一种安全性证明方式。本文亦采用这种方法进行安全性证明。

2.2 保护隐私的基础协议

2006 年，罗永龙等在文献[23]中提出了保护隐私的向量叉积问题，并给出了解决方案，该解决方案被称为是保护隐私的向量叉积协议 CPP_V(cross product protocol for two vector)。

2007 年，罗永龙等又在文献[22]中提出了保护隐私的点线叉积问题，并给出了解决方案，该解决方案被称为是保护隐私的点线叉积协议 CPP_PL (cross products protocol for a point with a line)。

罗永龙等在文献[14]中给出了一个安全两方点包含协议 PIP (point inclusion protocol)。该协议的原理是如果一个点在一个多边形内，假设多边形的边按逆时针方向排序，则该点在这个多边形每一条边的左侧。因此只需要利用安全叉积协议，即可判断点是否在多边形内。

2.3 Paillier 加密方案

Paillier 加密方案[24]的安全性依赖于合数剩余判定假设（DCRA, decisional composite residuosity assumption），即没有多项式时间算法来区分一个模数是否是模 n^2 的 n 次剩余。具体描述如下。

系统参数：选取 $n=pq$，其中 p 与 q 为 2 个大素数。选取随机整数 g，满足 $\gcd(l(g^l \bmod n^2),n)=1$，则公钥为 (n,g)，私钥为 $l(n)=lcm((p-1),(q-1))$，M 为明文消息。

加密：选择随机数 $r\in Z_p^*$，$E(M)=g^m r^n \bmod n^2$。

解密：$M=\dfrac{L(C^{l(N)}\bmod n^2)}{L(g^{l(N)}\bmod n^2)}\bmod n$。

Paillier 加密方案具有加同态特性，即 $D(E(m_1,r_1)\cdot E(m_2,r_2))=m_1+m_2$。

3 安全多方计算几何模型和框架

安全多方计算几何模型（如图 1 所示）可以描述为一个黑盒子。从盒子外看，各参与方输入自己的信息，仅能得到函数的输出结果。而在盒子内部，各参与方进行交互操作，共同计算函数的输出。

一个安全多方计算几何协议可以从数学模型、安全模型、通信模型 3 个维度展开描述。

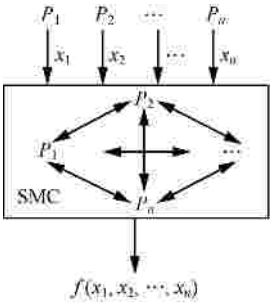

图 1　计算模型

数学模型是指运用数学的语言和方法，通过抽象、简化建立能近似刻画并“解决”实际问题的一种模型。在安全多方计算几何领域，常用的数学模型有：多边形求交点模型、多边形相似的模型、最近点对模型以及凸包并集模型。

安全模型分为半诚实模型和恶意模型[3]。这 2 种安全模型是按照参与者的不同来区分的。在安全计算几何协议中，参与者分为诚实参与者、半诚实参与者和恶意参与者。诚实参与者在协议执行过程中，完全按照协议要求完成各个步骤，同时保密自己的所有输入、输出以及中间结果。半诚实参与者在协议执行过程中，完全按照协议要求完成各个步骤，不会中途强行退出或恶意掺入虚假数据，但在协议执行过程中，他们可能会保留所有可以收集到的关于其他参与者的信息，以期望在协议结束后推断出对方的输入信息或泄露给攻击者。恶意参与者在协议的执行过程中，完全按照攻击者的意志执行协议的各个步骤，他不但将自己的所有输入、输出以及中间结果泄露给攻击者，还可以根据攻击者的意图改变输入信息、中间结果信息，甚至终止协议。如果所有参与者都是半诚实或诚实的，称此模型为半诚实模型。半诚实模型中的攻击者都是被动的。存在恶意参与者的模型称为恶意模型。恶意模型中的攻击者是主动的。

目前，在安全多方计算协议的研究中，几乎所有的协议都是建立在半诚实模型下。同时，半诚实模型下的各种安全多方计算协议也具有很强的应用背景。本文首先在半诚实模型下进行讨论，然后将协议推广到恶意模型下。

通信模型：安全多方计算几何协议中使用的通信模型包括同步和异步 2 种模型。同步通信模型是指所有参与方共同使用一个时钟服务器，同时接收或发送消息；异步通信模型是指各参与方按照不同的时钟周期接收或者发送消息。

可以用如图 2 所示表示一个安全多方计算几何协议的框架。

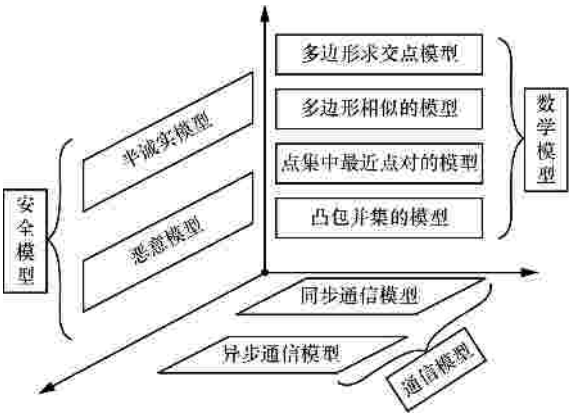

图 2　安全几何计算框架

4　安全两方线段求交协议

4.1　问题分析

问题 1 中的路线如果是线段，则问题 1 可以描述为：Alice 拥有线段 $A: y = a_1 x + b_1$ $(m_1 \le x \le n_1)$，Bob 拥有线段 $B: y = a_2 x + b_2$ $(m_2 \le x \le n_2)$。Alice 和 Bob 希望计算 2 条线段的交点。计算结束后，除了交点的坐标信息，对方不能获知其他任何信息。上述问题称为安全两方线段求交点问题。解决该问题的协议称为安全两方线段求交协议，记作 STPP_IL(secure two party protocol for intersection of line)。

在二维空间中，2 条线段的位置关系有如下几种情况：图 3(a)中，2 条线段相交于一点；图 3(b)中，2 条线段所在的直线相交于一点，但是 2 条线段无交点；图 3(c)中，2 条线段平行，无交点；图 3(d)中，2 条线段在同一条直线上，且满足 $n_2 < m_1$，此时线段无交点；图 3(e)中，2 条线段在同一条直线上，且满足 $n_1 \le m_2$，此时线段无交点；图 3(f)中，2 条线段在同一条直线上，且满足 $m_1 \le m_2, m_2 \le n_1$，$n_1 \le n_2$，此时线段的交构成一条线段：$y = a_1 x + b_1$ $(m_2 \le x \le n_1)$；图 3(g)中，2 条线段在同一条直线上，且满足 $m_2 \le m_1, n_1 \le n_2$，此时线段的交构成一条线段：$y = a_1 x + b_1$ $(m_1 \le x \le n_1)$，图 3(h)中，2 条线段在同一条直线上，且满足 $m_2 \le m_1$，$m_1 \le n_2$，$n_2 \le n_1$，此时线段的交构成一条线段：$y = a_1 x + b_1$ $(m_1 \le x \le n_2)$；图 3(i)中，2 条线段在同一条直线上，且满足 $m_1 \le m_2$，$n_2 \le n_1$，此时线段的交构成

一条线段：$y = a_1 x + b_1 \ (m_2 \le x \le n_2)$。

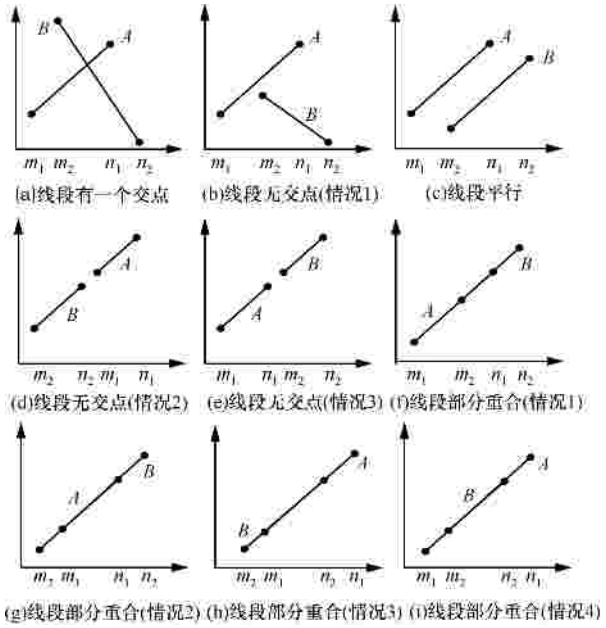

图 3 二维空间中的线段位置关系

安全两方线段求交点问题的数学模型就是已知 2 条线段求交点，归属于多边形求交点模型一类。下面使用异步通信模型和半诚实安全模型设计解决该问题的协议。图 4 中用灰色表示本节协议使用的模型。

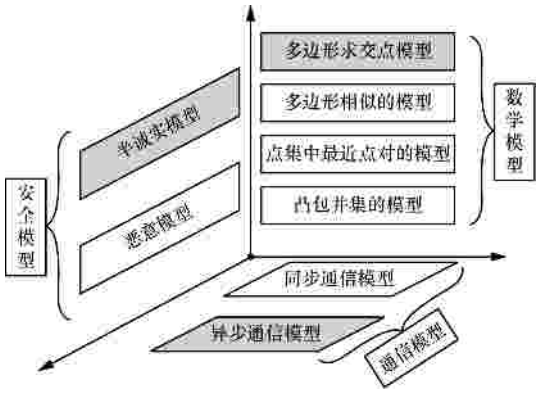

图 4 SP_IL 框架

4.2 协议描述

本文使用 Luo 等在文献[23]中提出的 SMC 协议的符号，如表 2 所示。

表 2 系统符号

符号名称	符号意义
A_i	Alice 在本地执行第 i 步
B_i	Bob 在本地执行第 i 步
$A_i \| B_i$	Alice 和 Bob 各自在本地执行第 i 步
$A_i \wedge B_i$	Alice 和 Bob 共同协作执行第 i 步
Generate	构造一个对象
Compute	执行一个基本操作
Send(A->B,s_1,…,s_m)	A 向 B 发送消息 s_1,…,s_m
Receive(A->B,s_1,…,s_m)	B 接收 A 发送的消息 s_1,…,s_m

系统参数：Alice 拥有 Paillier 同态加密系统的密钥对(pk,sk)，公钥 pk 是公开的。

STPP_IL(A,B):

{

A_1:

Compute: $E(a_1), E(-b_1)$;

//Alice 使用公钥加密 a_1 和 $-b_1$

Send(Alice->Bob, $E(a_1), E(-b_1)$);

B_2:

Generate: r // Bob 选择随机数 r

Compute: $[E(a_1)]^r E(-ra_2) = E(ra_1 - ra_2)$；

Compute: $[E(-b_1)]^r E(rb_2) = E(rb_2 - rb_1)$;

Send(Bob -> Alice, $E(ra_1 - ra_2), E(rb_2 - rb_1)$);

A_3:

Compute: $D(E(ra_1 - ra_2))$;

Compute: $D(E(rb_2 - rb_1))$;

if($D(E(ra_1 - ra_2)) == 0$)

{//2 条线段斜率相等

if($D(E(rb_2 - rb_1)) == 0$)

go to $A_4 \wedge B_4$

//2 条线段在同一条直线上，进入 $A_4 \wedge B_4$

else

{

Send(Alice->Bob, (0,0));

go to B_5;

//此时 2 条线段平行，进入 B_5

}

}

else //2 条线段不平行

{

Compute: $x = \dfrac{D(E(rb_2 - rb_1))}{D(E(ra_1 - ra_2))} = \dfrac{b_2 - b_1}{a_1 - a_2}$;

if($m_1 \le x \le n_1$)

{

Send(Alice->Bob, (x,1));

go to B_5;

```
}
else
{
      Send(Alice->Bob, (x,2));
      go to B5;
}
}
```

A_4^ B_4:

//2 **条线段在同一条直线上**

if(MillionaireProtocol(m_1, m_2)==1)

//使用百万富翁协议判断数据的大小，当

// $m_1 \geq m_2$ 时，协议返回 1**，否则返回** 0**；**

```
{
  if(MillionaireProtocol( m1, n2 )==1)
 End;//图 3(d)的情况，无交点；
else
{
 if(MillionaireProtocol( n1, n2 )==1)
{
      Send(Alice->Bob,  m1 );
      Send(Bob-> Alice,  n2 );
      Alice:  y = a1 x + b1 (m1 ≤ x ≤ n2 ) ;
      Bob:  y = a2 x + b2 (m1 ≤ x ≤ n2 ) ;
      //图 3(h)的情况，交点构成一条线段；
}
else
{
      Send(Alice->Bob,  m1 , n1 );
      Alice:  y = a1 x + b1 (m1 ≤ x ≤ n1 ) ;
       Bob:  y = a2 x + b2 (m1 ≤ x ≤ n1 ) ;
      //图 3(g)的情况，交点构成一条线段；
  }
 }
}
else
{// m1 ≤ m2
  if(MillionaireProtocol( m2, n1 )==1)
     End;//图 3(e)的情况，无交点；
  else
{
  if(MillionaireProtocol( n1, n2 )==1)
{
     Send(Bob->Alice,  m2 , n2 );
       Alice:  y = a1 x + b1 (m2 ≤ x ≤ n2 ) ;
       Bob:  y = a2 x + b2 (m2 ≤ x ≤ n2 ) ;
     //图 3(i)的情况，交点构成一条线段；
  }
  else
  {
     Send(Alice->Bob,  n1 );
     Send(Bob-> Alice,  m2 );
     Alice:  y = a1 x + b1 (m2 ≤ x ≤ n1 ) ;
     Bob:  y = a2 x + b2 (m2 ≤ x ≤ n1 ) ;
    //图 3(f)的情况，交点构成一条线段；
  }
 }
}
End;
```

B_5:

```
Receive(Alice->Bob, (x, k1 ) );
if( k1 = 0 )
   End; //2 条线段无交点，协议结束
elseif( k1 =1)
{
  if( m2 ≤ x ≤ n2 )
   {
     Send(Bob-> Alice, (x,1));
     Compute:  y = a2 x + b2 ;
   }
   else
     Send(Bob-> Alice, (0,2));
}
```

A_6:

```
Receive(Bob -> Alice,  (x, k2 ) );
if( k2 = 2 )
   End; //2 条线段无交点，协议结束
elseif( k2 =1)
   Compute:  y = a1 x + b1 ;
End;
}
```

4.3 性能分析

1) **正确性分析**

定理 1　半诚实模型下，上述协议是正确的。

证明

上述问题实际上就是求解式(1)在式(2)中的解

$$\begin{cases} y = a_1 x + b_1 \\ y = a_2 x + b_2 \end{cases} \tag{1}$$

取值范围：$m_1 \le x \le n_1$ 并且 $m_2 \le x \le n_2$ （2）

求解式（1）的解分为以下几种情况：当 $a_1 - a_2 \neq 0$ 时，式（1）的解为 $x = \dfrac{b_2 - b_1}{a_1 - a_2}$，$y = a_1 x + b_1$。求解 x 的值后验证是否满足式（2）即可；由于 Alice 选用了满足加法同态性的加密系统，有 $x = \dfrac{b_2 - b_1}{a_1 - a_2} = \dfrac{D(E(rb_2 - rb_1))}{D(E(ra_1 - ra_2))} = \dfrac{[E(-b_1)]^r E(rb_2)}{[E(a_1)]^r E(-ra_2)}$。当 $a_1 - a_2 = 0$ 时，若 $b_1 - b_2 \neq 0$，则此时 2 条线段平行，无交点；由于 Alice 选用了满足加法同态性的加密系统，此时满足 $D([E(a_1)]^r E(-ra_2)) = 0$ 并且 $D([E(-b_1)]^r E(rb_2)) \neq 0$。因此，$A_1$、$B_2$、$A_3$ 是正确的。B_5 和 A_6 中 Alice 和 Bob 进行通信，均发送数据对 (x,k)。其中，当 k=0 时，代表 2 条直线平行，无交点；当 k=1 时，x 有效并代表式（1）的解，Alice 和 Bob 只要确定 x 的值满足式（1）以及式（2）后，通过各自的线段方程即可确定 y 的值；当 k=2 时，代表一方确定 x 不在其取值范围内，因此线段无交点。

当 2 条线段在同一条直线上时，$A_4 \wedge B_4$ 利用百万富翁协议比较 x 的取值范围，根据 4.1 节中讨论的几种情况进行验证，因此是正确的。

综上所述，上述协议是正确的。

2) 安全性分析

定理 2 半诚实模型下，上述协议是安全的。

证明 当 2 条线段在同一条直线上时，上述协议调用百万富翁协议完成计算。由于半诚实模型下百万富翁协议是安全的，因此本协议也是安全的。下面证明当 2 条线段不在同一条直线上时的安全性。

Alice 输入线段 $A: y = a_1 x + b_1$ $(m_1 \le x \le n_1)$，Bob 输入线段 $B: y = a_2 x + b_2$ $(m_2 \le x \le n_2)$。协议输出 $output^{\Pi} = (x, y)$。Bob 的信息序列

$$view_I^{\Pi}(A,B,M,N) = (B, N, pk, r, E(a_1), E(-b_1), E(ra_1 - ra_2), E(rb_2 - rb_1)), (x, k_1), (x, k_2), (x, y))$$

下面构造模拟器 S 模拟 Bob 的协议执行过程。

步骤 1 S 的输入为 $(B, N, pk, f_1(A,B,M,N))$。其中，$f_1(A,B,M,N) = (r, E(ra_1 - ra_2), E(rb_2 - rb_1), (x, k_2), (x, y))$。

步骤 2 S 利用系统公钥 pk 执行加密操作，可得到 $E'(-ra_2), E(rb_2)$。则 $E'(a_1) = r\sqrt{\dfrac{E(ra_1 - ra_2)}{E'(-ra_2)}}$，$E'(-b_1) = r\sqrt{\dfrac{E(rb_2 - rb_1)}{E'(-rb_2)}}$。由于半诚实模型下同态加密系统是安全的，有 $E'(a_1) \overset{c}{\equiv} E(a_1)$，$E'(-b_1) \overset{c}{\equiv} E(-b_1)$。

步骤 3 S 判断 $f_1(A,B,M,N)$ 中 (x,y) 是否为有效值，如果是有效值，则 $k_1' = 1$；否则 $k_1' = 0$。易知，$k_1' = k_1$。

综上所述，

$$S(B, N, pk, f_1(A,B,M,N)) = (B, N, pk, r, E'(a_1), E'(-b_1))$$
$$E(ra_1 - ra_2), E(rb_2 - rb_1), (x, k_1'), (x, k_2), (x, y))$$

因为 $f(A,B,M,N) = (x,y)$，$output^{\Pi} = (x,y)$，所以

$$S(B, N, pk, f_1(A,B,M,N)) \overset{c}{\equiv}$$
$$\{view_I^{\Pi}(A,B,M,N), output^{\Pi}(A,B,M,N)\}$$

同样地，可以为 Alice 构造模拟器。

3) 效率分析

计算复杂度：本协议中，共执行加密操作 4 次，解密操作 2 次，加密数据乘法操作 2(r+1)次，乘法操作 5 次，加法操作 2 次，百万富翁协议至多 3 次。Paillier 加密算法的计算复杂度为 $O(2\log n)$，解密算法的复杂度为 $O(2\log n)$，每次自乘操作的复杂度为 $O(2\log n)$[24]，选用基于 Paillier 加同态加密方案的百万富翁协议[25]，则计算复杂度为 $O(n\log N)$。忽略乘法操作和加法操作，则本协议的计算复杂度为 $O(r\log n)$。

通信复杂度：本协议中，Alice 和 Bob 共通信 $4+3C_a$ 次，C_a 代表百万富翁协议的通信次数。

4.4 算法比较

在安全多方计算几何领域，很多文献给出的协议都调用了现有的安全多方基础算法，但是没有明确使用哪个具体的算法。这就为算法的性能比较带来了不便。本文在进行算法比较时，选用了经典的基础算法进行比较。表 3 是算法比较时使用的符合说明。

选用基于 Paillier 加同态加密方案的百万富翁协议[25]，则计算复杂度为 $O(n\log N)$。基于点积协议的保护隐私的点线叉积协议[22]计算复杂度为 $O(n^2)$。加同态加密系统采用 Paillier 协议，加密和解密操作的计算复杂度[24]均为 $O(2\log n)$。

表 3　系统符号

符号名称	符号意义
T_a	百万富翁协议的算法复杂度
T_c	保护隐私的点线叉积协议的算法复杂度
T_h	加同态加密操作的复杂度
T_d	加同态解密操作的复杂度
C_a	百万富翁协议的通信次数
C_c	保护隐私的点线叉积协议的通信次数

通过表 4 可以看出，本文提出的方案计算复杂度低于文献[17, 22]，略高于文献[26]；通信复杂度低于文献[22, 26]，略高于文献[17]。

表 4　复杂度对比

文献	计算复杂度（一般化）	计算复杂度（实例化）	通信次数
本文	$O(r\log N)$	$O(r\log N)$	$4+3C_a$
[17]	$O(n^2)$	$O(n^2)$	6
[22]	$4T_a+4T_c$	$O(n\log N+n^2)$	$4C_a+4C_c$
[26]	$4(4T_h+3T_d+T_a)$	$O(C\log N)$	$8+12C_a$

表 5 将近几年来提出的安全两方线段求交协议和本文提出的协议进行了功能对比。

表 5　功能比较

文献	计算交点坐标	判断出图 3(a)~图 3(c)	判断出图 3(d)~图 3(i)
本文	是	是	是
[17]	否	是	是
[22]	否	是	是
[26]	否	是	否

4.5　恶意模型下的推广

恶意模型下的安全两方线段求交协议和半诚实模型下的协议思想是一致的。由于私有数据在进行交互之前都进行了数据加密，因此，即使对方是不诚实的，也无法得知对方私密数据。但是，在恶意模型下一方需要通过验证得知对方是否是恶意的，一旦发现对方是恶意的，需要及时终止协议。下面在半诚实模型协议的基础上，Alice 和 Bob 需要进行多次验证性的交互，防止对方提供虚假数据。Alice 仍然采用 Paillier 加密系统，协议的第一步、第二步和半诚实模型下是一样的。

下面，根据二维空间中线段位置关系的不同分别进行讨论。

1) 2 条线段平行：Alice 计算 $D(E(ra_1-ra_2))=0$ 并且 $D(E(rb_2-rb_1))\neq 0$ 后，得知 2 条线段平行不相交，此时通知 Bob 结果，双方进行交互性验证,验证方式如下。

$A_i|B_i$:

Compute：$A_j=g^{a_j}$, $B_j=g^{b_j}$

Generate: $u_j\in_R Z_n$

Generate: $c_j\in_R Z_n$

Compute: $K_j=g^{u_j}$

//Alice 计算 j=1 的值，Bob 计算 j=2 的值；

Send(Alice->Bob, A_1, B_1, K_1, c_1);

Send(Bob->Alice, A_2, B_2, K_2, c_2);

$A_{i+1}|B_{i+1}$:

Compute: $s_j=u_j+c_j a_j$;

Compute: $t_j=u_j+c_j b_j$;

Compute: $H_{a_i}=H(a_i)$;

Compute: $H_{b_i}=H(b_i)$;

//Alice 计算 j=1 的值，Bob 计算 j=2 的值；

Send(Alice->Bob, $s_1, t_1, H_{a_1}, H_{b_1}$);

Send(Bob -> Alice, $s_2, t_2, H_{a_2}, H_{b_2}$);

A_{i+2}:

if(($g^{s_2}=K_2A_2^{c_2}$)&&($H_{a_2}=H(a_1)$)

&&($g^{t_2}=K_2B_2^{c_2}$)&&($H_{b_2}\neq H(b_1)$))

End;//此时 Alice 得知 Bob 是诚实的

else

END;//Bob 提供虚假数据，结束协议。

B_{i+3}:

if(($g^{s_1}=K_1A_1^{c_1}$)&&($H_{a_1}=H(a_2)$)

&&($g^{t_1}=K_1B_1^{c_1}$)&&($H_{b_1}\neq H(b_2)$))

End;//此时 Alice 得知 Bob 是诚实的

else

END;//Bob 提供虚假数据，结束协议。

2) 2 条线段所在直线交于一点：Alice 计算 $D(E(ra_1-ra_2))\neq 0$ 后,得知 2 条线段所在直线交于一点，此时通知 Bob 结果，双方进行交互性验证,验证方式如下。

$A_i|B_i$:

if($m_j\le x\le n_j$)

{

Compute: $y_j=a_jx+b_j$

Generate: r_j //选择随机数

//Alice 计算 j=1 的值，Bob 计算 j=2 的值；

Send(Alice->Bob,(x,1), r_1);

Send(Bob->Alice,(x,1), r_2);

}

else

{

Send(Alice->Bob,(0,2),0);

Send(Bob->Alice, (0,2),0);

}

$A_{i+1}|B_{i+1}$:

Receive(Alice->Bob, (x, k_1), r_1);

Receive(Bob -> Alice, (x,k_2), r_2);

//Alice 计算 j=2, i=1 时的值;

//Bob 计算 j=1,i=2 时的值；

if(k_j ==2)

{

t_1 =MillionaireProtocol(x, n_j);

t_2 =MillionaireProtocol(x, m_j);

//调用恶意模型下的百万富翁协议

if($t_1 \times t_2 > 0$)

End; //对方是诚实的，协议结束

else

End;//对方提供虚假数据，协议结束

}

elseif(k_j ==1)

{

Compute: $y_i = a_i x + b_i$;

Compute: $Y_i = H(r_j y_i)$;

Send(Alice->Bob, Y_1);

Send(Bob -> Alice, Y_2);

}

A_{i+2}:

Receive(Bob -> Alice, Y_2);

if($Y_2 == H(r_1 y_1)$)

End;//此时 Alice 得知 Bob 是诚实的;

else

End; //Bob 提供虚假数据，协议结束

B_{i+3}:

Receive(Alice -> Bob, Y_1);

if($Y_1 == H(r_2 y_2)$)

End;//此时 Bob 得知 Alice 是诚实的;

else

End; //Alice 提供虚假数据，协议结束

3) 2 条线段在同一条直线上：Alice 计算 $D(E(ra_1 - ra_2)) = 0$ 并且 $D(E(rb_2 - rb_1)) = 0$ 后，得知 2 条线段在同一条直线上，此时通知 Bob 结果。Alice 和 Bob 使用 2 条直线平行时验证数据 a_i 的方法验证 a_1 是否等于 a_2，b_1 是否等于 b_2，使用恶意模型下的百万富翁协议验证 2 条线段是否有交点。

5 保护隐私的凸包交集协议

5.1 问题分析

问题 2 中的区域如果描述为凸多边形，则问题 2 可以表述为：Alice 拥有凸多边形 $P = \{p_1, p_2, \cdots, p_n\}$，Bob 拥有凸多边形 $Q = \{q_1, q_2, \cdots, q_m\}$，顶点为逆时针顺序。Alice 和 Bob 希望求解 $P \cap Q$ 形成的凸包 P_{new}。同时，除了结果之外，Alice 和 Bob 不希望对方得到其他信息。该问题称为保护隐私的凸包交集问题。

保护隐私的凸包交集问题的数学模型是已知 2 个凸多边形求交集。本文选用凸包交集模型半诚实模型和异步通信模型设计保护隐私的凸包交集协议（如图 5 所示）。

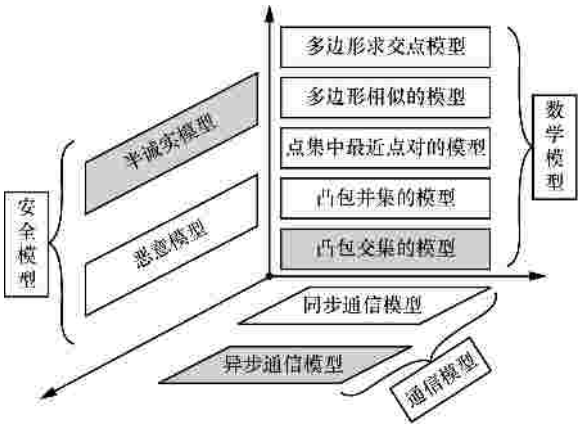

图 5 保护隐私凸包交集协议框架

5.2 数学原理

定义 1 所有内角都小于 π 的多边形称为凸多边形。凸多边形的所有顶点均为凸点[27]。

定理 3 如果一个凸多边形的顶点在另一个凸多边形内，则该顶点也是交集的一个顶点。

证明 假设 p_i 是凸多边形 P 的一个顶点，并且 p_i 在凸多边形 Q 内部，则顶点 p_i 对应的内角 $\angle 1 < \pi$。

利用反证法，假设 p_i 不是交集的顶点，存在一点 t 是交集的顶点，并且 $\overrightarrow{nt}, \overrightarrow{tm}$ 分别是交集多边形上逆时针方向的 2 条边。由于 p_i 是凸多边形 P 的一个顶点，并且在凸多边形 Q 内部，则 $p_i \in (P \cap Q)$。因此，p_i 在 $\overrightarrow{nt}, \overrightarrow{tm}$ 的左边。又由于 $\overrightarrow{nt}, \overrightarrow{tm}$ 都属于凸多

边形 P 内部或边上，因此 $\angle 2$ 是凸多边形 P 的一个内角，所以 $\angle 2 < \pi$。但这与 $\angle 1 < \pi$ 矛盾。因此，p_i 肯定是交集的一个顶点(如图 6 所示)。

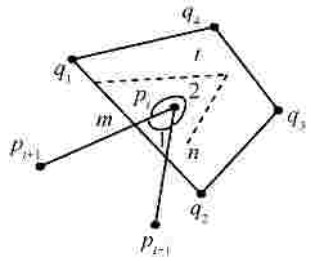

图 6　交集的顶点

得证。

求 2 个凸多边形的交集，也就是求出交集顶点的坐标。考虑如下情况。

图 7(a)中，交集的顶点均为两凸多边形的边相交产生的交点；图 7(b)中，除了两凸多边形的边相交产生的交点外，交集的顶点还包括原凸多边形的某些顶点，例如 p_4 ；图 7(c)中，交集的顶点就是被包含的凸多边形的顶点；图 7(d)中，交集的顶点是原凸多边形的一个顶点。即交集的顶点是原凸多边形的顶点或者是由两凸多边形的边相交产生的交点。

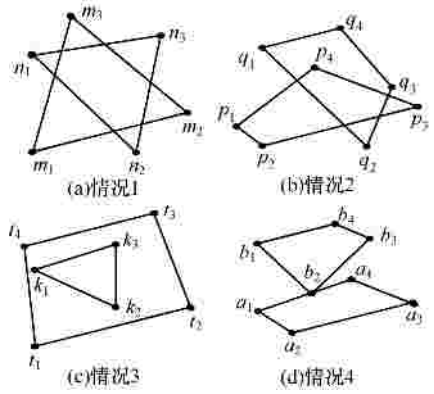

图 7　交集的顶点

2 个凸多边形相交，则交集可能是一个点、一条线段或者一个多边形。

定理 4　如果 2 个凸多边形的交是一个多边形，则该多边形为凸多边形。

证明

假设凸多边形 $P=\{p_1, p_2, \text{L}, p_n\}$ 和凸多边形 $Q=\{q_1, q_2, \text{L}, q_m\}$ 相交，交集的顶点坐标为 $T_{\text{new}}=\{t_1, t_2, \text{L}, t_k\}$，$k \geq 1$。

对于顶点 t_i，如果 t_i 是凸多边形 P 或者 Q 的一个顶点(例如 t_i 是凸多边形 P 的顶点 p_j)，则 $\angle t_{i-1}t_i t_{i+1} = \angle p_{i-1}p_i p_{i+1}$。因为 $\angle p_{i-1}p_i p_{i+1} < \pi$，所以 $\angle t_{i-1}t_i t_{i+1} < \pi$。

如果 t_i 不是凸多边形 P 或者 Q 的一个顶点，则 t_i 是由 P 和 Q 的边相交形成的交点。假设 $p_m p_n$ 和 $q_a q_b$ 相交形成交点 t_i，则 $\angle t_{i-1}t_i t_{i+1} = \angle p_m t_i q_a$ 或者 $\angle t_{i-1}t_i t_{i+1} = \angle p_n t_i q_a$。由于 $\angle p_m t_i q_a < \pi$，$\angle p_n t_i q_a < \pi$，因此 $\angle t_{i-1}t_i t_{i+1} < \pi$（如图 8 所示）。

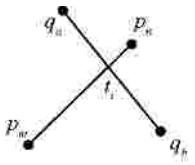

图 8　2 条线段的交点

综上所述，交集的每个内角的度数都小于 π，因此交多边形是一个凸多边形。得证。

由于交集的顶点是原凸多边形的顶点或者是由两凸多边形的边相交产生的交点，因此，关键问题是如何确定凸多边形的边何时相交以及交点的坐标。O'Rourke 在文献[28]中给出了一个高效地确定两凸多边形的边何时相交的算法，第 4 节给出了如果安全求解线段交点的算法。

假设凸多边形 $P=\{p_1, p_2, \text{L}, p_n\}$，凸多边形 $Q=\{q_1, q_2, \text{L}, q_m\}$，顶点为逆时针顺序。$A=\overrightarrow{p_{i-1}p_i}$ 和 $B=\overrightarrow{q_{j-1}q_j}$ 分别代表 2 个多边形上的有向边。O'Rourke 算法让 A 和 B 相互追赶，以便在有交点的时候相遇。有向边“追逐”的几种情况如图 9 所示。

1) 有向边 B 挡在 A 的正前方，此时如果让 A 前进，则有可能产生交点；

2) 有向边 A 挡在 B 的正前方，此时如果让 B 前进，则有可能产生交点；

3) 有向边 B 在 A 的外侧，此时如果让 B 前进，则有可能产生交点；

4) 有向边 A 的终点在 B 的外侧且 A 的起点在 B 的内侧，此时如果让 A 前进，则有可能产生交点；

5) 有向边 A 的终点在 B 的外侧且 A 的起点在 B 的外侧，此时如果让 A 前进，则有可能产生交点。

用数学语言描述为：令 $H(A)$ 代表 A 的左侧半平面。如果 $A\times B \geq 0$ 且 $q_j \in H(A)$ 或者 $A\times B < 0$ 且 $p_i \notin H(B)$，则让 A 前进；如果 $A\times B < 0$ 且 $p_i \in H(B)$ 或者 $A\times B \geq 0$ 且 $q_j \notin H(A)$，则让 B 前进。

5.3　协议描述

for i=1 to n

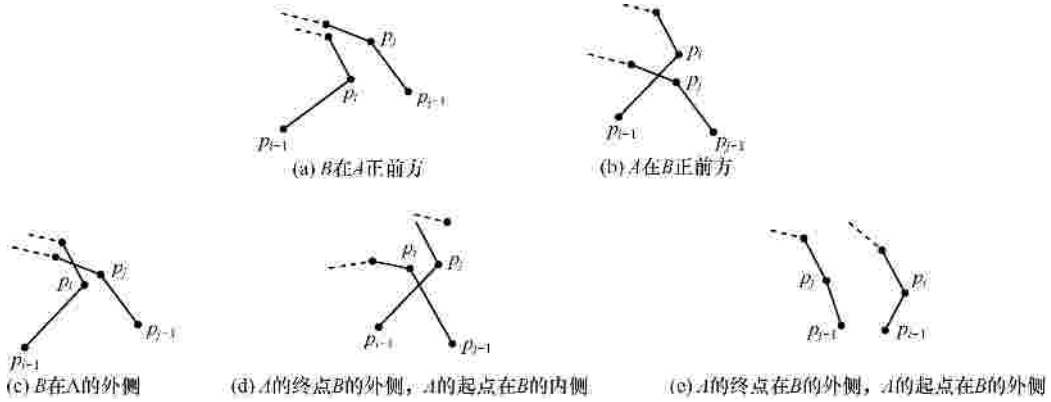

图 9 有向边“追逐”

```
{
  if(PIP(p_i,Q)==1)
     Send(Alice->Bob, p_i);
}
for i=1 to m
{
   if(PIP(q_i,P )==1)
     Send(Bob->Bob, q_i);
}
```

令 $i=j=1$;

$A=\overrightarrow{p_{i-1}p_i}$ 和 $B=\overrightarrow{q_{j-1}q_j}$ 分别为多边形 P 和 Q 的第一条边；

```
do{
STPP_IL(A,B)；//Alice 和 Bob 利用安全两方
//线段求交协议计算并输出边 A 和 B 的交点，
//并插入到各自输出点序列的相应位置。
if(CPP_V(A,B)) >0) //调用保护隐私的向量叉
//积协议，判断向量叉积是否为正
{
     if(CPP_PL (q_{j+1},A)==- 1)
     // q_{j+1} 在 A 的左侧
       i=i+1;
else
       j=j+1;
}
else
{
     if(CPP_PL (p_{i+1},B)==-1)
     // p_{i+1} 在 B 的左侧
          j=j+1;
     else
          i=i+1;
}
}while((i<n+1)&&(j<m+1))
```

5.4 性能分析

通过 5.2 节可知，本协议是正确的。

1) 安全性分析

定理 5 半诚实模型下，上述协议是安全的。

证明 本协议的安全性基于 O’Rourke 算法、安全两方线段求交协议、保护隐私的点线叉积协议、保护隐私的向量叉积协议和保护隐私的点包含协议。由于半诚实模型下，O’Rourke 算法、安全两方线段求交协议、保护隐私的点线叉积协议、保护隐私的向量叉积协议和保护隐私的点包含协议是安全的，因此本协议也是安全的。

2) 效率分析

通信复杂度：本协议最多需要进行 $3(m+n)$ 轮通信。计算复杂度：在最坏的情况下，Alice 和 Bob 共进行 $2(m+n)$ 次安全两方线段求交协议、$2(m+n)$ 次保护隐私的点线叉积协议、$2(m+n)$ 次保护隐私的向量叉积协议和 $(m+n)$ 次保护隐私的点包含协议。

5.5 实例

Alice 拥有 $P=\{(1,2),(2,1),(8,3),(4,5)\}$，Bob 拥有 $Q=\{(2,6),(6,1),(7,4),(5,7)\}$。Alice 和 Bob 使用保护隐私的凸包交集协议共同计算 $P\cap Q$（如图 10 所示）。

表 6 记录了协议每一步的计算过程和输出。

6 结束语

本文给出了安全两方线段求交协议和保护隐私的凸包求交集协议。其中，安全两方线段求交协议不仅可以判断 2 条线段是否相交，而且可以求出交点的坐标；本文不仅在半诚实模型下实现了安全两方线段求交协议，同时给出了恶意模型下的协

议；保护隐私的凸包求交集协议首次实现了求解凸包并集时的隐私保护。

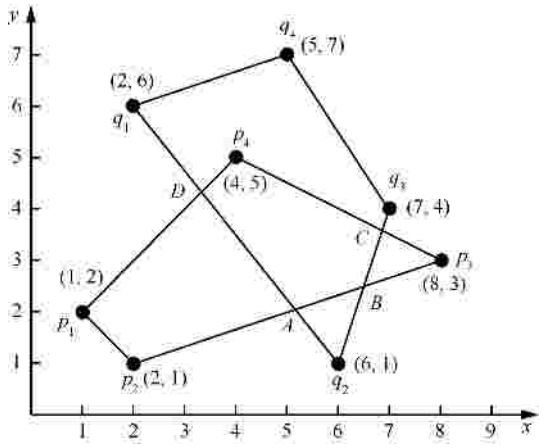

图 10　实例

表 6　　协议每一步的输出

k	交点	A	B	1)	2)	3)	i	j	协议输出
1	-	p_1	Q	-	-	-	-	-	
2	-	p_2	Q	-	-	-	-	-	
3	-	p_3	Q	-	-	-	-	-	
4	p_4	p_4	Q	-	-	-	-	-	$\{p_4\}$
5	-	P	q_1	-	-	-	-	-	$\{p_4\}$
6	-	P	q_2	-	-	-	-	-	$\{p_4\}$
7	-	P	q_3	-	-	-	-	-	$\{p_4\}$
8	-	P	q_4	-	-	-	-	-	$\{p_4\}$
9	-	p_2p_3	q_1q_2	-1	-	1	2	1	$\{p_4\}$
10	A	p_2p_3	q_1q_2	-1	-	-1	2	2	$\{A, p_4\}$
11	B	p_2p_3	q_2q_3	1	-1	-	3	2	$\{A,B, p_4\}$
12	C	p_3p_4	q_2q_3	-1	-	-1	3	3	$\{A,B,C, p_4\}$
13	-	p_3p_4	q_3q_4	-1	-	-1	3	4	$\{A,B,C, p_4\}$
14	-	p_3p_4	q_4q_1	1	-1	-	4	4	$\{A,B,C, p_4\}$
15	-	p_4p_1	q_4q_1	-1	-	-1	4	1	$\{A,B,C, p_4\}$
16	D	p_4p_1	q_1q_2	1	-1	-	1	1	$\{A,B,C, p_4,D\}$

说明：k：协议进行到第 k 步；A:Alice；B：Bob；1) CPP_V(A,B)；2) CPP_PL(q_{j+1}, p_ip_{i+1})；3) CPP_PL (p_{i+1}, q_jq_{j+1})。

参考文献：

[1] GOLDWASSER S. Multi-party computations: past and present[A]. Proceedings of the Sixteenth Annual ACM Symposium on Principles of Distributed Computing[C]. USA, 1997. 21-24.

[2] YAO A C. Protocols for secure computations[A]. Proceedings of 23th Annual IEEE Symposium on Foundations of Computer Science[C]. Chicago, USA, 1982. 160-164.

[3] GOLDREICH O. Secure multi-party computation[EB/OL]. http://www.wisdom.weizman.ac.il/~oded/pp.html, 1998.

[4] SANTOS M A S, MARGI C B. A secure multi-party protocol for sharing valuable information in public safety networks[A]. 2011 IEEE 8th International Conference on Mobile Ad Hoc and Sensor Systems[C]. Valencia, 2011. 935-940.

[5] TANG C M, SHI G H, YAO Z A. Secure multi-party commputation protocol for sequencing problem[J]. Science China Information Sciences, 2011, 54(8):1654-1662.

[6] **刘文，罗守山，陈萍. 利用** ElGamal **密码体制解决安全多方数据排序问题**[J].**通信学报**, 2007, 28(10):1-5.
LIU W, LUO S S, CHEN P. Solution of secure multi-party multi-data ranking problem based on ELGamal encryption[J]. Journal on Communications, 2007, 28 (10):1-5.

[7] **程柏良，曾国荪，揭安全. 基于安全多方计算的可信防共谋协议模型**[J]. **通信学报**, 2011,32(8):23-30.
CHENG B L, ZENG G S, JIE A Q. Trusted coalition-proof protocol model based on secure multi-part computing[J]. Journal on Communications, 2011, 32(8):23-30.

[8] MAHESHWARI N, KIYAWAT K. Structural framing of protocol for secure multiparty cloud computation[A]. The Fifth Asia Modelling Symposium[C]. Kuala Lumpur, 2011. 187-192.

[9] DIMA A, NOMAN M, BENJAMIN C M, *et al*. Secure distributed framework for achieving *e*-differential privacy[A]. Privacy Enhancing Technologies[C]. Berlin: Springer-Verlag, 2012. 120-139.

[10] WANG X M, WANG A, BIAN S Q. Secure multi-party computation-an important theory in electronic technology[A]. Advances in Mechanical and Electronic Engineering[C]. Berlin: Springer-Verlag, 2012. 605-608.

[11] GOLDREICH O , MICALI S A, WIGDERSON A. How to play any mental game[A].The 19rd Annual ACM Conference on Theory of Computing[C]. New York, USA,1987. 218-229.

[12] ATALLAH M J, DU W L. Secure multi-party computational geometry[A]. Algorithms and Data Structures[C]. Berlin: Spr nger, 2001. 165-179.

[13] **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.
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.

[14] 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 Electronic, 2006,15(4):578-582.

[15] **王涛春，罗永龙. 不同坐标系下点圆关系的安全判定协议**[J]. **计算机工程**, 2012, 38(1):105-108.
WANG T C, LUO Y L. Secure determination protocol of po nt-circle relationship under different coordinates[J]. Computer ngineering, 2012, 38(1):105-108.

[16] **李顺东，戴一奇，王道顺等. 几何相交问题的多方保密计算**[J]. **清华大学学报**, 2007,47(10):1692-1695.
LI S D, DAI Y Q, WANG D S, *et al*. Secure multi-party computations of geometric intersections[J]. Journal of Tsinghua Uni rsity, 2007,47(10):1692-1695.

[17] **罗永龙，黄刘生，徐维江等. 一个保护私有信息的多边形相交判定协议**[J]. **电子学报**, 2007, 35(4):685-691.
LUO Y L, HUANG L S, XU H J, *et al*. A protocol for priva-

cy-preserving intersect-determination of two polygons[J]. ACTA Electronica Sinica, 2007, 35 (4):685-691.

[18] **方兴, 仲红, 张守奇等. 保护私有信息的最近点对协议**[J]. **计算机技术与发展**, 2008, 18(12):153-158.
FANG X, ZHONG H, ZHANG S Q, *et al*. A protocol for privacy-preserving closet-pair of points[J]. Computer Technology and Development, 2008, 18(12):153-158.

[19] **仲红,孙彦飞,燕飞飞等.保护私有信息的空间最近点对协议**[J]. **计算机工程与应用**, 2011,48(4):87-89.
ZHONG H, SUN Y F, YAN F F, *et al*. Protocol for privacy-preserving space closet-pair of points[J]. Computer Engineering and Applications, 2011 , 48 (4):87-89.

[20] **逯绍锋,罗永龙**. Graham **算法求解凸包问题中的隐私保护**[J]. **计算机工程与应用**, 2008, 44(36):130-133.
LU S F, LUO Y L. Privacy-preserving in graham algorithm for finding convex hulls[J]. Computer Engineering and Application, 2008, 44(36): 130-133.

[21] WANG Q, LUO Y L, HUANG L S. Privacy- preserving protocols for finding the convex hulls[A]. ARES' 08[C]. Washington, USA, 2008. 727-732.

[22] **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.
LUO Y L, HUANG L S, JING W W, *et al*. Privacy-preserving cross product protocol and its application[J]. Chinese Journal of Computers , 2007, 30(2):248-254.

[23] LUO Y L, HUANG L S, CHEN G L, *et al*. Privacy-preserving distance measurement and its application[J]. Chinese Journal of Electionics, 2006, 15(2):237-241.

[24] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[A]. Cryptology-EUROCRYPT'99[C]. Berlin: Springer-Verlag, 1999. 223-238.

[25] BLAKE I F, KOLESNIKOV V. Strong conditional oblivious transfer and computing on intervals[A]. AISACRYPT 2004[C]. 2004. 515-529.

[26] **刘文, 罗守山, 陈萍. 保护私有信息的点线关系判定协议及其应用**[J]. **北京邮电大学学报**, 2008, 31(2):72-75.
LIU W, LUO S S, CHEN P. Privacy-preserving point-line relation determination protocol and its application[J]. Journal o Beijing University of Posts and Telecommunications, 2008, 31(2):72-75.

[27] **周培德. 计算几何算法设计与分析**[M]. **北京：清华大学出版社**, 2008.
ZHOU P D. Computational Geometry Algorithm Design and Analysis[M]. Beijing:Tsinghua University Press, 2008.

[28] O'ROURKE J. Computational Geometry in C[M]. Cambridge University Press,1998.

作者简介：

孙茂华（1986-），女，山东临沂人，北京邮电大学博士生，主要研究方向为信息安全、安全多方计算。

罗守山（1962-），男，安徽合肥人，北京邮电大学教授、博士生导师，主要研究方向为信息安全、密码学理论、安全多方计算等。

辛阳（1977-），男，山东烟台人，北京邮电大学副教授，主要研究方向为信息安全和密码学。

杨义先（1961-），男，四川盐亭人，北京邮电大学教授、博士生导师，主要研究方向为信息安全和密码学。