doi:10.11959/j.issn.1000-436x.2016075

保护私有信息的点包含协议研究

张静[1,2,3]，罗守山[2]，杨义先[1,2]，辛阳[2]
（1. 北京交通大学计算机与信息技术学院，北京 100044；2. 北京邮电大学信息安全中心，北京 100876；
3. 河南理工大学计算机科学与技术学院，河南 焦作 454000）

摘 要：对现有保护私有信息的点包含协议进行研究，针对算法复杂度高、协议本身的的局限性等问题，在半诚实模型下，提出一种保护隐私的判断点与凸包位置关系协议。首先，利用 OT_1^n 与矢量的几何性质，将传统的点线位置判断问题扩展，设计一种茫然安全点线位置关系判断协议；然后，将此协议作为基础协议，结合安全二分检索法提出最终解决方案。利用 Goldreich 证明法对协议进行安全性证明，同时分析协议的正确性与算法复杂度。分析结果表明，协议在效率上优于现有方案，并具有可扩展性。

关键词：点包含；茫然点线关系；隐私保护；安全多方几何计算
中图分类号：TN918.1 **文献标识码**：A

Research on the privacy-preserving point-in-polygon protocol

ZHANG Jing[1,2,3], LUO Shou-shan[2], YANG Yi-xian[1,2], XIN Yang[2]
(1.School of Computer and Information Technology，Beijing Jiaotong University, Beijing 100044, China;
2.Information Security Center，Beijing University of Posts and Telecommunications, Beijing 100876, China;
3.College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454000, China)

Abstract: A privacy-preserving point-in-polygon protocol was proposed under semi-honest model, to deal with the problem of high complexity and limitation of the existing protocols. First, an oblivious point-line protocol was designed by extending the traditional point-line protocol, making the use of 1-out-*n* oblivious transfer and the geometric properties of the vector. Then, based on this protocol and combined with the secure binary search protocol, the final solution was put forward. The security of the protocol was proved with Goldreich method. Meanwihle, the validity and the complexity of the protocol were also be analyzed. It is shown that this new protocol gets the advantage over the existing one in terms of efficiency and enjoys excellent expandability.

Key words: point-in-polygon, oblivious point-line protocol, privacy-preserving, secure multi-party geometry

1 引言

互联网的快速发展为多方合作开辟了巨大的机会，但是很多合作计算发生在互不信任的参与者或竞争对手之间。安全多方计算（SMC）则为保护互不信任的参与各方隐私安全问题提供有效的解决方案。理论上，利用电路评估协议计算可以解决一般安全多方计算问题。然而,有些计算复杂度是不切实际的，因此，需要特殊的解决方案来解决科学计算、计算几何、统计分析等特殊问题，才能提高效率。

安全多方计算几何的概念首先由 Atallah 等[1]提出。Du 等[2]指出安全多方计算几何主要包括点包含问题、多边形相交问题、最近点对问题以及凸包问题 4 个方面[3~14]。文献[3]利用安全点包含协议，结合 O'Rourke 算法，提出安全两方凸包求交和求并协议；文献[4]设计了一种安全两方求线段交点算法，该方法解决了保护隐私的凸包求交集问题；文献[5]利用安全点线距离协议，提出了安全两方直线与圆距离协议和安全两方圆距离协议；文献[6]基于

收稿日期：2015-06-11；修回日期：2015-10-28
基金项目：国家自然科学基金资助项目（No.61411146001）
Foundation Item: The National Natural Science Foundation of China（No.61411146001)

保护私有信息的向量相等性判定协议，设计出一种保护私有信息的直线上动点距离判定协议，并提出解决保护私有信息的动点距离判定问题的一般性解决方案；文献[7]利用向量差最小值协议和同态加密方案，解决安全多方最近点对问题，该协议不需要茫然第三方；文献[8]基于不经意传输协议设计了一个半诚实模型下安全两方计算最近点对协议；表1所示为安全两方点包含问题方面的部分研究成果。

表1 安全两方点包含研究成果一览

文献	主要研究成果
文献[3]	提出安全仰角计算协议，安全线段交计算协议和安全二分检索协议，并将其作为基础协议，提出了一种新的点与凸包包含协议
文献[9]	利用 Monte Carlo 方法，结合 Cantor 编码，提出一种解决任意几何图形的点包含的方法
文献[10]	提出安全两方向量叉积协议，并利用安全两方三点叉积协议实现安全两方点包含协议
文献[11]	利用矢量夹角比较法，提出了星形域上的点包含协议，并将其扩展为解决一般多边形域的包含问题
文献[12]	分别利用 Du 的两方点积协议和极角比较的方法，提出了2个有效的点与凸包包含关系协议
文献[13]	基于对称密钥的三角形面积协议，提出了一种有效的点与凸多边形包含协议
文献[14]	利用角度旋转方法，解决点与任意多边形的包含问题
文献[15]	将四面体体积作为黑盒工具，提出了一种新包括点面关系判断协议。
文献[16]	提出了安全两方超平面上的点与多维凸包之间的包含关系协议

可以看出，目前解决安全点包含问题的协议，大多是利用已有的基础协议实现的，只是不同的协议考虑的模型不同，或者是要求协议所具有的性质不同。文献[12]提出通过极角比较的方法解决点与凸包包含问题，但由于参与双方在进行坐标位移和极角计算时会泄露参与者的真实信息；文献[10,11,14]分别提出了点与凸包包含协议，点与星多边形包含协议和点与任意多边形包含协议，但三者所提出的协议均有较高的计算复杂度；而文献[3]的方案则只能局限于解决点与凸包包含问题。

针对上述问题，本文提出一种点与凸包包含问题解决方案。协议以茫然点线位置判断关系协议为基础，能够在不泄露双方信息的情况下，判断点和凸包的位置关系，并且可以扩展到点与简单多边形关系判断。协议的计算复杂度和通信复杂度均为 $O(n\log n)$，低于文献[10,11,14]。本文假设参与双方都是半诚实参与者，即在程序的执行过程中，双方能够严格遵守规程，但可能会保留自己所有收集到的信息。

2 预备知识

2.1 基础协议

OT_1^n 不经意传输问题（1-out-of-n oblivious transfer）。OT_1^n 问题是解决安全多方计算问题的基本的工具之一。具体描述为：Alice 拥有 n 个消息 $m_1,m_2,\cdots,m_n$，Bob 想要获得其中第 $k\left(1\leqslant k\leqslant n\right)$ 个消息。双方执行完协议后，Bob 得到第 k 个消息，但他不知道 Alice 其他个消息；而 Alice 不知道 Bob 的具体选择。本文利用文献[17]中提出的高效协议作为茫然点线关系的基础协议。该协议的计算复杂度为 $2n$+2 次方模幂运算，通信次数仅为 2 次。

向量点积协议(SPP, scalar products protocol)。SPP 问题广泛应用于解决保护隐私信息问题，目前已经成为 SMC 的一个基本协议。基本点积问题可以描述为：Alice 有一个私有向量 $\boldsymbol{u}=\left(u_1,u_2,\cdots,u_n\right)$，Bob 有一个私有向量 $\boldsymbol{v}=\left(v_1,v_2,\cdots,v_n\right)$，双方经计算后，Alice 得到值 $w=\boldsymbol{uv}+r=\sum_{i=1}^{n}u_iv_i+r$，$r$ 为 Bob 选择的随机数；Alice 不能从结果得到任何 v_i 的信息；Bob 不能得到任何 u_i 的信息。

百万富翁问题（MP, millionaire protorol）。MP 问题由 Yao[18]首次提出。具体表述为：2 个百万富翁 Alice 和 Bob，他们想知道谁更富有,但又不想让对方知道自己财富的任何信息。Yao 在提出问题后就利用不可信第三方提出了该问题的解决方案。在众多百万富翁解决方案中，Ioannis 等[19]提出的百万富翁解决方案的计算复杂度较小，其计算复杂度和通信复杂度都是 $O\left(2^d\right)$，这里 2^d 是参与双方想要对比数据量上界。

2.2 Paillier 加密算法

Paillier 加密算法[20]是一种依赖和数剩余判定假设的加密算法，具有加法同态性。在多方安全计算、数据库加密等领域中都发挥着重要的作用。算法具体描述如下。

1) 密钥选取

假设模 $N=pq$，$L\left(x\right)=\dfrac{x-1}{N}$。

随机选取 $g,g\in\left(\dfrac{Z}{N^2Z}\right)$，使之满足 $\gcd(L(g^{\lambda}\bmod N^2),N)=1$。则 (N,g) 为公钥，私钥为 $\lambda(N)=\mathrm{lcm}((p-1),(q-1))$。

2) 加密算法

对要加密消息 m，$\forall r \in Z_N^*$，计算密文 $E(m)=g^m r^N \bmod N^2$。

3) 解密算法

对于密文 $c=E(m)$，计算 $m=\dfrac{L\left(c^{\lambda(N)} \bmod N^2\right)}{L\left(g^{\lambda(N)} \bmod N^2\right)}$。

加法同态性分析：

给定消息 m_1、m_2 满足

$$E(m_1)E(m_2)=\left(g^{m_1}r_1^N\right)\left(g^{m_2}r_2^N\right)=g^{m_1+m_2}\left(r_1r_2^N\right)=E(m_1+m_2)$$

可以看出，参与者可利用此性质直接用密文代替明文进行某些运算,而不影响明文数据的机密性。即满足语义安全的概率下，$E(0)$、$E(1)$ 在计算上不可区分。

2.3 符号说明

本文使用文献[21]中提出的系统符号，具体说明如下。

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 各自本地执行第 i 步。

$A_i\text{^}B_i$：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。

$\text{Send}(\text{Alice}\rightarrow\text{Bob};m_1,m_2,\cdots,m_n)$：Alice 向 Bob 发送消息 $m_1,m_2,\cdots,m_n$。

$\text{Receive}(\text{Alice}\rightarrow\text{Bob};m_1,m_2,\cdots,m_n)$：Bob 接收 Alice 发送的消息 $m_1,m_2,\cdots,m_n$。

3 茫然点线位置关系判断协议

3.1 协议描述

问题描述：Alice 有 n 条共点直线，其向量为 $\overrightarrow{\boldsymbol{AA}_i}=\left(X_{A_i},Y_{A_i}\right),i=1,2,\cdots,n$，向量的公共点坐标为 $Z=(x_A,y_A)$，Bob 有一个点 $P=\left(x_p,y_p\right)$，在确保双方能够联合判断点 P 与第 m 条直线的位置关系的情况下，Bob 希望知道点线位置关系判断的最终结果，而又不希望 Alice 知道自己具体的选择。此问题称为保护隐私的茫然点线位置关系判断问题。协议的具体描述如下。

$PP\_OPLP\left(\left(L_1,L_2,\cdots,L_n\right),P,m\right)$

{

$A_1|B_1$:

Alice

Generate：$\left(X_{A_i},Y_{A_i}\right),i=1,2,\cdots,n$

Compute：$\left(E_{pk_A}\left(X_{A_i}\right),E_{pk_A}\left(Y_{A_i}\right)\right),i=1,2,\cdots,n$

//Alice 用自己公钥加密所有共点向量

Bob Generate m

//Bob 选择希望参与判断的第 m 条直线

$A_2\text{^}B_2$：

$OT_1^n(A,B)$

//Alice 和 Bob 调用不经意传输协议

//Bob 得到 $\left(E_{pk_A}\left(X_{A_m}\right),E_{pk_A}\left(Y_{A_m}\right)\right)$；

B_3：

Generate：r_1,r_2；

//Bob 随机选择 $r_1,r_2\in Z^+$ 且 $r_1\neq r_2$

Compute：

$E_{pk_A}\left(X_{A_m}'\right)=E_{pk_A}\left(X_{A_m}\right)E_{pk_A}(r_1)=E_{pk_A}\left(X_{A_m}+r_1\right)$；

Compute：

$E_{pk_A}\left(Y_{A_m}'\right)=E_{pk_A}\left(Y_{A_m}\right)E_{pk_A}(r_2)=E_{pk_A}\left(Y_{A_m}+r_2\right)$；

Send

$\left(\text{Bob}\rightarrow\text{Alice},\left(E_{pk_A}\left(X_{A_m}'\right),E_{pk_A}\left(Y_{A_m}'\right)\right)\right)$；

//Bob 将计算结果发送给 Alice

A_4：

Receive

$\left(\text{Bob}\rightarrow\text{Alice},\left(E_{pk_A}\left(X_{A_m}'\right),E_{pk_A}\left(Y_{A_m}'\right)\right)\right)$；

Compute：

$X_{A_m}'=D_{sk_A}\left(E_{pk_A}\left(X_{A_m}'\right)\right)$；

$Y_{A_m}'=D_{sk_A}\left(E_{pk_A}\left(Y_{A_m}'\right)\right)$；

//Alice 解密得到 $\left(X_{A_m}',Y_{A_m}'\right)$

$A_5|B_5$:

Alice

Compute: $u_A=-X_{A_m}'y_A+Y_{A_m}'x_A$;

Bob

Compute: $u_B=r_1y_P-r_2x_P$;

$A_6\text{^}B_6$:

$\text{SPP}\left(\left(X_{A_m}',Y_{A_m}',u_A\right),\left(y_P,-x_P,-1\right)\right)$;

//Alice 和 Bob 调用安全两方点积协议

//Alice 得到

$u_1 = y_P X_{A_m}{}' - x_P Y_{A_m}{}' - X_{A_m}{}' y_A + Y_{A_m}{}' x_A + v_1$

//Bob 得到 v_1；

$\mathrm{SPP}\left((x_A, y_A, 1), (r_2, r_1, u_B)\right)$；

//Alice 和 Bob 调用安全两方点积协议

//Alice 得到

$u_2 = r_2 x_A - r_1 y_A + r_1 y_P - r_2 x_P + v_2$

//Bob 得到 v_1；

$A_7|B_7$:

Alice Compute $u = u_1 - u_2$;

Bob Compute $v = v_1 - v_2$;

A_8^B_8:

Compute: $s = \mathrm{MP}(u, v)$;

//Alice 和 Bob 利用百万富翁协议比较 (u, v)

Return s;

//根据 s 判断点与第 m 个向量的关系；

}

如果 $s > 0$ 则点 P 在向量 $\overrightarrow{AA_i}$ 的逆时针方向，如果 $s < 0$ 则点 P 在向量 $\overrightarrow{AA_i}$ 的顺时针方向，如果 $s = 0$ 则点 P 与向量 $\overrightarrow{AA_i}$ 共线。

3.2 性能分析

定理 1 半诚实模型下，该协议能够正确判断点与第 m 条直线的位置关系。

证明 判断点与第 m 条直线位置关系等价于判断 $u = Y_{A_m} x_P - X_{A_m} y_P - x_A Y_{A_m} + y_A X_{A_m} + v$ 与 v 的大小关系。首先 Bob 要确定需要比较的直线向量，同时向量信息对 Alice 是茫然的，因此 Alice 和 Bob 调用 OT_1^n 不经意传输协议，协议 $A_1|B_1$,A_1^B_1 正确；B_3、A_4 利用 Paillier 算法的加法同态性，将 Bob 计算得到 $X_{A_m}{}' = X_{A_m} + r_1$，$Y_{A_m}{}' = Y_{A_m} + r_2$ 并传送给 Alice，由于 r_1、$r_2 \in Z^+$ 且 $r_1 \neq r_2$，Alice 不能得到向量的具体值，因此是正确的；u_1、u_2 由 Alice 和 Bob 利用安全两方点积协议得到，即 $A_5|B_5$、A_6^B_6 正确；因此有 $A_7|B_7$ 正确，即

$$\begin{aligned} u &= u_1 - u_2 \\ &= \left(y_P X_{A_m}{}' - x_P Y_{A_m}{}' - X'_{A_m} y_A + Y'_m x_A + v_1\right) - \\ &\quad \left(r_2 x_A - r_1 y_A + r_1 y_P - r_2 x_P + v_2\right) \\ &= \left(Y_{A_m} x_P - X_{A_m} y_P - x_A Y_{A_m} + y_A X_{A_m}\right) + \left(v_1 - v_2\right) \\ &= \left(Y_{A_m} x_P - X_{A_m} y_P - x_A Y_{A_m} + y_A X_{A_m}\right) + v \end{aligned}$$

最后，Alice 和 Bob 利用百万富翁协议返回 s，显然 A_9^B_9 是正确的。

综上，在半诚实模型下，该协议能够正确判断点与第 m 条直线的位置关系。

定理 2 半诚实模型下，茫然点线位置关系判断协议是安全的。

证明 根据半诚实模型下 OT_1^n 的安全性可知 A_2^B_2 是安全的；B_3 中 Bob 利用 Paillier 加密算法计算 $E_{pk_A}\left(X_{A_m} + r_1\right)$，$E_{pk_A}\left(Y_{A_m} + r_2\right)$，而无法解密，因此 Bob 不知道 X_{A_m}、Y_{A_m} 的具体值，B_3 是安全的；虽然 Alice 解密得到 $X_{A_m} + r_1$，$Y_{A_m} + r_2$，但 r_1、r_2 的随机性使 Alice 无法知道 X_{A_m}、Y_{A_m} 的具体信息，因此 A_4 是安全的；步骤 A_8^B_8 中的百万富翁比较协议保证了，双方除判断 u, v 的大小关系之外，不会泄露双方的任何其他信息。下面证明步骤 $A_5|B_5$、A_6^B_6、$A_7|B_7$ 是安全的。本文分别对 Alice 和 Bob 的协议执行过程构造模拟器。根据协议知模拟器的初始输入

$$A = \left\{\left(X_{A_m}{}', Y_{A_m}{}'\right), (x_A, y_A), u_A\right\}$$

$$B = \left\{r_1, r_2, (x_p, y_p), u_B\right\}$$

1) 构造模拟器 S_1 模拟 Alice 的协议执行如下过程。

step1 S_1 接收 $A, f_1(A,B)$ 作为输入，其中，$f_1(A,B) = \{u_1, u_2\}$；

step2 S_1 选取 $\left(x_p{}', y_p{}'\right)$，$r_1', r_2'$，计算 $u_B{}' = r_1' \cdot y_P{}' - r_2' \cdot x_P{}'$；

step3 S_1 构造向量

$\boldsymbol{U}_1 = \left(X_{A_m}{}', Y_{A_m}{}', u_A\right)$，$\boldsymbol{V}_1' = \left(x_p{}', -y_p{}', -1\right)$；

$\boldsymbol{U}_2 = (x_A, y_A, 1)$，$\boldsymbol{V}_2' = \left(r_2', r_1', u_B{}'\right)$；

选取 v_1', v_2'，建立等式

$\boldsymbol{U}_1 \boldsymbol{V}_1' + v_1' = u_1$，$\boldsymbol{U}_2 \boldsymbol{V}_2' + v_2' = u_2$；

step4 S_1 计算

$u' = \left(\boldsymbol{U}_1 \boldsymbol{V}_1' - \boldsymbol{U}_2 \boldsymbol{V}_2'\right) + \left(v_1' - v_2'\right)$；

step5 S_1 输出

$S_1\left(A, f_1(A,B)\right)$

$= \left\{\left(X_{A_m}{}', Y_{A_m}{}'\right), (x_A, y_A), u_A, u_1, u_2, u'\right\}$

根据 S_1 的构造结构，显然有 $u' \overset{c}{\equiv} u$；

又知 Alice 的信息序列为

$$VIEW_1^{\Pi}(x,y)$$

$$=\left\{\left(X_{A_m}{}',Y_{A_m}{}'\right),(x_A,y_A)_1,u_A,u_1,u_2,u\right\};$$

$$OUTPUT_2^{\Pi}(x,y)=f_2(x,y)=\{v_1,v_2\};$$

因此，有下式成立。

$$\left\{S_1(A,f_1(A,B)),f_2(A,B)\right\}$$

$$\overset{C}{\equiv}\left\{VIEW_1^{\Pi}(A,B),OUTPUT_2^{\Pi}(A,B)\right\}$$

2) 构造模拟器 S_2 模拟 Bob 的协议执行如下过程。

step1　S_2 接收 $B,f_2(A,B)$ 作为输入，其中，$f_2(A,B)=\{v_1,v_2\}$；

step2　S_2 选取 $\left(X_{A_m}{}'',Y_{A_m}{}''\right),\left(x_A{}',y_A{}'\right)$，计算 $u_A{}'=-\left(X_{A_m}{}''+r_1\right)y_A{}'+\left(Y_{A_m}{}''+r_2\right)x_A{}'$；

step3　S_2 构造向量

$$\boldsymbol{U}_1''=\left(\left(X_{A_m}{}''+r\right)_1,\left(Y_{A_m}{}''+r_2\right),u_A{}'\right),$$

$$\boldsymbol{V}_1=\left(x_p,-y_p,-1\right);$$

$$\boldsymbol{U}_2''=\left(x_A{}',y_A{}',1\right),\ \boldsymbol{V}_2=(r_2,r_1,u_B);$$

选取 $u_1{}',u_2{}'$，建立等式

$$u_1{}'-\boldsymbol{U}_1''\boldsymbol{V}_1=v_1,\ u_2{}'-\boldsymbol{U}_2\boldsymbol{V}_2{}'=v_2{}';$$

step4　S_2 计算

$$v'=\left(\boldsymbol{U}_1''\boldsymbol{V}_1-\boldsymbol{U}_2''\boldsymbol{V}_2\right)+\left(u_1{}'-u_2{}'\right);$$

step5　S_2 输出

$$S_2\left(B,f_2(A,B)\right)$$

$$=\left\{r_1,r_2,\left(x_p,y_p\right),u_B,v_1,v_2,v'\right\};$$

根据 S_2 的构造结构，显然有 $v'\overset{c}{\equiv}v$；

由于 Bob 的信息序列为

$$VIEW_2^{\Pi}(x,y)=\left\{r_1,r_2,\left(x_p,y_p\right),u_B,v_1,v_2,v\right\}$$

$$OUTPUT_1^{\Pi}(A,B)=f_1(A,B)=\{u_1,u_2\}$$

因此

$$\left\{f_1(A,B),S_2\left(B,f_2(A,B)\right)\right\}$$

$$\overset{C}{\equiv}\left\{OUTPUT_1^{\Pi}(A,B),VIEW_2^{\Pi}(A,B)\right\}$$

成立；

综上所述，半诚实模型下茫然点线位置关系判断协议是安全的。

定理 3　茫然点线位置关系判断协议的计算复杂度和通信复杂度都是为 $O(n)$。

证明　协议执行了 1 次 OT_1^n 协议，2 次安全两方点积协议，1 次百万富翁比较协议，2 次 Paillier 加密算法和 2 次 Paillier 解密算法，因此，协议的时间复杂度为

$$T_{\text{comp}}+2P_{\text{comp}}+Y_{\text{comp}}+4E_{\text{comp}}$$

$$=O\left(2n+2+2(2\mu n)+2^d+4\log N\right)=O(n)$$

其中，T_{comp}、P_{comp}、Y_{comp}、E_{comp} 分别代表上述 4 个协议的计算复杂度；在 B_3、A_4 中 Alice 和 Bob 双方有一次通信，且系统采用文献[18]中 OT_1^n 协议，其通信次数为 2 次，因此协议的通信复杂度为

$$3+2P_{\text{comm}}+Y_{\text{comm}}=O\left(3+2(2\mu n)+n\right)=O(n)$$

其中，P_{comm}、Y_{comm} 分别代表安全两方点积协议和百万富翁协议的通信次数。

4　保护隐私的两方点包含协议

作为安全多方几何计算的主要研究方向之一，安全两方点包含协议在军事，商业等领域具有广泛的应用场景。*A* 在某一地区拥有一个秘密军事区，*B* 希望在该地区进行军事演习，但又不想对 *A* 的秘密军事区造成影响。因此双方在不泄露自己军事秘密的情况下，确保 *B* 的演习地点不在 A 的秘密军事之内；*A*、*B* 这 2 个公司希望在某一地区进行业务拓展，但是为避免重复业务，两公司希望在不向对方泄露自己的具体商业（范围）位置信息的情况下，确保 *B* 公司计划开拓的新业务点不在 *A* 公司的计划发展区域内。

以上 2 个问题均可以抽象为安全两方点与凸多边形包含问题。即 Alice 有一个凸多边形的 n 个顶点 $\left(x_{A_i},y_{A_i}\right),i=1,2,\cdots,n$，Bob 有一个点 P，双方希望在不泄露各自信息的前提下，保密判断点 P 是否在凸多边形内。本文利用茫然点线位置关系判断协议，结合二分查找法，提出一种解决安全两方点与凸多边形位置关系判断协议。

4.1　基本思想

协议的基本思想是通过比较点与线的顺时针或逆时针关系，找到共同区域，最终判定出点与凸多边形的关系。

1) 在凸多边形内部找一点 A_Z。可以考虑在多边形上任取不共线的顶点所组成的三角形重心作

为 A_Z 点。按逆时针方向依次排列顶点 $A_1, A_2, \cdots, A_n$，以 A_Z 点为顶点分别向多边形 n 顶点 $A_i, i=1,2,\cdots,n$ 做矢量 $\overrightarrow{\boldsymbol{A}_Z\boldsymbol{A}_i}$，把平面分割成 n 个楔形。

2) 对于给定点 P,首先找到点 P 所在的楔形(含楔形的 2 个边)。从图 1（a）可以看出，点 P 与楔形 2 个边界的关系应满足下列条件之一。

①点 P 在向量 $\overrightarrow{\boldsymbol{A}_Z\boldsymbol{A}_i}$ 的逆时针方向并且在向量 $\overrightarrow{\boldsymbol{A}_Z\boldsymbol{A}_{i+1}}$ 的顺时针方向。

②点 P 与向量 $\overrightarrow{\boldsymbol{A}_Z\boldsymbol{A}_i}$ 共线并且在向量 $\overrightarrow{\boldsymbol{A}_Z\boldsymbol{A}_{i+1}}$ 的顺时针方向。

③点 P 向量 $\overrightarrow{\boldsymbol{A}_Z\boldsymbol{A}_{i+1}}$ 共线并且在向量 $\overrightarrow{\boldsymbol{A}_Z\boldsymbol{A}_i}$ 的逆时针方向。

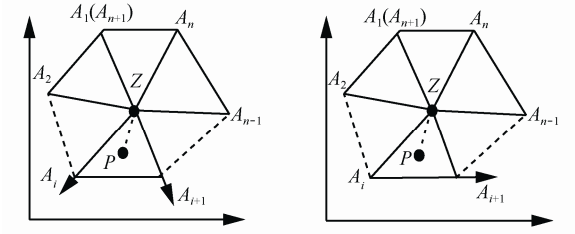
即

$$\left(\mathrm{sgn}\left(\overrightarrow{\boldsymbol{A}_Z\boldsymbol{A}_i}\times\overrightarrow{\boldsymbol{A}_Z\boldsymbol{P}}\right)=0\right)\wedge\left(\mathrm{sgn}\left(\overrightarrow{\boldsymbol{A}_Z\boldsymbol{A}_{i+1}}\times\overrightarrow{\boldsymbol{A}_Z\boldsymbol{P}}\right)=-1\right)$$

$$\left(\mathrm{sgn}\left(\overrightarrow{\boldsymbol{A}_Z\boldsymbol{A}_i}\times\overrightarrow{\boldsymbol{A}_Z\boldsymbol{P}}\right)=1\right)\wedge\left(\mathrm{sgn}\left(\overrightarrow{\boldsymbol{A}_Z\boldsymbol{A}_{i+1}}\times\overrightarrow{\boldsymbol{A}_Z\boldsymbol{P}}\right)=-1\right)$$

$$\left(\mathrm{sgn}\left(\overrightarrow{\boldsymbol{A}_Z\boldsymbol{A}_i}\times\overrightarrow{\boldsymbol{A}_Z\boldsymbol{P}}\right)=1\right)\wedge\left(\mathrm{sgn}\left(\overrightarrow{\boldsymbol{A}_Z\boldsymbol{A}_{i+1}}\times\overrightarrow{\boldsymbol{A}_Z\boldsymbol{P}}\right)=0\right)$$

3) 通过判断点 P 与 $\overrightarrow{\boldsymbol{A}_i\boldsymbol{A}_{i+1}}$ 的位置关系，即 $\mathrm{sgn}\left(\overrightarrow{\boldsymbol{A}_i\boldsymbol{A}_{i+1}}\times\overrightarrow{\boldsymbol{A}_i\boldsymbol{P}}\right)$，判断 P 与凸多边形 A 的位置关系（如图 1（b）所示）。



(a) 查找点P所在楔形　　(b) 点P与直线A_iA_{i+1}的位置关系

图 1　点与凸多边形的位置判断

4.2　协议具体描述

PPI_PIP（*A,B*）

{

A_1:

Sort：$\left(x_{A_1}, y_{A_1}\right),\left(x_{A_2}, y_{A_2}\right),...,\left(x_{A_n}, y_{A_n}\right)$；

//将凸边形 n 个顶点按照逆时针顺序依次排列

//其中 $\left(x_{A_{n+1}}, y_{A_{n+1}}\right)=\left(x_{A_1}, y_{A_1}\right)$

$\left(x_{A_0}, y_{A_0}\right)=\left(x_{A_n}, y_{A_n}\right)$

Generate：$A_z=\left(x_z, y_z\right)$；

//Alice 选择凸多边形已知内点 Z

Compute：

$\overrightarrow{\boldsymbol{A}_z\boldsymbol{A}_i}=\left(X_{A_i}, Y_{A_i}\right)=\left(x_{A_i}-x_{A_z}, y_{A_i}-y_{A_z}\right)$

其中，$i=1,2,\cdots,n$

//Alice 计算楔形边界向量 $\overrightarrow{\boldsymbol{A}_z\boldsymbol{A}_i}$

Compute：

$\overrightarrow{\boldsymbol{A}_i\boldsymbol{A}_{i+1}}=\left(X_{A_i}', Y_{A_i}'\right)=\left(x_{A_{i+1}}-x_{A_i}, y_{A_{i+1}}-y_{A_i}\right)$

其中，$i=1,2,\cdots,n$；

//Alice 计算凸多边形边界矢量 $\overrightarrow{\boldsymbol{A}_i\boldsymbol{A}_{i+1}}$

B_2:

Generate：$t=0$；

//Bob 初始化循环变量 t

Generate：$f=1, l=n, m$

//Bob 选择随机数 $f, m, l\in Z_n, f\leqslant m\leqslant l$

A_3^B_3:

For $t=0,1,2,\cdots$

$\{PP\_OPLP\left(\left(\overrightarrow{\boldsymbol{A}_z\boldsymbol{A}_i}, i=1,\cdots,n\right), P, m\right)$；

//两方调用 *PP_OPLP* 协议得到 s_m

If $\left(s_m>0\right)$

$\{PP\_OPLP\left(\left(\overrightarrow{\boldsymbol{A}_z\boldsymbol{A}_i}, i=1,\cdots,n\right), P, m+1\right)$；

//两方调用 *PP_OPLP* 协议得到 s_{m+1}

If $\left(s_{m+1}>0\right)$

B_4：{Compute：$f=m+1, m=\left\lfloor\dfrac{f+l}{2}\right\rfloor$；

//Bob 重新计算 m

}

Else If$\left(s_{m+1}\leqslant 0\right)$

$\{PP\_OPLP\left(\left(\overrightarrow{\boldsymbol{A}_i\boldsymbol{A}_{i+1}}, i=1,\cdots,n\right), P, m\right)$；

//两方调用 *PP_OPLP* 协议得到 s_p

End;

}

}

Else if$\left(s_m<0\right)$

$\{PP\_OPLP\left(\left(\overrightarrow{\boldsymbol{A}_z\boldsymbol{A}_i}, i=1,\cdots,n\right), P, m-1\right)$；

//两方调用 *PP_OPLP* 协议得到 v_{m-1}

If $\left(s_{m-1}<0\right)$

{

B_5:　　{Compute：$l=m-1, m=\left\lfloor\dfrac{f+l}{2}\right\rfloor$；

//Bob 重新计算 m

}

Else if $(s_{m-1} \geqslant 0)$

{$PP\_OPLP\left(\left(\overline{\boldsymbol{A}_{i-1}\boldsymbol{A}_i}, i=1,\cdots,n\right), P, m-1\right)$；

//两方调用 *PP_OPLP* 协议得到 s_p

End;

}

}

Else

$PP\_OPLP\left(\left(\overline{\boldsymbol{A}_i\boldsymbol{A}_{i+1}}, i=1,\cdots,n\right), P, m\right)$；

//两方调用 *PP_OPLP* 协议得到 s_p

End

}

如果Alice拥有的是简单多边形或者星多边形，将点 A_Z 选择为多边形的核，则该协议可以转化为解决点与简单多边形，点与星型多边形的位置关系判断问题。

4.3 性能分析

定理 4　保护隐私的点包含协议是正确的，安全的，并且计算复杂度和通信复杂度均为 $O(n\log n)$。

证明　（正确性）协议中步骤 A_1、B_2 是 Alice 和 Bob 各自计算初始数据，没有信息交互，因此是正确的。步骤 A_3^B_3 中，Alice 和 Bob 利用茫然两方点线位置关系安全计算并判断 s_m'、s_{m+1}、s_{m-1}，当 $(s_m>0)\wedge(s_{m+1}\leqslant 0)$ 或 $(s_m<0)\wedge(s_{m-1}\geqslant 0)$ 或 $\left(s_m'=0\right)$ 时，Bob 找到 P' 所在楔形的位置，即满足 4.1 节的条件 2)中寻找楔形条件，否则继续执行循环，因此是正确的。Alice 和 Bob 再次调用 *PP_OPLP* 协议计算 s_p'，满足 4.1 节的条件 3)中判断：如果 $s_p'>0$，则 P' 在凸多边形内；如果 $s_p'<0$，则 P' 在凸多边形外；如果 $s_p'=0$，则 P' 在凸多边形边界上。又由定理 1 可知，保护隐私的点包含协议是正确的。

（安全性）根据二分查找法的循环特点，只需对单次循环的协议执行过程构造模拟器。由协议知，模拟器的初始输入为

$$A=\left\{\left(\overline{\boldsymbol{A}_z\boldsymbol{A}_i}, i=1,\cdots,n\right), \left(\overline{\boldsymbol{A}_{i-1}\boldsymbol{A}_i}, i=1,\cdots,n\right)\right\}$$

$$B=\left\{\left(x_p, y_p\right), m\right\}$$

构造模拟器 S_1 模拟 Alice 的协议执行过程如下。

step1　S_1 接收 $A, f_1(A,B)$ 作为输入，其中，$f_1(A,B)=\left\{s_m, s_{m+1}(s_{m-1}), s_p\right\}$。

step2　S_1 选取 $\left(x_p', y_p'\right), m'$，调用 PP_OPLP 协议计算 s_m'、s_{m+1}'、s_{m-1}'。

step3　S_1 判断 s_m'，如果 $s_m'>0$，则 P' 在 $\overline{\boldsymbol{A}_z\boldsymbol{A}_{m+1}}$ 的逆时针方向；如果 $s_m'<0$，则 P' 在 $\overline{\boldsymbol{A}_z\boldsymbol{A}_{m+1}}$ 的顺时针方向；如果 $s_m'=0$，则 P' 与 $\overline{\boldsymbol{A}_z\boldsymbol{A}_{m+1}}$ 共线。因此根据茫然两方点线关系判断协议的安全性有 $s_m' \overset{c}{\equiv} s_m$；同理，如果 $s_m'>0$，S_1 调用 *PP_OPLP* 协议计算并判断 s_{m+1}'，由茫然两方点线关系判断协议的安全性知 $s_{m+1}' \overset{c}{\equiv} s_{m+1}$；如果 $s_m'<0$，S_1 调用 *PP_OPLP* 协议计算并判断 s_{m-1}'，由茫然两方点线关系判断协议的安全性知 $s_{m-1}' \overset{c}{\equiv} s_{m-1}$。

step4　当 $\left(s_m'=0\right)$ 或 $\left(s_m'>0\right)\wedge\left(s_{m+1}'\leqslant 0\right)$ 或 $\left(s_m'<0\right)\wedge\left(s_{m-1}'\geqslant 0\right)$ 时，S_1 找到 P' 所在楔形的位置，调用 *PP_OPLP* 协议计算 s_p'，根据茫然两方点线关系判断算法的安全性有 $s_p' \overset{c}{\equiv} s_p$。

step5　S_1 输出

$$S_1\left(A, f_1(A,B)\right)$$
$$=\left\{\left(\overline{\boldsymbol{A}_z\boldsymbol{A}_i}\right), \left(\overline{\boldsymbol{A}_{i-1}\boldsymbol{A}_i}\right), s_m', s_{m+1}'\left(s_{m-1}'\right), s_p'\right\}$$

其中，$i=1,2,\cdots,n$。

由协议知：Alice 的信息序列

$$VIEW_1^{\Pi}(x,y)$$
$$=\left\{\left(\overline{\boldsymbol{A}_z\boldsymbol{A}_i}\right), \left(\overline{\boldsymbol{A}_{i-1}\boldsymbol{A}_i}\right), s_m, s_{m+1}(s_{m-1}), s_p\right\}$$

其中，$i=1,2,\cdots,n$。

因此有 $\left\{S_1\left(A, f_1(A,B)\right)\right\} \overset{C}{\equiv} \left\{VIEW_1^{\Pi}(A,B)\right\}$ 成立。类似地，可以构造模拟器 S_2 模拟 *Bob* 的协议执行过程。

（复杂性）协议中 A_1 计算复杂度是 $O(n)$；二分查找法的时间复杂度为 $O(\log n)$，每次循环最多调用 3 次 *PP_OPLP* 协议，因此忽略加法乘法计算，在最差情况下，协议计算复杂度和通信复杂度分别为

$$O\left(n+\left(3PP\_OPLP_{\text{comp}}\right)\log n\right)=O(n\log n)$$

$$O\left(\left(3PP\_OPLP_{\text{comm}}\right)\log n\right)=O\left(n\log n\right)$$

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，但没有明确使用的具体算法。为了方便计算，本文统一选用经典的基础算法的复杂度进行计算和比较。

由表 2 可知，本文提出的方案计算复杂度和通信复杂度都低于文献[10, 11, 14]，略高于文献[3]。

表 2　　复杂度对比

方法	计算复杂度	通信复杂度
本文	$O(n\log n)$	$O(n\log n)$
文献[3]	$O(n\log N)$	$O(nd)$
文献[10]	$O(n^2)$	$O(n^2)$
文献[11]	$O(n\log n\log N)$	$O(nd\log n)$
文献[14]	$O(n^2)$	$O(n^2)$

表 3 是相关点包含协议在基础协议和功能方面的对比。

表 3　　基础协议和功能比较

方法	基础协议	判断点与凸包关系	判断点与简单多边形关系
本文	茫然点线关系协议	是	是
文献[3]	仰角比较协议	是	否
文献[10]	安全叉积协议	是	否
文献[11]	极角比较协议	是	是
文献[14]	角度旋转协议	是	是

5 结束语

本文在半诚实模型下，设计了一个茫然安全两方点线位置关系判断协议，并利用该协议为基础，结合安全两方二分检索协议，提出一个保护隐私的两方点包含协议。虽然茫然判断协议存在无法控制协议双方使用留存信息获取对方隐私的安全隐患，但本文在进行茫然判断时，参与双方的留存信息均是以密文或明文的变换形式存在，而且在本论文分析过程中，没有发现利用留存信息获取对方隐私的方式。

需要指出的是，本文方案还不能判断点和任意多边形的位置关系，希望以后能做进一步的研究。

参考文献：

[1] ATALLAH M J, DU W. Secure multi-party computational geometry[M]. Algorithms and Data Structures. Springer Berlin HeidelBerg, 2001: 165-179.

[2] DU W L, ATALLAH M J. Secure multi-party computation problems and their applications: a review and open problems[C]//The 2001 Workshop on New Security Paradigms. c2001: 13-22.

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

[4] 孙茂华, 罗守山, 辛阳, 等. 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[J]. 通信学报, 2013, 34(1): 30-42.
SUN M H, LUO S S, XIN Y, et al. Secure two-party line segments intersection scheme and its application in privacy-preserving convex hull intersection[J]. Journal of Communications, 2013, 34(1): 30-42.

[5] YANG B, SUN A D, ZHANG W Z. Secure two-party protocols on planar circles[J]. Journal of Information, 2011, 8(1): 29-40.

[6] 耿涛, 李海成, 罗守山, 等. 保护私有信息的动点距离判定协议及其推广[J]. 北京邮电大学学报, 2012, 35(3): 47-51.
GENG T,LI H C,LUO S S, et al. A privacy-preserving dynamic point distance determination protocol and its extension[J]. Journal of Beijing University of Posts and Telecommunications. 2012, 35(3): 47-51.

[7] 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.

[8] 周敏, 杨波, 万军洲, 等. 保留隐私的计算最近点对协议[J]. 西南师范大学学报: 自然科学版, 2013,38(2): 111-115.
ZHOU M, YANG B, WAN J Z. A protocol for privacy-preserving closest-pair of points[J]. Journal of Southwest China Normal UniversityJ], 2013, 38(2): 111-115.

[9] 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.

[10] 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.

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

[12] YUN Y, LIU S H, WEI Y, et al. Efficient secure protocols to determine

whether a point is inside a convex hull[C]// International Symposium on Information Engineering and Electronic Commerce, IEEC'09. c2009: 100-105.

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

[14] CHEN L, LIN B. Privacy-preserving point-inclusion two-party computation protocol[C]//2013 Fifth International Conference on Computational and Information Sciences (ICCIS). c2013: 257-260.

[15] 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.

[16] TRONCOSO-PASTORIZA J R, KATZENBEISSER S, CELIK M, et al. A secure multidimensional point inclusion protocol[C]//The 9th Workshop on Multimedia & Security. c2007: 109-120.

[17] TZENG W G. Efficient 1-out-of-*n* oblivious transfer schemes with universally usable parameters[J]. IEEE Transactions on Computers, 2004, 53(2): 232-240.

[18] YAO A C. Protocols for secure computations[C]//The 23th Annual IEEE Symposium on Foundations of Computer Science. Chicago, USA, c1982: 160-164.

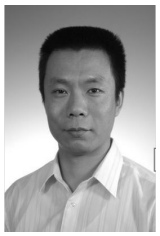
[19] IOANNIDIS I, GRAMA A. An efficient protocol for Yao's millionaires' problem[C]//The 36th Annual Hawaii International Conference on System Sciences. c2003: 6.

[20] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]//Advances in Cryptology—EUROCRYPT'99. Springer Berlin HeidelBerg, c1999: 223-238.

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

作者简介：

张静（1978-），女，河南焦作人，北京交通大学博士生、副教授，主要研究方向为信息安全、安全多方计算等。



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。

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、密码学等。

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、密码学等。