# 点包含问题的安全多方计算

杨晓艺,刘 新,亢 佳
(陕西师范大学 计算机科学学院,陕西 西安 710119)

**摘 要**:安全多方计算是近年来国际密码学界研究的热点问题,计算几何的多方保密计算越来越受到重视,点包含问题的多方保密计算作为保密计算几何中的一个重要问题也越来越受到关注。考虑到要保密地解决点包含的问题,基于安全多方计算的几个基础协议,即向量点积协议和姚式百万富翁协议,设计了一个可以保密判断线段是否相交的协议,基于此协议的核心思想同时联系相关几何知识,设计了可以保密判断点包含问题的协议,理论分析结果表明所设计的协议在半诚实模型下是正确的和安全的。它们作为重要的安全多方计算基础协议对解决保密计算几何其他相关问题有着重要的实用价值,可以用来进一步解决两个或多个图形是否相交的问题、多个点是否包含在一个图形中的问题等。

**关键词**:安全多方计算;保密计算几何;点包含问题;线段相交问题
**中图分类号**:TP31 **文献标识码**:A **文章编号**:1673-629X(2017)05-0120-03
doi:10.3969/j.issn.1673-629X.2017.05.025

# Secure Multi-party Computation for Point Inclusion Problems

YANG Xiao-yi, LIU Xin, KANG Jia
(School of Computer Science, Shaanxi Normal University, Xi'an 710119, China)

**Abstract**: Secure multi-party computation is one of the hot spots in international cryptography research community in recent years, and more and more attention has been paid to the secure computational geometry. As an important problem of secure computational geometry, more interests have been paid on point-inclusion problem. A secure protocol for determining whether two segments are intersecting with several basic protocols, Scalar Product Protocol and Yao's Millionaire's Protocol, has been developed. Thus based on core of the protocol designed and related geometric knowledge, a secure protocol to solve the point-inclusion problem has been developed. Theoretical analysis results show that these two protocols are correct and secure under semi honest model. As a part of important secure multi-party computational protocols, they both imply important practical value in solving the problem of secure multi-party computational geometry and can be used to solve the problems, whether two or more graphics are intersected and whether multiple points are contained in a graphic etc..

**Key words**: secure multi-party computation; computational geometry; point-inclusion problem; segment-intersection problem

## 0 引 言

安全多方计算是近年来国际密码学界的一个研究热点。这一研究领域由 Yao[1] 在 1982 年提出,Goldreich 等[2-3] 丰富和发展了安全多方计算的理论。安全多方计算包含了密码学中很多的基本模块,具有很大的实用价值,因此受到了越来越多的关注。

安全多方计算的研究在密码学研究中占有非常重要的地位。Goldwasser 曾预言[4],安全多方计算今天所处的地位正是公开密钥密码学 10 年前所处的地位,成为密码学领域里一个极端重要的工具;丰富的理论将使它成为计算领域一个必不可少的组成部分;它在现实中的应用才刚刚开始,丰富的理论将使它成为计算科学中一个必不可少的组成部分。Goldwasser 的这一预言激励着密码学者的不断研究和探索。Goldreich 的工作[2-3,5] 奠定了安全多方计算的理论基础,即一般的安全多方计算问题理论上都是可解的。但是 Goldreich 指出,应用一般条件下导出的通用解决方案解决具体问题是不切实际的-效率问题很难解决,因此对于具体问题需要研究具体的解决方案。

Goldwasser 的预言和 Goldreich 的理论促进了具有实际应用背景的安全多方计算问题的研究,所研究的问题包括比较百万富翁问题[1,6]、保密的计算几何

**收稿日期**:2016-06-17 **修回日期**:2016-09-28 **网络出版时间**:2017-03-13
**基金项目**:中央高校基本科研业务费专项(GK20150417);内蒙古自治区包头市科技计划项目(2014S2004-2-1-15)
**作者简介**:杨晓艺(1993-),女,硕士研究生,研究方向为计算机与网络安全。

问题[7-8]、保密的数据挖掘问题[9]、保密拍卖问题[10]等等。

几何是科学研究中一个非常重要的分支,现实中的许多问题都可以通过一定的方式转成几何问题进行恰当表达。计算几何问题的保密计算是安全多方计算中一个新的研究方向,这些问题具有广泛的应用背景[11]。Du 等研究了保密的计算几何问题中的两线段相交问题并给出了解决方案[12],Luo 等研究了两直线之间的位置关系的保密计算问题[13]。在 Du 的启发下,很多研究人员也开始对保密计算几何问题进行深入研究[13-18]。点包含问题就是计算几何问题中的一个研究热点,基于此问题的研究已有很多。

利用安全多方计算领域的两个基础协议-向量点积协议与姚式百万富翁协议,在半诚实模型下,设计了一个可以保密地判断一私有点与一私有多边形的包含关系的协议,在很大程度上解决了现实生活中的某些实际问题。

## 1　预备知识

### 1.1　安全性定义

半诚实参与者[19]:每个参与者都是完全严格按照协议的规定执行协议的每一步,并且在协议执行过程中不会恶意输入虚假数据,也不会中途退出协议。但是它们可能会通过分析和利用协议交互过程中自己所得到的信息来推断其他参与方的相关私有输入信息。

大部分安全多方计算的研究工作都是假设参与者是半诚实的,这是因为 Goldreich 曾经指出:只要能够在半诚实参与者模型下设计出保密计算 $f$ 的协议 $\pi$,就可以通过位承诺方法将 $\pi$ 转换成恶意攻击者参与的模型下保密计算 $f$ 的协议[3]。在这个转换协议中,一个恶意的参与者将被迫按照半诚实参与者的要求执行协议,否则将会被发现。简单地说,半诚实参与者在协议执行过程中将完全按照协议要求执行协议,但他们可能会保留计算的中间结果试图推导出其他参与者的输入。半诚实模型不仅仅是一个重要的研究方法,而且为许多应用环境提供了一个很好的模型。

### 1.2　向量点积协议

问题描述:Alice 有一个私有向量 $\boldsymbol{X}=(x_1,x_2,\cdots,x_n)$,Bob 有一个私有向量 $\boldsymbol{Y}=(y_1,y_2,\cdots,y_n)$,双方希望在不泄露自身私有数据的情况下可以保密地计算两个向量的点积。二者可以执行向量点积协议,协议完成后 Alice 得到数据 $u=\boldsymbol{X}\cdot\boldsymbol{Y}+v=\sum_{i=1}^{n}x_iy_i+v$,其中 $v$ 是 Bob 选取的随机数。也就是说通过执行该协议,Alice 无法推断出任何 $\boldsymbol{Y}$ 的信息,Bob 也无法推断出任何 $\boldsymbol{X}$ 的信息。



### 1.3　姚式百万富翁协议

问题描述:Alice 有一个私有数据 $a$,Bob 有一个私有数据 $b$,双方希望在不泄露自身数据的情况下可以保密地比较两个数据的大小,即得到 $a>b$,$a<b$,$a=b$ 其中一个结果。二者可以执行百万富翁协议,协议完成后双方得到上述一个结果,但双方并不会得到任何与对方数据相关的信息。

### 1.4　向量叉积

$\boldsymbol{v}_1,\boldsymbol{v}_2$ 为两个向量,其中 $\boldsymbol{v}_1=\overrightarrow{op_1},\boldsymbol{v}_2=\overrightarrow{op_2},p_1=(x_1,y_1),p_2=(x_2,y_2),o=(0,0)$。

两个向量的叉积由下面的行列式确定:

$$\boldsymbol{v}_1\times\boldsymbol{v}_2=\begin{vmatrix}x_1 & x_2\\ y_1 & y_2\end{vmatrix}=x_1y_2-x_2y_1$$

两个向量的叉积具有以下性质:

若叉积为正,那么 $\boldsymbol{v}_1$ 在 $\boldsymbol{v}_2$ 的顺时针方向;若叉积为负,那么 $\boldsymbol{v}_1$ 在 $\boldsymbol{v}_2$ 的逆时针方向;若叉积为零,那么 $\boldsymbol{v}_1$ 与 $\boldsymbol{v}_2$ 共线。

定理 1:若两线段的端点分别在对方线段的两侧,则两线段必相交。

## 2　问题描述及协议实现

基于预备知识中介绍的密码学中的基本协议,对如何保密地判断两线段相交问题及点包含问题进行了描述,并对所提出协议的正确性和安全性进行了分析和讨论。

### 2.1　线段相交问题的描述

Alice 有一个私有的线段 $P$,端点坐标为 $p_1=(x_1,y_1),p_2=(x_1',y_1')$。Bob 有一个私有的线段 $Q$,端点坐标为 $q_1=(x_2,y_2),q_2=(x_2',y_2')$。Alice 与 Bob 想判断两线段是否相交但又不想泄露自己线段的信息。

协议 1:线段相交问题的保密协议。

输入:Alice 的私有数据 $P$:$p_1=(x_1,y_1),p_2=(x_1',y_1')$,Bob 的私有数据 $Q$:$q_1=(x_2,y_2),q_2=(x_2',y_2')$。

输出:$P$ 与 $Q$ 是否相交。

(1) Alice 构造向量 $\boldsymbol{P}_1=(x_1,-y_1,1,-1),\boldsymbol{P}_2=(x_1',-y_1',1,-1),\boldsymbol{P}_3=(y_1'-y_1,x_1'-x_1,x_1y_1,x_1y_1')$。

(2) Bob 构造向量 $\boldsymbol{Q}_1=(y_2'-y_2,x_2'-x_2,x_2'y_2,x_2y_2')$,$\boldsymbol{Q}_2=(x_2,-y_2,1,-1)$,$\boldsymbol{Q}_3=(x_2',-y_2',1,-1)$。

(3) Alice 与 Bob 共同执行向量点积协议。

$u_1=\boldsymbol{P}_1\cdot\boldsymbol{Q}_1+v_1$

$u_2=\boldsymbol{P}_2\cdot\boldsymbol{Q}_1+v_2$

$u_3=\boldsymbol{P}_3\cdot\boldsymbol{Q}_2+v_3$

$u_4=\boldsymbol{P}_3\cdot\boldsymbol{Q}_2+v_4$

其中 Alice 得到 $u_1,u_3,v_2,v_4$,Bob 得到 $u_2,u_4$,

$v_1, v_3$。

(4)Alice 与 Bob 共同执行 4 次姚式百万富翁协议得到对应的 $u_i, v_i$ 的大小。

(5)若下式中存在一个成立,则输出 $P$ 与 $Q$ 是否相交,否则输出不相交。

$$u_1 > v_1 \wedge u_2 < v_2 \wedge u_3 > v_3 \wedge u_4 < v_4$$
$$u_1 < v_1 \wedge u_2 > v_2 \wedge u_3 < v_3 \wedge u_4 > v_4$$
$$u_1 > v_1 \wedge u_2 < v_2 \wedge u_3 < v_3 \wedge u_4 > v_4$$
$$u_1 < v_1 \wedge u_2 > v_2 \wedge u_3 > v_3 \wedge u_4 < v_4$$

协议 1 的正确性:Alice 与 Bob 构造的向量做点积运算得到:

$$x_1(y_2' - y_2) - y_1(x_2' - x_2) + x_2'y_2 - x_2y_2' =$$
$$(x_1y_2' - x_2'y_1) + (x_2y_1 - x_1y_2) + (x_2'y_2 - x_2y_2') =$$
$$\begin{vmatrix} x_1 - x_2 & x_2' - x_2 \\ y_1 - y_2 & y_2' - y_2 \end{vmatrix} = \overrightarrow{q_1p_1} \times \overrightarrow{q_1q_2}$$

这正是一个叉积,因此可以根据叉积的正负也就是 $u_i$ 和 $v_i$ 的大小来判断这两向量的顺逆时针。因此,若协议 1 步骤(5)中任一成立,则说明 Alice 的私有线段端点在 Bob 线段的两侧且 Bob 的私有线段端点在 Alice 线段的两侧,由定理 1 可知两线段相交。

协议 1 的安全性:在协议 1 步骤(3)中,点积协议的结果分别是两个人交叉得到,因此两人无法根据一个结果推出对方线段的端点坐标信息。根据向量点积协议的安全性与姚式百万富翁协议的安全性以及步骤(3)中的交叉处理可知,协议 1 在半诚实模型下是安全的。

### 2.2 点包含问题的描述

Alice 有一个私有的多边形 $Q$,$Q = (x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n)$,其中每一对 $(x_i, y_i)$ 表示多边形各端点的坐标值。Bob 有一个私有的点 $P$,$P = (x_p, y_p)$。Alice 与 Bob 想判断点 $P$ 是否在多边形 $Q$ 中,又不想泄露自己的私有信息,这一问题即为保密的判断点包含的问题。

协议 2:保密判断点包含的协议。

输入:Alice 输入多边形 $Q = (x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n)$,Bob 输入点 $P = (x_p, y_p)$。

输出:$P$ 在 $Q$ 中或 $P$ 不在 $Q$ 中。

(1)Bob 选择一个随机大整数 $r$,构造一点 $P' = (r, y_p)$,令 $PP'$ 近似看作一条射线;

(2)Alice 与 Bob 共同执行协议 1 求得 $PP'$ 与多边形的各边是否有交点(其中多边形汇总的水平边不参与计算);

(3)若交点数为奇数,则输出 $P$ 在 $Q$ 中,否则输出 $P$ 不在 $Q$ 中。

协议**万方数据**性:由图 1 可得协议 2 的正确性。

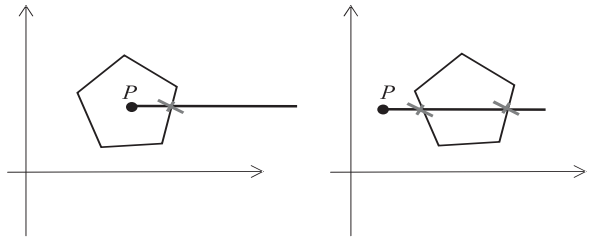


图 1 协议 2 的正确性说明

协议 2 的安全性:由协议 1 的安全性可知协议 2 在半诚实模型下是安全的。

## 3 结束语

保密计算几何中的问题在现实生活的实际意义越来越重要,应用价值越来越高。通过利用向量点积协议、姚式百万富翁协议以及其他一些相关几何知识,提出了在半诚实模型下判断两线段是否相交问题和点包含问题的保密解决方案,同时分析和讨论了这些协议的正确性和安全性。这两个协议可以作为研究其他某些保密计算几何问题的基础协议,对于解决安全多方计算领域的其他相关问题也有重要的理论意义。在后面的工作中,将对协议的性能进行深入分析,进而提出更加安全、高效的解决方案,也会进一步研究多个点是否包含在一个图形中的问题以及两个或多个图形是否相交的问题等。

**参考文献:**

[1] Yao A. Protocols for secure computations[C]//23rd annual symposium on foundations of computer science. [s. l.]: IEEE,1982:160-164.

[2] Goldreich O, Micali S, Wigderson A. How to play any mental game[C]//Proceedings of the nineteenth annual ACM symposium on theory of computing. [s. l.]: ACM, 1987: 218-229.

[3] Goldreich O. Foundations of cryptography: volume 2, basic applications[M]. [s. l.]: Cambridge University Press, 2004.

[4] Goldwasser S. Multi party computations: past and present [C]//Proceedings of the sixteenth annual ACM symposium on principles of distributed computing. [s. l.]: ACM, 1997: 1-6.

[5] Goldreich O. Secure multi-party computation(working draft) [EB/OL]. 2002. http://www. wisdom. weizmann. ac. il home oded public-html foc. html.

[6] 李顺东,戴一奇,游启友. 姚氏百万富翁问题的高效解决方案[J]. 电子学报,2005,33(5):769-773.

[7] Shen C, Zhang H G, Feng D G, et al. Survey of information security[J]. Science in China Series F: Information Sciences, 2007,50(3):273-298.

[8] Cao Z, Zhu H, Lu R. Provably secure robust threshold partial

(下转第 127 页)

[7] 李古月,胡爱群,石　乐. 无线信道的密钥生成方法[J]. 密码学报,2014,1(3):211-224.

[8] 隋　雷,郭渊博,姜文博,等. 基于无线信道特征的密钥生成与提取研究[J]. 计算机科学,2015,42(2):137-141.

[9] Kim H S. Measurement and model based characterization of indoor wireless channels[D]. Lowell: University of Massachusetts,1989.

[10] Wang Q, Su H, Ren K, et al. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks[C]//Proceedings of In INFOCOM. [s. l.]: IEEE, 2011:1422-1430.

[11] Wang Q, Su H, Ren K. Cooperative secret generation from phase estimation in narrowband fading channels[J]. IEEE Journal on Selected Areas in Communications,2012,30(9): 1666-1674.

[12] 周百鹏,黄开枝,金　梁,等. 一种基于多径相对时延的密钥生成方法[J]. 计算机应用研究,2011,28(6):2196-2198.

[13] 魏　浩,郑宝玉,侯晓赟,等. 基于放大转发的双向中继信道密钥生成[J]. 电子与信息学报,2013,35(6):1344-1350.

[14] Aono T, Higuchi K, Ohira T, et al. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels[J]. IEEE Transactions on Antennas and Propagation,2005,53(11):3776-3784.

[15] Jana S, Premnath S N, Clark M, et al. On the effectiveness of secret key extraction from wireless signal strength in real environments[C]//Proceedings of the 15th annual international conference on mobile computing and networking. [s. l.]: ACM,2009:321-332.

[16] Ohira T. Secret key generation exploiting antenna beam steering and wave propagation reciprocity[C]//Proceedings of EUMC. London, UK: [s. n.],2005:23-27.

[17] Maurer U, Wolf S. Secret-key agreement over unauthenticated public channels. i: definitions and a completeness result [J]. IEEE Transactions on Information Theory, 2003, 49(4):832-838.

[18] Brassard G, Salvail L. Secret-key reconciliation by public discussion[C]//EU-ROCRYPT 93. Berlin: Springer, 1994: 410-423.

[19] Bennett C H, Brassard G, Robert J M. Secret-key reconciliation by public discussion[M]. Berlin: Springer-Vering, 1986.

[20] Buttler W T, Lamoreaux S K, Torgerson J R, et al. Fast efficient error reconciliation for quantum cryptography[J]. Physical Review A,2003,67:052303.

[21] Madisek M G, McGuire M L, Nevilile S S, et al. Secret key generation and agreement in UWB communication channels [C]//IEEE global telecommunications conference. [s. l.]: IEEE,2008:1-5.

[22] Liu H, Wang Y, Yang J, et al. Collaborative secret key extraction leveraging received signal strength in mobile wireless networks[C]//IEEE international conference on computer computer communication. [s. l.]: IEEE,2012:927-935.

[23] Wilson R, Tse D, Scholtz R A. Channel identification: secret sharing using reciprocity in ultrawideband channels[J]. IEEE Transaction on Information Forensics and Security, 2007, 2(3):364-375.

[24] Armando A, Basin D, Boichut Y, et al. The AVISPA tool for the automated validation of internet security protocols and applications[C]//Proceedings of computer aided verification. [s. l.]: [s. n.],2005:281-285.

[25] 周百鹏. 基于无线信道特征提取的密钥生成技术研究[D]. 郑州:解放军信息工程大学,2011.

[26] Bennett C H, Brassard G, Crépeau C, et al. Generalized privacy amplification[J]. IEEE Transactions on Information Theory,1995,41(6):1915-1923.

[27] Maurer U, Wolf S. Secret-key agreement over unauthenticated public channels. III: privacy amplification[J]. IEEE Transactions on Information Theory,2003,49(4):839-851.

(上接第 122 页)

blind signature[J]. Science in China Series F: Information Sciences,2006,49(5):604-615.

[9] Lindell Y, Pinkas B. Privacy preserving data mining[J]. Journal of Cryptology,2002,15(3):177-206.

[10] Cachin C. Efficient private bidding and auctions with an oblivious third party[C]//Proceedings of the 6th ACM conference on computer and communications security. [s. l.]: ACM,1999:120-127.

[11] 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.

[12] Du W, Atallah M J. Secure multi-party computation problems and their applications: a review and open problems [C]//Proceedings of new security paradigms workshop. New York: ACM Press,2001:13-22.

[13] 罗永龙,黄刘生,荆巍巍,等. 空间几何对象相对位置判定中的私有信息保护[J]. 计算机研究与发展,2006,43(3):410-416.

[14] 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.

[15] 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.

[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:自然科学版,2007,47(10):1692-1695.

[17] 杨晓莉,李顺东,左祥建. 计算几何问题的多方保密计算[J]. 密码学报,2016,3(1):33-41.

[18] 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.

[19] 李顺东,王道顺,戴一奇,等. 两个集合相等的多方保密计算[J]. 中国科学:信息科学,2009,39(3):305-310.