安全多方计算在空间几何问题中的应用①

王 斑[1], 罗文俊[2]

[1](山西职业技术学院 计算机工程系, 太原 030006)
[2](重庆邮电大学 计算机科学与技术学院, 重庆 400065)

摘 要: 研究安全多方计算在空间几何问题中的应用, 提出了空间中基于阈值的两点之间、点线之间距离关系的保密判定协议, 空间中点与两平行平面位置关系的保密判定协议; 并利用这些协议作为子协议为空间中基于阈值的点与线段之间距离关系的保密判定问题构造了相应的保密解决方案. 所提出的协议和解决方案在工程、商业和军事等领域中具有潜在的应用价值.

关键词: 安全多方计算; 计算几何; 阈值; 百万富翁协议; 点积协议

Applications of Secure Multi-Party Computation in Space Geometry Problems

WANG Ting[1], LUO Wen-Jun[2]

[1](Department of Computer Engineering, Shanxi Vocational Poly-Tech College, Taiyuan 030006, China)
[2](College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: The paper researches some applications of secure multi-party computation in space geometry problems. First, private-preserving determination protocol of distance relation of two-point in space based on threshold and private-preserving determination protocol of distance relation of point-line in space based on threshold are presented. Second, a private-preserving determination protocol of position relation of point and two parallel planes in space is presented. Finally, a private-preserving solution for private-preserving determination problem of distance relation of point and line segment in space based on threshold is constructed using the first two protocols. These protocols and solutions have potential application values in engineering, commerce and military field.

Key words: secure multi-party computation; computational geometry; threshold; millionaires' protocol; dot product protocol

现代密码学中的安全多方计算问题由 Yao 教授首次提出并做了初步的分析与研究[1], 随后, 该问题又被 Goldreich 等学者进行了一定的扩展性研究[2]. 根据安全多方计算的理论研究, 任何安全多方计算问题都能够通过使用电路求值协议在理论上被解决[3], 但是使用一般的解决方案去解决某些特殊情形下的安全多方计算问题一般是不切实际的. 例如, 先后被相关密码学者提出并研究的保密统计分析, 保密信息检索, 保密数据挖掘, 安全多方科学计算, 保密计算几何等特殊安全多方计算问题. 所以由此推动并出于效率等因素的考虑, 密码学研究人员正在不断对各种特殊的安全多方计算问题进行研究并为之设计特定的解决方案[4-10].

其中, 保密计算几何作为一类特殊的安全多方计算问题, 主要研究的是在一个分布式环境中两个或多个参与方分别利用各自的秘密几何信息作为输入数据进行协作计算, 从而获得各自所需的正确计算结果, 并且在计算结束后每个参与方没有把自己的秘密信息泄露给其他的参与方. 文献[11-15]对保密计算几何领域中涉及的部分问题进行了初步的研究.

本文在文献[15]的基础上, 通过运用基本的密码学知识在部分基础安全多方计算协议之上通过分析空间中基于阈值的两点之间、点线之间距离关系, 空间中点与两平行平面之间位置关系的判定问题, 分别提出了相应的保密判定协议, 并将这几个协议应用于空

① 基金项目:国家自然科学基金(60963023);重庆市自然科学基金(2010BB2402)
收稿时间:2014-04-29;收到修改稿时间:2014-06-03

间中基于阈值的点与线段之间距离关系的保密判定协议中. 另外, 本文假设所有的参与方都是半诚实的, 半诚实的参与方会严格按照协议规定执行每一步, 同时在协议执行过程中不会主动退出协议或恶意输入虚假信息, 但是可能会通过分析和利用协议执行过程中自己得到的中间信息来推导其他参与方的相关私有输入信息.

1 预备知识

这一节介绍本文涉及到的安全多方计算中的两个重要协议和基本空间几何知识.

1.1 两个基本协议

百万富翁协议(millionaires' protocol). 协议的目的是比较两个秘密数, 例如判断哪一个数更大. 该协议最早作为百万富翁问题由 Yao[1]提出,可以被描述为: 两个百万富翁 Alice 与 Bob 想知道他们两个谁更富有, 但他们都不想让对方知道自己财富的任何信息, 这就是百万富翁问题. 同时 Yao 在文献中给出了一个最初的解决方案, 但计算和通信复杂度都比较高. 后来, 也有学者对该协议做了进一步的研究[16,17]. 百万富翁问题的解决方案是构造许多安全多方计算问题解决方案的一个基本模块, 同样也是本文将要提出的部分解决方案的一个基本模块或子协议.

保密点积协议(privacy-preserving dot product protocol). 该问题最初被 Du 和 Atallah 提出[11], 协议可描述为: 假设有两个参与者, Alice 拥有秘密输入向量 $X=(x_1,\cdots,x_n)$, Bob 拥有秘密输入向量 $Y=(y_1,\cdots,y_n)$, 他们希望进行合作计算并在协议结束后, Alice 得到值 $r_A=X\cdot Y-r_B$ (这里 r_B 是 Bob 选取的一个随机值). 同时要满足 Alice 不能从 r_A 中得到有关 $X\cdot Y$ 的值, 也不能从自己获取的信息中推出任何有关 y_i 的信息; Bob 不能得到 r_A 的值, 也不能推出有关 x_i 的信息. 保密点积协议已经成为安全多方计算领域的一个重要密码学协议, 文献[6,11,18]分别提出了几个具有不同安全性的解决方案.

1.2 基本空间几何知识

假设 $P_0(x_0,y_0,z_0)$, $P_1(x_1,y_1,z_1)$ 表示空间中的两个点, $\pi(A,B,C,D):Ax+By+Cz+D=0$ 表示空间中的一个平面; 用 $S(S_1(x_1,y_1,z_1),S_2(x_2,y_2,z_2))$ 表示空间中的一条线段, 其中 $S_1(x_1,y_1,z_1)$, $S_2(x_2,y_2,z_2)$ 是线段的两个端点. 那么根据空间解析几何相关知识可以有以下结论:

(1) $P_0(x_0,y_0,z_0)$ 和 $P_1(x_1,y_1,z_1)$ 之间的距离 $d=\sqrt{(x_1-x_0)^2+(y_1-y_0)^2+(z_1-z_0)^2}$.

(2) 点 $P_0(x_0,y_0,z_0)$ 与平面 $\pi(A,B,C,D):Ax+By+Cz+D=0$ 之间的距离可表示为 $d=\dfrac{|Ax_0+By_0+Cz_0+D|}{\sqrt{A^2+B^2+C^2}}$.

(3)点 $P_0(x_0,y_0,z_0)$ 到经过线段 S_1S_2 的直线的距离 $d=\dfrac{|\overrightarrow{S_1S_2}\times\overrightarrow{S_1P_0}|}{|\overrightarrow{S_1S_2}|}$(其中×表示两向量的叉积).

2 问题描述及协议实现

2.1 空间中基于阈值的两点之间距离关系的保密判定协议

问题描述: 假设有两个参与方, Alice 拥有空间中一个秘密点 $P_0(x_0,y_0,z_0)$, Bob 拥有空间中一个秘密点 $P_1(x_1,y_1,z_1)$; 另外有一个双方约定的阈值 T. 他们希望在没有把自己的私有信息泄露给对方的前提下协作判定点 P_0 与 P_1 之间的距离是否大于给定的阈值 T.

协议实现:

输入: Alice 拥有空间中一个秘密点 $P_0(x_0,y_0,z_0)$, Bob 拥有空间中一个秘密点 $P_1(x_1,y_1,z_1)$; 一个双方约定的阈值 T.

输出: Alice 与 Bob 协作判定 P_0, P_1 两点之间的距离 d 是否大于给定的阈值 T.

步骤:

①Alice 计算 $\vec{a}=<x_0^2,-2x_0,1,y_0^2,-2y_0,1,z_0^2,-2z_0,1>$, Bob 计算 $\vec{b}=<1,x_1,x_1^2,1,y_1,y_1^2,1,z_1,z_1^2>$.

②Alice 与 Bob 执行一次保密点积协议计算 $\vec{a}$ 与 $\vec{b}$ 的点积 $d^2=<\vec{a},\vec{b}>$, Alice 得到 $s_A=d^2-s'_B$, Bob 得到 s'_B(其中 s'_B 是是执行保密点积协议过程中 Bob 选取的一个新鲜的随机值).

③ Bob 利用公开的阈值 T 计算 $s_B=T^2-s'_B$.

④Alice 与 Bob 对 s_A 与 s_B 使用一次百万富翁协议, 若 $s_A>s_B$, 则可判定空间中点 P_0 与 P_1 之间的距离大于给定的阈值 T, 否则判定空间中点 P_0 与 P_1 之间的距离不超过给定的阈值 T.

2.2 空间中基于阈值的点线之间距离关系的保密判定协议

问题描述: 假设有两个参与方, Alice 拥有空间中一个秘密点 $P_0(x_0,y_0,z_0)$, Bob 拥有一条过空间两点 $S_1(x_1,y_1,z_1)$ 和 $S_2(x_2,y_2,z_2)$ 的秘密直线

$L:\frac{x-x_1}{x_2-x_1}=\frac{y-y_1}{y_2-y_1}=\frac{z-z_1}{z_2-z_1}$; 另外有一个双方约定的阈值$T$. 他们希望在没有把自己的私有信息泄露给对方的前提下协作判定点P_0到直线L之间的距离是否大于给定的阈值T.

协议实现:

输入: Alice 拥有空间中一个秘密点$P_0(x_0,y_0,z_0)$, Bob 拥有一条过空间两点$S_1(x_1,y_1,z_1)$和$S_2(x_2,y_2,z_2)$的秘密直线$L:\frac{x-x_1}{x_2-x_1}=\frac{y-y_1}{y_2-y_1}=\frac{z-z_1}{z_2-z_1}$; 一个双方约定的阈值$T$.

输出: Alice 与 Bob 协作判定点P_0到直线L之间的距离d是否大于给定的阈值T.

说明: 因为向量$\overrightarrow{S_1S_2}=<x_2-x_1,y_2-y_1,z_2-z_1>$, $\overrightarrow{S_1P_0}=<x_0-x_1,y_0-y_1,z_0-z_1>$, 有$\left|\overrightarrow{S_1S_2}\right|=\sqrt{(x_2-x_1)^2+(y_2-y_1)^2+(z_2-z_1)^2}$; 若令$A=(y_2-y_1)(z_0-z_1)-(z_2-z_1)(y_0-y_1)$, $B=(x_2-x_1)(z_0-z_1)-(z_2-z_1)(x_0-x_1)$, $C=(x_2-x_1)(y_0-y_1)-(y_2-y_1)(x_0-x_1)$; 则向量$\overrightarrow{S_1S_2}$与$\overrightarrow{S_1P_0}$叉积的模可表示为$\left|\overrightarrow{S_1S_2}\times\overrightarrow{S_1P_0}\right|=\sqrt{A^2+B^2+C^2}$. 又因为线段$S_1S_2$位于直线$L$上, 那么点$P_0$到直线$L$之间的距离可表示为$d=\frac{\left|\overrightarrow{S_1S_2}\times\overrightarrow{S_1P_0}\right|}{\left|\overrightarrow{S_1S_2}\right|}$. 对于$\left|\overrightarrow{S_1S_2}\times\overrightarrow{S_1P_0}\right|$, 双方可以通过以下方法求得: Alice 利用自己的秘密点P_0构造一个秘密向量$\vec{a}$, Bob 利用自己的秘密点S_1和S_2构造一个秘密向量$\vec{b}$(构造方法类似于 2.1 节中协议的步骤 1), 并使得所构造的向量能够满足等式: $<\vec{a},\vec{b}>=\left|\overrightarrow{S_1S_2}\times\overrightarrow{S_1P_0}\right|^2$.

步骤:

①Alice 与 Bob 按照等式$<\vec{a}_1,\vec{b}_1>=\left|\overrightarrow{S_1S_2}\times\overrightarrow{S_1P_0}\right|^2$分别构造秘密向量$\vec{a}_1$和$\vec{b}_1$; 同时 Alice 构造向量$\vec{a}_2=<T^2,T^2,T^2>$, Bob 构造向量$\vec{b}_2=<(x_2-x_1)^2,(y_2-y_1)^2,(z_2-z_1)^2>$.

②Alice 与 Bob 执行一次保密点积协议计算$\vec{a}_1$与$\vec{b}_1$的点积$d_L=<\vec{a}_1,\vec{b}_1>=\left|\overrightarrow{S_1S_2}\times\overrightarrow{S_1P_0}\right|^2$, Alice 得到$s_{AL}=d_L-s_{BL}$, Bob 得到$s_{BL}$(其中$s_{BL}$是执行保密点积协议过程中 Bob 选取的一个新鲜的随机值). 双方再执行一次保密点积协议计算$\vec{a}_2$与$\vec{b}_2$的点积$d_R=<\vec{a}_2,\vec{b}_2>=T^2\left[(x_2-x_1)^2+(y_2-y_1)^2+(z_2-z_1)^2\right]$, Alice 得到$s_{AR}=d_R-s_{BR}$, Bob 得到$s_{BR}$($s_{BR}$同样是执行保密点积协议过程中 Bob 选取的一个新鲜的随机值).

③Alice 计算$s_A=s_{AL}-s_{AR}$, Bob 计算$s_B=s_{BR}-s_{BL}$.

④Alice 与 Bob 对s_A与s_B使用一次百万富翁协议, 若$s_A>s_B$, 则可判定空间中点P_0到直线L之间的距离大于给定的阈值T, 否则判定空间中点P_0到直线L之间的距离不超过给定的阈值T.

2.3 空间中点与两平行平面位置关系的保密判定协议

问题描述: 假设有两个参与方, Alice 拥有空间中一个秘密点$P_0(x_0,y_0,z_0)$, Bob 拥有空间中两个相互平行的秘密平面$\pi_1(A_1,B_1,C_1,D_1):A_1x+B_1y+C_1z+D_1=0$, $\pi_2(A_2,B_2,C_2,D_2):A_2x+B_2y+C_2z+D_2=0$, $D_1\neq D_2$. 他们希望在没有把自己的私有信息泄露给对方的前提下协作判定点P_0是否落在两平行平面π_1与π_2所夹区域之间.

协议实现:

输入: Alice 拥有空间中一个秘密点$P_0(x_0,y_0,z_0)$, Bob 拥有空间中两个相互平行的秘密平面$\pi_1(A_1,B_1,C_1,D_1):A_1x+B_1y+C_1z+D_1=0$与$\pi_2(A_2,B_2,C_2,D_2):A_2x+B_2y+C_2z+D_2=0$.

输出: Alice 与 Bob 协作判定点P_0是否落在两平行平面π_1与π_2所夹区域之间.

步骤:

①Alice 构造向量$\vec{a}=<x_0,y_0,z_0>$, Bob 构造向量$\vec{b}_1=<A_1r,B_1r,C_1r>$, $\vec{b}_2=<A_2r,B_2r,C_2r>$(其中$r$是 Bob 选取的一个新鲜的正随机值); Bob 分别计算两平面的法式化因子$\lambda_1=\pm\frac{1}{\sqrt{A_1^2+B_1^2+C_1^2}}$, $\lambda_2=\pm\frac{1}{\sqrt{A_2^2+B_2^2+C_2^2}}$(正负号根据实际的平面方程进行确定); 然后计算值$k_1=\frac{1}{r\sqrt{A_1^2+B_1^2+C_1^2}}$, $k_2=\frac{1}{r\sqrt{A_2^2+B_2^2+C_2^2}}$, 并将$k_1$, k_2顺序发送给 Alice.

② Alice 与 Bob 执行一次保密点积协议计算$\vec{a}$与$\vec{b}_1$的点积$d=<\vec{a},\vec{b}_1>=A_1rx_0+B_1ry_0+C_1rz_0$, Alice 得到$s_{A1}=d+D_1r$, Bob 得到$-D_1r$(其中$r$是步骤 1 中 Bob 选取的那个新鲜的随机值). 双方再执行一次保密点积协议计算$\vec{a}$与$\vec{b}_2$的点积$d=<\vec{a},\vec{b}_2>=A_2rx_0+B_2ry_0+C_2rz_0$, Alice 得到$s_{A2}=d+D_2r$, Bob 得到$-D_2r$(其中$r$同样是步骤 1 中 Bob 选取的那个新鲜的随机值).

③ Alice 计算$s_A=\frac{|s_{A1}|}{k_1}+\frac{|s_{A2}|}{k_2}$.

④ Bob 计算$s_B=\left|\lambda_1D_1-\lambda_2D_2\right|$.

⑤ Alice 与 Bob 对s_A与s_B执行一次百万富翁协议,

若 $s_A = s_B$，则可判定空间中点 P_0 落在两平行平面 π_1 与 π_2 所夹区域之间；否则判定空间中点 P_0 落在两平行平面 π_1 与 π_2 所夹区域的外部.

2.4 空间中基于阈值的点与线段之间距离关系的保密判定协议

问题描述：假设有两个参与方，Alice 拥有空间中一个秘密点 $P_0(x_0,y_0,z_0)$，Bob 拥有空间中一条秘密线段 $S(S_1(x_1,y_1,z_1),S_2(x_2,y_2,z_2))$；另外有一个双方约定的阈值 T．他们希望在没有把自己的私有信息泄露给对方的前提下协作判定点 P_0 到线段 S 之间的距离是否大于给定的阈值 T．

协议实现：

输入：Alice 拥有空间中一个秘密点 $P_0(x_0,y_0,z_0)$，Bob 拥有空间中一条秘密线段 $S(S_1(x_1,y_1,z_1),S_2(x_2,y_2,z_2))$；一个双方约定的阈值 T．

输出：Alice 与 Bob 协作判定点 P_0 到线段 S 的距离 d 是否大于给定的阈值 T．

步骤：

① Alice 与 Bob 对 $P_0(x_0,y_0,z_0)$、$S_1(x_1,y_1,z_1)$ 和阈值 T 执行 2.1 节的空间中基于阈值的两点之间距离关系的保密判定协议判断 P_0 与 S_1 之间的距离是否大于 T，若不大于，则判定点 P_0 到线段 S 的距离不超过阈值 T，协议结束；否则转到步骤 2 继续执行协议.

② Alice 与 Bob 对 $P_0(x_0,y_0,z_0)$、$S_2(x_2,y_2,z_2)$ 和阈值 T 执行 2.1 节的空间中基于阈值的两点之间距离关系的保密判定协议判断 P_0 与 S_2 之间的距离是否大于 T，若不大于，则判定点 P_0 到线段 S 的距离不超过阈值 T，协议结束；否则转到步骤 3 继续执行协议.

③ Bob 计算通过线段 S 的空间直线方程，记作 $L:\frac{x-x_1}{x_2-x_1}=\frac{y-y_1}{y_2-y_1}=\frac{z-z_1}{z_2-z_1}$，然后，Alice 与 Bob 对点 $P_0(x_0,y_0,z_0)$、直线 L 以及阈值 T 执行 2.2 节的空间中基于阈值的点线之间距离关系的保密判定协议判断 P_0 到直线 L 之间的距离是否大于 T，若大于，则判定点 P_0 到线段 S 的距离大于阈值 T，协议结束；否则转到步骤 4 继续执行协议.

④Bob 利用点法式计算通过 S 两端点且垂直于 S 的两个空间平面的方程，分别记作：$\pi_1(A_1,B_1,C_1,D_1):A_1x+B_1y+C_1z+D_1=0$ 与 $\pi_2(A_2,B_2,C_2,D_2):A_2x+B_2y+C_2z+D_2=0$；然后，Alice 与 Bob 对 $P_0(x_0,y_0,z_0)$、$\pi_1(A_1,B_1,C_1,D_1)$ 和 $\pi_2(A_2,B_2,C_2,D_2)$ 执行 2.3 节的空间中点与两平行平面位置关系的保密判定协议判断空间中点 P_0 是否落在平行平面 π_1 与 π_2 之间，若 P_0 落在两平面所夹区域之间，则判定空间中点 P_0 到线段 S 的距离不超过阈值 T，否则判定空间中点 P_0 到线段 S 的距离大于阈值 T，协议结束.

3 结语

本文提出了空间中基于阈值的两点之间、点线之间距离关系的保密判定协议，空间中点与两平行平面位置关系的保密判定协议；最后利用这几个协议作为子协议为空间中基于阈值的点与线段之间距离关系的保密判定问题构造了相应的保密解决方案．基于本文所研究的保密计算几何这一特殊的安全多方计算问题在工程、商业和军事等领域中潜在的巨大应用价值．提出其它种类的保密计算几何问题并设计适合于它们的有效解决方案是下一步的研究重点.

参考文献

1 Yao AC. Protocols for secure computation. Proc. of the 23rd IEEE Symposium on Foundations of Computer Science. 1982. 160–164.

2 Goldreich O, Micali S, Wigderson A. How to play any mental game. 19th Annual ACM Symposium on Theory of Computing. 1987. 218–229.

3 Goldreich O. Secure multi-party computation (working draft). http://www.wisdom.weizmann. ac.il/~oded/pp. html, 1998.

4 Cachin C, Micali S, Stadler M. Computationally private information retrieval with polylogarithmic communication. Proc. of the Advances in Cryptology-EUROCRYPT'99. Lecture Notes in Computer Science. 1999, 1592. 402–414.

5 Chor B, Goldreich O, Kushilevitz E, et al. Private information retrieval. Journal of the ACM (JACM), 1995, 45(6): 965–981.

6 Du WL, Atallah MJ. Privacy-preserving statistical analysis. Proc. of the 17th Annual Computer Security Applications Conference. New Orleans, Louisiana, USA. December 10-14 2001. 102–110.

7 Du W, Atallah MJ. Privacy-preserving cooperative scientific computations. Proc. of the 14th IEEE workshop on Computer Security Foundations. 2001. 273–282.

8 Luo WJ, Li X. A study of secure multi-party elementary function computation protocols. Proc. of the 3rd International

Conference on Information Security. 2004. 5– 12.

9 罗文俊,李祥.多方安全矩阵乘积协议及应用.计算机学报,2005,28(7):1230–1235.

10 Lindell Y, Pinkas B. Privacy preserving data mining. Proc. of the 20th Annual International Cryptology Conference on Advances in Cryptology. Lecture Notes in Computer Science. 2000, 1880. 36–54.

11 Atallah MJ, Du W. Secure multi-party computational geometry. Proc. of the 7th International Workshop on Algorithms and Data Structures. 2001. 165–179.

12 罗永龙,黄刘生,荆巍巍,徐维江.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,2006,43(3):410–416.

13 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.北京邮电大学学报,2008,31(2):72–75.

14 Zhu YW, Huang LS, et al. Privacy-preserving approximate convex hulls protocol. Proc. of the 2009 First International Workshop on Education Technology and Computer Science. IEEE Computer Society. 2009, 2. 208–214.

15 王珽,罗文俊.基于阈值的点线距离与位置关系保密判定协议.计算机工程与应用,2010,46(13):87–89.

16 Ioannidis I, Grama A. An Efficient Protocol for Yao's Millionaires' Problem. Proc. of the 36th Hawaii International Conference on System Science. 2003. 6–9.

17 Li SD, Dai YQ, You QY. Secure multi-party computation solution to Yao's Millionaires' problem based on set-inclusion. Progress in Natural Science, 2005, 15(9): 851 – 856.

18 Vaidya J, Clifton C. Privacy preserving association rule mining in vertically partitioned data. Proc. 8th ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining. New York: ACM Press, 2002: 639–644.