

计算两相交圆精确面积的安全协议

赵书峰¹, 黄刘生²

(1 阜阳职业技术学院 信息技术系, 安徽 阜阳 236031; 2 中国科学技术大学 计算机科学与技术系, 安徽 合肥 230026)

摘 要: 本文提出了一种能够计算两相交圆精确面积的安全协议. 通过调用该协议, 参与者能够安全的计算出两个相交圆的面积, 并且保证各方的私有数据不会泄漏, 分析证明该协议具有安全性和高效性.

关键词: 安全多方计算; 计算几何; 相交圆; 点积协议; 加到乘变换协议

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2011)07-0098-04

Secure Protocol to Compute the Accurate Area of Two Intersecting Circles

ZHAO Shu-feng¹, HUANG Liu-sheng²

(1 Department of Information Technology, FYZY, Fuyang 236031, China;

2 Department of Computer Science and Technology, USTC, Hefei 230026, China)

Abstract: This paper proposes a secure protocol to compute the accurate area of two intersecting circles. By invoking the secure protocol, two participants can securely compute the accurate area of two private intersecting circles, while no privacy is disclosed. Analysis confirms that the new protocol is secure and effective.

Key words: secure multiparty computation; computational geometry; intersecting circle; scalar product protocol; privacy-preserving add to multiply protocol

1 引言

随着网络技术的快速发展, 如何在数据共享的同时实现隐私保护已经成为一个重要的研究课题. 安全多方计算技术^[1-2]是实现隐私保护的重要技术手段之一. 针对不同的应用问题, 需要设计相应的安全计算协议. 安全计算两相交圆面积属于安全计算几何^[3]是安全多方计算中的重要问题之一, 在商业以及国防军事合作等领域有重要的实用意义. 文献[4]提出了一种安全计算两相交圆面积的蒙特卡罗协议, 然而该协议采用随机算法, 无法计算精确的结果. 为此, 本文设计一个新的安全协议, 用于安全的计算两相交圆的精确面积.

2 预备知识

2.1 点积协议

点积协议是一个重要的安全多方计算基础协

议, 它的应用非常广泛^[5]. 点积协议中有两个参与者, 记为 Alice 和 Bob, 他们分别有一个私有向量 a 和 b , 通过执行点积协议, Alice 和 Bob 分别得到私有数据 u 和 v , 使得 $u + v = a \cdot b$. 基于同态加密系统^[6], 文献[5]实现了一种安全高效的计算两方点积的协议方案, 其通信复杂度和计算复杂度都是 $O(n)$, 其中 n 为私有向量 a 和 b 的长度. 文中的安全协议将调用该点积协议, 实现部分安全过程.

2.2 加到乘变换协议

文献[7]提出了加到乘变换协议, 没有设计出相应的安全实现方法. Y. Zhu^[8]等设计了三种实现安全加到乘变换的方案, 并在文献[9]中证明了等价关系. 因此, 加到乘变化协议的通信复杂度和计算复杂度同一维点积协议相同, 均为 $O(1)$. 在加到乘变换协议中, Alice 和 Bob 分别持有一个私有数据 x 和 y , 通过合作执行该协议, 他们可以分别安全地得

到私有数据 u 和 v , 使得 $u \cdot v = x + y$. 加到乘变换协议也是安全协议所调用的一个重要子过程.

3 问题定义与安全模型

3.1 问题定义

文中的安全协议的两方为 Alice 和 Bob. 其中 Alice 拥有私有的圆 O_1 , 圆心 O_1 的坐标为 (x_1, y_1) ; Bob 拥有私有的圆 O_2 , 圆心 O_2 的坐标为 (x_2, y_2) , 两圆相交. 他们希望合作计算出两圆的相交面积大小, 同时保证不泄漏任何私有数据. 具体而言, Alice 得到私有的数据 s_a , Bob 得到私密的数据 s_b , 使得 $s_a + s_b$ 等于相交部分面积(如图 1 中的阴影部分所示). 计算完成之后, Alice 的圆心和半径不会泄漏给 Bob 或者他人, Bob 私有数据也同样不会泄漏.

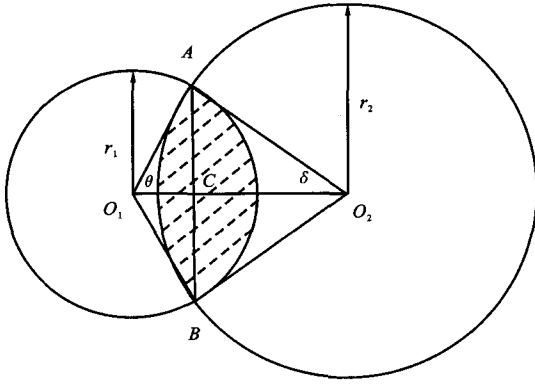


图 1 两圆相交问题

3.2 安全模型

现有的安全多方计算协议, 大多是在半可信模型下的. 文中也同样采用这一安全假设, 即, 协议参与者会按照协议的步骤执行协议, 不会输入虚假数据, 只是会记录中间数据, 试图通过其收集到的中间数据分析出别人的私有数据. O. Goldreich^[2]给出了半可信模型下的安全性定义, 简而言之, 一个多方计算协议是安全的当且仅当每个参与者收到的中间数据都可以通过该参与者的私有输入和秘密输出以及随机数模拟得到. 利用零知识证明协议可以将任意的半可信模型下的安全协议转换到恶意模型下.

文中设计的协议是在半可信模型下进行的.

4 计算两相交圆精确面积的安全协议

如图 1 所示, 这里记 $d = |O_1O_2|$, 则 $d^2 = (x_1 - x_2)^2 + (y_1 - y_2)^2$. 通过调用点积协议^[8], 文中首先实现了安全计算 d^2 的过程, 详细内容如协议 1 所示.

协议 1 计算两圆心的距离平方(d^2)

输入: Alice 拥有私有的圆 O_1 , 圆心 O_1 的坐标为 (x_1, y_1) ; Bob 拥有私有的圆 O_2 , 圆心 O_2 的坐标为 (x_2, y_2) , 记 $d^2 = (x_1 - x_2)^2 + (y_1 - y_2)^2$.

输出: Alice 得到私有的数据 u , Bob 得到私密的数据 v , 使得 $u + v = d^2$.

步骤 1. Alice 令其私有向量 $a = (x_1, y_1)$, Bob 令其私有向量 $b = (x_2, y_2)$.

步骤 2. Alice 和 Bob 合作利用点积协议, 分别得到 u_1 和 v_1 , 使得 $u_1 + v_1 = a \cdot b = x_1x_2 + y_1y_2$.

步骤 3. Alice 计算 $u = x_1^2 + y_1^2 - 2u_1$, Bob 计算 $v = x_2^2 + y_2^2 - 2v_1$ // 协议结束.

通过调用协议 1, 文中设计了计算相交圆精确面积的安全协议, 其详细过程如协议 2 所示.

协议 2 计算相交圆精确面积的安全协议

输入: Alice 拥有私有的圆 O_1 , 圆心 O_1 的坐标为 (x_1, y_1) ; Bob 拥有私有的圆 O_2 , 圆心 O_2 的坐标为 (x_2, y_2) , 记 $d^2 = (x_1 - x_2)^2 + (y_1 - y_2)^2$.

输出: Alice 得到私有的数据 s_a , Bob 得到私密的数据 s_b , 使得 $s_a + s_b$ 等于相交部分面积(见图 1 中的阴影部分).

步骤 1. Alice 和 Bob 合作利用协议 1, 分别得到正数 u 和 v , 使得 $u + v = d^2$.

步骤 2. Alice 和 Bob 各自计算出 $u_1 = u + r_1^2$ 和 $v_1 = v - r_2^2$, 然后他们合作执行加到乘变换协议分别得到私有数据 u_2 和 v_2 , 使得 $u_2 \cdot v_2 = u_1 + v_1$.

步骤 3. Alice 和 Bob 各自计算出 $u_3 = u - r_1^2$ 和 $v_3 = v + r_2^2$, 然后他们合作执行加到乘变换协议分别得到私有数据 u_4 和 v_4 , 使得 $u_4 \cdot v_4 = u_3 + v_3$.

步骤 4. Alice 和 Bob 合作利用加到乘变换协议, 分别得到正数 u_5 和 v_5 , 使得 $u_5 \cdot v_5 = u + v$.

步骤 5. Alice 独自计算出 $u_6 = \frac{u_2}{r_1 \sqrt{u_5}}$ 和 $u_7 = \frac{u_4}{2 \sqrt{u_5}}$, Bob 单独计算出 $v_6 = \frac{v_2}{2 \sqrt{v_5}}$ 和 $v_7 = \frac{v_4}{r_2 \sqrt{v_5}}$.

然后, Alice 令其私有向量 $a_1 = (r_1^2 u_6, \frac{u_3^3 r_1^2}{2})$ 和 $a_2 = (u_7, \frac{u_7^3}{2})$, Bob 计算其私有向量 $b_1 = (v_6, \frac{v_6^3}{3})$ 和 $b_2 = (r_2^2 v_7, \frac{v_7^3 r_2^2}{3})$.

步骤 6. Alice 和 Bob 合作执行点积协议, 使 Alice 得到私有数据 u_8 和 u_9 , Bob 得到私有数据 v_8 和 v_9 , 满足 $u_8 + v_8 = a_1 \cdot b_1$, $u_9 + v_9 = a_2 \cdot b_2$ // 两个弧的面积.

步骤 7. Alice 计算向量 $a_3 = (r_1^2, -r_1^2 u_6^2 u, r_1^2 u_6^2)$, Bob 计算私有向量 $b_3 = (v, v_6^2, -v_6^2 v)$, 然后他们合作执行点积协议, 使 Alice 得到私有数据 u_{10} , Bob 得到私有数据 v_{10} , 满足 $u_{10} + v_{10} = a_3 \cdot b_3$.

步骤 8. Alice 和 Bob 合作利用加到乘变换协议, 分别得到正数 u_{11} 和 v_{11} , 使得 $u_{11} \cdot v_{11} = (r_1^2 u + u_{10}) + v_{10}$, 然后 Alice 和 Bob 合作执行点积协议, 使 Alice 得到私有数据 u_{12} , Bob 得到私有数据 v_{12} , 满足 $u_{12} + v_{12} = (\sqrt{u_{11}}) \cdot (\sqrt{v_{11}}) //$ 三角面积和.

步骤 9. Alice 和 Bob 分别计算出 $s_a = \frac{r_1^2 \pi}{2} - u_8 - u_9 - u_{12}$ 和 $s_b = \frac{r_2^2 \pi}{2} - v_8 - v_9 - v_{12}$.

5 协议分析

5.1 正确性分析

为了证明协议 2 可以精确计算出两相机圆的面积, 只需要说明 $s_a + s_b$ 恰好等于图 1 中阴影部分的面积. 其证明过程如下,

从协议 2 的步骤 9 可以看出:

$$\begin{aligned} s_a + s_b &= \frac{r_1^2 \pi}{2} + \frac{r_2^2 \pi}{2} - u_8 - u_9 - u_{12} - v_8 - v_9 - v_{12} \\ &= \left(\frac{r_1^2 \pi}{2} - u_8 - v_8 \right) + \left(\frac{r_2^2 \pi}{2} - u_9 - v_9 \right) - (u_{12} + v_{12}) \\ \text{因为 } u_8 + v_8 &= a_1 \cdot b_1 = r_1^2 u_6 v_6 + \frac{u_6^3 r_1^2}{2} \frac{v_6^3}{3} = \\ &= r_1^2 \left(u_6 v_6 + \frac{(u_6 v_6)^3}{6} \right), \text{ 所以} \end{aligned}$$

$$\frac{r_1^2 \pi}{2} - u_8 - v_8 = r_1^2 \left(\frac{\pi}{2} - u_6 v_6 - \frac{(u_6 v_6)^3}{6} \right)$$

从协议 2 的步骤 1, 2, 4, 5 和 6 可知:

$$\begin{aligned} u_6 v_6 &= \frac{u_2 v_2}{2r_1 \sqrt{u_5 v_5}} = \frac{u_1 + v_1}{2r_1 \sqrt{u + v}} \\ &= \frac{u + r_1^2 + v - r_2^2}{2r_1 d} = \frac{r_1^2 + d^2 - r_2^2}{2r_1 d} \end{aligned}$$

所以, 由余弦定理可知, $\cos \theta = u_6 v_6$ (θ 取值如图 1 所示). 由泰勒展开式可知, $\arccos x = \frac{\pi}{2} - x - \frac{x^3}{6} - o(x^3)$, $\forall x: |x| < 1$. 显然, $o(x^3) = \frac{\pi}{2} - x - \frac{x^3}{6}$, 舍去极小项 $o(x^3)$ 后, $\arccos x = \frac{\pi}{2} - x - \frac{x^3}{6}$, $\forall x: |x| < 1$. 所以, $\theta = \arccos(u_6 v_6) = \frac{\pi}{2} - u_6 v_6 - \frac{(u_6 v_6)^3}{6}$.

如图 1 所示, Alice 私有的圆 O_1 中半径 $O_1 A$, $O_1 B$ 和弧 $\widehat{AB}$ (靠近点 O_2 那段) 所围成扇形 $O_1 AB$ 的面积为, $s_{O_1 AB} = \frac{1}{2} r_1 \cdot (2\theta \cdot r_1) = \theta r_1^2$, 进一步

$$\begin{aligned} s_{O_1 AB} &= r_1^2 \left(\frac{\pi}{2} - u_6 v_6 - \frac{(u_6 v_6)^3}{6} \right) \\ &= \frac{r_1^2 \pi}{2} - u_8 - v_8 \end{aligned}$$

同理可得, 从协议 2 的步骤 1, 3, 4, 5 和 6 可知, Alice 私有的圆 O_2 中半径 $O_2 A$, $O_2 B$ 和弧 $\widehat{AB}$ (靠近点 O_1 那段) 所围成扇形 $O_2 AB$ 的面积为

$$\begin{aligned} s_{O_2 AB} &= \frac{1}{2} r_2 \cdot (2\delta \cdot r_2) = \delta r_2^2 \\ &= \frac{r_2^2 \pi}{2} - u_9 - v_9 \end{aligned}$$

从协议 2 的步骤 7 和 8 可知

$$\begin{aligned} u_{12} + v_{12} &= (\sqrt{u_{11}}) \cdot (\sqrt{v_{11}}) \\ &= \sqrt{(r_1^2 u + u_{10}) + v_{10}} \\ &= \sqrt{r_1^2 u + (r_1^2 v - r_1^2 u_6^2 v_6^2 u - r_1^2 u_6^2 v_6^2 v)} \end{aligned}$$

$$\begin{aligned} \text{所以, } u_{12} + v_{12} &= \sqrt{r_1^2 (u + v - u_6^2 v_6^2 u - u_6^2 v_6^2 v)} \\ &= \sqrt{r_1^2 (1 - u_6^2 v_6^2) (u + v)}. \end{aligned}$$

$$\begin{aligned} \text{协议 2 的步骤 1 可知, } u + v &= d^2, \text{ 那么, } u_{12} + v_{12} \\ &= r_1 \sqrt{(1 - u_6^2 v_6^2) \cdot d}. \end{aligned}$$

$$\begin{aligned} \text{前文已经说明了, } \cos \theta &= u_6 v_6, \text{ 则, } \sin \theta = \\ &= \sqrt{(1 - u_6^2 v_6^2)}. \text{ 即, } u_{12} + v_{12} = r_1 \sin \theta \cdot d. \end{aligned}$$

$$\begin{aligned} \text{易于得到, 图 1 中四边形 } O_1 A O_2 B \text{ 的面积 } s_{O_1 A O_2 B} \\ \text{有, } s_{O_1 A O_2 B} &= 2 \left(\frac{1}{2} r_1 \sin \theta \cdot d \right) = r_1 \sin \theta \cdot d. \text{ 那么, } u_{12} \\ &+ v_{12} = s_{O_1 A O_2 B}. \end{aligned}$$

$$\begin{aligned} \text{显然, 图 1 中的阴影部分面积为 } s_{\text{shade}} &= s_{O_1 AB} + \\ s_{O_2 AB} - s_{O_1 A O_2 B}. \text{ 所以, } s_{\text{shade}} &= \left(\frac{r_1^2 \pi}{2} - u_8 - v_8 \right) + \\ \left(\frac{r_2^2 \pi}{2} - u_9 - v_9 \right) - (u_{12} + v_{12}) &= s_a + s_b. \text{ 也就是说,} \\ \text{协议 2 可以精确地计算出两圆相交部分的面积.} \end{aligned}$$

5.2 安全性分析

根据点积协议和加到乘变换协议的安全性, 本协议是安全的. 因为所有的数据交换过程都只是通过点积协议和加到乘变换协议发生的, 因此协议双方的私有数据都可以得到安全保护.

5.3 通信复杂度和计算复杂度

协议 1 只调用了一次二维点积协议, 所以其通信复杂度和计算复杂度为 $O(1)$. 协议 2 调用了常数级二维或三维的点积协议和加到乘变换协议, 因此

其通信复杂度和计算复杂度也都是 $O(1)$ 。

6 结束语

文中提出了一种能够计算两相交圆精确面积的安全协议,利用该协议,参与者能够安全地计算出两个相交圆的面积,并且保证各方的私有数据不会泄漏,分析证实了该协议的安全性和有效性。未来的工作是为其他计算几何问题设计出安全有效的多方计算协议。

参考文献:

- [1] Yao C. Protocols for secure computations[C]// Proc 23rd Annual IEEE Symposium on Foundations of Computer Science. Los Alamitos: IEEE Computer Society Press, 1982:160—164.
- [2] Goldreich. Foundations of cryptography: Volume II, basic applications[D]. Cambridge: Cambridge University Press, 2004.
- [3] Atallah M J, Du W L. Secure multi-party computational geometry[C]// Proc of 7th International Workshop on Algorithms and Data Structures (WADS). Berlin: Springer, 2001:165—179.
- [4] 荆巍巍. 安全多方计算中若干基础协议及应用的研究[D]. 安徽:中国科学技术大学,2008.
- [5] Goethals B, Laur S, Lipmaa H, et al. On private scalar product computation for privacy-preserving data mining[C]// proceedings of the 7th Annual International Conference in Information Security and Cryptology. Seoul, Korea: Springer, 2004:104—120.
- [6] Paillier P. Public key cryptosystems based on composite degree residuosity classes[C]// Proceedings of the 17th international conference on theory and application of cryptographic techniques. Berlin, Heidelberg: Springer-Verlag, 1999:223—238.
- [7] 徐维江. 网络计算中的私有数据保护问题及其应用研究[D]. 安徽:中国科学技术大学,2008.
- [8] Zhu Youwen, Huang Liusheng, et al. Three new approaches to privacy-preserving add to multiply protocol and its application[C]// Second International workshop on Knowledge Discovery and Data Mining, Moscow: IEEE, 2009:554—558.
- [9] Youwen Zhu, Liusheng Huang et al. Relation of PPA-TMP and Scalar Product Protocol and Their Applications [C]// Proceedings of the IEEE Symposium on Computers and Communications. Washington, DC, USA: IEEE Computer Society, 2010:184—189.

作者简介:

赵书峰 男,(1967—),副教授.研究方向为信息安全.
黄刘生 男,(1957—),博士生导师,教授.研究方向为包括信息安全、分布式计算以及无线传感器网络.

(上接第97页)

- [2] Yang FC, Su S, Li Z. Hybrid QoS-aware semantic web service composition strategies[J]. Science in China Series E, Information Science, 2008, 38(10): 1697—1716.
- [3] Zeng L Z, Benatallah B, Ngu A H H, et al. QoS-aware middleware for web services composition [J]. IEEE Trans Software Eng, 2004, 30(5): 311—327.
- [4] Dai Y, Yang L, Zhang B, et al. QoS for composite web services and optimizing [J]. Journal of Computers, 2006, 29(07): 1167—1178.
- [5] Menascé D A, Emiliano Casalicchio, Vinod Dubey, et al. On optimal service selection in Service Oriented Architectures[J]. Performance Evaluation, 2010, 67(8): 659—675.
- [6] Alrifai M, Risse T. Combining global optimization with local selection for efficient QoS-aware service composition. WWW 2009:881—890.
- [7] Schrijver A. Theory of linear and integer programming [J]. John Wiley & Sons, 1986.
- [8] Huang A F M, Lan C W, Yang S J H. An optimal QoS-based Web service selection scheme [J]. Inf Sci, 2009, 179(19): 3309—3322.
- [9] Wolsey L A. Integer Programming, John Wiley [R]. New York: 1998.
- [10] Maros I. Computational Techniques of the Simplex Method[M]. NY: Springer, 2003.
- [11] Huang S. Inverse problems of some NP-complete problems[J]. Algorithmic Applications in Management (AAIM 2005), LNCS 3521:422—426.

作者简介:

王广正 男,(1980—),硕士,讲师.研究方向为语义 Web 服务.