有理区间的安全多方计算与应用

窦家维[1],王文丽[1],刘旭红[1],李顺东[2]
(1. 陕西师范大学数学与信息科学学院,陕西西安 710119;2. 陕西师范大学计算机科学学院,陕西西安 710119)

摘 要: 本文研究了有理数与有理区间的位置关系以及两个有理区间位置关系的安全多方计算.它们已广泛应用于数据库匹配、定位搜索等领域,是保密科学计算的一个重要分支.但目前已有文献在解决有理数与有理区间的位置关系时提出的协议效率较低,且两个有理区间位置关系问题的研究较为有限.针对这些问题,本文首先用多项式表示区间,将有理数与有理区间位置关系问题转化为整数向量的内积符号判定问题,设计了新的有理数与有理区间的保密计算协议.其次,以有理数与有理区间协议作为基础模块,设计了两个有理区间位置关系的保密计算协议.最后,理论分析及实验结果均表明本文方案是安全高效的,并给出了本文协议在有理数域上的百万富翁问题及计算几何问题的应用.

关键词: 密码学;安全多方计算;有理数;有理区间;数据库匹配;定位搜索;百万富翁问题;计算几何
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2018)09-2057-06
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.09.002

Secure Multiparty Computation of Rational Interval and Its Applications

DOU Jia-wei[1], WANG Wen-li[1], LIU Xu-hong[1], LI Shun-dong[2]
(1. *School of Mathematics and Information Science, Shaanxi Normal University, Xi'an, Shaanxi* 710119, *China*;
2. *School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710119, *China*)

Abstract: The SMC (Secure Multiparty Computation) of the location relation between rational numbers and intervals, and that between two rational intervals has been investigated. As an important branch of the confidential scientific computing, this problem was widely applied in database matching, positioning search, etc. However, there still exist many problems, for example, current solutions to the location relation between rational numbers are low efficiency and the research on the location relation between two rational intervals is limited. In order to address the above gaps, firstly, we use polynomials to represent the interval, and convert the problem into determining the scalar product signs of two integer vectors. Thus, the new protocol of the problem between rational number and interval is worked out. Secondly, with the proposed scheme as the basic module, we construct the protocol of the location relation between two rational intervals. Finally, the theoretical analysis and experimental results prove that our protocols are safe and efficient, and we give the application of millionaire problem and computational geometry problem in rational domain.

Key words: cryptography; secure multiparty computation; rational number; rational interval; database matching; positioning search; millionaire problem; computation geometry

1 引言

安全多方计算是指在互不信任的网络空间中,参与者在不泄露私有数据的情况下合作完成某项计算.该问题首先是Yao[1]提出的,Goldreich,Cramer等人[2,3]对其进行了深入研究,广泛的应用前景使其成为国际密码学界的一个研究热点.保密的科学计算是安全多方计算的一个重要研究领域,主要涉及保密信息比较[1,4],向量保密计算[5],保密排序[6],集合计算问题[7]等,为研究更复杂的问题提供基础模块.

有理区间的安全多方计算属于保密的科学计算,包括:(1)有理数与有理区间位置关系的保密计算.(2)两个有理区间位置关系的保密计算.有理区间的保密计算问题首先由Nishid等人[8]提出.郭等人[9]基于计

收稿日期:2017-09-20;修回日期:2018-02-08;责任编辑:覃怀银
基金项目:国家自然科学基金(No.61272435)

算几何理论将所输入的有理数或区间端点作为坐标系中过原点的直线斜率,将区间保密计算问题转化为直线之间的位置关系判定问题提出了有理数与有理区间保密计算的解决方案. 以上文献虽然均给出了有理数与有理区间的解决方案,但协议的执行效率并不理想,且对于两个有理区间位置关系问题并未提及.

本文研究的目的,是不但应用新方法解决有理数和有理区间的位置关系问题,提高协议的效率. 其次要进一步提出两个有理区间位置关系的保密判定协议,填补该问题的空白,推进有理区间安全多方计算问题的发展.

2 预备知识

2.1 计算模型及安全性定义[3]

半诚实模型 简单地说,半诚实参与者将会严格执行协议,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. 如果参与者是半诚实的,称这样的模型为半诚实模型. 本文假设所有的参与者均为半诚实参与者.

一些记号 假设 Alice 拥有 x,Bob 拥有 y,他们要在保证 x,y 隐私性的前提下,合作计算函数 $f(x,y)=(f_1(x,y),f_2(x,y))$. 合作计算的目的是 Alice 和 Bob 分别得到函数 f 的两个分量 $f_1(x,y)$ 和 $f_2(x,y)$. 设 π 表示计算 f 的协议,Alice 在执行协议 π 的过程中所得到的信息序列记为

$$\text{view}_1^{\pi}(x,y)=(x,r_1,m_1^1,\cdots,m_1^t,f_1(x,y)),$$

其中 r_1 表示 Alice 独立的硬币抛掷结果;$m_1^i(i=1,\cdots,t)$ 表示 Alice 收到的第 i 个信息. 执行协议 π 后,Alice 得到的输出记作 $f_1(x,y)$. Bob 得到的信息序列可类似定义.

半诚实模型下协议的安全性 对于计算函数 f 的协议 π,如果存在概率多项式时间算法 S_1 与 S_2 使得

$$\{S_1(x,f_1(x,y))\}_{x,y}\overset{c}{\equiv}\{\text{view}_1^{\pi}(x,y)\}_{x,y} \tag{1}$$

$$\{S_2(y,f_2(x,y))\}_{x,y}\overset{c}{\equiv}\{\text{view}_2^{\pi}(x,y)\}_{x,y} \tag{2}$$

则称 π 保密地计算了函数 f,其中 $\overset{c}{\equiv}$ 表示计算上不可区分.

要证明一个多方计算协议是安全的,就需要构造出使式(1)和(2)成立的模拟器 S_1,S_2,如此证明安全性的方法称为模拟范例.

2.2 Paillier 加密方案

Paillier 加密系统是一种具有加法同态性的公钥加密系统,并且是语义安全的. 描述如下[10]:

密钥生成 给定一个安全参数 k,选择两个素数 p,q,记 $N=p\times q,\lambda=1\text{cm}(p-1,q-1)$,随机选择一个 $g\in Z_{N^2}^*$ 使得 $\gcd(L(g^{\lambda}\bmod N^2),N)=1$,定义 $L(x)=(x-1)/N$. 公钥为 (g,N),私钥为 λ,加密及解密算法分别记为 E 和 D.

加密 加密明文 $m(m<N)$,选择随机数 $r<N$,密文为:

$$c=E(m)=g^m r^N \bmod N^2.$$

解密 对于密文 $c<N^2$,解密得到明文为:

$$m=D(c)=\frac{L(c^{\lambda}\bmod N^2)}{L(g^{\lambda}\bmod N^2)}\bmod N.$$

同态性质 Paillier 加密算法具有加法同态性:

$$E(m_1)\times E(m_2)=(g^{m_1}r_1^N)(g^{m_2}r_2^N)\bmod N^2$$
$$=g^{m_1+m_2}(r_1r_2)^N\bmod N^2=E(m_1+m_2).$$

注解 1 在 Paillier 加密算法中 $N=p\times q$,其中 p,q 为大素数,假设整数 m 满足 $|m|\in[0,N/2)$,记 $R=D(E(m))$. 由群论的知识可知,若 $R\in(0,N/2)$,则 $m\in(0,N/2)$;若 $R\in(N/2,N)$ 或 $R=0$,则 $m\in(-N/2,0]$. 因此可由解密结果 R 的所属范围来判定数据 m 的正负.

由于 $N=p\times q$,而 p,q 为素数,$N/2$ 不能是整数,因此 R 和 $|m|$ 不可能取值 $N/2$.

3 有理数与有理区间的位置关系保密计算协议

对于有理数 x 可表示为 $x=x_1/x_2$ 的形式,规定 x_2 为正整数,x_1 为整数,且 $\gcd(x_1,x_2)=1$. 若 x 和 y 均为有理数,则称区间 $[x,y]$ 为有理区间.

3.1 问题描述及计算原理

问题描述 假设 Alice 有有理数 $a=a_1/a_2$,Bob 有有理区间 $I=[c,d]=[c_1/c_2,d_1/d_2]$,他们希望保密判断有理数 a 与区间 $[c,d]$ 的位置关系,而不泄露其他信息.

计算原理 对于有理数 a 及有理区间 $[c,d]$,$a\in[c,d]\Leftrightarrow(a-c)(a-d)\leqslant 0$. 因此如果将区间 $[c,d]$ 用多项式 $g(y)=(y-c)(y-d)$ 表示,通过保密判定函数值 $g(a)$ 的正负即可解决该问题. 为此,计算

$$g(a)=A(A_1a_1^2+A_2a_1a_2+A_3a_2^2),$$

其中 $A=1/(a_2^2c_2d_2)$,$A_1=c_2d_2$,$A_2=-c_2d_1-c_1d_2$,$A_3=c_1d_1$.

因为 $A>0$,所以只需判断 $s_a=A_1a_1^2+A_2a_1a_2+A_3a_2^2$ 的正负. 若 $s_a\leqslant 0$,则 $a\in[c,d]$;否则,$a\notin[c,d]$. 具体协议如下.

3.2 协议设计

为叙述方便,定义函数 $P(a,I)$:如果 $a\in I$,记 $P(a,I)=1$;否则,记 $P(a,I)=0$.

协议 1 有理数与有理区间位置关系判定协议

输入:Alice 输入有理数 a,Bob 输入有理区间 $[c,d]$.

输出:Alice 输出 $P(a,[c,d])$.

准备:Alice 运行 Paillier 加密系统生成公私钥,并公布公钥(g,N).

1. Alice 加密 a_1^2, a_1a_2, a_2^2,得到 $E(a_1^2), E(a_1a_2), E(a_2^2)$. 将其发送给 Bob.

2. Bob 选择随机数 $0<r<N$,计算 $Z_a=E(a_1^2)^{A_1}E(a_1a_2)^{A_2}E(a_2^2)^{A_3}r^N$,将 Z_a 发送给 Alice.

3. Alice 解密 Z_a,得到 z_a.

4. 若 $z_a\in(0,N/2)$,Alice 输出 $P(a,[c,d])=0$;否则,Alice 输出 $P(a,[c,d])=1$.

3.3　正确性分析

在协议 1 中,Bob 计算

$$Z_a=E(a_1^2)^{A_1}E(a_1a_2)^{A_2}E(a_2^2)^{A_3}r^N=E(s_a).$$

Alice 解密 Z_a 得到 z_a. 在 Paillier 加密算法中,假定 N 充分大,满足 $|s_a|\in[0,N/2)$. 由注解 1 可知,Alice 由 z_a 所属范围可判定 s_a 的正负,即函数值 $g(a)$ 的正负. 因此协议 1 是正确的.

3.4　安全性分析

下面用模拟范例严格证明协议 1 的安全性,即构造模拟器 S_1,S_2,使式(1)和(2)成立.

首先构造模拟器 S_1,接收到输入 $(a,f_1(a,[c,d])=P(a,[c,d])$ 后,S_1 按如下方式运行:

①S_1 任意选择 $c'=c'_1/c'_2, d'=d'_1/d'_2$,使得 $P(a,[c',d'])=P(a,[c,d])$ 成立.

②S_1 选择随机数 r',计算 $A'_1=c'_2d'_2, A'_2=-c'_2d'_1-c'_1d'_2, A'_3=c'_1d'_1$,及

$$Z'_a=E(a_1^2)^{A'_1}E(a_1a_2)^{A'_2}E(a_2^2)^{A'_3}r'^N.$$

③S_1 解密 Z'_a,得到 z'_a.

在协议执行过程中,

$$\text{view}_1^{\pi}(a,[c,d])=(a,Z_a,P(a,[c,d])),$$

在模拟过程中产生的信息序列为

$$S_1(a,f_1(a,[c,d]))=(a,Z'_a,P(a,[c',d'])),$$

由于 r 是 Bob 选择的随机数,对 Alice 来说:$Z'_a\overset{c}{\equiv}Z_a$. 进一步由于 $P(a,[c',d'])=P(a,[c,d])$,因此

$$\{S_1(a,f_1(a,[c,d]))\}_{a,c,d}\overset{c}{\equiv}\{\text{view}_1^{\pi}(a,[c,d])\}_{a,c,d}.$$

模拟器 S_2 可类似构造,并有下式成立

$$\{S_2([c,d],f_2(a,[c,d]))\}_{a,c,d}\overset{c}{\equiv}\{\text{view}_2^{\pi}(a,[c,d])\}_{a,c,d}.$$

证毕.

注解 2　若 Alice 拥有的数 a 及 Bob 的区间端点 c,d 均为整数,对于这种特殊情形,协议 1 在解决整数与整数区间的位置关系时可适当简化.

4　两个有理区间位置关系保密计算协议

4.1　问题描述及计算原理

问题描述　假设 Alice 有有理区间 $[a,b]=[a_1/a_2,b_1/b_2]$,Bob 有有理区间 $[c,d]=[c_1/c_2,d_1/d_2]$,他们想知道两个区间的位置关系,而不泄露其他信息. 本部分主要考虑无端点重合的情形,一般情形下的判定问题可类似考虑,详见注解 3.

两个有理区间的位置关系可分为相离、相交及包含三大类,如图 1 ~3 所示. 为了保密,在相离(相交)情形下要求不能具体获知是图 1(图 2)(a)与(b)哪种相离(相交)情形. 即在保密计算中,仅需判断四种位置关系:(1)相离;(2)相交;(3)$[a,b]\subset[c,d]$,如图 3(a);(4)$[c,d]\subset[a,b]$,如图 3(b).

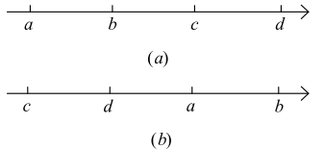

图1　两个区间相离

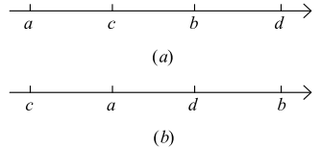

图2　两个区间相交

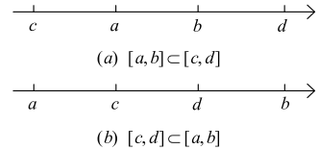

图3　两个区间包含

计算原理　Bob 将区间 $[c,d]$ 用多项式 $g(y)=(y-c)(y-d)$ 表示,双方首先合作(混合)判定函数值 $g(a),g(b)$ 的正负:若 $g(a),g(b)$ 异号,两个区间相交. 若 $g(a),g(b)$ 同负,则 $[a,b]\subset[c,d]$. 若 $g(a),g(b)$ 同正时,两个区间相离或 $[c,d]\subset[a,b]$. 为区分最后两种情形,需进一步计算:Alice 将区间 $[a,b]$ 用多项式 $h(x)=(x-a)(x-b)$ 表示,Bob 任选有理数 $e=e_1/e_2\in[c,d]$,双方合作判定函数值 $h(e)$ 的正负:若 $h(e)$ 为负,则 $[c,d]\subset[a,b]$;否则,两个区间相离. 具体协议如下.

4.2　协议设计

为叙述方便,定义函数 $F(I_1,I_2)$:若 I_1 与 I_2 相离,记 $F(I_1,I_2)=-1$;若 I_1 与 I_2 相交,记 $F(I_1,I_2)=0$;若 $I_1\subset I_2$,记 $F(I_1,I_2)=1$;若 $I_2\subset I_1$,记 $F(I_1,I_2)=2$.

协议 2　两个有理区间位置关系判定协议

输入:Alice 输入有理区间 $[a,b]$,Bob 输入有理区间 $[c,d]$.

输出:$F([a,b],[c,d])$.

准备:Alice 和 Bob 分别运行 Paillier 加密系统生成加密方案的公私钥,并公布公钥(g_A,N_A)及(g_B,N_B);将其加密及解密算法分别记为 E_A,D_A 和 E_B,D_B.

1. Alice 用公钥 E_A 加密 $a_1^2,a_1a_2,a_2^2,b_1^2,b_1b_2,b_2^2$,得到 $E_A(a_1^2)$,$E_A(a_1a_2),E_A(a_2^2),E_A(b_1^2),E_A(b_1b_2),E_A(b_2^2)$,将其发送给 Bob.

2. Bob 选择随机数 $0<r_a,r_b<N_A$,计算

$$Z_a=E_A(a_1^2)^{A_1}E_A(a_1a_2)^{A_2}E_A(a_2^2)^{A_3}r_a^{N_A},$$

$$Z_b=E_A(b_1^2)^{A_1}E_A(b_1b_2)^{A_2}E_A(b_2^2)^{A_3}r_b^{N_A}.$$

其中 $A_1=c_2d_2$, $A_2=-c_2d_1-c_1d_2$, $A_3=c_1d_1$.

3. Bob 产生随机置换 ϕ,将 ϕ 作用于 Z_a, Z_b,得到 $Z_{\phi(a)}$, $Z_{\phi(b)}$,并发送给 Alice.

4. Alice 用私钥 D_A 解密 $Z_{\phi(a)}$, $Z_{\phi(b)}$,得到 $z_{\phi(a)}$, $z_{\phi(b)}$.

5. 若 $z_{\phi(a)}\in(0,N_A/2)$, $z_{\phi(b)}\in(N_A/2,N_A)$(或 $z_{\phi(b)}\in(0,N_A/2)$, $z_{\phi(a)}\in(N_A/2,N_A)$),Alice 输出 $F([a,b],[c,d])=0$. 若 $z_{\phi(a)}$, $z_{\phi(b)}\in(N_A/2,N_A)$,Alice 输出 $F([a,b],[c,d])=1$. 若 $z_{\phi(a)}$, $z_{\phi(b)}\in(0,N_A/2)$,继续执行协议.

6. Bob 任选有理数 $e=e_1/e_2\in[c,d]$,用公钥 E_B 加密 e_1^2, e_1e_2, e_2^2,得 $E_B(e_1^2)$, $E_B(e_1e_2)$, $E_B(e_2^2)$,并发送给 Alice.

7. Alice 选择随机数 $0<r_e<N_B$,计算 $Z_e=E_B(e_1^2)^{B_1}E_B(e_1e_2)^{B_2}E_B(e_2^2)^{B_3}r_e^{N_B}$,其中 $B_1=a_2b_2$, $B_2=-a_2b_1-a_1b_2$, $B_3=a_1b_1$. 将 Z_e 发送给 Bob.

8. Bob 用私钥 D_B 解密 Z_e,得到 z_e. 若 $z_e\in(N_B/2,N_B)$,Bob 输出 $F([a,b],[c,d])=2$. 若 $z_e\in(0,N_B/2)$,Bob 输出 $F([a,b],[c,d])=-1$.

4.3 协议的正确性与安全性

协议的正确性由计算原理容易证得,下面主要讨论其安全性. 为方便描述,我们将协议 2 分为两部分,第一部分为第 1 ~ 5 步,第二部分为第 6 ~ 8 步.

(1)首先我们证明通过执行协议 2,只能获知四类区间位置关系中的某一类,不会泄露额外信息.

由于 Bob 在第 3 步给 Alice 发送数据之前进行了随机置换,这样 Alice 用私钥解密,得到 $z_{\phi(a)}$, $z_{\phi(b)}$,但不知道具体的对应关系. 若此时终止协议,仅能获知位置关系为图 3(a)的类型或图 2 的类型,但无法区分是图 2(a)与(b)哪种情形. 若继续执行第二部分,得到 z_e. 此时仅能获知位置关系为图 3(b)的类型或图 1 的类型,但无法区分是图 1(a)与(b)哪种情形.

(2)其次,需证明协议 2 中两方数据都是安全的. 下面将用模拟范例严格证明协议的安全性,即构造模拟器 S_1, S_2,使式(1)和(2)成立.

首先构造模拟器 S_1,对于输入($[a,b]$, $f_1([a,b],[c,d])=F([a,b],[c,d])$), S_1 按如下方式运行:

① S_1 任意选择 $c'=c'_1/c'_2$, $d'=d'_1/d'_2$,使得 $F([a,b],[c',d'])=F([a,b],[c,d])$.

② S_1 选择随机数 $s_a,s_b<N_A$,计算

$$Z'_a=E_A(a_1^2)^{B'_1}E_A(a_1a_2)^{B'_2}E_A(a_2^2)^{B'_3}s_a^{N_A},$$

$$Z'_b=E_A(b_1^2)^{B'_1}E_A(b_1b_2)^{B'_2}E_A(b_2^2)^{B'_3}s_b^{N_A},$$

其中 $B'_1=c'_2d'_2$, $B'_2=-c'_2d'_1-c'_1d'_2$, $B'_3=c'_1d'_1$.

③ S_1 产生随机置换 ϕ',将 ϕ'作用于 Z'_a, Z'_b,得到 $Z'_{\phi'(a)}$, $Z'_{\phi'(b)}$,解密得到 $z'_{\phi'(a)}$, $z'_{\phi'(b)}$.

若此时终止协议,在协议执行过程中,

$$\text{view}_1^{\pi}([a,b],[c,d])=([a,b],Z_{\phi(a)},Z_{\phi(b)},F([a,b],[c,d])),$$

S_1 在模拟过程中产生的信息序列为

$$S_1([a,b],F([a,b],[c,d]))=([a,b],Z'_{\phi'(a)},Z'_{\phi'(b)},F([a,b],[c',d'])).$$

由于 r_a, r_b 为 Bob 选择的随机数,对 Alice 来说, $Z'_{\phi'(a)}\overset{c}{\equiv}Z_{\phi(a)}$, $Z'_{\phi'(b)}\overset{c}{\equiv}Z_{\phi(b)}$. 进一步由于 $F([a,b],[c',d'])=F([a,b],[c,d])$,所以

$$\{S_1([a,b],f_1([a,b],[c,d]))\}_{a,b,c,d}\overset{c}{\equiv}\{\text{view}_1^{\pi}([a,b],[c,d])\}_{a,b,c,d} \tag{3}$$

模拟器 S_2 可用类似的方法构造,并有下式成立

$$\{S_2([c,d],f_2([a,b],[c,d]))\}_{a,b,c,d}\overset{c}{\equiv}\{\text{view}_2^{\pi}([a,b],[c,d])\}_{a,b,c,d} \tag{4}$$

若继续执行第二部分,后续模拟过程如下:

④ S_1 运行 Paillier 加密系统,将相应的加密及解密算法分别记为 E'_B, D'_B. 并且 S_1 任选有理数 $e'=e'_1/e'_2\in[c',d']$,应用 E'_B 加密 $e_1'^2$, $e'_1e'_2$, $e_2'^2$,得到 $E'_B(e_1'^2)$, $E'_B(e'_1e'_2)$, $E'_B(e_2'^2)$.

⑤ S_1 计算 $Z_{e'}=E'_B(e_1'^2)^{A_1}E'_B(e'_1e'_2)^{A_2}E'_B(e_2'^2)^{A_3}$.

⑥ S_1 用 D'_B 解密 $Z_{e'}$得到 $z_{e'}$.

在整个协议执行过程中,

$\text{view}_1^{\pi}([a,b],[c,d])=([a,b],Z_{\phi(a)},Z_{\phi(b)},E_B(e_1^2),E_B(e_1e_2),E_B(e_2^2),F([a,b],[c,d]))$,

S_1 在模拟过程中产生的信息序列为

$S_1([a,b],f_1([a,b],[c,d]))=([a,b],Z'_{\phi'(a)},Z'_{\phi'(b)},E'_B(e_1'^2),E'_B(e'_1e'_2),E'_B(e_2'^2),F([a,b],[c',d']))$,

由于 E_B 是 Bob 的公钥,Alice 没有私钥解密,对 Alice 来说:

$$E_B(e_1^2)\overset{c}{\equiv}E'_B(e_1'^2),$$

$$E_B(e_1e_2)\overset{c}{\equiv}E'_B(e'_1e'_2),E_B(e_2^2)\overset{c}{\equiv}E'_B(e_2'^2).$$

结合第一部分的讨论,可知在此情形下式(3)依然成立. 模拟器 S_2 可类似构造,并且式(4)也依然成立,因此协议 2 是安全的. 证毕.

注解 3 协议 2 仅考虑了两个区间端点无重合情形下的位置关系,对于区间端点有重合的情形可类似考虑. 在实际保密计算中我们应设法避免端点重合情形发生(若有端点重合情形,可能会猜出是哪个端点重合,影响安全性). 某一方(或两方)可通过对区间的端点数值分别加上一个不影响实际判定结果的随机有理数(如取自区间(0,1)),如此处理后,再发生区间端点重合的情形认为是一个小概率事件,可忽略不计. 在协议 1 中,可用类似的方法避免有理数和区间端点重合的问题.

5 效率分析

目前关于有理数与有理区间的位置关系的研究较少,本节将本文协议 1 与文[9]中效率较高的协议 3 相

比较,并对协议 2 的复杂性进行分析. 由于协议均基于 Paillier 加密方案,1 次加密或解密都需要 2 次模指数运算. 为方便分析,只考虑协议中最费时的模指数运算,其他花费忽略不计.

计算复杂性与通信复杂性　在协议 1 中,Alice 需 3 次加密和 1 次解密运算,Bob 计算 Z_a 需 4 次模指数运算,因此协议 1 共需 12 次模指数运算,2 轮通信.

在文[9]的协议 3 中,两方共需 4 次加密和 1 次解密运算,1 次密文运算,在密文运算中需 3 次模指数,因此共需 13 次模指数运算,2 轮通信. 但该协议调用了百万富翁协议,会额外增加计算与通信复杂性. 各协议的性能分析详见表 1.

表 1　协议 1 与文献[9]协议 3 的性能分析

	计算复杂性	通信复杂性	适用正有理数	适用负有理数
文献[9]协议 3	13	2	是	否
本文协议 1	12	2	是	是

为验证协议的效率,我们采用了 Java 编程语言在 MyEclipse 上对文献[9]协议 3,本文协议 1 进行编程实现. 并对实验结果随机抽取 1000 组数据求平均值,详见表 2. 计算机的配置如下:Windows 7 旗舰版,Intel(R) Core(TM) i3-2100CPU @ 3.10GHz,安装内存 4.00GB,32 位操作系统. 本文所做模拟实验均在此环境下进行.

表 2　协议 1 与文献[9]协议 3 的实验结果比较

	Alice 运算耗时(ms)	Bob 运算耗时(ms)	总运算耗时(ms)
文献[9]协议 3	15.525	16.853	32.375
本文协议 1	14.450	11.324	25.774

通过以上分析,协议 1 只需相对较少的模指数运算及通信复杂性就可解决问题,理论分析和实验结果都表明协议 1 是高效的.

对于协议 2,若仅执行协议的第一部分,Alice 需 6 次加密和 2 次解密运算,Bob 需 2 次密文运算,1 次密文运算需 4 次模指数,因此共需 24 次模指数运算,2 轮通信.

若继续执行第二部分,Alice 还需 1 次密文运算,Bob 还需 3 次加密和 1 次解密运算. 因此协议 2 共需 36 次模指数运算,4 轮通信. 我们同样采用 Java 语言在 MyEclipse 上对协议 2 的两种情形进行编程实现,并对实验结果随机抽取 1000 组数据求平均值. 结果见表 3.

表 3 中第二行括号外(内)的数据为执行协议第一部分(执行整个协议)所需的时空开销. 分析可知,协议 2 仅需较少的模指数运算及通信复杂性就可解决两个有理区间位置关系判定问题,理论分析与实验结果表明协议 2 是高效的.

表 3　协议 2 的性能分析

	计算复杂性	通信复杂性	Alice 运算耗时(ms)	Bob 运算耗时(ms)	总运算耗时(ms)
本文协议 2	24 (36)	2(4)	30.273 (46.904)	18.417 (27.642)	48.690 (74.546)

6　区间保密计算协议的推广应用

6.1　两个有理数大小比较问题

有理数大小比较问题可描述为:Alice 有有理数 a,Bob 有有理数 c,他们想保密判定 a,c 的大小. 解决方案的主要思想如下:

(1) Alice 与 Bob 商定有理数 v,满足 $v >> a$,$v >> c$.

(2) Bob 选择随机有理数 $d > v$,考虑区间 $[c,d]$,将区间 $[c,d]$ 用多项式 $g(y) = (y-c)(y-d)$ 表示.

因此,有理数 a 与 c 的大小比较问题即可转化为判定 $g(a)$ 的正负问题. 调用协议 1 即可解决.

6.2　直线与圆的相交问题

该问题可描述为:Alice 有直线 $l: Ax + By + C = 0$,Bob 有圆 $\odot o: x^2 + y^2 = r^2$,他们想保密判定直线与圆是否相交. 如图 4. 由几何知识可知,直线与圆相交当且仅当 $d \in [0, r]$ $(d = |C| / \sqrt{A^2 + B^2})$,调用协议 1 进行判断.

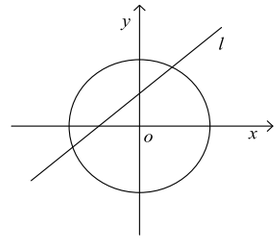

图4　保密直线与圆的相交问题

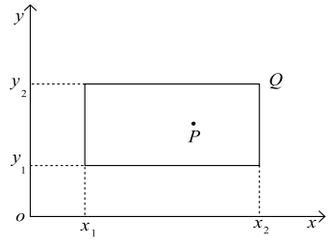

图5　点与矩形位置关系问题

6.3　有理点与矩形的位置关系问题

该问题可描述为:Alice 有点 $P(x_0, y_0)$,Bob 有矩形 $Q: [x_1, x_2] \times [y_1, y_2]$,其中 $x_i, y_i (i = 0, 1, 2)$ 均为有理数,他们想保密判断点 P 是否属于矩形 Q(如图 5). 由

图 5 可知,$P \in Q \Leftrightarrow (x_0 \in [x_1, x_2]) \wedge (y_0 \in [y_1, y_2])$. 可调用协议 1 进行判断.

6.4 两个矩形的位置关系问题

记 $I_1 = [x_1, x_2], J_1 = [y_1, y_2], I_2 = [x_3, x_4], J_2 = [y_3, y_4]$,其中 $x_i, y_i (i = 1, 2, 3, 4)$ 均为有理数. 矩形位置关系问题可描述为:Alice 有矩形 $A_1 = I_1 \times J_1$,Bob 有矩形 $A_2 = I_2 \times J_2$,他们想保密判断两个矩形的位置关系是相离、包含或相交的哪种情形. 经过分析有下述结论成立:

(1)若 $I_2 \subset I_1$ 与 $J_2 \subset J_1$ 同时成立,则 $A_2 \subset A_1$. 若 $I_1 \subset I_2$ 和 $J_1 \subset J_2$ 同时成立,则 $A_1 \subset A_2$.

(2)若 I_1 与 I_2 相交且 J_1 与 J_2 相交或包含,或者 J_1 与 J_2 相交且 I_1 与 I_2 相交或包含,则两个矩形相交.

(3)若 I_1 与 I_2 及 J_1 与 J_2 两组区间位置关系中至少有一组是相离的,则两个矩形相离.

由以上分析可知,该问题可调用协议 2 得到解决.

7 结论

本文研究了有理数与有理区间的位置关系和两个有理区间位置关系的保密判定问题,提出了相应的解决方案,本文的解决方案都假设参与者是半诚实的,所构造协议在半诚实模型下是安全的,因此进一步的研究工作拟探索恶意模型下的解决方案.

参考文献

[1] Yao A C. Protocols for secure computations[A]. Proceedings of the 23th IEEE Symposium on Foundations of Computer Science[C]. Chicago, USA: IEEE Computer Society Press, 1982. 160 – 164.

[2] Cramer R, Damgard I B, Nielsen JB. Secure Multiparty Computation [M]. London, UK: Cambridge University Press, 2015.

[3] Goldreich O. The Fundamental of Cryptography: Basic Applications [M]. London, UK: Cambridge University Press, 2004.

[4] 李顺东,王道顺. 基于同态加密的高效多方保密计算[J]. 电子学报,2013,41(4):798 – 803.
Li Shun-dong, Wang Dao-shun. Efficient secure multiparty computation based on homomorphic encryption[J]. Acta Electronica Sinica, 2013, 41(4): 798 – 803. (in Chinese)

[5] 李顺东,左祥建,杨晓莉,等. 安全向量优势协议及其应用[J]. 电子学报,2017,45(5):1117 – 1123.
Li Shun-dong, Zuo Xiang-jian, Yang Xiao-li, et al. Secure vector dominance protocol and its applications[J]. Acta Electronica Sinica, 2017, 45(5): 1117 – 1123. (in Chinese)

[6] Tang Chun-ming, Shi Gui-hua, Yao Zheng-an. Secure multi-party computation protocol for sequencing problem [J]. Science China Information Sciences, 2011, 54(8): 1654 – 1662.

[7] Zhou Su-fang, Li Shun-dong, Dou Jia-wei, et al. Efficient secure multiparty subset computation[J]. Security & Communication Networks, 2017, 2017(3): 1 – 11.

[8] Nishide T, Ohta K. Multiparty Computation for Interval, Equality and Comparison Without Bit-Decomposition Protocol [M]. Berlin: Springer Berlin Heidelberg, 2007. 343 – 360.

[9] 郭奕旻,周素芳,窦家维,等. 高效的区间保密计算及应用[J]. 计算机学报,2017,40(07):1664 – 1679.
Guo Yi-min, Zhou Su-fang, Dou Jia-wei, et al. Efficient privacy-preserving interval computation and its applications [J], Chinese Journal of Computers, 2017, 40(07): 1664 – 1679. (in Chinese)

[10] Paillier P. Public-key cryptosystems based on composite degree residuosity classes[A]. G. Goos. Lecture Notes in Computer Science 1592 [C]. NY: Springer, 1999. 223 – 238.

作者简介

窦家维 女,1963 年生于陕西. 现为陕西师范大学数学与信息科学学院硕士生导师. 主要研究方向为应用数学和密码学.
E-mail: jiawei@ snnu. edu. cn

王文丽 女,1991 年生于河南. 研究生. 主要研究方向为应用数学和密码学.
E-mail: wenliwang@ snnu. edu. cn

刘旭红 女,1992 年生于山西. 研究生. 主要研究方向为应用数学和密码学.
E-mail: xuhongliu@ snnu. edu. cn

李顺东 男,1963 年生于河南. 陕西师范大学计算机科学学院博士生导师. 主要研究方向为信息安全.
E-mail: shundong@ snnu. edu. cn