软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2020,31(12):3950−3967 [doi: 10.13328/j.cnki.jos.005858]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

数轴上保密关系测定协议*

巩林明[1,4], 李顺东[2], 邵连合[1], 薛 涛[1], 王道顺[3]

[1](西安工程大学 计算机科学学院 新型网络智能信息服务国家地方联合工程研究中心,陕西 西安 710048)

[2](陕西师范大学 计算机科学学院,陕西 西安 710119)

[3](清华大学 计算机科学与技术系,北京 100084)

[4](陕西省功能性服装面料重点实验室(西安工程大学),陕西 西安 710048)

通讯作者: 巩林明, 李顺东, 王道顺, E-mail: glmxinjing@163.com, shundong@snnu.edu.cn, daoshun@tsinghua.edu.cn

摘 要: 近些年来,安全多方计算一直是信息安全领域的热点问题之一,已经成为分布式网络用户在协同计算中用于隐私保护的关键技术.信息安全学者已经提出若干安全多方计算问题的解决方案,但更多的安全多方计算问题还有待研究.研究数轴上的保密关系测定问题,着重探讨 3 个子问题:(1) 面向有理数的点(或数)与区间保密关系测定问题;(2) 面向有理数的多维点与区间保密关系测定问题;(3) 面向有理数的区间与区间保密关系测定问题.数轴上的保密关系测定问题在隐私保护领域有着广泛的应用,可以作为基础模块用于构造其他安全多方计算协议.基于由加密方计算(或选取)加密底数的 Paillier 变体同态加密方案,设计了 3 个数轴上的保密关系测定协议:面向有理数的数与区间保密关系测定协议、面向有理数的多维点与区间保密关系测定协议以及面向有理数的区间与区间保密关系测定协议.并在标准模型下,采用模拟范例(ideal/real)分析了 3 个协议的安全性.这 3 个协议中的保密比值计算思想直接可以用于解决有理数范围内的百万富翁问题.更广泛地,这 3 个协议还可以作为基础模块用于解决保密点与圆环区域关系判定问题、点与凸多边型位置关系判定问题、保密近感探测问题等安全多方计算问题.

关键词: 保密关系测定;隐私保护;安全多方计算;分布式协同计算

中图法分类号: TP309

中文引用格式: 巩林明,李顺东,邵连合,薛涛,王道顺.数轴上保密关系测定协议.软件学报,2020,31(12):3950−3967. http://www.jos.org.cn/1000-9825/5858.htm

英文引用格式: Gong LM, Li SD, Shao LH, Xue T, Wang DS. Protocols for secure test on relationship on number axis. Ruan Jian Xue Bao/Journal of Software, 2020,31(12):3950−3967 (in Chinese). http://www.jos.org.cn/1000-9825/5858.htm

Protocols for Secure Test on Relationship on Number Axis

GONG Lin-Ming[1,4], LI Shun-Dong[2], SHAO Lian-He[1], XUE Tao[1], WANG Dao-Shun[3]

[1](The National and Local Joint Engineering Research Center for Advanced Networking & Intelligent Information Service, School of Computer Science, Xi'an Polytechnic University, Xi'an 710048, China)

[2](School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

[3](Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)

[4](Shaanxi Key Laboratory on Functional Cloths (Xi'an Polytechnic University), Xi'an 710048, China)

Abstract: In recent years, secure multiparty computation (SMC) is one of research focuses in the field of information security, and a key technology of privacy protecting for distributed users in their jointly evaluating. Researchers have proposed many schemes for SMC

* 基金项目: 西安工程大学博士科研启动基金(107020331); 陕西省教育厅重点科学研究计划(20JS052); 陕西省 2020 年技术创新引导专项计划(2020CGXNG-012); 国家自然科学基金(61972225)

Foundation item: Research Fund for the Doctoral Program of Xi'an Polytechnic University (107020331); Key Scientific Research Program Project of Department of Education of Shaanxi Province (20JS052); Special Plan for Technological and Innovation Guidance of Shaanxi Province in 2020 (2020CGXNG-012); National Natural Science Foundation of China (61972225)

收稿时间: 2018-04-21; 修改时间: 2018-11-16; 采用时间: 2019-04-23

problem, however, there are many other secure multi-computation problems needed to be investigated. This study involves private relationship test on number axis, which covers three subproblems: (1) secure test on the relationship between a confidential number and a private interval; (2) multi-dimensional secure test on the relationship between multi-number and multi-interval; (3) secure test on the relationship between two confidential intervals. Private relationship test on number axis has an extensive application in the field of privacy protection, and it can be employed as a basic block to construct other SMC protocols. Based on a variant encryption scheme of Paillier's homomorphic encryption (in which, who encrypts message who evaluates the base), three protocols for private relationship test on number axis are designed. They are secure test on the relationship between a confidential number and a private interval, multi- dimension secure test on the relationship between multi-number and multi-interval, and secure test on the relationship between two confidential intervals. And their security is analyzed using simulation framework (idea/real) in the standard model. The idea of private ratio calculation in these three protocols can be directly used to solve the millionaire problem within the range of rational numbers. More widely, these three protocols can be employed as a basic block to solve the following SMC problems: private test on relationship between a point and an annulus, private test on relationship between a point and a convex polygon, and private proximity test.

Key words: private relationship test; privacy protection; multiparty secure computation; distributed and collaborative computation

安全多方计算(secure multiparty computation,简称 SMC)首先由 Yao[1]以百万富翁问题的形式提出,是分布式环境下一种用于保护用户隐私或数据安全的关键技术,是一种将密码学和分布式计算融合于一体的隐私保护技术,是空间网络安全领域的研究热点之一,对于大数据用户隐私保护[2−4]、物联网用户隐私保护[5]、社交网络用户隐私保护[6,7]、数据挖掘用户隐私保护[8]等具有重要意义.

自 SMC 提出后的 30 年间,很多学者从其可行性、计算模型与方法论、安全证明模型及理论、公平性以及专有协议(或称用于解决专门问题的协议)等方面进行了大量研究并取得成果,但安全多方计算在分布式协同计算领域还有若干值得研究的内容.在基础理论研究方面,需要研究一些更实用的理论模型;在基础协议方面,需要设计更多高效的基础协议作为基本模块来构造其他安全多方计算协议.另外,还需要设计更多简单、高效且实用的安全多方计算协议来满足越来越多的实际应用问题.

越来越多的实际应用需要将现有整数轴上关系的保密测定推广到有理数轴上关系的安全测定,迫切需要解决点与区间关系的安全测定、多维点与区间关系的安全测定和区间之间关系的安全测定等问题.

(1) 点与区间关系的保密测定问题具体可以描述为:两个互不信任的参与者(其中一个拥有一个有理数 a,另外一个拥有一个数据区间$[b_L,b_R]$,其中,b_L,b_R 皆为有理数)想通过协同计算完成保密关系的测定 $a\overset{?}{\in}[b_L,b_R]$而不泄露双方的隐私.解决该问题的协议需要实现:两个互不信任的参与者协同完成保密关系判定后,双方只能得到信息"保密有理数是否在区间内";并且当保密有理数不在数域中时,协同计算不会泄露保密有理数与数域上、下界的关系(小于上界、大于下界);

(2) 多维点与区间保密关系测定问题实质是点与区间保密关系测定问题的拓展,多维点与区间保密关系测定问题具体描述为:不失一般性,假定 Alice 和 Bob 是两个参与者,他们分别拥有保密向量 $A=([a_{11},a_{12}],[a_{21},a_{22}],\ldots,[a_{n1},a_{n2}])$和 $B=(b_1,b_2,\ldots,b_n)$,其中,a_{i1} 和 a_{i2} 分别表示第 i 个区间$[a_{i1},a_{i2}]$的上、下界,$a_{i1}<a_{i2},i=1,2,\ldots,n$,并且 a_{i1},a_{i2},b_i 皆为有理数.Alice 与 Bob 想协同完成向量 B 与向量 A 关系的保密测定,具体而言,Alice 与 Bob 想协同完成保密测定:对于任意的 $i=1,2,\ldots,n$ 而言,$a_{i1}<b_i<a_{i2}$ 是否都成立;

(3) 两个区间关系的保密测定问题实质也是点与区间保密关系测定问题的拓展,两个区间关系的保密测定具体可以描述为:两个互不信任的参与者(分别拥有一个上下界为有理数的区间)想通过协同计算完成两区间保密关系的测定而不泄露双方的隐私.解决该问题的协议需要实现:分布式网络中的两个用户(分别拥有一个上下界为有理数的数域)协同完成保密关系判定后,双方只能得到信息"保密区间相交与否";并且当两个保密区间相交时,协同计算不会泄露相交区间相交于双方各自区间的哪一端.

数轴上的保密关系测定问题不仅是安全多方计算中一个独立的新分支问题,还可作为基础工具,用于解决分布式环境中某些专门安全多方计算问题.例如,可以作为基础工具,用于解决安全点与圆域包含关系测定问题、安全点与无限区域包含关系测定问题、点与凸多边形包含关系测定问题(关于这些应用的具体阐释详见本文第 2.2 节和第 3.2 节).

解决数轴上的保密关系测定问题实质是解决同一进程中一个数与两个数关系的保密比较问题,属于安全多方计算中百万富翁问题的推广.一般百万富翁问题是两个数据的一次保密比较,而点和与区间关系的保密测定问题是一个数与两个数在同一进程中的保密比较问题,它比一般百万富翁问题在安全性方面要求更苛刻.区间上的保密计算问题与百万富翁问题有相同之处,同时也有它独有的特点:设计解决区间上的保密计算问题的协议时,一方面需要采用百万富翁问题的思想;另一方面,还需要考虑同一进程中被重复利用两次的私有数据的特殊安全性问题.

- 相关研究

姚期智教授在文献[1]中提出了著名的百万富翁问题:两个百万富翁想通过协同计算得知谁更富有,但协同计算完成后,二者在得到谁更富有的同时,不能向对方泄露彼此的财产值,因此需要设计一个安全比较协议满足:在不泄露双方私有数据的前提下,参与双方通过协同计算得出双方私有数据的大小关系.该问题激发了密码学者们的研究热情,目前,研究者在该领域取得了诸多成果.

Boudot 等人[9]基于离散对数困难假设构造了一个解决百万富翁问题的公平协议,该协议在公平模型下解决了两个数的相等与否的保密测定.Fischlin[10]基于概率加密方案[11],在半诚实模型下设计了一个非交互式百万富翁协议.该协议的一次执行可以保密地测定出两个数的关系是大于还是小于等于,却不能具体测定出小于和等于的关系.Ioannidis 等人[12]构造了基于二选一不经意传输的百万富翁协议,该协议的效率取决于保密输入的长度和安全参数.文献[13]设计了相比 Yao 协议效率高、解决百万富翁问题的协议,但该协议仍然存在计算冗余.文献[14]首先提出一种 0-1 编码方法,然后利用该方法将百万富翁问题归约到保密集合交集计算问题,最后结合同态加密,漂亮地解决了百万富翁问题,该协议的效率会随着保密输入长度的增加而降低.Garay 等人[15]构造了两个通信复杂度分别为对数轮和常数轮的协议,它们只能用于解决整数范围内的百万富翁问题.文献[16]首先设计了一个新的 0-1 编码方法,然后利用该方法将百万富翁问题归约到保密向量标积计算问题,最后基于 Paillier 同态加密方案,构造了一个高效的百万富翁协议,该协议的效率会随着保密输入长度的增加而降低.Gordon 等人[17]基于不经意函数计算思想构造了一个完全公平的、解决百万富翁问题的协议,该协议的一次执行可以测定出两个保密数是大于还是小于等于,却不能测定出小于和等于.

文献[18]利用对称密码和归约思想(将百万富翁问题归约到保密集合元素的测定问题)设计了一个解决百万富翁问题的高效协议,该协议因采用对称密码设计,效率较上述协议有了很大提高,但该协议的一次执行不能测定出两个保密数是大于和等于的关系.有限集合元素的测定问题可以形式化描述为测定一个正整数是否是一个正整数构成的集合的元素: $x\overset{?}{\in}X$,其中,$X=\{x_1,\ldots,x_k\}$,$x,x_1,\ldots,x_k\in Z^+$.该问题可以看作数轴上保密关系测定问题的一种特殊情形,因为集合 X 是由数轴上离散的整数点构成,因而解决保密集合元素测定协议的计算开销会随着集合元素的增多而呈线性增长.而以有理数为端点的区间是无限集合,在此种情况下,面向整数的保密有限集合元素测定协议将变得不实用.

上述诸多成果非常好地解决了百万富翁问题,但还存在一些问题需要改进和一些未彻底解决的问题需要继续解决:现有解决百万富翁问题的协议大都解决的是整数集上的比较问题,数轴上保密关系测定问题实质是百万富翁协议在一个进程的两次执行,如果也采用这些协议中的方法解决数轴上保密关系测定问题,则注定所设计的数轴上保密关系测定协议只能解决整数集上的问题,从而限定了数轴上保密关系测定问题的研究意义和应用范围.如果数轴上保密关系测定能够解决以有理数为端点的连续区间上的保密计算(一个保密有理数与一个以保密有理数为端点的连续区间的包含关系测定)问题,则其具有更大的研究价值和应用价值.因此在研究数轴上保密关系测定问题时,不仅要借鉴现有百万富翁协议问题的解决方法,还需要在此方法上加以创新,才能使数轴上保密关系测定协议具有更广泛的应用天地,更贴合实际的应用场景.

数轴上保密区间关系测定问题最初由 Nishide 等人[19]以保密区间计算问题的形式提出.Nishide 等人设计的保密区间计算协议很好地解决了整数轴上关于开区间上关系的保密测定问题,但在安全性方面,并没有实现对参与方隐私的充分保护,会造成整数点靠近保密区间上界还是下界这一信息泄露的安全隐患.文献[20]采用几何保密计算方法设计了一个点与区间关系的保密测定协议,漂亮地解决了有理点与有理区间关系的保密测

定问题,但该协议在调用 Paillier 同态加密方案的基础还需要 3 次调用百万富翁协议.文献[21]采用比特值串联和放大倍数的思想设计了一个点与区间关系的保密测定协议,该协议试图解决一个实数点是与一个连续实数区间关系测定问题,但该协议并未考虑下列不成功的情形:假定实数点为 a=30.0000000073,连续实数区间的一个端点为 b_j=30.0000000073221,$j\in\{L,R\}$,L,R 分别用于标识一个区间的下、上界,如果采用该方法都扩大 10^{10} 后再作为保密输入解决一个实数点与一个连续实数区间关系测定问题,不但不能解决问题,还给协议带来繁重的计算开销.

上述 3 个区间保密计算协议很好地解决了数轴上保密关系测定问题的一个子问题:点与区间保密关系测定,但还有很多需要改进的地方,还有其他保密区间计算问题需要开拓.

本文借鉴百万富翁问题的解决思路,采用两个数的比值与 1 的保密关系测定,将保密区间计算问题拓展到新的、更大的解决范围:保密数和区间的端点为有理数.将保密区间计算问题转化为一个分数与两个分数的保密比较在同一进程中一次并发执行问题.基于该方法设计了 3 个高效的区间保密计算协议:(1) 面向有理数或分数的点与区间关系的保密测定协议;(2) 面向有理数或分数的多维点与区间保密关系测定协议;(3) 面向有理数或分数的区间与区间关系的保密测定协议.

本文的主要贡献:

1. 提出了数轴上的保密关系测定问题应分为 3 个值得研究的子问题:(1) 点与区间关系的保密测定;(2) 多维点与区间保密关系测定;(3) 区间与区间关系的保密测定;
2. 基于“两个数的安全比值与 1 的关系判定两个数的大小”,设计了 3 个用于解决面向有理数或分数的保密区间计算协议,拓展了问题的解决范围;
3. 提出一种高效的百万富翁问题通用解决方法,该方法可以用于解决同一进程中一个数与两个数关系的保密比较问题,同时还将百万富翁问题的解决范围拓展至分数范围.

1 预备知识

1.1 Paillier变体同态加密方案

文献[22]构造了一个 Paillier 变体同态加密方案,如图 1 所示.

符号记法:

p 与 q 是大素数,$|p|=|q|$,$n=pq$,$\lambda=lcm(p-1,q-1)$,$g=1+n$,

$$L(X)=\frac{X-1}{n},X\in Z_{n^2}^*$$

加密:

对于明文 $m<n$

选择 3 个随机数 $0<k,r_1,r_2<n$

计算密文:

$g_k=(1+n)^k \bmod n^2$, $c_1=g_k^m r_1^n \bmod n^2$, $c_2=g_k r_2^n \bmod n^2$;

对于密文对(c_1,c_2),其中,$c_1,c_2<n^2$

恢复明文 $m=\dfrac{L(c_1^\lambda \bmod n^2)}{L(c_2^\lambda \bmod n^2)} \bmod n$

Fig.1 A variant scheme from Paillier’s homomorphic scheme

图 1 Paillier 变体同态加密方案

该方案在高阶剩余类判定性困难假设下被证明具有选择明文攻击不可区分安全性(证明详见文献[22]第 2.3 节).该方案与 Paillier 原方案相比具有如下性质.

(1) 该方案中两个密文分量各自保持了良好的加法同态性:

$$C_i(x+y)=C_i(x)\cdot C_i(y) \tag{1a}$$

$$C_i(x\times y)=C_i^y(x)=C_i^x(y) \tag{1b}$$

其中,$C_i(x)$,$C_i(y)$,$C_i(x+y)$分别是明文 x,y 与 $x+y$ 对应的第 $i(i\in\{1,2\})$个密文分量.

(2) 加密底数可以由无密钥一方计算的良好性质,该性质在半诚实模型下的保密计算两个数的比值与“1”的大小关系问题中可以确保无密钥一方私有数据的安全性.

保密计算两个数的比值与“1”的大小关系问题描述:不失一般性,假设 Alice(私有输入为 x_a)和 Bob(私有输入为 x_b)是两个参与方,二者通过协作计算 x_a/x_b 与“1”的大小关系而不泄露 x_a 与 x_b 的数值.

假定 Alice 拥有 Paillier 变体加密方案的私钥,Bob 只有公钥,则 Alice 与 Bob 按照如下方式可以保密计算 x_a/x_b 与“1”的大小关系而不泄露 x_a 与 x_b 的数值.

① Alice 随机选择一个数 $r_{a1}\in Z_n^+$,并用自己的公钥做部分加密计算下式,然后将 C_{a1} 发送给 Bob:

$$C_{a1}=Enc(x_a)=(1+x_a\cdot n)r_a^n \bmod n^2;$$

② 在 Alice 计算 C_{a1} 的同时,Bob 随机选择 4 个数 $r_{b1},r_{b2},r_{b3},k\in Z_n^+$,并计算:

$$C_2=g^{k\cdot x_b+r_{b3}}r_{b2}^n \bmod n^2=(1+(k\cdot x_b+r_{b3})\cdot n)r_{b2}^n \bmod n^2;$$

收到 C_{a1} 后,Bob 利用密文分量的同态特性实施换底运算下式,然后将密文对(C_1,C_2)发送给 Alice:

$$C_1=C_{a1}^k g^{r_{b3}}r_{b1}^n \bmod n^2=(1+(k\cdot x_a+r_{b3})n)r_{b1}^n \bmod n^2;$$

③ Alice 收到(C_1,C_2)后,利用自己的私钥计算:

$$m_R=\frac{L(C_1^\lambda \bmod n^2)}{L(C_2^\lambda \bmod n^2)}=\frac{k\cdot x_a+r_{b3}}{k\cdot x_b+r_{b3}},$$

根据 m_R 与 1 的关系,Alice 可以得出 x_a 与 x_b 的大小关系.

显然,在该协议中,Alice 虽然是加密系统私钥的拥有者,她却无法通过解密运算得到 Bob 的私有输入 x_b.这是因为在这个过程中至多得到两个关于 3 个未知数 x_b,r_{b3},k 的方程.具体的安全性证明与本文中定理 1 的证明过程相同,在此不再赘述.

(3) 与其他同态加密方案相比,文献[22]所述方案更适用于解决数轴上的保密关系测定问题.数轴上保密关系测定问题实质是保密计算两个数的比值与“1”的大小关系问题;而保密比值传递是解决保密计算两个数的比值与“1”的大小关系问题的关键技术.相比 ElGamal[23],DJ[24]和 Paillier 等同态加密方案,文献[22]所述方案更适用于解决保密比值传递(具体论述详见文献[22]的第 2.4 节).

1.2 关于安全多方计算的安全性定义[22,25]

本文用到的关于安全多方计算的安全性定义包括定义 1(理想保密计算协议)、定义 2(半诚实参与者)以及函数的保密计算的形式化定义,这些定义的详细表述请见文献[22].

根据定义[22,25],对于 f,如果存在概率多项式时间模拟算法$\mathcal{S}_1$与$\mathcal{S}_2$使得:

$$\{(\mathcal{S}_1(a,f_1(a,b)),f_2(a,b))\}_{a,b}\overset{c}{\equiv}\{(view_1^\pi(a,b),output_2^\pi(a,b))\}_{a,b} \tag{2a}$$

$$\{(f_1(a,b),\mathcal{S}_2(a,f_2(a,b)))\}_{a,b}\overset{c}{\equiv}\{(output_1^\pi(a,b),view_2^\pi(a,b))\}_{a,b} \tag{2b}$$

成立(其中,$\overset{c}{\equiv}$表示计算上不可区分),则称π可以保密地计算 $f(a,b)$.

1.3 安全多方计算通信模型

安全多方计算协议包含两种通信模型:信息论模型和密码学模型.信息论模型规定参与者之间必须通过一条安全信道传递所有信息,并且假定攻击者具有无限的计算能力;密码学模型规定攻击者可以看到通信者之间传递的信息但不能改动这些信息,并且假定攻击者具有概率多项式时间的攻击能力.因本文协议是基于同态密码系统设计的,即参与者之间的通信属于密码学模型通信范畴,所以本文从同态密码学语义不可区分安全的角度去分析协议的安全性.

2 数轴上数与区间保密关系测定通用协议

本文中,数与区间保密关系测定“通用协议”指的是数与区间保密关系测定协议不仅可以解决整数范围内

的问题,还可以解决(分数形式的)实数范围内的问题,其实质是保密测定某数(本身是有理数)是否属于一个区间(上、下界为有理数)但不泄露该数和区间的上、下界.具体描述如下:Alice 和 Bob 是分布式环境下的两个实体,其中, Alice 拥有一个上、下界为分数或整数的区间 $dom_A=[\boldsymbol{a}_L,\boldsymbol{a}_R]$,Bob 拥有一个有理数 $\boldsymbol{b}$,二者通过协同计算,测定 $\boldsymbol{b}$ 是否落在区间 dom_A 内,但不泄露下列有关双方的私有信息:$\boldsymbol{a}_L,\boldsymbol{a}_R,\boldsymbol{b}$ 的具体数值、$\boldsymbol{a}_L$ 与 $\boldsymbol{b}$ 的关系、$\boldsymbol{a}_R$ 与 $\boldsymbol{b}$ 的关系.

2.1 数轴上数与区间保密关系测定协议Π_1

数 $\boldsymbol{b}$ 和区间 $dom_A=[\boldsymbol{a}_L,\boldsymbol{a}_R]$(其中,$\boldsymbol{b},\boldsymbol{a}_L,\boldsymbol{a}_R$ 均为有理数)的关系在数值上有 3 种情况:$\boldsymbol{a}_L<\boldsymbol{b}<\boldsymbol{a}_R$,$\boldsymbol{b}<\boldsymbol{a}_L$,$\boldsymbol{b}>\boldsymbol{a}_R$,这 3 种情形在数轴上表现为 3 种位置关系,如图 2 所示.

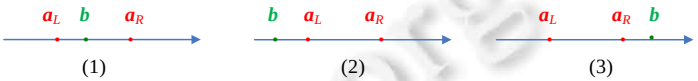


Fig.2 Relationship between a point and a interval

图 2 点与区间的关系

1. 具体协议.

输入:系统安全参数$\kappa=\log n$,Alice 的保密区间 $dom_A=[\boldsymbol{a}_L,\boldsymbol{a}_R]$,Bob 的保密数 $\boldsymbol{b}$,其中,$\boldsymbol{b},\boldsymbol{a}_L,\boldsymbol{a}_R$ 均为有理数;

输出:$\boldsymbol{b}\overset{?}{\in}dom_A=\partial=\begin{cases}1, & \dfrac{b_1}{b_2}\notin dom_A\\ -1, & \dfrac{b_1}{b_2}\in dom_A\end{cases}$.

准备工作:Bob 先运行方案$\mathcal{E}$的密钥生成算法,产生公私钥对(K_{Pub},K_{Pri}),其中,$K_{Pub}=1+n,K_{Pri}=\lambda$;Alice 和 Bob 分别将自己的数 $\boldsymbol{a}_L,\boldsymbol{a}_R$ 和 $\boldsymbol{b}$ 表示成数对形式 $(a_{L_1},a_{L_2}),(a_{R_1},a_{R_2})$ 与(b_1,b_2),使得:

$$\boldsymbol{a}_L=\frac{a_{L_1}}{a_{L_2}},\boldsymbol{a}_R=\frac{a_{R_1}}{a_{R_2}},\boldsymbol{b}=\frac{b_1}{b_2},\gcd(a_{L_1},a_{L_2})=\gcd(a_{R_1},a_{R_2})=\gcd(b_1,b_2)=1.$$

此处假定有理数都已经表示成分数形式了.

Step 1:Bob 利用自己的公钥将自己的数对(b_1,b_2)加密:

$$C_{b_1}=(1+n)^{b_1}r_{b_1}^n \bmod n^2 \tag{3a}$$

$$C_{b_2}=(1+n)^{b_2}r_{b_2}^n \bmod n^2 \tag{3b}$$

并将得到的 (C_{b_1},C_{b_2}) 发送给 Alice.

Step 2:Alice 收到 (C_{b_1},C_{b_2}) 后按照如下方式工作.

① 随机选择 6 个不等的、长度为⌊log$n$⌋–1 的随机数 $k_{a_1},k_{a_2},k'_{a_1},k'_{a_2},k'_{a_3},k'_{a_4}$ 和 4 个随机数 $r_{a_1},r_{a_2},r_{a_3},r_{a_4}\in Z_n^*$,利用 Paillier 变体方案加密及其同态性计算 2 个密文对 $(C_{(a_{L_2}\cdot b_1)+k'_{a_1}},C_{(a_{L_1}\cdot b_2)+k'_{a_1}}),(C_{(a_{R_2}\cdot b_1)+k'_{a_2}},C_{(a_{R_1}\cdot b_2)+k'_{a_2}})$:

$$C_{(a_{L_2}\cdot b_1)+k'_{a_1}}=((C_{b_1})^{k_{a_1}\cdot a_{L_2}} \bmod n^2)\times(1+k_{a_1}k'_{a_1}n)r_{a_1}^n \bmod n^2 \tag{4a}$$

$$C_{(a_{L_1}\cdot b_2)+k'_{a_1}}=((C_{b_2})^{k_{a_1}\cdot a_{L_1}} \bmod n^2)\times(1+k_{a_1}k'_{a_1}n)r_{a_2}^n \bmod n^2 \tag{4b}$$

$$C_{(a_{R_2}\cdot b_1)+k'_{a_2}}=((C_{b_1})^{k_{a_2}\cdot a_{R_2}} \bmod n^2)\times(1+k_{a_2}k'_{a_2}n)r_{a_3}^n \bmod n^2 \tag{5a}$$

$$C_{(a_{R_1}\cdot b_2)+k'_{a_2}}=((C_{b_2})^{k_{a_2}\cdot a_{R_1}} \bmod n^2)\times(1+k_{a_2}k'_{a_2}n)r_{a_2}^n \bmod n^2 \tag{5b}$$

② 对两个密文对 $(C_{(a_{L_2}\cdot b_1)+k'_{a_1}},C_{(a_{L_1}\cdot b_2)+k'_{a_1}}),(C_{(a_{R_2}\cdot b_1)+k'_{a_2}},C_{(a_{R_1}\cdot b_2)+k'_{a_2}})$ 同时在组内做相同的随机置换,并对两个密文对也做随机置换得到密文对序列: $(c_{L_1},c_{R_1}),(c_{L_2},c_{R_2})$,简单地讲,随机选择下式并发给 Bob:

$$((c_{L_1},c_{R_1}),(c_{L_2},c_{R_2}))\in\{((C_{(a_{L_2}\cdot b_1)+k'_{a_1}},C_{(a_{L_1}\cdot b_2)+k'_{a_1}}),(C_{(a_{R_2}\cdot b_1)+k'_{a_2}},C_{(a_{R_1}\cdot b_2)+k'_{a_2}})),$$
$$((C_{(a_{R_2}\cdot b_1)+k'_{a_2}},C_{(a_{R_1}\cdot b_2)+k'_{a_2}}),(C_{(a_{L_2}\cdot b_1)+k'_{a_1}},C_{(a_{L_1}\cdot b_2)+k'_{a_1}})),$$
$$((C_{(a_{L_1}\cdot b_2)+k'_{a_1}},C_{(a_{L_2}\cdot b_1)+k'_{a_1}}),(C_{(a_{R_1}\cdot b_2)+k'_{a_2}},C_{(a_{R_2}\cdot b_1)+k'_{a_2}})),$$
$$((C_{(a_{R_1}\cdot b_2)+k'_{a_2}},C_{(a_{R_2}\cdot b_1)+k'_{a_2}}),(C_{(a_{L_1}\cdot b_2)+k'_{a_1}},C_{(a_{L_2}\cdot b_1)+k'_{a_1}}))\}.$$

Step 3:Bob 收到 $(c_{L_1},c_{R_1}),(c_{L_2},c_{R_2})$ 后计算下式,然后将∂发送给 Alice:

$$\partial=P\left(\frac{L(c_{L_1}^{\lambda})}{L(c_{R_1}^{\lambda})}\right)P\left(\frac{L(c_{L_2}^{\lambda})}{L(c_{R_2}^{\lambda})}\right),\text{其中},P(X)=\begin{cases}-1, & X\leqslant 1\\ 1, & X>1\end{cases}\tag{6}$$

2. 数理计算的正确性.

(1) 如果 $\boldsymbol{b}\in dom_A$,即 $\boldsymbol{a}_L<\boldsymbol{b}<\boldsymbol{a}_R$,则有 $\frac{\boldsymbol{a}_L}{\boldsymbol{b}}\leqslant 1,\frac{\boldsymbol{a}_R}{\boldsymbol{b}}\geqslant 1$,所以 $\frac{\boldsymbol{a}_L}{\boldsymbol{b}},\frac{\boldsymbol{a}_R}{\boldsymbol{b}}$ 经函数 $P(X)=\begin{cases}-1, & X\leqslant 1\\ 1, & X>1\end{cases}$ 作用后的乘积满足:

$$\partial=P\left(\frac{\boldsymbol{a}_L}{\boldsymbol{b}}\right)\cdot P\left(\frac{\boldsymbol{a}_R}{\boldsymbol{b}}\right)=-1;$$

(2) 如果$(\boldsymbol{b}\notin dom_A)\wedge(\boldsymbol{b}<\boldsymbol{a}_L)$,则有 $\frac{\boldsymbol{a}_L}{\boldsymbol{b}}>1,\frac{\boldsymbol{a}_R}{\boldsymbol{b}}>1$,因此 $\frac{\boldsymbol{a}_L}{\boldsymbol{b}},\frac{\boldsymbol{a}_R}{\boldsymbol{b}}$ 经函数 $P(X)=\begin{cases}-1, & X\leqslant 1\\ 1, & X>1\end{cases}$ 作用后的乘积:

$$\partial=P\left(\frac{\boldsymbol{a}_L}{\boldsymbol{b}}\right)\cdot P\left(\frac{\boldsymbol{a}_R}{\boldsymbol{b}}\right)=(-1)\cdot(-1)=1;$$

(3) 如果$(\boldsymbol{b}\notin dom_A)\wedge(\boldsymbol{a}_R<\boldsymbol{b})$,则有 $\frac{\boldsymbol{a}_L}{\boldsymbol{b}}<1,\frac{\boldsymbol{a}_R}{\boldsymbol{b}}<1$,因此 $\frac{\boldsymbol{a}_L}{\boldsymbol{b}},\frac{\boldsymbol{a}_R}{\boldsymbol{b}}$ 经函数 $P(X)=\begin{cases}-1, & X\leqslant 1\\ 1, & X>1\end{cases}$ 作用后的乘积:

$$\partial=P\left(\frac{\boldsymbol{a}_L}{\boldsymbol{b}}\right)\cdot P\left(\frac{\boldsymbol{a}_R}{\boldsymbol{b}}\right)=1\cdot 1=1.$$

3. 安全性

定理 1. 在半诚实模型下,保密测定某数(有理数)是否属于一个(上、下界为有理数的)区间协议Π_1是安全的.

证明:衡量保密测定某数是否属于某个区间协议的安全性,关键是看协议执行结束后有没有造成 Alice 与 Bob 两方私有信息的泄露.下面将严格按照定义 1 与定义 2 声明的安全标准和方法证明:通过协同执行第 2.1 节中的保密计算协议,Alice 与 Bob 会得到保密计算结果(属于或者不属于),但不会得到对方的具体数值$(\boldsymbol{a}_L,\boldsymbol{a}_R,\boldsymbol{b})$.

I. Bob 私有信息在协议执行后是安全的.

在最坏的情形下,即在 Alice 受控于攻击者的情形下,构造一个模拟器 $\mathcal{S}_1^{\Pi_1}$ 模拟协议Π_1的执行过程.显然,模拟器是潜在的、能力最强的攻击者.如果多项式时间内的敌手 $\mathcal{S}_1^{\Pi_1}$ 获得的信息并不多于 Alice 在实际执行协议中的视图内容,则称协议Π_1执行完毕后没有造成 Bob 具体数值 $\boldsymbol{b}$ 的泄露,即 Bob 私有信息是安全的.

构造一个在最坏的情形下,即在 Alice 受敌手控制的情形下、能够在多项式时间内模拟协议Π_1整个执行过程的模拟器 $\mathcal{S}_1^{\Pi_1}$,其输入为:敌手根据 Alice 区间的下、上界 $\boldsymbol{a}_L,\boldsymbol{a}_R$(二者均为分数形式的有理数)随机选择利于它获取 Bob 数值 $\boldsymbol{b}$ 的两个分数 $\boldsymbol{a}'_L,\boldsymbol{a}'_R$、Bob 随机选择的两个不等的随机数 $r_{b_1},r_{b_2}\in Z_n^*$ 以及 Bob 的数值对应的整型有序对表示(b_1,b_2) (gcd(b_1,b_2)=1).作为能力最强的、多项式时间的敌手,模拟器 $\mathcal{S}_1^{\Pi_1}$ 产生的视图为

$$(C_{b_1}=(1+n)^{b_1}r_{b_1}^n \bmod n^2,C_{b_2}=(1+n)^{b_2}r_{b_2}^n \bmod n^2,(c'_{L_1},c'_{R_1}),(c'_{L_2},c'_{R_2})),$$

其中,

$$C'_{(a'_{L_2}\cdot b_1)+k'_{a_1}}=((C_{b_1})^{k_{a_1}\cdot a'_{L_2}} \bmod n^2)\times(1+k_{a_1}k'_{a_1}n)r_{a_1}^n \bmod n^2$$
$$C'_{(a'_{L_1}\cdot b_1)+k'_{a_1}}=((C_{b_2})^{k_{a_1}\cdot a'_{L_1}} \bmod n^2)\times(1+k_{a_1}k'_{a_1}n)r_{a_2}^n \bmod n^2$$
$$C'_{(a'_{R_2}\cdot b_1)+k'_{a_2}}=((C_{b_1})^{k_{a_2}\cdot a'_{R_2}} \bmod n^2)\times(1+k_{a_2}k'_{a_2}n)r_{a_3}^n \bmod n^2$$
$$C'_{(a'_{R_1}\cdot b_2)+k'_{a_2}}=((C_{b_2})^{k_{a_2}\cdot a'_{R_1}} \bmod n^2)\times(1+k_{a_2}k'_{a_2}n)r_{a_2}^n \bmod n^2$$

$$((c'_{L_1},c'_{R_1}),(c'_{L_2},c'_{R_2}))\in\{((C'_{(a'_{L_2}\cdot b_1)+k'_{a_1}},C'_{(a'_{L_1}\cdot b_2)+k'_{a_1}}),(C'_{(a'_{R_2}\cdot b_1)+k'_{a_2}},C'_{(a'_{R_1}\cdot b_2)+k'_{a_2}})),$$
$$((C'_{(a'_{L_1}\cdot b_2)+k'_{a_1}},C'_{(a'_{L_2}\cdot b_1)+k'_{a_1}}),(C'_{(a'_{R_1}\cdot b_2)+k'_{a_2}},C'_{(a'_{R_2}\cdot b_1)+k'_{a_2}})),$$
$$((C'_{(a'_{R_2}\cdot b_1)+k'_{a_2}},C'_{(a'_{R_1}\cdot b_2)+k'_{a_2}}),(C'_{(a'_{L_2}\cdot b_1)+k'_{a_1}},C_{(a'_{L_1}\cdot b_2)+k'_{a_1}})),$$
$$((C'_{(a'_{R_1}\cdot b_2)+k'_{a_2}},C'_{(a'_{R_2}\cdot b_1)+k'_{a_2}}),(C'_{(a'_{L_1}\cdot b_2)+k'_{a_1}},C'_{(a'_{L_2}\cdot b_1)+k'_{a_1}}))\}.$$

而 Alice 在协议Π_1的实际执行中产生的视图为

$$(C_{b_1}=(1+n)^{b_1}r_{b_1}^n \bmod n^2, C_{b_2}=(1+n)^{b_2}r_{b_2}^n \bmod n^2,(c_{L_1},c_{R_1}),(c_{L_2},c_{R_2})),$$

其中,

$$C_{(a_{L_2}\cdot b_1)+k'_{a_1}}=((C_{b_1})^{k_{a_1}\cdot a_{L_2}} \bmod n^2)\times(1+k_{a_1}k'_{a_1}n)r_{a_1}^n \bmod n^2$$
$$C_{(a_{L_1}\cdot b_2)+k'_{a_1}}=((C_{b_2})^{k_{a_1}\cdot a_{L_1}} \bmod n^2)\times(1+k_{a_1}k'_{a_1}n)r_{a_2}^n \bmod n^2$$
$$C_{(a_{R_2}\cdot b_1)+k'_{a_2}}=((C_{b_1})^{k_{a_2}\cdot a_{R_2}} \bmod n^2)\times(1+k_{a_2}k'_{a_2}n)r_{a_3}^n \bmod n^2$$
$$C_{(a_{R_1}\cdot b_2)+k'_{a_2}}=((C_{b_2})^{k_{a_2}\cdot a_{R_1}} \bmod n^2)\times(1+k_{a_2}k'_{a_2}n)r_{a_2}^n \bmod n^2$$
$$((c_{L_1},c_{R_1}),(c_{L_2},c_{R_2}))\in\{((C_{(a_{L_2}\cdot b_1)+k'_{a_1}},C_{(a_{L_1}\cdot b_2)+k'_{a_1}}),(C_{(a_{R_2}\cdot b_1)+k'_{a_2}},C_{(a_{R_1}\cdot b_2)+k'_{a_2}})),$$
$$((C_{(a_{R_2}\cdot b_1)+k'_{a_2}},C_{(a_{R_1}\cdot b_2)+k'_{a_2}}),(C_{(a_{L_2}\cdot b_1)+k'_{a_1}},C_{(a_{L_1}\cdot b_2)+k'_{a_1}})),$$
$$((C_{(a_{L_1}\cdot b_2)+k'_{a_1}},C_{(a_{L_2}\cdot b_1)+k'_{a_1}}),(C_{(a_{R_1}\cdot b_2)+k'_{a_2}},C_{(a_{R_2}\cdot b_1)+k'_{a_2}})),$$
$$((C_{(a_{R_1}\cdot b_2)+k'_{a_2}},C_{(a_{R_2}\cdot b_1)+k'_{a_2}}),(C_{(a_{L_2}\cdot b_1)+k'_{a_1}},C_{(a_{L_1}\cdot b_2)+k'_{a_1}})),$$
$$((C_{(a_{R_2}\cdot b_1)+k'_{a_2}},C_{(a_{R_1}\cdot b_2)+k'_{a_2}}),(C_{(a_{L_1}\cdot b_2)+k'_{a_1}},C_{(a_{L_2}\cdot b_1)+k'_{a_1}})),$$
$$((C_{(a_{L_2}\cdot b_1)+k'_{a_1}},C_{(a_{L_1}\cdot b_2)+k'_{a_1}}),(C_{(a_{R_2}\cdot b_1)+k'_{a_2}},C_{(a_{R_1}\cdot b_2)+k'_{a_2}})),$$
$$((C_{(a_{R_1}\cdot b_2)+k'_{a_2}},C_{(a_{R_2}\cdot b_1)+k'_{a_2}}),(C_{(a_{L_1}\cdot b_2)+k'_{a_1}},C_{(a_{L_2}\cdot b_1)+k'_{a_1}})),$$
$$((C_{(a_{L_1}\cdot b_2)+k'_{a_1}},C_{(a_{L_2}\cdot b_1)+k'_{a_1}}),(C_{(a_{R_1}\cdot b_2)+k'_{a_2}},C_{(a_{R_2}\cdot b_1)+k'_{a_2}}))\}.$$

Alice 无论在模拟协议还是实际协议中,接收到的有关 Bob(或$\mathcal{S}_1^{\Pi_1}$)的信息都是经$\mathcal{E}$加密后的密文,一方面因为 Alice 没有$\mathcal{E}$的解密密钥;另一方面,加密方案$\mathcal{E}$已被证明在选择明文攻击下具有语义不可区分安全,即经加密方案$\mathcal{E}$加密生成的密文是语义不可区分的.因此可得:

模拟视图 $(C'_{b_1}=(1+n)^{b_1}r_{b_1}^n \bmod n^2, C'_{b_2}=(1+n)^{b_2}r_{b_2}^n \bmod n^2,(c'_{L_1},c'_{R_1}),(c'_{L_2},c'_{R_2}))$ 与真实视图 $(C_{b_1}=(1+n)^{b_1}r_{b_1}^n \bmod n^2, C_{b_2}=(1+n)^{b_2}r_{b_2}^n \bmod n^2,(c_{L_1},c_{R_1}),(c_{L_2},c_{R_2}))$ 是计算不可区分的.也就说,$\mathcal{S}_1^{\Pi_1}$满足安全定义关系式(1a).

II. Alice 私有信息在协议执行后是安全的.

在最坏的情形下,即在 Bob 受控于攻击者的情形下,构造一个模拟器$\mathcal{S}_2^{\Pi_1}$模拟协议Π_1的执行过程.显然,模拟器是潜在的、能力最强的攻击者;如果多项式时间内的敌手$\mathcal{S}_2^{\Pi_1}$获得的信息并不多于 Bob 在实际执行协议中的视图内容,则称协议Π_1完成后没有造成 Alice 区间下、上界$\boldsymbol{a}_L,\boldsymbol{a}_R$($\boldsymbol{a}_L,\boldsymbol{a}_R$为有理数)的泄露,即 Alice 私有信息是安全的.

假定敌手$\mathcal{S}_2^{\Pi_1}$控制着 Bob,并且在 Bob 不参与的情况下,能够在多项时间内模拟协议Π_1执行的全过程.如果在该假定条件下,多项式时间内的敌手$\mathcal{S}_2^{\Pi_1}$获得的信息并不多于 Bob 在实际执行协议中的视图内容,则 Alice 私有信息(区间的下、上界$\boldsymbol{a}_L,\boldsymbol{a}_R$)是安全的.

首先构造一个在 Bob 受敌手控制的情形下、能够在多项式时间内模拟协议Π_1整个执行过程的模拟器$\mathcal{S}_2^{\Pi_1}$,其输入为:敌手根据 Bob 数值 $\boldsymbol{b}$($\boldsymbol{b}$是分数形式的实数或有理数)随机选择利于它获取 Alice 区间的下、上界$\boldsymbol{a}_L,\boldsymbol{a}_R$的一个分数形式的实数或有理数$\boldsymbol{b}'$、Bob 随机选择的两个不等的随机数$r_{b_1},r_{b_2}\in Z_n^*$以及 Alice 区间的下、上界$\boldsymbol{a}_L$, $\boldsymbol{a}_R$对应的整型有序对表示$(a_{L_1},a_{L_2}),(a_{R_1},a_{R_2})(\gcd(a_{L_1},a_{L_2})=1,\gcd(a_{R_1},a_{R_2})=1)$.作为潜在的、能力最强的敌手,模拟器$\mathcal{S}_2^{\Pi_1}$产生的视图为$(C_{b'_1},C_{b'_2},(c'_{L_1},c'_{R_1}),(c'_{L_2},c'_{R_2}))$,其中,

- $C_{b'_1},C_{b'_2}$是$\mathcal{S}_2^{\Pi_1}$利用 Bob 的公钥按照如下计算的:$C_{b'_1}=(1+n)^{b'_1}r_{b'_1}^n \bmod n^2, C_{b'_2}=(1+n)^{b'_2}r_{b'_2}^n \bmod n^2$;

- 密文 (c'_{L_i},c'_{R_i}) 是 Alice 经过下述方式构造的.

(1) 由密文 $C_{b'_1},C_{b'_2}$,利用方案$\mathcal{E}$计算:

$$\begin{aligned}
C_{(a_{L_2}\cdot b'_1)+k'_{a_1}} &= ((C_{b'_1})^{k_{a_1}\cdot a_{L_2}} \bmod n^2)\times(1+k_{a_1}k'_{a_1}n)r_{a_1}^n \bmod n^2,\\
C_{(a_{L_1}\cdot b'_2)+k'_{a_1}} &= ((C_{b'_2})^{k_{a_1}\cdot a_{L_1}} \bmod n^2)\times(1+k_{a_1}k'_{a_1}n)r_{a_2}^n \bmod n^2,\\
C_{(a_{R_2}\cdot b'_1)+k'_{a_2}} &= ((C_{b'_1})^{k_{a_2}\cdot a_{R_2}} \bmod n^2)\times(1+k_{a_2}k'_{a_2}n)r_{a_3}^n \bmod n^2,\\
C_{(a_{R_1}\cdot b'_2)+k'_{a_2}} &= ((C_{b'_2})^{k_{a_2}\cdot a_{R_1}} \bmod n^2)\times(1+k_{a_2}k'_{a_2}n)r_{a_2}^n \bmod n^2;
\end{aligned}$$

(2) 随机选取一个:

$$\begin{aligned}
((c'_{L_1},c'_{R_1}),(c'_{L_2},c'_{R_2}))\in\{&((C_{(a_{L_2}\cdot b'_1)+k'_{a_1}},C_{(a_{L_1}\cdot b'_2)+k'_{a_1}}),(C_{(a_{R_2}\cdot b'_1)+k'_{a_2}},C_{(a_{R_1}\cdot b'_2)+k'_{a_2}})),\\
&((C_{(a_{L_1}\cdot b'_2)+k'_{a_1}},C_{(a_{L_2}\cdot b'_1)+k'_{a_1}}),(C_{(a_{R_1}\cdot b'_2)+k'_{a_2}},C_{(a_{R_2}\cdot b'_1)+k'_{a_2}})),\\
&((C_{(a_{R_2}\cdot b'_1)+k'_{a_2}},C_{(a_{R_1}\cdot b'_2)+k'_{a_2}}),(C_{(a_{L_2}\cdot b'_1)+k'_{a_1}},C_{(a_{L_1}\cdot b'_2)+k'_{a_1}})),\\
&((C_{(a_{R_1}\cdot b'_2)+k'_{a_2}},C_{(a_{R_2}\cdot b'_1)+k'_{a_2}}),(C_{(a_{L_1}\cdot b'_2)+k'_{a_1}},C_{(a_{L_2}\cdot b'_1)+k'_{a_1}})),\\
&((C_{(a_{R_2}\cdot b'_1)+k'_{a_2}},C_{(a_{R_1}\cdot b'_2)+k'_{a_2}}),(C_{(a_{L_2}\cdot b'_1)+k'_{a_1}},C_{(a_{L_1}\cdot b'_2)+k'_{a_1}})),\\
&((C_{(a_{L_2}\cdot b'_1)+k'_{a_1}},C_{(a_{L_1}\cdot b'_2)+k'_{a_1}}),(C_{(a_{R_2}\cdot b'_1)+k'_{a_2}},C_{(a_{R_1}\cdot b'_2)+k'_{a_2}})),\\
&((C_{(a_{R_1}\cdot b'_2)+k'_{a_2}},C_{(a_{R_2}\cdot b'_1)+k'_{a_2}}),(C_{(a_{L_1}\cdot b'_2)+k'_{a_1}},C_{(a_{L_2}\cdot b'_1)+k'_{a_1}})),\\
&((C_{(a_{L_1}\cdot b'_2)+k'_{a_1}},C_{(a_{L_2}\cdot b'_1)+k'_{a_1}}),(C_{(a_{R_1}\cdot b'_2)+k'_{a_2}},C_{(a_{R_2}\cdot b'_1)+k'_{a_2}}))\}.
\end{aligned}$$

而 Alice 在协议Π_1的实际执行中生成的实际视图为 $(C_{b_1},C_{b_2},(c_{L_1},c_{R_1}),(c_{L_2},c_{R_2}))$,其中,$C_{b_1},C_{b_2}$ 是 Bob 利用自己的公钥通过计算 $C_{b_1}=(1+n)^{b_1}r_{b_1}^n \bmod n^2, C_{b_2}=(1+n)^{b_2}r_{b_2}^n \bmod n^2$ 得到的,密文 (c_{L_i},c_{R_i}) 是 Alice 经过下述方式构造的.

(1) 由密文 C_{b_1},C_{b_2} 利用方案$\mathcal{E}$同态性计算得到:

$$\begin{aligned}
C_{(a_{L_2}\cdot b_1)+k'_{a_1}} &= ((C_{b_1})^{k_{a_1}\cdot a_{L_2}} \bmod n^2)\times(1+k_{a_1}k'_{a_1}n)r_{a_1}^n \bmod n^2,\\
C_{(a_{L_1}\cdot b_2)+k'_{a_1}} &= ((C_{b_2})^{k_{a_1}\cdot a_{L_1}} \bmod n^2)\times(1+k_{a_1}k'_{a_1}n)r_{a_2}^n \bmod n^2,\\
C_{(a_{R_2}\cdot b_1)+k'_{a_2}} &= ((C_{b_1})^{k_{a_2}\cdot a_{R_2}} \bmod n^2)\times(1+k_{a_2}k'_{a_2}n)r_{a_3}^n \bmod n^2,\\
C_{(a_{R_1}\cdot b_2)+k'_{a_2}} &= ((C_{b_2})^{k_{a_2}\cdot a_{R_1}} \bmod n^2)\times(1+k_{a_2}k'_{a_2}n)r_{a_2}^n \bmod n^2;
\end{aligned}$$

(2) 随机选择一个:

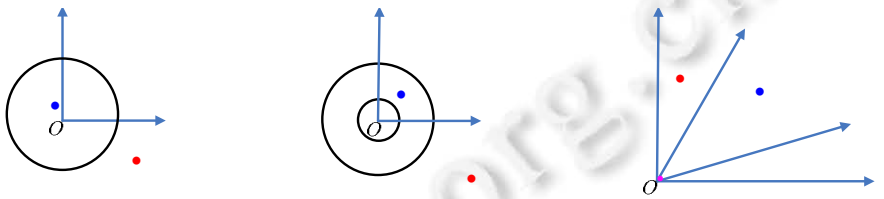
$$\begin{aligned}
((c_{L_1},c_{R_1}),(c_{L_2},c_{R_2}))\in\{&((C_{(a_{L_2}\cdot b_1)+k'_{a_1}},C_{(a_{L_1}\cdot b_2)+k'_{a_1}}),(C_{(a_{R_2}\cdot b_1)+k'_{a_2}},C_{(a_{R_1}\cdot b_2)+k'_{a_2}})),\\
&((C_{(a_{L_1}\cdot b_2)+k'_{a_1}},C_{(a_{L_2}\cdot b_1)+k'_{a_1}}),(C_{(a_{R_1}\cdot b_2)+k'_{a_2}},C_{(a_{R_2}\cdot b_1)+k'_{a_2}})),\\
&((C_{(a_{R_2}\cdot b_1)+k'_{a_2}},C_{(a_{R_1}\cdot b_2)+k'_{a_2}}),(C_{(a_{L_2}\cdot b_1)+k'_{a_1}},C_{(a_{L_1}\cdot b_2)+k'_{a_1}})),\\
&((C_{(a_{R_1}\cdot b_2)+k'_{a_2}},C_{(a_{R_2}\cdot b_1)+k'_{a_2}}),(C_{(a_{L_1}\cdot b_2)+k'_{a_1}},C_{(a_{L_2}\cdot b_1)+k'_{a_1}})),\\
&((C_{(a_{R_2}\cdot b_1)+k'_{a_2}},C_{(a_{R_1}\cdot b_2)+k'_{a_2}}),(C_{(a_{L_2}\cdot b_1)+k'_{a_1}},C_{(a_{L_1}\cdot b_2)+k'_{a_1}})),\\
&((C_{(a_{L_2}\cdot b_1)+k'_{a_1}},C_{(a_{L_1}\cdot b_2)+k'_{a_1}}),(C_{(a_{R_2}\cdot b_1)+k'_{a_2}},C_{(a_{R_1}\cdot b_2)+k'_{a_2}})),\\
&((C_{(a_{R_1}\cdot b_2)+k'_{a_2}},C_{(a_{R_2}\cdot b_1)+k'_{a_2}}),(C_{(a_{L_1}\cdot b_2)+k'_{a_1}},C_{(a_{L_2}\cdot b_1)+k'_{a_1}})),\\
&((C_{(a_{L_1}\cdot b_2)+k'_{a_1}},C_{(a_{L_2}\cdot b_1)+k'_{a_1}}),(C_{(a_{R_1}\cdot b_2)+k'_{a_2}},C_{(a_{R_2}\cdot b_1)+k'_{a_2}}))\}.
\end{aligned}$$

敌手 $\mathcal{S}_2^{\Pi_1}$ (或者 Bob)获得 (c'_{L_i},c'_{R_i}) 与 (c_{L_i},c_{R_i}) 后,通过解密运算后,最多只能得到由 4 个方程(其中,每个方程各包含 3 个不同的未知数)组成的方程组,不可能通过联立方程组计算出具体的 $a_{L_1},a_{L_2},a_{R_1},a_{R_2}$.即 $\mathcal{S}_2^{\Pi_1}$ 满足安全定义关系式(1b).

综上,在半诚实模型下,用于保密判定某一有理数是否属于一个上、下界为有理数区间的协议是安全的. □

2.2 数轴上分数范围内的点与区间保密关系测定协议应用举例

点与区间保密关系测定协议可以作为基础模块,用于构造解决保密几何计算[26]与保密社交[27]等问题的协议.而分数范围内的点与区间保密关系测定协议更符合现实应用场景.例如:可用点 a 与区间$[b_L,b_R]$保密关系测定协议解决点 $P(x,y)$与圆面 $x^2+y^2\leqslant b_R^2$ 保密关系测定问题如图 3(a)所示,可以用于解决点 $P(x,y)$与环面 $b_L^2\leqslant x^2+y^2\leqslant b_R^2$ 保密关系测定问题如图 3(b)所示,还可以用于解决点 $P(x,y)$与无限射影区域关系测定问题如图 3(c)所示.



(a) (b) (c)

Fig.3 Relationship between a rational number and a rational interval

图 3 点与区间的关系

3 多维点与区间关系保密测定问题

本节将点与区间关系保密问题拓展成多维点与区间保密关系测定问题.多维点与区间保密关系测定问题具体描述为:不失一般性,假定 Alice 和 Bob 是两个参与者,他们分别拥有保密向量 A=($[a_{11},a_{12}]$,$[a_{21},a_{22}]$,…,$[a_{n1},a_{n2}]$)和 B=($b_1,b_2,\ldots,b_n$),其中,a_{i1} 和 a_{i2} 分别表示第 i 个区间$[a_{i1},a_{i2}]$的下、上界,a_{i1},a_{i2},b_i 是分数形式的实数或有理数,$a_{i1}<a_{i2}$,i=1,2,…,n.Alice 与 Bob 协同完成向量 B 与向量 A 关系的保密测定.具体而言,二者协同完成关系测定:对于任意的 i=1,2,…,n,$a_{i1}\leqslant b_i\leqslant a_{i2}$ 是否都成立,但协同计算不会泄露双方的保密输入,如图 4 所示.

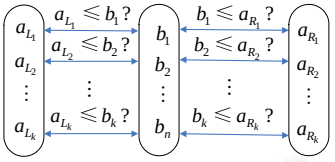


Fig.4 Relationship of multi-dimensional rational point and multi-dimensional rational interval

图 4 多维点与区间的关系

3.1 多维点与区间保密关系测定协议Π_2

协议的输入:Alice 的私有向量 $A=([a_{11},a_{12}],[a_{21},a_{22}],\ldots,[a_{\ell 1},a_{\ell 2}])$ 和 Bob 的私有向量 $B=(b_1,b_2,\ldots,b_\ell)$,其中,$[a_{i1},a_{i2}]$表示一个端点为有理数的连续区间,$a_{i1}$ 与 a_{i2} 分别是此区间的下、上界,b_i 为有理数,i=1,2,…,ℓ.

协议的输出:二进制向量 $O=(O_1,O_2,\ldots,O_\ell)$,其中,$O_i$=0 表示 $b_i\notin[a_{i1},a_{i2}]$,O_i=1 表示 $b_i\in[a_{i1},a_{i2}]$.

准备阶段:Bob 运行密钥生成算法$\mathcal{E}$生成密钥对(K_{Pub},K_{Pri}),其中,K_{Pub}=1+n,K_{Pri}=λ;Alice 和 Bob 分别将他们的 $\boldsymbol{a}_L$ 和 $\boldsymbol{a}_R$,($\boldsymbol{b}$)表示成整数对 $(\hat{a}_{L_i},\breve{a}_{L_i})$ 与 $(\hat{a}_{R_i},\breve{a}_{R_i})$,$((\hat{b}_i,\breve{b}_i))$,使得构成这些整数对的元素满足:

$$\boldsymbol{a}_{L_i}=\frac{\hat{a}_{L_i}}{\breve{a}_{L_i}},\boldsymbol{a}_{R_i}=\frac{\hat{a}_{R_i}}{\breve{a}_{R_i}},\boldsymbol{b}_i=\frac{\hat{b}_i}{\breve{b}_i},\gcd(\hat{a}_{L_i},\breve{a}_{L_i})=\gcd(\hat{a}_{R_i},\breve{a}_{R_i})=\gcd(\hat{b}_i,\breve{b}_i)=1.$$

并行计算阶段:对于 i=1,2,…,ℓ,Alice 与 Bob 按照如下方式协同运算.

Step 1:Bob 利用自己的公钥计算数对 $(\hat{b}_i,\breve{b}_i)$ 对应的密文:

$$C_{\hat{b}_i}=(1+n)^{\hat{b}_i}r_{\breve{b}_i}^n \bmod n^2 \tag{7a}$$

$$C_{\bar{b}_i}=(1+n)^{b_2}r_{\bar{b}_i}^{n} \bmod n^2 \tag{7b}$$

并将密文对 $(C_{\hat{b}_i},C_{\bar{b}_i})$ 发送给 Alice.

Step 2:收到 $(C_{\hat{b}_i},C_{\bar{b}_i})$ 后,Alice 按照如下方式执行.

① 随机选择 6 个长度为$\lfloor \log n-1 \rfloor$的数 $k_{a_1},k_{a_2},k'_{a_1},k'_{a_2},k'_{a_3},k'_{a_4}$ 和 4 个 $r_{a_1},r_{a_2},r_{a_3},r_{a_4}\in Z_n^*$,并利用同态加密,按照如下方式计算密文对 $(C_{(a_{L_2}\cdot b_1)+k'_{a_1}},C_{(a_{L_1}\cdot b_2)+k'_{a_1}}),(C_{(a_{R_2}\cdot b_1)+k'_{a_2}},C_{(a_{R_1}\cdot b_2)+k'_{a_2}})$.

$$C_{(a_{L_2}\cdot b_1)+k'_{a_1}}=((C_{b_1})^{k_{a_1}\cdot a_{L_2}} \bmod n^2)\times(1+k_{a_1}k'_{a_1}n)r_{a_1}^{n} \bmod n^2 \tag{8a}$$

$$C_{(a_{L_1}\cdot b_2)+k'_{a_1}}=((C_{b_2})^{k_{a_1}\cdot a_{L_1}} \bmod n^2)\times(1+k_{a_1}k'_{a_1}n)r_{a_2}^{n} \bmod n^2 \tag{8b}$$

$$C_{(a_{R_2}\cdot b_1)+k'_{a_2}}=((C_{b_1})^{k_{a_2}\cdot a_{R_2}} \bmod n^2)\times(1+k_{a_2}k'_{a_2}n)r_{a_3}^{n} \bmod n^2 \tag{9a}$$

$$C_{(a_{R_1}\cdot b_2)+k'_{a_2}}=((C_{b_2})^{k_{a_2}\cdot a_{R_1}} \bmod n^2)\times(1+k_{a_2}k'_{a_2}n)r_{a_2}^{n} \bmod n^2 \tag{9b}$$

② 随机选择一个密文对:

$$\begin{aligned}((c_{L_1},c_{R_1}),(c_{L_2},c_{R_2}))\in\{&((C_{(a_{L_2}\cdot b_1)+k'_{a_1}},C_{(a_{L_1}\cdot b_2)+k'_{a_1}}),(C_{(a_{R_2}\cdot b_1)+k'_{a_2}},C_{(a_{R_1}\cdot b_2)+k'_{a_2}})),\\ &((C_{(a_{R_2}\cdot b_1)+k'_{a_2}},C_{(a_{R_1}\cdot b_2)+k'_{a_2}}),(C_{(a_{L_2}\cdot b_1)+k'_{a_1}},C_{(a_{L_1}\cdot b_2)+k'_{a_1}})),\\ &((C_{(a_{L_1}\cdot b_2)+k'_{a_1}},C_{(a_{L_2}\cdot b_1)+k'_{a_1}}),(C_{(a_{R_1}\cdot b_2)+k'_{a_2}},C_{(a_{R_2}\cdot b_1)+k'_{a_2}})),\\ &((C_{(a_{R_1}\cdot b_2)+k'_{a_2}},C_{(a_{R_2}\cdot b_1)+k'_{a_2}}),(C_{(a_{L_1}\cdot b_2)+k'_{a_1}},C_{(a_{L_2}\cdot b_1)+k'_{a_1}})),\\ &((C_{(a_{R_2}\cdot b_1)+k'_{a_2}},C_{(a_{R_1}\cdot b_2)+k'_{a_2}}),(C_{(a_{L_2}\cdot b_1)+k'_{a_1}},C_{(a_{L_1}\cdot b_2)+k'_{a_1}})),\\ &((C_{(a_{L_2}\cdot b_1)+k'_{a_1}},C_{(a_{L_1}\cdot b_2)+k'_{a_1}}),(C_{(a_{R_2}\cdot b_1)+k'_{a_2}},C_{(a_{R_1}\cdot b_2)+k'_{a_2}})),\\ &((C_{(a_{L_1}\cdot b_2)+k'_{a_1}},C_{(a_{L_2}\cdot b_1)+k'_{a_1}}),(C_{(a_{R_1}\cdot b_2)+k'_{a_2}},C_{(a_{R_2}\cdot b_1)+k'_{a_2}}))\}\end{aligned}$$

发送给 Bob.

Step 3:收到 $(c_{L_1},c_{R_1}),(c_{L_2},c_{R_2})$ 后,Bob 计算:

$$\partial_i=P\left(\frac{L(c_{L_1}^{\lambda})}{L(c_{R_1}^{\lambda})}\right)P\left(\frac{L(c_{L_2}^{\lambda})}{L(c_{R_2}^{\lambda})}\right),\text{其中},P(X)=\begin{cases}-1, & X\leqslant 1\\ 1, & X>1\end{cases} \tag{10}$$

并将计算结果∂发送给 Alice.

定理 2. 在半诚实模型下,面向有理数的多维点与区间保密测定协议Π_2是计算安全的.

证明:面向有理数的多维点与区间保密测定协议实质是多个(有理数)数与(上、下界为有理数的)区间保密关系测定协议的一次并行执行,因为在第 2.2 节中我们已经证明:在半诚实模型下,有理数与区间(上、下界为有理数的)保密关系测定协议是计算安全的.所以在半诚实模型下,面向分数形式的实数或有理数的多维点与区间保密测定协议也是计算安全的. □

3.2 多维点与区间保密关系测定在保密位置测定中的应用

多维点与区间保密关系测定协议可以作为基础模块,例如:二维点与区间保密关系测定协议可以用于解决点与扇面关系(如图 5(a)所示)的保密测定问题、点与三边形关系(如图 5(b)所示)的保密测定问题以及点与四边形关系(如图 5(c)所示)的保密测定问题;三维点与区间保密关系测定协议可以用于解决点与五边形关系(如图 5(d)所示)的保密测定问题.显然,在研究多维点与区间保密关系测定问题时,如果点和区间端点为有理数或者分数形式的无理数,则更符合现实应用场景.

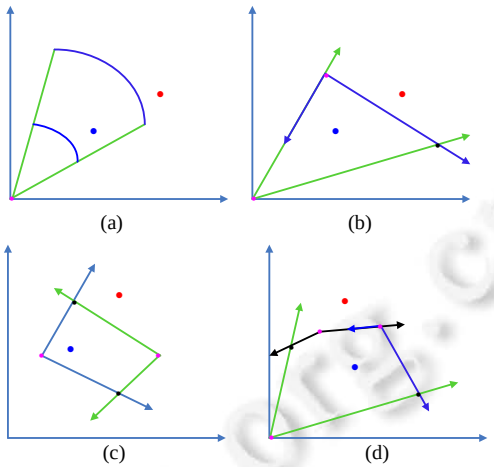


Fig.5 Multi-dimensional relation between a rational number and a rational domain

图 5 点与区间的关系

4 数轴上面向有理数的保密区间关系测定问题

面向有理数的保密区间关系测定问题,实质就是保密测定两个(上下界为有理数的)区间相交与否,并且协同计算完成后不会泄露双方的私有信息 $\boldsymbol{a}_L,\boldsymbol{a}_R,\boldsymbol{b}_L,\boldsymbol{b}_R$ 以及相交区间位于各自区间的哪一端.具体描述如下.

Alice 和 Bob 是分布式环境下的两个实体,他们分别拥有一个(上下界为分数形式的实数或有理数的)区间 $dom_A=[\boldsymbol{a}_L,\boldsymbol{a}_R]$和 $dom_B=[\boldsymbol{b}_L,\boldsymbol{b}_R]$,二者通过协作保密测定两个区间的关系,如果相交,二者协同计算完成后不会泄露双方的私有信息 $\boldsymbol{a}_L,\boldsymbol{a}_R,\boldsymbol{b}_L,\boldsymbol{b}_R$ 以及 $\boldsymbol{a}_L$ 与 $\boldsymbol{b}_R,\boldsymbol{a}_R$ 与 $\boldsymbol{a}_L,\boldsymbol{a}_R,\boldsymbol{b}_L,\boldsymbol{b}_R$ 的大小关系.

4.1 数轴上面向有理数的保密区间关系测定协议Π_3

两个(上下界为有理数的)区间 $dom_A=[\boldsymbol{a}_L,\boldsymbol{a}_R]$和 $dom_B=[\boldsymbol{b}_L,\boldsymbol{b}_R]$的相对位置关系在数轴上表现为 4 种情型,如图 6 所示.

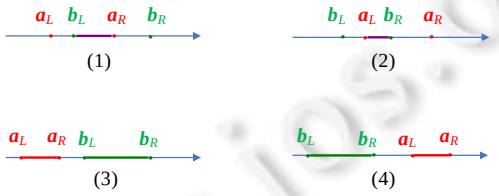


Fig.6 Relationship between two rational intervals

图 6 两有理区间的关系

1. 具体协议.

输入:系统安全参数:$\kappa=\log n$,Alice 的(上、下界为有理数的)区间 $dom_A=[\boldsymbol{a}_L,\boldsymbol{a}_R]$,Bob 的(上、下界为有理数的)区间 $dom_B=[\boldsymbol{b}_L,\boldsymbol{b}_R]$;

输出:$\partial=\begin{cases}1, & dom_B\cap dom_A\neq\varnothing\\ 0, & dom_B\cap dom_A=\varnothing\end{cases}$.

准备工作:Bob 先运行方案$\mathcal{E}$的密钥生成算法,产生公私钥对(K_{Pub},K_{Pri}),其中,$K_{Pub}=1+n,K_{Pri}=\lambda$;Alice 和 Bob 分别将自己的区间 $dom_A=[\boldsymbol{a}_L,\boldsymbol{a}_R],dom_B=[\boldsymbol{b}_L,\boldsymbol{b}_R]$的端点表示成数对形式 $(a_{L_1},a_{L_2}),(a_{R_1},a_{R_2})$ 与 $(b_{L_1},b_{L_2}),(b_{R_1},b_{R_2})$,使得:

$$\boldsymbol{a}_L=\frac{a_{L_1}}{a_{L_2}}\wedge\boldsymbol{a}_R=\frac{a_{R_1}}{a_{R_2}}\wedge\gcd(a_{L_1},a_{L_2})=\gcd(a_{R_1},a_{R_2})=1,\boldsymbol{b}_L=\frac{b_{L_1}}{b_{L_2}}\wedge\boldsymbol{b}_R=\frac{b_{R_1}}{b_{R_2}}\wedge\gcd(b_{L_1},b_{L_2})=\gcd(b_{R_1},b_{R_2})=1.$$

Step 1:Bob 利用自己的公钥将自己的数对 $(b_{L_1},b_{L_2}),(b_{R_1},b_{R_2})$ 加密:

$$C_{b_{L_1}}=(1+n)^{b_{L_1}}r_{b_{L_1}}^n \mod n^2 \tag{11a}$$

$$C_{b_{L_2}}=(1+n)^{b_{L_2}}r_{b_{L_2}}^n \mod n^2 \tag{11b}$$

$$C_{b_{R_1}}=(1+n)^{b_{R_1}}r_{b_{R_1}}^n \mod n^2 \tag{12a}$$

$$C_{b_{R_2}}=(1+n)^{b_{R_2}}r_{b_{R_2}}^n \mod n^2 \tag{12b}$$

并将 $(C_{b_{L_1}},C_{b_{L_2}})$ 和 $(C_{b_{R_1}},C_{b_{R_2}})$ 发送给 Alice;

Step 2:Alice 收到 $(C_{b_{L_1}},C_{b_{L_2}})$ 和 $(C_{b_{R_1}},C_{b_{R_2}})$ 后,按照如下方式工作.

① 对于每一个 $\boldsymbol{a}_I\in\{\boldsymbol{a}_L,\boldsymbol{a}_R\},I\in\{L,R\}$随机选择6个不等的长度为⌊log$n$−1⌋的随机数 $k_{a_{I1}},k_{a_{I2}},k'_{a_{I1}},k'_{a_{I2}},k'_{a_{I3}},k'_{a_{I4}}$ 和 4 个随机数 $r_{a_{I1}},r_{a_{I2}},r_{a_{I3}},r_{a_{I4}}\in Z_n^*$,并利用文献[22]中提出的同态加密方案计算 2 个密文对 $(C_{(a_{I_2}\cdot b_{L_1})+k'_{a_{I1}}},C_{(a_{I_1}\cdot b_{L_2})+k'_{a_{I1}}}),(C_{(a_{I_2}\cdot b_{R_1})+k'_{a_{I2}}},C_{(a_{I_1}\cdot b_{R_2})+k'_{a_{I2}}})$:

$$C_{(a_{I_2}\cdot b_{L_1})+k'_{a_{I1}}}=((C_{b_{L_1}})^{k_{a_{I1}}\cdot a_{L_2}} \mod n^2)\times(1+k_{a_{I1}}k'_{a_{I1}}n)r_{a_{I1}}^n \mod n^2 \tag{13a}$$

$$C_{(a_{I_1}\cdot b_{L_2})+k'_{a_{I1}}}=((C_{b_{L_2}})^{k_{a_{I1}}\cdot a_{L_1}} \mod n^2)\times(1+k_{a_{I1}}k'_{a_{I1}}n)r_{a_{I2}}^n \mod n^2 \tag{13b}$$

$$C_{(a_{I_2}\cdot b_{R_1})+k'_{a_{I2}}}=((C_{b_{L_1}})^{k_{a_{I2}}\cdot a_{L_2}} \mod n^2)\times(1+k_{a_{I2}}k'_{a_{I2}}n)r_{a_{I3}}^n \mod n^2 \tag{14a}$$

$$C_{(a_{I_1}\cdot b_{R_2})+k'_{a_{I2}}}=((C_{b_{L_2}})^{k_{a_{I2}}\cdot a_{L_1}} \mod n^2)\times(1+k_{a_{I2}}k'_{a_{I2}}n)r_{a_{I4}}^n \mod n^2 \tag{14b}$$

② 对密文对 $(C_{(a_{I_2}\cdot b_{L_1})+k'_{a_{I1}}},C_{(a_{I_1}\cdot b_{L_2})+k'_{a_{I1}}})$ 和 $(C_{(a_{I_2}\cdot b_{R_1})+k'_{a_{I2}}},C_{(a_{I_1}\cdot b_{R_2})+k'_{a_{I2}}})$ 同时在组内实施一致的元组元素间的随机置换,然后再对两个密文对实施对间随机置换,得到密文对序列 $(c_{L_{I1}},c_{R_{I1}}),(c_{L_{I2}},c_{R_{I2}})$,即随机选择一个:

$$\begin{aligned}((c_{L_{I1}},c_{R_{I1}}),(c_{L_{I2}},c_{R_{I2}}))\in\{&((C_{(a_{I_2}\cdot b_{L_1})+k'_{a_{I1}}},C_{(a_{I_1}\cdot b_{L_2})+k'_{a_{I1}}}),(C_{(a_{I_2}\cdot b_{R_1})+k'_{a_{I2}}},C_{(a_{I_1}\cdot b_{R_2})+k'_{a_{I2}}})),\\&((C_{(a_{I_2}\cdot b_{R_1})+k'_{a_{I2}}},C_{(a_{I_1}\cdot b_{R_2})+k'_{a_{I2}}}),(C_{(a_{I_2}\cdot b_{L_1})+k'_{a_{I1}}},C_{(a_{I_1}\cdot b_{L_2})+k'_{a_{I1}}})),\\&((C_{(a_{I_1}\cdot b_{L_2})+k'_{a_{I1}}},C_{(a_{I_2}\cdot b_{L_1})+k'_{a_{I1}}}),(C_{(a_{I_1}\cdot b_{R_2})+k'_{a_{I2}}},C_{(a_{I_2}\cdot b_{R_1})+k'_{a_{I2}}})),\\&((C_{(a_{I_1}\cdot b_{R_2})+k'_{a_{I2}}},C_{(a_{I_2}\cdot b_{R_1})+k'_{a_{I2}}}),(C_{(a_{I_1}\ b_{L_2})+k'_{a_{I1}}},C_{(a_{I_2}\ b_{L_1})+k'_{a_{I1}}}))\}\end{aligned}$$

并发给 Bob.

Step 3:Bob 收到 $(c_{L_{I1}},c_{R_{I1}}),(c_{L_{I2}},c_{R_{I2}})$ 后计算:

$$\left(P\left(\frac{L(c_{L_{I1}}^{\lambda})}{L(c_{R_{I1}}^{\lambda})}\right),P\left(\frac{L(c_{L_{I2}}^{\lambda})}{L(c_{R_{I2}}^{\lambda})}\right)\right),\text{其中},I\in\{L,R\},P(X)=\begin{cases}-1, & X\leqslant 1\\ 1, & X>1\end{cases} \tag{15}$$

然后,将 $\left(P\left(\frac{L(c_{L_{I1}}^{\lambda})}{L(c_{R_{I1}}^{\lambda})}\right),P\left(\frac{L(c_{L_{I2}}^{\lambda})}{L(c_{R_{I2}}^{\lambda})}\right)\right)$ 发送给 Alice.

Step 4:Bob 和 Alice 根据元组 $\left(\left(P\left(\frac{L(c_{L_{L1}}^{\lambda})}{L(c_{R_{L1}}^{\lambda})}\right),P\left(\frac{L(c_{L_{L2}}^{\lambda})}{L(c_{R_{L2}}^{\lambda})}\right)\right),\left(P\left(\frac{L(c_{L_{R1}}^{\lambda})}{L(c_{R_{R1}}^{\lambda})}\right),P\left(\frac{L(c_{L_{R2}}^{\lambda})}{L(c_{R_{R2}}^{\lambda})}\right)\right)\right)$ 可以得出两数域相交与否(如果元组为((−1,1),(−1,1)),((−1,1),(1,−1)),((1,−1),(−1,1)),((1,−1),(1,−1))中之一,则二者相交).

2. 数理计算的正确性.

(1) 如果 $\boldsymbol{b}_L\in dom_A$,即 $\boldsymbol{a}_L<\boldsymbol{b}_L<\boldsymbol{a}_R$,则有 $\frac{\boldsymbol{a}_L}{\boldsymbol{b}_L}\leqslant 1,\frac{\boldsymbol{a}_R}{\boldsymbol{b}_L}\geqslant 1$,所以 $\frac{\boldsymbol{a}_L}{\boldsymbol{b}_L},\frac{\boldsymbol{a}_R}{\boldsymbol{b}_L}$ 经函数 $P(X)=\begin{cases}-1, & X\leqslant 1\\ 1, & X>1\end{cases}$ 作用后的乘积:

$$\partial=P\left(\frac{\boldsymbol{a}_L}{\boldsymbol{b}_L}\right)\cdot P\left(\frac{\boldsymbol{a}_R}{\boldsymbol{b}_L}\right)=-1;$$

(2) 如果 $\boldsymbol{b}_R\in dom_A$,即 $\boldsymbol{a}_L<\boldsymbol{b}_R<\boldsymbol{a}_R$,则有 $\frac{\boldsymbol{a}_L}{\boldsymbol{b}_R}\leqslant 1,\frac{\boldsymbol{a}_R}{\boldsymbol{b}_R}\geqslant 1$,所以 $\frac{\boldsymbol{a}_L}{\boldsymbol{b}_R},\frac{\boldsymbol{a}_R}{\boldsymbol{b}_R}$ 经函数 $P(X)=\begin{cases}-1, & X\leqslant 1\\ 1, & X>1\end{cases}$ 作用后的乘积:

$$\partial = P\left(\frac{\boldsymbol{a}_L}{\boldsymbol{b}_R}\right)\cdot P\left(\frac{\boldsymbol{a}_R}{\boldsymbol{b}_R}\right)=-1;$$

(3) 如果$(\boldsymbol{b}_R\notin dom_A)\wedge(\boldsymbol{b}_R<\boldsymbol{a}_L)$,则有 $\frac{\boldsymbol{a}_L}{\boldsymbol{b}_R}>1,\frac{\boldsymbol{a}_R}{\boldsymbol{b}_R}>1$,因此 $\frac{\boldsymbol{a}_L}{\boldsymbol{b}},\frac{\boldsymbol{a}_R}{\boldsymbol{b}}$ 经函数 $P(X)=\begin{cases}-1, & X\leqslant 1\\ 1, & X>1\end{cases}$ 作用后的乘积:

$$\partial = P\left(\frac{\boldsymbol{a}_L}{\boldsymbol{b}}\right)\cdot P\left(\frac{\boldsymbol{a}_R}{\boldsymbol{b}}\right)=(-1)\cdot(-1)=1;$$

(4) 如果$(\boldsymbol{b}_L\notin dom_A)\wedge(\boldsymbol{a}_R<\boldsymbol{b}_L)$,则有 $\frac{\boldsymbol{a}_L}{\boldsymbol{b}_L}<1,\frac{\boldsymbol{a}_R}{\boldsymbol{b}_L}<1$,因此 $\frac{\boldsymbol{a}_L}{\boldsymbol{b}_L},\frac{\boldsymbol{a}_R}{\boldsymbol{b}_L}$ 经函数 $P(X)=\begin{cases}-1, & X\leqslant 1\\ 1, & X>1\end{cases}$ 作用后的乘积:

$$\partial = P\left(\frac{\boldsymbol{a}_L}{\boldsymbol{b}_L}\right)\cdot P\left(\frac{\boldsymbol{a}_R}{\boldsymbol{b}_L}\right)=1\cdot 1=1.$$

3. 安全性

定理 3. 在半诚实模型下,保密判两个(上、下界为有理数的)区间关系的协议Π_3是计算安全的.

证明:衡量保密判定两个(上、下界为有理数的)区间关系协议的安全性,关键是看协议执行结束后有没有造成 Alice 与 Bob 两方私有信息的泄露.下面将严格按照定义 1 与定义 2 声明的安全标准和方法证明:通过协同执行保密判两个(上、下界为有理数的)区间关系的协议,Alice 与 Bob 会得到保密计算结果(区间相交与否),但不会向对方泄露各自的具体数值$(\boldsymbol{a}_L,\boldsymbol{a}_R,\boldsymbol{b}_L,\boldsymbol{b}_R)$以及它们的大小关系.

I. Bob 私有信息在Π_3执行完毕后是安全的:

在最坏的情形下,即在 Alice 受控于攻击者的情形下,构造一个模拟器 $\mathcal{S}_1^{\Pi_3}$ 模拟协议Π_3的执行过程.显然,模拟器是潜在的、能力最强的攻击者.如果多项式时间内的敌手 $\mathcal{S}_1^{\Pi_3}$ 获得的信息并不多于 Alice 在实际执行协议中的视图内容,则称协议Π_3执行完成后没有造成 Bob 具体数值 $\boldsymbol{b}_L,\boldsymbol{b}_R$ 的泄露,即 Bob 私有信息是安全的.

构造一个在最坏的情形下,即在 Alice 受敌手控制的情形下、能够在多项式时间内模拟协议Π_3整个执行过程的模拟器 $\mathcal{S}_1^{\Pi_3}$,其输入为:敌手根据 Alice(上、下界为有理数的)区间的下、上界 $\boldsymbol{a}_L,\boldsymbol{a}_R$ 随机选择利于它获取 Bob 数值 $\boldsymbol{b}_L,\boldsymbol{b}_R$ 的两个有理数 $\boldsymbol{a}'_L,\boldsymbol{a}'_R$、Bob 随机选择的 4 个不等的随机数 $r_{b_{L_1}},r_{b_{L_2}},r_{b_{R_1}},r_{b_{R_2}}\in Z_n^*$ 以及 Bob 的有理数对应的整型有序对表示 $(b_{L_1},b_{L_2}),(b_{R_1},b_{R_2})(\gcd(b_{L_1},b_{L_2})=1,\gcd(b_{R_1},b_{R_2})=1)$.作为能力最强的、多项式时间内的敌手,模拟器 $\mathcal{S}_1^{\Pi_3}$ 产生的视图为$((C_{b_{L_1}},C_{b_{L_2}}),(C_{b_{R_1}},C_{b_{R_2}}),(c'_{L_{I1}},c'_{R_{I1}}),(c'_{L_{I2}},c'_{R_{I2}}),I\in\{L,R\})$,其中,

$$C_{(a'_{I_2}\cdot b_{L_1})+k'_{a'_{I1}}}=((C_{b_{L_1}})^{k_{a'_{I1}}\cdot a'_{L_2}}\bmod n^2)\times(1+k_{a'_{I1}}k'_{a'_{I1}}n)r_{a'_{I1}}^n \bmod n^2,$$

$$C_{(a'_{I_1}\cdot b_{L_2})+k'_{a'_{I1}}}=((C_{b_{L_2}})^{k_{a'_{I1}}\cdot a'_{L_1}}\bmod n^2)\times(1+k_{a'_{I1}}k'_{a'_{I1}}n)r_{a'_{I2}}^n \bmod n^2,$$

$$C_{(a'_{I_2}\cdot b_{R_1})+k'_{a'_{I2}}}=((C_{b_{L_1}})^{k_{a'_{I2}}\cdot a'_{L_2}}\bmod n^2)\times(1+k_{a'_{I2}}k'_{a'_{I2}}n)r_{a'_{I3}}^n \bmod n^2,$$

$$C_{(a'_{I_1}\cdot b_{R_2})+k'_{a'_{I2}}}=((C_{b_{L_2}})^{k_{a'_{I2}}\cdot a'_{L_1}}\bmod n^2)\times(1+k_{a'_{I2}}k'_{a'_{I2}}n)r_{a'_{I4}}^n \bmod n^2;$$

$$\begin{aligned}(c'_{L_{I1}},c'_{R_{I1}}),(c'_{L_{I2}},c'_{R_{I2}})\in\{&((C_{(a'_{I_2}\cdot b_{L_1})+k'_{a'_{I1}}},C_{(a'_{I_1}\cdot b_{L_2})+k'_{a'_{I1}}}),(C_{(a'_{I_2}\cdot b_{R_1})+k'_{a'_{I2}}},C_{(a'_{I_1}\cdot b_{R_2})+k'_{a'_{I2}}})),\\ &((C_{(a'_{I_2}\cdot b_{R_1})+k'_{a'_{I2}}},C_{(a'_{I_1}\cdot b_{R_2})+k'_{a'_{I2}}}),(C_{(a'_{I_2}\cdot b_{L_1})+k'_{a'_{I1}}},C_{(a'_{I_1}\cdot b_{L_2})+k'_{a'_{I1}}})),\\ &((C_{(a'_{I_1}\cdot b_{L_2})+k'_{a'_{I1}}},C_{(a'_{I_2}\cdot b_{L_1})+k'_{a'_{I1}}}),(C_{(a'_{I_1}\cdot b_{R_2})+k'_{a'_{I2}}},C_{(a'_{I_2}\cdot b_{R_1})+k'_{a'_{I2}}})),\\ &((C_{(a'_{I_1}\cdot b_{R_2})+k'_{a'_{I2}}},C_{(a'_{I_2}\cdot b_{R_1})+k'_{a'_{I2}}}),(C_{(a'_{I_1}\cdot b_{L_2})+k'_{a'_{I1}}},C_{(a'_{I_2}\cdot b_{L_1})+k'_{a'_{I1}}}))\}.\end{aligned}$$

而 Alice 在实际执行协议Π_3中产生的视图为$((C_{b_{L_1}},C_{b_{L_2}}),(C_{b_{R_1}},C_{b_{R_2}}),(c_{L_{I1}},c_{R_{I1}}),(c_{L_{I2}},c_{R_{I2}}),I\in\{L,R\})$,其中,

$$C_{(a_{I_2}\cdot b_{L_1})+k'_{a_{I1}}}=((C_{b_{L_1}})^{k_{a_{I1}}\cdot a_{L_2}} \bmod n^2)\times(1+k_{a_{I1}}k'_{a_{I1}}n)r_{a_{I1}}^n \bmod n^2,$$

$$C_{(a_{I_1}\cdot b_{L_2})+k'_{a_{I1}}}=((C_{b_{L_2}})^{k_{a_{I1}}\cdot a_{L_1}} \bmod n^2)\times(1+k_{a_{I1}}k'_{a_{I1}}n)r_{a_{I2}}^n \bmod n^2,$$

$$C_{(a_{I_2}\cdot b_{R_1})+k'_{a_{I2}}}=((C_{b_{L_1}})^{k_{a_{I2}}\cdot a_{L_2}} \bmod n^2)\times(1+k_{a_{I2}}k'_{a_{I2}}n)r_{a_{I3}}^n \bmod n^2,$$

$$C_{(a_{I_1}\cdot b_{R_2})+k'_{a_{I2}}}=((C_{b_{L_2}})^{k_{a_{I2}}\cdot a_{L_1}} \bmod n^2)\times(1+k_{a_{I2}}k'_{a_{I2}}n)r_{a_{I4}}^n \bmod n^2;$$

$$\begin{aligned}(c_{L_{I1}},c_{R_{I1}}),(c_{L_{I2}},c_{R_{I2}})\in\{&((C_{(a_{I_2}\cdot b_{L_1})+k'_{a_{I1}}},C_{(a_{I_1}\cdot b_{L_2})+k'_{a_{I1}}}),(C_{(a_{I_2}\cdot b_{R_1})+k'_{a_{I2}}},C_{(a_{I_1}\cdot b_{R_2})+k'_{a_{I2}}})),\\&((C_{(a_{I_2}\cdot b_{R_1})+k'_{a_{I2}}},C_{(a_{I_1}\cdot b_{R_2})+k'_{a_{I2}}}),(C_{(a_{I_2}\cdot b_{L_1})+k'_{a_{I1}}},C_{(a_{I_1}\cdot b_{L_2})+k'_{a_{I1}}})),\\&((C_{(a_{I_1}\cdot b_{L_2})+k'_{a_{I1}}},C_{(a_{I_2}\cdot b_{L_1})+k'_{a_{I1}}}),(C_{(a_{I_1}\cdot b_{R_2})+k'_{a_{I2}}},C_{(a_{I_2}\cdot b_{R_1})+k'_{a_{I2}}})),\\&((C_{(a_{I_1}\cdot b_{R_2})+k'_{a_{I2}}},C_{(a_{I_2}\cdot b_{R_1})+k'_{a_{I2}}}),(C_{(a_{I_1}\cdot b_{L_2})+k'_{a_{I1}}},C_{(a_{I_2}\cdot b_{L_1})+k'_{a_{I1}}}))\}.\end{aligned}$$

无论在模拟协议还是实际协议中,Alice 接收到的有关 Bob(或 $\mathcal{S}_1^{\Pi_3}$)的信息都是经$\mathcal{E}$加密后的密文,一方面,因为 Alice 没有$\mathcal{E}$的解密密钥;另一方面,又因方案$\mathcal{E}$已被证明在选择明文攻击下具有语义不可区分安全,即经加密方案$\mathcal{E}$加密生成的密文是语义不可区分的.因此可得:模拟视图$((C_{b_{L_1}},C_{b_{L_2}}),(C_{b_{R_1}},C_{b_{R_2}}),(c'_{L_{I1}},c'_{R_{I1}}),(c'_{L_{I2}},c'_{R_{I2}}),I\in\{L,R\})$与真实视图$((C_{b_{L_1}},C_{b_{L_2}}),(C_{b_{R_1}},C_{b_{R_2}}),(c_{L_{I1}},c_{R_{I1}}),(c_{L_{I2}},c_{R_{I2}}),I\in\{L,R\})$是计算不可区分的.也就说,$\mathcal{S}_1^{\Pi_3}$ 满足安全定义关系式(1a).

II. Alice 私有信息在Π_3执行完毕后是安全的.

在最坏的情形下,即在 Bob 受控于攻击者的情形下,构造一个模拟器 $\mathcal{S}_2^{\Pi_3}$ 模拟协议Π_3 的执行过程.显然,模拟器是潜在的、能力最强的攻击者.如果多项式时间内的敌手 $\mathcal{S}_2^{\Pi_3}$ 获得的信息并不多于 Bob 在实际执行协议中的视图内容,则称协议Π_3完成后没有造成 Alice(上、下界为有理数的)区间下、上界 $\boldsymbol{a}_L,\boldsymbol{a}_R$ 的泄露,即 Alice 私有信息是安全的.

假定敌手 $\mathcal{S}_2^{\Pi_3}$ 控制着 Bob,并且在 Bob 不参与的情况下,能够在多项时间内模拟协议Π_3执行的全过程.如果在该假定条件下,多项式时间内的敌手 $\mathcal{S}_2^{\Pi_3}$ 获得的信息并不多于 Bob 在实际执行协议中的视图内容,则 Alice 私有信息((上、下界为有理数的)区间的下、上界 $\boldsymbol{a}_L,\boldsymbol{a}_R$)是安全的.

首先构造一个在 Bob 受敌手控制的情形下、能够在多项式时间内模拟协议Π_3整个执行过程的模拟器 $\mathcal{S}_2^{\Pi_3}$,其输入为:敌手根据 Bob(有理数的)区间端点 $\boldsymbol{b}_L,\boldsymbol{b}_R$ 随机选择利于它获取 Alice 有理数域的下、上界 $\boldsymbol{a}_L,\boldsymbol{a}_R$ 的数值 $\boldsymbol{b}'_L,\boldsymbol{b}'_R$、Bob 随机选择的两个不等的随机数 $r_{b_{L_1}},r_{b_{L_2}},r_{b_{R_1}},r_{b_{R_2}}\in Z_n^*$ 以及 Alice 有理数域的下、上界 $\boldsymbol{a}_L,\boldsymbol{a}_R$ 对应的整型有序对表示 $(a_{L_1},a_{L_2}),(a_{R_1},a_{R_2})$(其中,$\gcd(a_{L_1},a_{L_2})=1,\gcd(a_{R_1},a_{R_2})=1$).作为潜在的、能力最强的敌手,模拟器 $\mathcal{S}_2^{\Pi_3}$ 产生的视图为 $(C_{b'_{L_1}},C_{b'_{L_2}}),(C_{b'_{R_1}},C_{b'_{R_2}}),(c'_{L_{I1}},c'_{R_{I1}}),(c'_{L_{I2}},c'_{R_{I2}})$),其中:$C_{b'_{L_1}},C_{b'_{L_2}},C_{b'_{R_1}},C_{b'_{R_2}}$ 是 $\mathcal{S}_2^{\Pi_3}$ 利用 Bob 的公钥通过计算 $C_{b'_{L_1}}=(1+n)^{b'_{L_1}}r_{b_{L_1}}^n \bmod n^2, C_{b'_{L_2}}=(1+n)^{b'_{L_2}}r_{b_{L_2}}^n \bmod n^2, C_{b'_{R_1}}=(1+n)^{b'_{R_1}}r_{b_{R_1}}^n \bmod n^2, C_{b'_{R_2}}=(1+n)^{b'_{R_2}}r_{b_{R_2}}^n \bmod n^2$ 得到的;密文 $(c'_{L_{I1}},c'_{R_{I1}}),(c'_{L_{I2}},c'_{R_{I2}})$ 是 Alice 经过下述方式构造的.

(1) 由密文 $C_{b'_{L_1}},C_{b'_{L_2}},C_{b'_{R_1}},C_{b'_{R_2}}$,利用方案$\mathcal{E}$计算:

$$C_{(a_{I_2}\cdot b'_{L_1})+k'_{a_{I1}}}=((C_{b'_{L_1}})^{k_{a_{I1}}\cdot a_{L_2}} \bmod n^2)\times(1+k_{a_{I1}}k'_{a_{I1}}n)r_{a_{I1}}^n \bmod n^2,$$

$$C_{(a_{I_1}\cdot b'_{L_2})+k'_{a_{I1}}}=((C_{b'_{L_2}})^{k_{a_{I1}}\cdot a_{L_1}} \bmod n^2)\times(1+k_{a_{I1}}k'_{a_{I1}}n)r_{a_{I2}}^n \bmod n^2,$$

$$C_{(a_{I_2}\cdot b'_{R_1})+k'_{a_{I2}}}=((C_{b'_{L_1}})^{k_{a_{I2}}\cdot a_{L_2}} \bmod n^2)\times(1+k_{a_{I2}}k'_{a_{I2}}n)r_{a_{I3}}^n \bmod n^2,$$

$$C_{(a_{I_1}\cdot b'_{R_2})+k'_{a_{I2}}}=((C_{b'_{L_2}})^{k_{a_{I2}}\cdot a_{L_1}} \bmod n^2)\times(1+k_{a_{I2}}k'_{a_{I2}}n)r_{a_{I4}}^n \bmod n^2;$$

(2) 随机选取一个:

$$((c'_{L_{I1}},c'_{R_{I1}}),(c'_{L_{I2}},c'_{R_{I2}}))\in\{((C_{(a_{I_2}\cdot b'_{L_1})+k'_{aI1}},C_{(a_{I_1}\cdot b'_{L_2})+k'_{aI1}}),(C_{(a_{I_2}\cdot b'_{R_1})+k'_{aI2}},C_{(a_{I_1}\cdot b'_{R_2})+k'_{aI2}})),$$
$$((C_{(a_{I_2}\cdot b'_{R_1})+k'_{aI2}},C_{(a_{I_1}\cdot b'_{R_2})+k'_{aI2}}),(C_{(a_{I_2}\cdot b'_{L_1})+k'_{aI1}},C_{(a_{I_1}\cdot b'_{L_2})+k'_{aI1}})),$$
$$((C_{(a_{I_1}\cdot b'_{L_2})+k'_{aI1}},C_{(a_{I_2}\cdot b'_{L_1})+k'_{aI1}}),(C_{(a_{I_1}\cdot b'_{R_2})+k'_{aI2}},C_{(a_{I_2}\cdot b'_{R_1})+k'_{aI2}})),$$
$$((C_{(a_{I_1}\cdot b'_{R_2})+k'_{aI2}},C_{(a_{I_2}\cdot b'_{R_1})+k'_{aI2}}),(C_{(a_{I_1}\cdot b'_{L_2})+k'_{aI1}},C_{(a_{I_2}\cdot b'_{L_1})+k'_{aI1}}))\}.$$

而 Alice 在实际中执行协议Π_3生成的实际视图为$((C_{b_{L_1}},C_{b_{L_2}}),(C_{b_{R_1}},C_{b_{R_2}}),(c_{L_{I1}},c_{R_{I1}}),(c_{L_{I2}},c_{R_{I2}}),I\in\{L,R\})$,其中,

- $C_{b_{L_1}},C_{b_{L_2}}),(C_{b_{R_1}},C_{b_{R_2}})$是 Bob 利用自己的公钥通过计算$C_{b_{L_1}}=(1+n)^{b_{L_1}}r_{b_{L_1}}^n \bmod n^2, C_{b_{L_2}}=(1+n)^{b_{L_2}}r_{b_{L_2}}^n \bmod n^2, C_{b_{R_1}}=(1+n)^{b_{R_1}}r_{b_{R_1}}^n \bmod n^2, C_{b_{R_2}}=(1+n)^{b_{R_2}}r_{b_{R_2}}^n \bmod n^2$得到的;
- 密文$(c_{L_{I1}},c_{R_{I1}}),(c_{L_{I2}},c_{R_{I2}}),I\in\{L,R\}$是 Alice 经过下述方式构造的.

① 由密文$C_{b_{L_1}},C_{b_{L_2}},C_{b_{R_1}},C_{b_{R_2}}$,利用方案$\mathcal{E}$同态性计算得到:

$$C_{(a_{I_2}\cdot b_{L_1})+k'_{aI1}}=((C_{b_{L_1}})^{k_{aI1}\cdot a_{L_2}} \bmod n^2)\times(1+k_{a_{I1}}k'_{a_{I1}}n)r_{a_{I1}}^n \bmod n^2,$$
$$C_{(a_{I_1}\cdot b_{L_2})+k'_{aI1}}=((C_{b_{L_2}})^{k_{aI1}\cdot a_{L_1}} \bmod n^2)\times(1+k_{a_{I1}}k'_{a_{I1}}n)r_{a_{I2}}^n \bmod n^2,$$
$$C_{(a_{I_2}\cdot b_{R_1})+k'_{aI2}}=((C_{b_{L_1}})^{k_{aI2}\cdot a_{L_2}} \bmod n^2)\times(1+k_{a_{I2}}k'_{a_{I2}}n)r_{a_{I3}}^n \bmod n^2,$$
$$C_{(a_{I_1}\cdot b_{R_2})+k'_{aI2}}=((C_{b_{L_2}})^{k_{aI2}\cdot a_{L_1}} \bmod n^2)\times(1+k_{a_{I2}}k'_{a_{I2}}n)r_{a_{I4}}^n \bmod n^2;$$

② 随机选择一个:

$$((c_{L_{I1}},c_{R_{I1}}),(c_{L_{I2}},c_{R_{I2}}))\in\{((C_{(a_{I_2}\cdot b_{L_1})+k'_{aI1}},C_{(a_{I_1}\cdot b_{L_2})+k'_{aI1}}),(C_{(a_{I_2}\cdot b_{R_1})+k'_{aI2}},C_{(a_{I_1}\cdot b_{R_2})+k'_{aI2}})),$$
$$((C_{(a_{I_2}\cdot b_{R_1})+k'_{aI2}},C_{(a_{I_1}\cdot b_{R_2})+k'_{aI2}}),(C_{(a_{I_2}\cdot b_{L_1})+k'_{aI1}},C_{(a_{I_1}\cdot b_{L_2})+k'_{aI1}})),$$
$$((C_{(a_{I_1}\cdot b_{L_2})+k'_{aI1}},C_{(a_{I_2}\cdot b_{L_1})+k'_{aI1}}),(C_{(a_{I_1}\cdot b_{R_2})+k'_{aI2}},C_{(a_{I_2}\cdot b_{R_1})+k'_{aI2}})),$$
$$((C_{(a_{I_1}\cdot b_{R_2})+k'_{aI2}},C_{(a_{I_2}\cdot b_{R_1})+k'_{aI2}}),(C_{(a_{I_1}\cdot b_{L_2})+k'_{aI1}},C_{(a_{I_2}\cdot b_{L_1})+k'_{aI1}}))\}.$$

敌手$\mathcal{S}_2^{\Pi_3}$(或者 Bob)获得$(c_{L_{I1}},c_{R_{I1}}),(c_{L_{I2}},c_{R_{I2}}),I\in\{L,R\}$后,通过解密运算后,最多只能得到由 8 个方程(其中,每个方程各包含 3 个不同的未知数)组成的方程组,不可能通过联立方程组计算出具体的$a_{L_1},a_{L_2},a_{R_1},a_{R_2}$.这也就说,$\mathcal{S}_2^{\Pi_3}$满足安全定义关系式(1b).

综上所述,在半诚实模型下,保密判定某一有理数是否属于一个有理数域协议是安全的. □

5 比较分析

文献[20]采用几何保密计算方法解决了有理点与有理区间关系的保密测定问题,但该协议在调用 Paillier 同态加密方案的基础上,还需要 3 次调用百万富翁协议;文献[21]采用比特值串联和放大倍数的思想,试图解决一个实数点是与一个连续实数区间关系测定问题,但该协议并未考虑下列不成功的情形:假定实数点为 a=30.0000000073,连续实数区间的一个端点为 b_j=30.0000000073221,$j\in\{L,R\}$,L,R 分别用于标识一个区间的下、上界,如果采用该方法都扩大 10^{10} 后再作为保密输入解决一个实数点是与一个连续实数区间关系测定问题,不但不能解决问题,还给协议带来繁重的计算开销;本文协议Π_1 利用保密比值计算思想解决了面向分数形式的实数或有理数的点与区间关系的保密测定问题,较之于文献[20,21]拓展了解决问题的范围,较之于文献[20],Π_1 无需调用复杂的百万富翁协议;协议Π_2 和Π_3 所解决的问题是新问题,属于首次提出.表 1 是本文协议Π_1~Π_3 与文献[20]中的协议和文献[21]中的协议从解决问题的范围、是否彻底解决所提出的问题、是否需要调用百万富翁协议以及是否是新问题 4 个方面的比较分析.

Table 1 Comparative analysis of secure interval computing protocols
表 1 保密区间计算协议间的对比分析

协议	解决问题的范围	是否彻底解决所提出的问题	是否需要调用百万富翁协议	是否是新问题
文献[20]中的协议	有理数	✓	✓	×
文献[21]中的协议	声称实数	×	×	×
Π_1	有理数	✓	×	×
Π_2	有理数	✓	×	✓
Π_3	有理数	✓	×	✓

注:✓表示具有某种性能,×表示不具有某种性能

6 结束语

本文首先提出数轴上的保密关系测定问题应当分为3个值得研究的子问题:(1) 点与区间关系的保密测定;(2) 多维点与区间保密关系测定;(3) 区间与区间关系的保密测定.然后采用“两个数的安全比值与 1 的关系判定两个数的大小”的方法,基于同态加密设计了 3 个高效的保密区间计算协议.最后,采用模拟范例(ideal/real)分析了3个协议的安全性.分析表明:(1) 这3个协议突破了 Paillier 等加密方案不能进行保密差值计算的瓶颈;(2) 这 3 个协议还可以作为基础模块用于解决其他若干安全多方计算问题,例如保密点与圆环区域关系判定问题、点与凸多边形位置关系判定问题、保密近感探测问题等.而如何解决无理数轴上的一个无理数一次同时与两个无理数的安全比较依然是个开问题,需要进一步探索解决.

References:

[1] Yao ACC. Protocols for secure computations. In: Proc. of the 23rd Annual Symp. on Foundations of Computer Science (SFCS'82). Washington: IEEE Computer Society Press, 1982. 160−164.

[2] Liu S, Qu Q, Chen L, Ni LM. SMC: A practical schema for privacy-preserved data sharing over distributed data streams. IEEE Trans. on Big Data, 2015,1(2):68−81.

[3] Xu L, Jiang C, Chen Y, Wang J, Ren Y. A framework for categorizing and applying privacy-preservation techniques in big data mining. Computer, 2016,49(2):54−62.

[4] Xu L, Jiang C, Wang J, Yuan J, Ren Y. Information security in big data: privacy and data mining. IEEE Access, 2014,2:1149−1176.

[5] Sharma S, Chen K, Sheth A. Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems. IEEE Internet Computing, 2018,22(2):42−51.

[6] Zhang L, Li XY, Liu K, Jung T, Liu YH. Message in a sealed bottle: Privacy preserving friending in mobile social networks. IEEE Trans. on Mobile Computing, 2015,14(9):1888−1902.

[7] Zhang L, Jung T, Liu C, Li X, Liu Y. Pop: Privacy-preserving outsourced photo sharing and searching for mobile devices. In: Proc. of the 2015 IEEE 35th Int'l Conf. on Distributed Computing Systems. Washington: IEEE, 2015. 308−317.

[8] Saranya K, Premalatha K, Rajasekar SS. A survey on privacy preserving data mining. In: Proc. of the 2015 2nd Int'l Conf. on Electronics and Communication Systems (ICECS). Washington: IEEE, 2015. 1740−1744.

[9] Boudot F, Schoenmakers B, Traore J. A fair and efficient solution to the socialist millionaires' problem. Discrete Applied Mathematics, 2001,111(1-2):23−36.

[10] Fischlin M. A cost-effective pay-per-multiplication comparison method for millionaires. In: Proc. of the Cryptographers' Track at the RSA Conf. Berlin, Heidelberg: Springer-Verlag, 2001. 457−471.

[11] Goldwasser S, Micali S. Probabilistic encryption. Journal of Computer and System Sciences, 1984,28(2):270−299.

[12] Ioannidis I, Grama A. An efficient protocol for Yao's millionaires' problem. In: Proc. of the 36th Annual Hawaii Int'l Conf. on IEEE. Washington: IEEE, 2003.

[13] Li SD, Dai YQ, You QY. Efficient solution to Yao's Millionaires' problem. Dianzi Xuebao (Acta Electronica Sinica), 2005,33(5): 769−773 (in Chinese with English abstract).

[14] Lin HY, Tzeng WG. An efficient solution to the millionaires' problem based on homomorphic encryption. In: Proc. of the Int'l Conf. on Applied Cryptography and Network Security. Berlin, Heidelberg: Springer-Verlag, 2005. 456−466.

[15] Garay J, Schoenmakers B, Villegas J. Practical and secure solutions for integer comparison. In: Proc. of the Int'l Workshop on Public Key Cryptography. Berlin, Heidelberg: Springer-Verlag, 2007. 330−342.

[16] Li SD, Wang DS. Efficient secure multiparty computation based on homomorphic encryption. Dianzi Xuebao (Acta Electronica Sinica), 2013,41(4):798−803 (in Chinese with English abstract).

[17] Gordon SD, Hazay C, Katz J, Lindell Y. Complete fairness in secure two-party computation. Journal of the ACM, 2008,(6):303.
[18] Shundong L, Daoshun W, Yiqi D, Ping L. Symmetric cryptographic solution to Yao's millionaires' problem and an evaluation of secure multiparty computations. Information Sciences, 2008,178(1):244−255.
[19] Nishide T, Ohta K. Multiparty computation for interval, equality, and comparison without bit-decomposition protocol. In: Proc. of the Int'l Workshop on Public Key Cryptography. Berlin, Heidelberg: Springer-Verlag, 2007. 343−360.
[20] Guo YM, Zhou SF, Dou JW, Li SD, Wang DS. Efficient privacy-preserving interval computation and its applications. Chinese Journal of Computers, 2016,39:1−17 (in Chinese with English abstract).
[21] Chen ZH, Li SD, Chen LC, Huang Q, Zhang WG. Fully privacy-preserving determination of point-range relationship. Scientia Sinica Informationis, 2018,48:187−204 (in Chinese with English abstract).
[22] Gong LM, Li SD, Dou JW, Guo YM, Wang DS. Homomorphic encryption scheme and a protocol on secure computing a line by two private points. Ruan Jian Xue Bao/Journal of Software, 2017,28(12):3274−3292 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5239.htm [doi: 10.13328/j.cnki.jos.005239]
[23] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. on Information Theory, 1985,31(4):469−472.
[24] Damgård I, Jurik M. A generalisation, a simplication and some applications of paillier's probabilistic public-key system. In: Proc. of the Int'l Workshop on Public Key Cryptography. Berlin, Heidelberg: Springer-Verlag, 2001. 119−136.
[25] Goldreich O. Foundations of Cryptography: Vol.2, Basic Applications. Cambridge: Cambridge University Press, 2004. 615−626.
[26] Du W, Atallah MJ. Secure multi-party computation problems and their applications: A review and open problems. In: Proc. of the 2001 Workshop on New Security Paradigms. New York: ACM, 2001. 13−22.
[27] Mu B, Bakiras S. Private proximity detection for convex polygons. Tsinghua Science and Technology, 2016,21(3):270−280.

附中文参考文献:

[13] 李顺东,戴一奇,游启友.姚氏百万富翁问题的高效解决方案.电子学报,2005,33(5):769−773.
[16] 李顺东,王道顺.基于同态加密的高效多方保密计算.电子学报,2013,41(4):798−803.
[20] 郭奕旻,周素芳,窦家维,李顺东,王道顺.高效的区间保密计算及应用.计算机学报,2016,39:1−17.
[21] 陈振华,李顺东,陈立朝,黄琼,张卫国.点和区间关系的全隐私保密判定.中国科学:信息科学,2018,48:187−204.
[22] 巩林明,李顺东,窦家维,郭奕旻,王道顺.同态加密方案及安全两点直线计算协议.软件学报,2017,28(12):3274−3292. http://www.jos.org.cn/1000-9825/5239.htm [doi: 10.13328/j.cnki.jos.005239]

巩林明(1979－),男,博士,讲师,主要研究领域为密码学,信息安全.

李顺东(1963－),男,博士,教授,博士生导师,主要研究领域为公钥密码,安全多方计算.

邵连合(1988－),男,博士,副教授,CCF 专业会员,主要研究领域为量子信息及量子信息安全.

薛涛(1973－),男,博士,教授, CCF 专业会员,主要研究领域为分布式计算,云计算安全,大数据安全.

王道顺(1964－),男,博士,副教授,博士生导师,主要研究领域为公钥密码,视觉密码.