区间位置关系的保密判定

窦家维[1)] 王文丽[1)] 李顺东[2)]

[1)](陕西师范大学数学与信息科学学院 西安 710062)

[2)](陕西师范大学计算机科学学院 西安 710062)

摘 要 安全多方计算是目前国际密码学界研究的热点,有理数与有理区间以及两个有理区间位置关系的保密计算问题属于安全多方科学计算中的重要问题,在保密的计算几何以及商品价格商议等方面有重要的应用前景.目前关于这类问题的研究结果还很少,仅有少量关于有理数与有理区间位置关系保密判定问题的研究结果,关于两个有理区间位置关系保密计算问题尚未见到任何研究.本文首先采用以多项式表示区间的技巧,将有理数域内点与区间的保密计算问题转化为整数集上向量内积值的正负判定问题,设计构造了关于有理数域内点与区间位置关系判定问题安全高效的新协议,并以此为基础设计构造了保密判定两区间位置关系的判定协议,首次研究解决了两个有理区间位置关系判定问题.本文还将两个有理数的大小比较问题转化为整数集上向量内积值的正负判定问题,设计了有理数大小比较问题高效的判定协议.严格证明了本文协议在半诚实模型下的安全性,并进一步设计了恶意模型下点与区间位置关系的安全判定协议.文中最后举例说明了有理区间保密判定协议在解决实际问题中的应用,并将本文所设计的协议与已有相关结果进行了分析比较及实例验证,理论分析和实验结果都表明本文协议具有较高的计算效率.

关键词 密码学;安全多方计算;有理数;有理区间;区间保密计算;安全性

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2019.01031

Privately Determining Interval Location Relation

DOU Jia-Wei[1)] WANG Wen-Li[1)] LI Shun-Dong[2)]

[1)](*School of Mathematics and Information Science, Shaanxi Normal University, Xi'an* 710062)

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

Abstract Secure multiparty computation is a focus in the international cryptographic community in recent years, which has wide application in both information security and privacy-preserving practice. Secure multiparty computation can be classified into the following fields: secure scientific computation; secure geometric computation; secure multiparty statistical analysis; privacy-preserving data mining; and secure multiparty computation application system construction. Secure multiparty scientific computation is an important field of secure multiparty computation. In this field, cryptographic scholars have studied many secure multiparty scientific computation problems such as private comparing, sorting, maximum computing, set operations, scalar product, Hamming distance computing, and there are still many secure multiparty scientific computation problems need to be further studied. In this paper, we study how to privately determine the relation between a rational number and a rational interval, and the relation between two rational intervals. They are two secure multiparty scientific computation problems which have important application prospect in secure multiparty computational geometry and e-commerce. As far as we know, there hardly are works on these problems. There are a few literatures addressing the relation between a rational

收稿日期:2017-12-12;在线出版日期:2018-11-27.本课题得到国家自然科学基金面上项目(61272435)资助.**窦家维**,博士,副教授,主要研究方向为应用数学与密码学.E-mail: jiawei@snnu.edu.cn.**王文丽**,硕士研究生,主要研究方向为应用数学与密码学.**李顺东**,博士,教授,博士生导师,主要研究领域为密码学与信息安全.E-mail: shundong@snnu.edu.cn.

number and a rational interval. The relation between two rational intervals has not been investigated in the scenarios of secure multiparty computation. Representing an interval as a polynomial, we reduce privately determining the relation between a rational number and a rational interval to privately determining the sign of the scalar product of two integer vectors, and design, using the Paillier additively homomorphic cryptosystem, an efficient protocol to privately compute the sign of the scalar product of two private vectors, and further use it to construct a protocol to privately determine the relation between a rational number and a rational interval. This protocol achieves constant computational complexity. Using this protocol as a building block, we design a new protocol to privately determine the relation between two rational intervals. This is the first protocol for privately determining the relationship between two rational intervals. We also reduce the problem of privately comparing two rational numbers to privately determining the sign of the scalar product of two integer vectors, and further design a simple efficient protocol for rational millionaires' problem. Comparing with the existing protocols for rational millionaires' problem, our protocol is more efficient. We prove that, using the simulation benchmark, all our protocols are secure against semi-honest attackers, and we further construct a protocol that is secure in the malicious model for determining the relation between a rational number and a rational interval. This is the first protocol which is secure in the malicious model, is more practical and can be applied in practice. We show how to use the rational interval protocol to solve some computational geometric problem, and its application in e-commerce and so on. We further analyze the efficiency of the protocols, and theoretically compare the efficiency of our protocols with that of related results. We implement our protocols on a personal computer to test their efficiency. Theoretical analysis and the simulation results show that our protocols are efficient.

Keywords cryptography; secure multiparty computation; rational number; rational interval; privacy-preserving interval evaluation; security

1 引 言

近年来网络得到了迅速发展，这为多个参与者利用各自的保密数据进行合作计算提供了可能.利用多方数据进行合作计算可以充分发挥这些数据的价值以造福人类,但同时也给参与者私密数据的机密性与隐私保护带来了巨大的挑战.如果多个参与者能够以各自的私密数据为输入联合进行保密计算,计算结束后每个参与者仅可获得规定的输出结果,这样的计算模式即为安全多方计算,安全多方计算问题研究已受到人们的广泛关注[1-2].

图灵奖获得者姚期智[3]首先提出了安全多方计算问题,并引起国际密码学界的重视[4-5],Goldreich等人[6-7]对安全多方计算进行了深入的研究,并给出了安全多方计算问题通用的解决方案.但由于效率的原因,在实际中针对具体问题仍然需要研究具体的解决方案.

关于保密的科学计算问题已有很多好的研究成果,包括两个数大小关系的保密比较[3,8-11]、向量内积保密计算[12-14]、几何问题保密计算[15-17]、集合问题保密计算[18-20]等.

目前,关于有理数域内区间问题保密计算的研究结果还很少,有少量文献研究了有理数与有理区间位置关系保密判定问题,即保密判定给定的有理数 w 是否在某一有理区间 $I=[u,v]$ 内.我们注意到,两个有理区间位置关系保密判定问题,即保密判定两个有理区间 $[a,b]$ 和 $[c,d]$ 具有相离、相交或某种包含关系也是一类重要的多方保密计算问题.本文对这类问题给出明确的定义,并对其研究构造高效安全的解决方案.

研究设计有关区间问题的安全计算协议在现实生活中具有重要的应用,这类协议可以广泛应用于保密判定一些几何区域是否相交,保密判定约会时间安排是否可行或在商品交易中预先保密比较买卖双方的价格区间是否有重叠.例如,商家 B 希望购

买公司 A 的某类物品，B 能承担的价格范围在 c 元到 d 元之间，公司 A 对该物品的定价在 a 元到 b 元之间. 由于商家和公司对该物品的定价范围属于商业机密，因此商家 B 和公司 A 需要进行一次保密比较决定是否有成交的可能. 如果它们的价位区间 $[a,b]$ 与 $[c,d]$ 相交或具有包含关系，它们就可以通过进一步谈判达成交易. 如果两区间相离，它们就放弃达成交易的努力. 如果能设计构造一个保密判定两个区间位置关系的协议，就可以利用该协议判断它们是否有可能成交，是否继续磋商，从而节约交易成本.

有理数域内区间保密计算问题是整数范围内集合保密计算问题的自然推广. 直观上看，区间保密计算问题可转化为百万富翁问题进行求解. 即通过调用有理数域内的百万富翁协议，逐个比较给定有理数与区间两端点的大小可判定有理数与区间的位置关系；类似地，通过分别比较区间 I_1 端点值和 I_2 端点值的大小可判定两个有理区间的位置关系. 但直接这样做将会泄露很多不应泄露的信息. 因此需要对这类问题设计构造新的安全高效的解决方案.

Nishide 等人在文献[21]中首先研究了区间的保密计算问题. 文献[22]通过重新定义长度单位将有理数输入转化为整数情形，将区间的保密计算问题转化为有限集合的包含问题. 该协议当区间长度较小时效率较高，当区间长度较大时由于集合元素过多，导致计算复杂性很高. 文献[23]基于 Paillier 加密方案构造了一个点与区间的位置关系判定协议，其中保密点和保密区间的两个端点分别由不同的参与方持有，该协议是一个三方计算协议，不适合两方计算情形. 文献[24]提出了一个点与区间位置关系保密计算方案，由于协议中需要调用百万富翁问题协议，协议的通信与计算复杂性都较高. 目前，关于区间有关保密计算问题的研究结果较少，上面提到的几个协议仅研究了有理数与区间的保密计算问题，据我们所知，关于两个有理区间位置关系保密计算问题尚未有任何研究结果. 本文首先构造了有理数域内点与区间位置关系的一个新的保密判定协议，并在此基础上进一步设计构造了两个区间位置关系保密判定协议. 本文的贡献如下：

(1) 采用以多项式表示区间的技巧，将有理数域内点与区间的保密计算问题转化为整数集上向量内积值的正负判定问题. 并以 Paillier 加密方案为基础设计构造了关于有理数域内点与区间位置关系的保密判定协议(协议 1). 该协议具有较高的计算效率，并证明协议对半诚实敌手是安全的. 进一步设计了恶意模型下点与区间位置关系问题的安全计算协议(协议 4).

(2) 利用新构造的有理数域内点与区间位置关系判定协议的设计思想，构造了保密判定两区间位置关系的判定协议(协议 2)，该协议具有常数复杂性，是安全高效的协议. 就我们所知这是目前关于两个有理区间位置关系判定问题全新的研究结果.

(3) 将两个有理数的大小比较问题转化为整数集上向量内积值的正负判定问题，设计了有理数域内百万富翁问题的保密判定协议(协议 3)，与目前已有的相关协议相比，该协议更加高效简洁.

(4) 阐述了利用有理区间保密判定协议解决实际问题的应用实例：包括保密判定若干类型几何区域相交问题以及在商品交易中保密比较买卖双方的价格区间等方面的应用. 并将本文协议与已有相关结果进行了分析比较及实例验证，理论分析和实验结果都表明本文协议具有较高的计算效率.

2　预备知识

2.1　安全性定义

理想模型. 参与者 P_1,P_2 分别将自己的私密数据 x_1,x_2 告诉一个双方都信任的第三方，第三方计算 $f(x_1,x_2)=(f_1(x_1,x_2),f_2(x_1,x_2))$，然后将规定的输出结果 $f_1(x_1,x_2),f_2(x_1,x_2)$ 分别告诉 P_1 和 P_2，这样的计算模型称为理想模型. 理想模型下的计算协议既简单又安全，但由于在现实中参与者都信任的第三方不易找到，因此需要设计无需第三方参与的保密计算协议.

半诚实模型[7]. 在半诚实模型中，参与者完全按要求执行协议，但他们会保留协议执行中相关的数据和信息，协议结束后试图从所保留的信息中推导出超出协议规定的额外信息. 半诚实模型下两方计算协议的安全性描述如下：

两个参与者 P_1 和 P_2，分别拥有私密数据 x_1,x_2，他们希望应用协议 π 保密计算 $f(x_1,x_2)$. 参与者 P_i 在执行 π 时所得到的信息表示如下：

$$view_i^{\pi}(x_1,x_2)=(x_i,r^i,m_i^1,\cdots,m_i^t),$$

其中 $i=1,2,j=1,\cdots,t,r^i$ 和 m_i^j 分别表示 P_i 在协议中产生的随机数以及收到的第 j 个信息. 关于半诚实模型下保密计算协议的安全性，通常应用下面的模拟范例方法进行证明.

定义 1[7]. 在半诚实模型中，如果存在两个概

率多项式时间算法 S_1, S_2，使得

$$\{S_1(x_1, f_1(x_1,x_2))\}_{x_1,x_2} \overset{c}{\equiv} \{view_1^{\pi}(x_1,x_2)\}_{x_1,x_2} \quad (1)$$

$$\{S_2(x_2, f_2(x_1,x_2))\}_{x_1,x_2} \overset{c}{\equiv} \{view_2^{\pi}(x_1,x_2)\}_{x_1,x_2} \quad (2)$$

成立，其中$\overset{c}{\equiv}$表示计算上不可区分，则称协议 π 保密地计算函数 $f(x_1,x_2)$.

恶意模型. 文献[7]详细阐述了恶意模型中参与者可能发生的恶意行为以及协议的安全性定义，并给出了以半诚实模型下的保密计算协议为基础获得恶意模型下安全计算协议的一般方法，具体可参看文献[7].

2.2 Paillier 密码系统

一般的公钥加密方案包括三个算法：密钥生成算法 $G(\tau)$，给定安全参数 τ 以后，$G(\tau)$ 生成私钥 sk 和对应的公钥 pk；加密算法 E 用来加密明文消息以及解密算法 D 用来解密密文. 同态加密方案还要求加密算法具有一定的同态性质. 加法同态性可表示为

$$E(M_1+M_2)=E(M_1)\oplus E(M_2),$$

其中 $\oplus$ 表示密文之间的某种代数运算.

Paillier 加密方案是一种公钥加密方案，并具有加法同态性. 具体描述如下[25]：

密钥生成. 令 $N=pq$，其中 p 和 q 是两个大素数. 记 $\omega=\mathrm{lcm}(p-1,q-1)$ 是 $p-1$ 和 $q-1$ 的最小公倍数. 并记

$$B=\{x \mid x^{N\mu} \bmod N^2=1, \mu\in\{1,2,\cdots,\omega\}\},$$

$$S_N=\{u<N^2 \mid u\equiv 1 \bmod N\},$$

$$L(u)=\frac{u-1}{N}, \forall u\in S_N.$$

任意取定 $g\in B$，则可选取 g, N 为公钥，ω 为私钥. 明文空间和密文空间分别为 Z_N 和 $Z_{N^2}^*$.

加密. 对于明文 m，按下面方式加密：

$$c=g^m r^N \bmod N^2,$$

其中 $r\in Z_N^*$ 为随机数.

解密. 对于密文 c，按下面方式解密：

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

加法同态性. 由于下面性质成立：

$$\begin{aligned} E(m_1)\cdot E(m_2) &= g^{m_1} r_1^N \cdot g^{m_2} r_2^N \bmod N^2 \\ &= g^{m_1+m_2}(r_1 r_2)^N \bmod N^2 \\ &= E(m_1+m_2 \bmod N), \end{aligned}$$

因此 Paillier 公钥加密方案具有加法同态性.

本文假设在加密方案中 N 取得充分大，以保证所涉及的明文都在明文空间 Z_N 中.

注解 1. 关于 Paillier 加密方案的安全性简单叙述如下：首先，由于 Paillier 加密方案是概率加密方案，因此是 IND-CPA 安全的；又由于 Paillier 加密方案具有加法同态性，因此不具有 IND-CCA2 安全性. Paillier 加密方案是否具有同态加密系统中最强的 IND-CCA1 安全性是众多学者近年来一直努力解决的一个公开问题. 近期文献[26]关于这一问题给出了下面的结果：Paillier 加密方案是 IND-CCA1 安全的当且仅当 $\mathrm{DCR}^{\mathrm{SCCR}}$ 问题是困难的. 文献[26]同时指出 $\mathrm{DCR}^{\mathrm{SCCR}}$ 是一个新的(虽然自然产生的)问题，因此对其困难性进行彻底分析是可取的(advisable)，并将这个问题留待进一步分析解决(上面所出现的各种缩写符号的具体含义以及对于研究结果的详细论证请参阅文献[26]).

3 有理数域内点与区间位置关系判定问题

在下文中，对任意有理数 w，按如下方式将其表示为唯一的分数形式 $w=\frac{w_1}{w_2}$，其中 w_1, w_2 为两个互素的整数，且要求 $w_2\geq 1$.

3.1 问题描述及计算原理

问题描述. 假设 Alice 有一有理数 $w=\frac{w_1}{w_2}$，Bob 有一有理区间 $I=[u,v]$，其中 $u=\frac{u_1}{u_2}$，$v=\frac{v_1}{v_2}$(有理区间$[u,v]$指介于有理数 u 和 v 之间的所有有理数构成的集合). 他们想保密地判断点 w 与区间 I 的位置关系，即保密判定 $w\in(u,v)$，$w\notin[u,v]$或 w 与区间某端点重合三种情形中具体哪种情形发生，而不泄露其他任何信息.

计算原理. 我们以多项式 $f_I(x)=(x-u)(x-v)$ 表示区间 $I=[u,v]$，于是，判断点 w 与区间 I 的位置关系问题可转化为判断函数值 $f_I(w)$ 的正负问题.

在下文中，记 $\alpha=u_2v_2$，$\beta=-u_2v_1-u_1v_2$，$\gamma=u_1v_1$，可得到：

$$\begin{aligned} f_I(w)=(w-u)(w-v) &= \left(\frac{w_1}{w_2}-\frac{u_1}{u_2}\right)\left(\frac{w_1}{w_2}-\frac{v_1}{v_2}\right) \\ &= \frac{1}{w_2^2 u_2 v_2}(\alpha w_1^2+\beta w_1 w_2+\gamma w_2^2) \end{aligned} \quad (3)$$

由于 u_2, v_2, w_2 均为正整数，由式(3)，判断 $f_I(w)$ 的符号问题即转化为判断两个整数向量 $\boldsymbol{V}_w=$

(w_1^2, w_1w_2, w_2^2)与$\boldsymbol{V}_{[u,v]}=(\alpha,\beta,\gamma)$的内积符号问题. 如果定义点$w$与区间$[u,v]$的位置关系符号函数为$S(w,[u,v])=\mathrm{sgn}(\boldsymbol{V}_w\cdot\boldsymbol{V}_{[u,v]})$，则有：

命题 1. 对于点w与区间$[u,v]$有下面结论成立：

$$S(w,[u,v])=\mathrm{sgn}(\boldsymbol{V}_w\cdot\boldsymbol{V}_{[u,v]})=\begin{cases}-1, & \text{如果 } w\in(u,v)\\ 0, & \text{如果 } w=u \text{ 或 } w=v\\ 1, & \text{如果 } w\notin[u,v]\end{cases}\quad(4)$$

由命题 1，根据$S(w,[u,v])$的取值即可获知点w与区间$[u,v]$的位置关系.

3.2 点与区间位置关系保密判定协议

我们将以命题 1 为基础构造点与区间位置关系保密判定协议. 下文中所涉及的随机数均取为正整数，并约定如果在协议中某一方没有获得输出时，以λ表示之.

协议 1. 保密判定点与区间位置关系.

输入：Alice 输入有理数$w=\dfrac{w_1}{w_2}$，Bob 输入有理区间$I=[u,v]=\left[\dfrac{u_1}{u_2},\dfrac{v_1}{v_2}\right]$.

输出：Alice 输出$y=S(w,[u,v])$，Bob 输出λ.

准备：Bob 运行 Paillier 加密方案生成私钥sk和对应的公钥$pk=(g,N)$. Alice 和 Bob 分别选择随机数$s>0$以及$r>0$.

1. Bob 选择随机数r_w，使得$\bar{\beta}=\beta+r_w>0$. Bob 加密$r\alpha, r\bar{\beta}, r\gamma$，并将密文$E(r\alpha), E(r\bar{\beta}), E(r\gamma)$发送给 Alice.

2. Alice 计算下面密文：

$$R_w=E(r\alpha)^{sw_1^2}E(r\bar{\beta})^{sw_1w_2}E(r\gamma)^{sw_2^2}\bmod N^2,$$

并将R_w发送给 Bob.

3. Bob 解密R_w，得到u_w，并将u_w以及rr_w发送给 Alice.

4. Alice 计算$z_w=u_w-rr_w s w_1w_2$.

5. Alice 输出$y=\mathrm{sgn}(z_w)$.

协议 1 的正确性. 由 Paillier 加密方案的加法同态性可知，Bob 在第 3 步的解密结果为

$$u_w=rs(\alpha w_1^2+\bar{\beta}w_1w_2+\gamma w_2^2),$$

进一步，第 4 步中 Alice 的计算结果为

$$z_w=u_w-rr_w s w_1w_2=rs(\alpha w_1^2+\beta w_1w_2+\gamma w_2^2),$$

由于$r>0, s>0$，因此，z_w的符号即为向量$\boldsymbol{V}_w$与$\boldsymbol{V}_{[u,v]}$的内积值符号，根据命题 1 可知协议 1 获得了正确的输出结果.

协议 1 的安全性.

定理 1. 有理点与有理区间的位置关系保密判定协议 1 在半诚实模型下是安全的.

证明. 根据半诚实模型下协议的安全性定义，需要构造模拟器S_1, S_2，使得式(1)和式(2)成立.

接收到输入$(w,S(w,[u,v]))$后，S_1按照如下方式运行：

(1) 任意选择有理区间$[u',v']=\left[\dfrac{u_1'}{u_2'},\dfrac{v_1'}{v_2'}\right]$，满足$S(w,[u',v'])=S(w,[u,v])$.

(2) 选择随机数r_w', r'，使得$\bar{\beta}'=\beta'+r_w'>0$，加密得到密文$E(r'\alpha'), E(r'\bar{\beta}'), E(r'\gamma')$(这里$\alpha'=u_2'v_2', \beta'=-u_2'v_1'-u_1'v_2', \gamma'=u_1'v_1'$).

(3) 计算

$$R_w'=E(r'\alpha')^{sw_1^2}E(r'\bar{\beta}')^{sw_1w_2}E(r'\gamma')^{sw_2^2}\bmod N^2.$$

(4) 计算$u_w'=r's(\alpha' w_1^2+\bar{\beta}'w_1w_2+\gamma' w_2^2)$.

(5) 计算$z_w'=u_w'-r'r_w' s w_1w_2$.

在协议的执行中，

$$view_1^{\pi}(w,[u,v])=\{w,E(r\alpha),E(r\bar{\beta}),E(r\gamma),u_w,rr_w,S(w,[u,v])\}.$$

令

$$S_1(w,S(w,[u,v]))=\{w,E(r'\alpha'),E(r'\bar{\beta}'),E(r'\gamma'),u_w',r'r_w',S(w,[u',v'])\}.$$

因为 Paillier 加密方案是 IND-CPA 安全的[26]，因此，对于 Alice 来说，

$$E(r\alpha)\overset{c}{\equiv}E(r'\alpha'),\ E(r\bar{\beta})\overset{c}{\equiv}E(r'\bar{\beta}'),\ E(r\gamma)\overset{c}{\equiv}E(r'\gamma'),$$

又由于r_w, r以及r_w', r'是随机数，故有$rr_w\overset{c}{\equiv}r'r_w'$，并由于$r$是 Bob 选择的随机数，对于 Alice 来说$u_w$与$u_w'$计算上不可区分，而$S(w,[u,v])=S(w,[u',v'])$，因此，

$$\{S_1(w,S(w,[u,v]))\}_{u,v,w}\overset{c}{\equiv}\{view_1^{\pi}(w,[u,v])\}_{u,v,w}.$$

接收到输入$([u,v],\lambda)$后S_2按如下方式运行：

(1) 任意选择有理数$w'=\dfrac{w_1'}{w_2'}$.

(2) 加密得到密文$E(r\alpha), E(r\bar{\beta}), E(r\gamma)$.

(3) 选择随机数s'，计算

$$R_{w'}=E(r\alpha)^{s'w'^2_1}E(r\bar{\beta})^{s'w_1'w_2'}E(r\gamma)^{s'w'^2_2}\bmod N^2.$$

(4) 计算$u_{w'}=rs'(\alpha w'^2_1+\bar{\beta}w_1'w_2'+\gamma w'^2_2)$.

(5) 计算$z_{w'}=u_{w'}-rr_w s' w_1'w_2'$.

在协议的执行中，

$$view_2^{\pi}(w,[u,v])=\{[u,v],R_w,\lambda\}.$$

令$S_2([u,v],\lambda)=\{[u,v],R_{w'},\lambda\}$.

由于s是 Alice 选择的随机数，虽然 Bob 能够解密，但对于 Bob 来说

$$R_w=E(r\alpha)^{sw_1^2}E(r\bar{\beta})^{sw_1w_2}E(r\gamma)^{sw_2^2}\bmod N^2$$

与

$$R_{w'}=E(r\alpha)^{s'w'^2_1}E(r\bar{\beta})^{s'w_1'w_2'}E(r\gamma)^{s'w'^2_2}\bmod N^2$$

是计算不可区分的.因此,

$$\{S_2([u,v],\lambda)\}_{u,v,w}\overset{c}{\equiv}\{view_2^{\pi}(w,[u,v])\}_{u,v,w}.$$

证毕.

注解 2. 在定理 1 的基础上,我们从现代密码学的角度,以 Paillier 加密方案的安全性为基础进一步分析协议 1 的安全性.根据文献[26]的结论分析如下:首先,由于 Paillier 加密系统是 IND-CPA 安全的,因此 Alice 根据 Bob 所发送的密文 $E(r\alpha)$, $E(r\bar{\beta})$, $E(r\gamma)$ 无法通过选择明文攻击(CPA)而获得 Bob 数据的任何额外信息,这时协议 1 是安全的(即具有通常所说的 IND-CPA 安全性).进一步,如果 DCR^{SCCR} 问题是困难的,Paillier 加密方案就是 IND-CCA1 安全的,那么即使 Alice 进一步通过(Non-adaptive)选择密文攻击(CCA1),也无法从密文 $E(r\alpha)$, $E(r\bar{\beta})$, $E(r\gamma)$ 中获得 Bob 数据的任何额外信息,这时即可保证协议 1 是 IND-CCA1 安全的.

4 两个有理区间位置关系保密判定协议

以前面所设计的有理数与有理区间位置关系判定协议为基础,本节进一步研究有理区间保密计算有关问题.

4.1 问题描述以及计算原理

问题描述. 对于两个区间 $I_A=[a,b]$, $I_B=[c,d]$,如果它们无重合端点,则共有四类位置关系:包含,即其中一个区间为另一个区间的真子集(如图 1 或图 2);相离,即两区间的交集为空集(如图 3);除去相离和包含关系,其他均为相交关系(如图 4).如果两区间有重合端点,这时除了可能具有关系 $I_A=I_B$ 外,还有 $I_A\subset I_B$, $I_B\subset I_A$,以及 I_A 与 I_B 相交(左右相接)三类位置关系,分别如图 5、图 6 和图 7 所示.

我们将设计两个有理区间位置关系问题保密判定协议,协议的执行结果,或显示两区间完全相同,

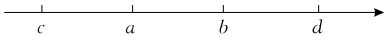


图 1 $[a,b]\subset[c,d]$

图 2 $[c,d]\subset[a,b]$

(a)

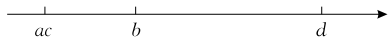
(b)

图 3 两区间相离

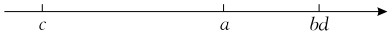
(a)

(b)

图 4 两区间相交



(a)



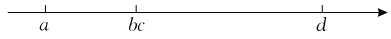
(b)

图 5 $[a,b]\subset[c,d]$

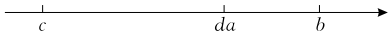
(a)

(b)

图 6 $[c,d]\subset[a,b]$



(a)



(b)

图 7 两区间相交(前后相接)

或具体指出图 1～图 7 中的某类位置关系发生(对于图 3～图 7,要求保密具体的情形(a)或(b)).并且除了协议执行结果所蕴含的信息外,关于两区间端点的其他信息应该完全保密.

计算原理. 首先由前面所定义的点与区间位置关系符号函数计算 I_A(或 I_B)的两端点 a,b(或 c,d)与区间 I_B(或 I_A)的关系符号,并记 $S_a=S(a,[c,d])$, $S_b=S(b,[c,d])$, $S_c=S(c,[a,b])$, $S_d=S(d,[a,b])$.根据图 1～图 7,并结合命题 1,容易证明下面结论.

命题 2. 由 S_a,S_b,S_c,S_d 的不同符号可判断区间 $I_A=[a,b]$ 和 $I_B=[c,d]$ 的位置关系如下:

(1) 如果 S_a,S_b 同负,则 $I_A\subset I_B$(为图 1 类型);如果 S_a 与 S_b 异号,则 I_A,I_B 相交(为图 4 类型).如果 S_a,S_b 同正,进一步根据 S_c 与 S_d 的不同情况有下面结果:如果 S_c,S_d 同负,则 $I_B\subset I_A$(为图 2 类型);否则,如果 S_c,S_d 同正,则 I_A 与 I_B 相离(为图 3 类型).

(2) 如果 S_a 与 S_b 一个为零,一个为负,则 $I_A\subset I_B$(为图 5 类型).如果 S_a 与 S_b 一个为零,一个为正,进一步根据 S_c 与 S_d 的不同情况有下面结果:如果 S_c 与 S_d 一个为零,一个为负,则 $I_B\subset I_A$(为图 6 类型);否则,如果 S_c 与 S_d 一个为零,一个为正,则 I_A 与 I_B 相交(左右相接)(为图 7 类型).

(3) 最后,如果 $S_a=S_b=0$,则 $I_A=I_B$.

证明.　我们需要证明命题 2 能够正确区分 I_A 与 I_B 的各种位置关系(包括全部八类位置关系：图 1～图 7 共七类，以及两区间相同).

(1)首先考虑无重合端点情形. 显然，当 S_a 与 S_b 同负(异号)时，为图 1(图 4)所示类型. 当 S_a，S_b 同正时，无法区分图 2 与图 3 两种类型，因此需要进一步考虑 S_c 与 S_d 的符号(这时必有 S_c，S_d 同号)：当 S_c，S_d 同为负时，为图 2 的类型，有 $I_B \subset I_A$；否则，有 S_c，S_d 同正，这时为图 3 的类型，I_A 与 I_B 相离.

(2)其次考虑有重合端点情形. 显然当 S_a 与 S_b 一个为零，一个为负时，为图 5 的类型，此时 $I_A \subset I_B$. 当 S_a 与 S_b 一个为零，一个为正时，无法区分图 6 与图 7 两类关系，因此需要进一步考虑 S_c 与 S_d 的符号(这时 S_c，S_d 中必有一个为零，另一个不为零)：当 S_c 与 S_d 中一个为零，一个为负时，为图 6 的类型，这时 $I_B \subset I_A$；否则，S_c 与 S_d 中一定有一个为零，一个为正，这时为图 7 的类型，即 I_A 与 I_B 相交(左右相接).

(3)最后，当 $S_a=S_b=0$ 时显然有 $I_A=I_B$，即两区间相同.　　证毕.

4.2　协议设计

下面，以命题 2 为基础，并应用协议 1 的设计思想，设计两个有理区间位置关系保密判定协议. 为叙述方便，定义函数 $S(I_A, I_B)$ 如下：如果 $I_A=I_B$，令 $S(I_A, I_B)=0$；否则，如果 I_A，I_B 的位置关系为图 k 的类型，则令 $S(I_A, I_B)=k(k=1,\cdots,7)$.

下文中，记 $\alpha_A=a_2b_2$，$\beta_A=-a_2b_1-a_1b_2$，$\gamma_A=a_1b_1$，$\alpha_B=c_2d_2$，$\beta_B=-c_2d_1-c_1d_2$，$\gamma_B=c_1d_1$.

协议 2.　两个有理区间位置关系保密判定协议.

输入：Alice 输入私密有理区间 $I_A=[a,b]=\left[\frac{a_1}{a_2},\frac{b_1}{b_2}\right]$，Bob 输入私密有理区间 $I_B=[c,d]=\left[\frac{c_1}{c_2},\frac{d_1}{d_2}\right]$.

输出：$y=S(I_A, I_B)$.

准备：Alice 和 Bob 分别运行 Paillier 加密方案，分别生成私钥/公钥 sk_A/pk_A 以及 sk_B/pk_B，并将公钥告知对方(假设公钥中的模数分别为 N_A，N_B).

1. Bob 选择随机数 r_a，r_b，r_1，r_2，使得

$$\bar{\beta}_a=\beta_B+r_a>0,\ \bar{\beta}_b=\beta_B+r_b>0.$$

Bob 应用 pk_B 加密 $r_1\alpha_B$，$r_1\gamma_B$，$r_1\bar{\beta}_a$ 以及 $r_2\alpha_B$，$r_2\gamma_B$，$r_2\bar{\beta}_b$，并将这些密文发送给 Alice.

2. Alice 选择随机数 s_1，计算

$$R_a=E(r_1\alpha_B)^{s_1a_1^2}E(r_1\bar{\beta}_a)^{s_1a_1a_2}E(r_1\gamma_B)^{s_1a_2^2}\bmod N_B^2,$$

$$R_b=E(r_2\alpha_B)^{s_1b_1^2}E(r_2\bar{\beta}_b)^{s_1b_1b_2}E(r_2\gamma_B)^{s_1b_2^2}\bmod N_B^2,$$

并将 R_a，R_b 发送给 Bob.

3. Bob 应用 sk_B 解密 R_a，R_b，得到 u_a，u_b，并将两个数对 (u_a, r_1r_a) 与 (u_b, r_2r_b) 随机置换后发送给 Alice.

4. Alice 计算 $z_a=u_a-s_1r_1r_aa_1a_2$ 与 $z_b=u_b-s_1r_2r_bb_1b_2$，并将 $\mathrm{sgn}(z_a)$ 与 $\mathrm{sgn}(z_b)$ 随机置换后发送给 Bob.

5. 如果 z_a 与 z_b 同负，则输出 $y=1$；如果 z_a 与 z_b 异号(或一个为零，一个为负)，则输出 $y=4$(或 $y=5$)；如果 z_a 与 z_b 均为零，则输出 $y=0$. 如果上面某种情形确实发生，则在输出相应结果后协议终止. 否则，继续执行下一步.

6. Alice 选择随机数 s_c，s_d，s_2，s_3，使得

$$\bar{\beta}_c=\beta_A+s_c>0,\ \bar{\beta}_d=\beta_A+s_d>0.$$

Alice 应用 pk_A 加密 $s_2\alpha_A$，$s_2\gamma_A$，$s_2\bar{\beta}_c$ 以及 $s_3\alpha_A$，$s_3\gamma_A$，$s_3\bar{\beta}_d$，并将这些密文发送给 Bob.

7. Bob 选择随机数 r_3，计算：

$$R_c=E(s_2\alpha_A)^{r_3c_1^2}E(s_2\bar{\beta}_c)^{r_3c_1c_2}E(s_2\gamma_A)^{r_3c_2^2}\bmod N_A^2,$$

$$R_d=E(s_3\alpha_A)^{r_3d_1^2}E(s_3\bar{\beta}_d)^{r_3d_1d_2}E(s_3\gamma_A)^{r_3d_2^2}\bmod N_A^2,$$

并将 R_c，R_d 发送给 Alice.

8. Alice 应用 sk_A 解密 R_c，R_d，得到 u_c，u_d，并将两个数对 (u_c, s_2s_c) 与 (u_d, s_3s_d) 随机置换后发送给 Bob.

9. Bob 计算 $z_c=u_c-r_3s_2s_cc_1c_2$ 与 $z_d=u_d-r_3s_3s_dd_1d_2$，并将 $\mathrm{sgn}(z_c)$ 与 $\mathrm{sgn}(z_d)$ 随机置换后发送给 Alice.

10. 如果 z_c 与 z_d 同正时输出 $y=3$；同负时输出 $y=2$；一个为零，一个为负时输出 $y=6$；如果 z_c 与 z_d 一个为零，一个为正(这时必有 z_c 与 z_d 一个为零，一个为正)，则输出 $y=7$.

4.3　协议 2 的正确性

在协议第 3 步，由加密算法的加法同态性，Bob 解密得到

$$u_a=r_1s_1(\alpha_Ba_1^2+\bar{\beta}_aa_1a_2+\gamma_Ba_2^2),$$

$$u_b=r_2s_1(\alpha_Bb_1^2+\bar{\beta}_bb_1b_2+\gamma_Bb_2^2),$$

在协议第 4 步，Alice 计算 z_a 与 z_b，由于

$$z_a=u_a-s_1r_1r_aa_1a_2=r_1s_1(\alpha_Ba_1^2+\beta_Ba_1a_2+\gamma_Ba_2^2),$$

$$z_b=u_b-s_1r_2r_bb_1b_2=r_2s_1(\alpha_Bb_1^2+\beta_Bb_1b_2+\gamma_Bb_2^2),$$

因此 $\mathrm{sgn}(z_a)=S_a$，$\mathrm{sgn}(z_b)=S_b$. 类似地，在第 9 步计算中，可得到 $\mathrm{sgn}(z_c)=S_c$，$\mathrm{sgn}(z_d)=S_d$. 因此由命题 2，协议 2 能正确区分两区间的各类位置关系.

4.4　协议 2 的安全性

定理 2.　两个有理区间的位置关系保密判定协议 2 是安全的.

证明.　(1)在协议 2 的前半部分(第 1～5 步)，实际上是 Alice 以私密有理数 a 以及 b 为输入，Bob 以有理区间 $[c,d]$ 为输入，通过应用与协议 1 完全相同的设计思想同时获得了 S_a 和 S_b. 如果有必要，在协议后半部分(第 6～10 步)，Alice 和 Bob 交换角色，这时 Bob 以私密有理数 c 以及 d 为输入，Alice 以有理区间 $[a,b]$ 为输入，与前半部分类似计算可同时得到 S_c，S_d. 由于协议 2 应用了与协议 1 完全类似的设计思想，由协议 1 的安全性知协议 2 关于两

方区间端点保密数据都是安全的.

(2)我们还需证明通过执行协议2,其结果只能获知区间关系为八类位置关系中的某一类,不会泄露其他额外信息.

在协议前(或后)半部分执行中,由于在第3步以及第4步(或第8步以及第9步)中Alice和Bob在给对方发送数据之前分别进行了一次随机置换,这样做的目的是使得双方都仅能获得$\{S_a,S_b\}=\{t_1,t_2\}$(或$\{S_c,S_d\}=\{t_1,t_2\}$),但不知道具体的对应关系,这里$t_1,t_2\in\{0,-1,1\}$.

如果获得$\{S_a,S_b\}=\{-1,-1\}$,协议即终止.这时只知a,b两点均在(c,d)之内,仅能获知位置关系为图1的类型,再无其他信息泄露.

如果获得$\{S_a,S_b\}=\{1,-1\}$,协议即终止.这时只知a,b两点其中一个在(c,d)之内,另一个在(c,d)之外,仅能获知位置关系为图4的类型,无法确切区分其为图4(a)、(b)中哪种情形.也再无其他信息泄露.

如果获得$\{S_a,S_b\}=\{0,-1\}$,协议即终止.这时只知a,b两点其中之一在(c,d)之内,另一点与c,d中某一点重合,仅能获知位置关系为图5的类型,无法确切区分其为图5(a)、(b)中哪种情形.也再无其他信息泄露.

如果获得$\{S_a,S_b\}=\{0,0\}$,协议即终止.这时可获知$a=c,b=d$,即两个区间相同.

如果获得$\{S_a,S_b\}=\{1,1\}$(或$\{S_a,S_b\}=\{0,1\}$),因无法区分图2与图3的类型(或图6与图7的类型),需要继续执行协议的第6～10步.与前面的分析类似,通过执行协议的第6～10步进一步获得S_c,S_d的符号,由S_c,S_d的不同符号,仅能区分出图2与图3的类型(或图6与图7的类型),而无其他额外的信息泄露. 证毕.

注解3. 协议2适合于需要比较出两个区间具有八种类型关系的应用场景,即图1～图7七种类型以及两区间完全相同.如果有某种端点重合的情形发生,参与方可能会猜测出具体是哪个端点重合,这样就会泄露一些额外信息.区间端点有重合属于比较特殊的情形,在实际应用中可以设法避免这种情形发生.比如在实际商品交易中,Alice可以将其价格区间$[a,b]$修改为$[a+r_1,b+r_2]$,其中r_1,r_2为两个并不影响交易的很小的随机有理数,如此,再发生保密区间端点重合的情形可认为是一个小概率事件,即此种情形发生的可能性可以忽略[27].

在协议1中,应用类似的方法可以避免有理数和区间端点值有可能重合的问题.

4.5 应用门限密码系统构造区间位置关系保密判定协议

在上面协议2中整个协议需要Bob和Alice分别构造公钥系统,并由其各自单独解密,如此设计协议在公平性方面有一定缺陷.为了克服这个不足,可以应用Paillier门限密码系统[28]设计协议.具体如下:Alice和Bob应用Paillier门限密码系统合作产生公钥,记为pk,对应的私钥分别为sk_A与sk_B.以pk替代协议2中的pk_A,pk_B进行加密,解密过程需要两人合作完成,对协议2稍加修改即可保密判定两区间位置关系.

我们写出对协议2第1～5步的修改,如果需要,对第6～10步可类似修改.

(1)Bob选择随机数r_a,r_b,r_1,r_2,使得$r_1r_a=r_2r_b$,并且$\bar{\beta}_a=\beta_B+r_a>0$,$\bar{\beta}_b=\beta_B+r_b>0$.

Bob应用pk加密$r_1\alpha_B$,$r_1\gamma_B$,$r_1\bar{\beta}_a$以及$r_2\alpha_B$,$r_2\gamma_B$,$r_2\bar{\beta}_b$,将这些密文以及r_1r_a发送给Alice.

(2)(a)Alice选择随机数s_1,s_2,计算:

$$R_a=E(r_1\alpha_B)^{s_1a_1^2}E(r_1\bar{\beta}_a)^{s_1a_1a_2}E(r_1\gamma_B)^{s_1a_2^2}E(s_2),$$

$$R_b=E(r_2\alpha_B)^{s_1b_1^2}E(r_2\bar{\beta}_b)^{s_1b_1b_2}E(r_2\gamma_B)^{s_1b_2^2}E(s_2),$$

并将R_a,R_b随机置换后发送给Bob.

(b)Bob应用pk加密零得到两个不同密文$E_1(0),E_2(0)$,计算$T_a=R_aE_1(0)$,$T_b=R_bE_2(0)$,并将T_a,T_b随机置换后发送给Alice.

(3)Alice和Bob合作解密T_a,T_b,得到

$$u_a=r_1s_1(\alpha_Ba_1^2+\bar{\beta}_aa_1a_2+\gamma_Ba_2^2)+s_2,$$

$$u_b=r_2s_1(\alpha_Bb_1^2+\bar{\beta}_bb_1b_2+\gamma_Bb_2^2)+s_2.$$

(4)Alice计算

$$z_a=u_a-s_1r_1r_aa_1a_2-s_2,z_b=u_b-s_1r_2r_bb_1b_2-s_2,$$

并将$\mathrm{sgn}(z_a)$与$\mathrm{sgn}(z_b)$发送给Bob.

(5)如果z_a与z_b同负,则输出$y=1$;如果z_a与z_b异号(或一个为零,一个为负),则输出$y=4$(或$y=5$);如果$z_a=z_b=0$,则输出$y=0$,协议终止.否则,需要进一步执行协议.

注解4. 以门限密码系统设计的区间位置关系保密判定协议的第3和第4步与协议2稍有不同,由于在协议2的前五步中,Bob有独立的解密能力,故在第3步Bob解密后对结果明文做一个随机置换,则可保证Alice无法区分u_a和u_b.在门限密码系统中,由于需要双方合作才能解密,因此要使Alice对u_a和u_b无法识别,Bob利用Paillier公钥系统的

加法同态性，在第 2 步(b)中首先给 R_a，R_b 乘以零的不同密文，再对结果密文进行随机置换，从而达到使 Alice 无法区分 u_a 和 u_b 的目的.

5　两个有理数大小比较问题

问题描述. Alice 和 Bob 分别具有私密有理数 $a=\frac{a_1}{a_2}$ 和 $b=\frac{b_1}{b_2}$，他们想保密地判断两个数的大小关系，而不泄露任何其他信息.

计算原理. 类似于点与区间位置关系判定原理，Bob 构造一次多项式 $\phi(x)=x-b$，而根据函数值 $\phi(a)$ 的正负来判定 a 与 b 的大小关系. 由于 $\phi(a)=a-b=\frac{a_1}{a_2}-\frac{b_1}{b_2}=\frac{a_1b_2-a_2b_1}{a_2b_2}$，且 a_2，b_2 均为正整数，因此，两个有理数 a 与 b 大小比较问题转化成了 Alice 和 Bob 各自的向量 $\boldsymbol{V}_A=(a_1,a_2)$ 和 $\boldsymbol{V}_B=(b_2,-b_1)$ 的内积值符号问题：如果 $\boldsymbol{V}_A\cdot\boldsymbol{V}_B=0$，则 $a=b$；如果 $\boldsymbol{V}_A\cdot\boldsymbol{V}_B<0$，则 $a<b$；如果 $\boldsymbol{V}_A\cdot\boldsymbol{V}_B>0$，则 $a>b$. 具体设计保密计算协议如下：

协议 3.　两个有理数大小比较协议.

输入：Alice 和 Bob 分别输入 $a=\frac{a_1}{a_2}$ 以及 $b=\frac{b_1}{b_2}$.

输出：Alice 输出 $y=\mathrm{sgn}(a-b)$，Bob 输出 λ.

准备：Bob 运行 Paillier 加密方案的密钥生成算法，生成私钥 sk 和对应的公钥 $pk=(g,N)$.

1. Bob 选择随机数 r,r_a，使得 $B=-b_1+r_a>0$. Bob 加密 rb_2，rB，并将 $E(rb_2)$，$E(rB)$ 发送给 Alice.

2. Alice 选择随机数 s，计算：

$$R_a=E(rb_2)^{sa_1}E(rB)^{sa_2}\bmod N^2,$$

并将 R_a 发送给 Bob.

3. Bob 解密 R_a，得到 u_a，并将 u_a 以及 rr_a 发送给 Alice.

4. Alice 计算 $z_a=u_a-rr_asa_2$.

5. Alice 输出 $y=\mathrm{sgn}(z_a)$.

正确性. 由于

$u_a=rs(a_1b_2+a_2B)$，$z_a=u_a-rr_asa_2=rs(a_1b_2-a_2b_1)$，由上式可知 z_a 与 $\boldsymbol{V}_A\cdot\boldsymbol{V}_B$ 的符号相同，由计算原理，$\boldsymbol{V}_A\cdot\boldsymbol{V}_B$ 的正负完全刻画了 a 与 b 的大小关系，因此协议 3 正确地判定了有理数 a 与 b 的大小关系.

安全性. 类似于协议 1 的证明有下面结论.

定理 3. 两个有理数大小比较协议 3 是安全的.

注解 5. 由于协议 2 是以协议 1 的设计思想为基础构造的，协议 3 的设计思想也与协议 1 类似，因此对协议 2 和协议 3 的 CCA 安全性分析与协议 1 完全类似(参看注解 2)，在定理 2 和定理 3 的基础上进一步分析可知，如果 Paillier 加密方案是 IND-CCA1 安全的，这时协议 2 和协议 3 也是 IND-CCA1 安全的.

6　效率分析

关于有理数域内的区间保密计算问题，目前已有的研究结果很少. 文献[24]首先提出了一个有理数与有理区间位置关系的保密判定协议，本文对这一问题进行进一步的推广，提出了判定有理数与有理区间位置关系更高效安全的判定协议，并进一步提出了两个有理区间位置关系问题以及两个有理数大小比较问题的保密判定协议. 本部分主要分析这些协议的计算复杂性与通信复杂性，并将判定有理数与有理区间位置关系协议 1 与文献[24]的协议 2 和协议 3，以及将关于有理数大小比较的协议 3 与文献[10]中的相关协议(协议 2 和协议 3)的执行效率进行比较. 由于目前尚未见到关于两个区间位置关系保密判定问题的相关研究，仅对协议 2 的复杂性进行分析. 在分析协议的计算复杂性时只考虑费时较多的模指数运算次数，协议的准备工作和其他简单计算忽略不计.

协议 1 的复杂性分析与比较. 本文协议 1 中，Bob 加密 3 次，解密 1 次，共需要进行 8 次模指数运算；Alice 在第 2 步计算 R_w 时要做 3 次模指数运算. 协议 1 共需要模指数运算 11 次和 2 轮通信.

在文献[24]中，研究有理数与有理区间位置关系的协议 2 需要 20 次模指数运算，需要 2 轮通信；而协议 3 需要 13 次模指数运算，需要 3 轮通信.

协议 3 的复杂性分析与比较. 本文协议 3 的执行中，Bob 需加密 2 次，解密 1 次，共需要 6 次模指数运算；Alice 在第 2 步计算 R_w 时要做 2 次模指数运算. 协议 3 共需要模指数运算 8 次和 2 轮通信.

在文献[10]中研究了有理数域内的百万富翁问题，其中协议 2(协议 3)共需要 10 次(8 次)模指数运算，以及 2 轮(3 轮)通信.

协议 2 的复杂性分析. 本文协议 2 分前后两部分，如果前部分执行后协议结束，那么需要 22 次模指数运算和 2 轮通信，如果需要前后两部分全部执行完才能获得结果，则共需要 44 次模指数运算和 4 轮通信.

本文协议复杂性更清晰的分析结果在表 1 中列出.

表 1 协议效率的分析比较

比较的文献	计算复杂性	通讯复杂性
本文协议 1	11	2
[24,协议 2]	20	2
[24,协议 3]	13	3
本文协议 3	8	2
[10,协议 2]	10	2
[10,协议 3]	8	3
本文协议 2	22(44)	2(4)

为了测试协议的计算效率,应用 Java 编程语言实现了三个协议.实现的平台如下:操作系统为旗舰版 Windows 7,CPU 为 Intel(R)酷睿 i3-2100@3.10GHz;内存 4.00GB,64 位操作系统.实验设定 Paillier 加密算法中使用的大素数 p 和 q 的位数为 256 bits.分别对文献[24],文献[10]以及本文协议进行实际计算,结果如表 2～表 4 所示(表中的数据为 1000 组随机实验数据的平均值).

表 2 有理数与有理区间位置关系协议的实验结果

比较的文献	Alice 耗时/ms	Bob 耗时/ms	总耗时/ms
[24,协议 2]	10.652	40.931	51.583
[24,协议 3]	5.982	22.245	28.227
本文协议 1	1.937	21.825	23.762

表 3 有理数大小比较协议的实验结果

比较的文献	Alice 耗时/ms	Bob 耗时/ms	总耗时/ms
[10,协议 2]	22.3270	5.7179	28.0449
[10,协议 3]	1.0826	21.7516	22.8342
本文协议 3	1.0394	21.0031	22.0425

表 4 两有理区间位置关系判定协议的实验结果

	Alice 耗时/ms	Bob 耗时/ms	总耗时/ms
本文协议 2	2.013	44.128	46.141

文献[24]和[10]的协议 2 中均需要调用整数集上的社会主义百万富翁协议,在验证协议的执行时间时,未包含这部分调用协议所需时间.因此,理论分析和实验结果都表明本文协议具有较高的计算效率.

7 恶意模型下有理数域内点与区间位置关系判定问题

7.1 协议编译器

下面简要介绍如何应用文献[7]中的协议编译器,以半诚实模型下保密计算某一个函数 f 的协议 π 为基础(在协议 π 中,每一方有一个局部输入,并使用一个均匀分布的局部随机带(random-tape)),编译产生一个在恶意模型下安全的"等价协议".为了阐明构造协议编译器的原理,首先考虑一个恶意方可能做的事情(超越半诚实参与者所做的).

(1)一个恶意方在协议的实际执行中可能用了一个不同于它的设定输入(即"替代了它的输入"),这种行为无法避免.但协议需要保证所做的替代与其他方的输入不相关,即替代仅依赖于它原本的设定输入,可应用输入承诺函数[7]实现此目的.

(2)一个恶意方可能在协议的实际执行中应用了并非均匀分布的随机带.我们所需要做的是强迫该参与方应用一个均匀分布的随机带,可应用增强掷币函数[7]实现此目的.

(3)一个恶意方可能试图去发送不同于原模型(半诚实模型)中所规定的信息.我们所要做的是强迫该参与者去发送由它(已经承诺)的局部输入和随机带按规定所计算的结果,可应用认证计算函数[7]以及零知识证明系统[29]实现此目的.

以协议 1 为基础可以构造出在恶意模型下安全的计算协议.

协议 4. 恶意模型下有理数与有理区间位置关系判定协议.

输入:Alice 输入有理点 $w=\frac{w_1}{w_2}$,Bob 输入有理区间 $I=[u,v]=\left[\frac{u_1}{u_2},\frac{v_1}{v_2}\right]$.

输出:Alice 输出 $y=S(w,[u,v])$,Bob 输出 λ.

准备:在 Paillier 门限密码方案中,Alice 和 Bob 共同分享解密密钥 sk,用于加密的公钥为 $pk=(g,N)$.

在协议执行中 Alice 和 Bob 需要验证他们收到的所有证明的正确性,如有证明未通过验证,则中止协议.

1. Alice 和 Bob 应用增强掷币函数为 Bob(或 Alice)生成随机数 r_w,r(或 s).

2. Bob 计算密文 $E(r\alpha)$,$E(r\bar{\beta})$,$E(r\gamma)$,将这些密文随同关于其对应明文知识的证明发送给 Alice.

3. Alice 对 w_1,w_2 进行承诺,并应用认证计算函数计算下面密文:

$$R_w=E(r\alpha)^{sw_1^2}E(r\bar{\beta})^{sw_1w_2}E(r\gamma)^{sw_2^2}\bmod N^2,$$

Alice 将 R_w 发送给 Bob.

4. Alice 和 Bob 联合解密 R_w,得到 $u_w=D(R_w)$,并向对方发送正确解密的证明.

5. Alice 计算 $z_w=u_w-rr_wsw_1w_2$,并输出 $y=\mathrm{sgn}(z_w)$.

7.2 安全性分析

如果在协议执行中 Alice 和 Bob 对于其收到的所有证明都能通过验证,则协议是安全的.简要说明如下:

(1)首先要求 Alice 和 Bob 应用增强掷币函数生成协议中所需要的随机数,这样即可保证 r_w,r 以

及 s 确实是随机的.

(2) Bob 在发送 $E(r\alpha)$, $E(r\bar{\beta})$, $E(r\gamma)$时,同时发送了关于这些密文对应明文的证明,这可保证这些加密运算的正确性.

(3) Alice 根据认证计算函数计算 R_w,能保证所发送的 R_w是正确的.

(4) 在协议 4 中,应用了 Paillier 门限密码系统[28],此时两人可单独加密,但需要两人联合才可以解密任何密文. 解密过程中,双方需要向对方发送正确解密的证明,这可保证解密结果 $u_w=D(R_w)$的正确性.

由此可知,在协议 4 中参与者都必须按要求正确地执行协议,任何偏离协议规定的行为都会引起协议中止,如果协议正常结束,则结果一定是正确的. 给出下面定理,限于篇幅,证明省略.

定理 4.　协议 4 是恶意模型下关于有理数与有理区间位置关系问题的安全计算协议.

8　区间保密计算的实际应用

研究解决有关区间保密计算问题有重要的理论意义和实际应用价值. 在文献[24]中,详细阐述了有理数与区间保密计算的一些具体应用,本部分主要阐述两个区间位置关系在计算几何中的一些有趣应用以及在商品交易和约会时间安排中的一些实际应用.

8.1　在计算几何中的应用

(1) 保密几何中两个圆环的位置关系

利用两个区间的位置关系协议可以保密判断两个圆环形区域的位置关系. 问题具体描述如下:假设 Alice 和 Bob 分别拥有一个保密的圆环形区域(圆心相同),其圆环内圆半径分别为 r_1, r_2,外圆半径分别为 R_1, R_2,需要保密判别两个区域是否相交,相离或具有某种包含关系. 保密判断两个圆环的位置关系问题即可转换为保密判断两个区间$[r_1, R_1]$与$[r_2, R_2]$的关系问题,可以调用协议 2 进行保密判定. 图 8 所示情形表示所给的两个圆环区域相交,深色区域为两个圆环的交集部分.

(2) 保密几何中两个矩形的位置关系

问题描述如下:在平面直角坐标系中,Alice 和 Bob 各有一个保密的矩形区域 $\Omega_A=[x_1, x_2]\times[y_1, y_2]$, $\Omega_B=[x_3, x_4]\times[y_3, y_4]$,他们要保密判定两个矩形区域是否相交,相离或具有某种包含关系. 这个问题可以转化为两组区间$[x_1, x_2]$与$[x_3, x_4]$以及$[y_1, y_2]$与$[y_3, y_4]$的关系判定问题得到解决. 具体地,有下面结论:

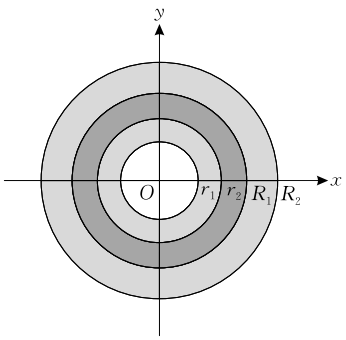


图 8　两个圆形区域位置关系(相交情形)

① 如果$[x_1, x_2]\subseteq[x_3, x_4]$与$[y_1, y_2]\subseteq[y_3, y_4]$同时成立,则 $\Omega_A\subseteq\Omega_B$. 如果$[x_3, x_4]\subseteq[x_1, x_2]$与$[y_3, y_4]\subseteq[y_1, y_2]$同时成立,则 $\Omega_B\subseteq\Omega_A$.

② 如果$[x_1, x_2]$与$[x_3, x_4]$以及$[y_1, y_2]$与$[y_3, y_4]$两组区间中至少有一组是相离的,则两矩形相离.

③ 其他情形下两矩形相交.

图 9 所示情形表示所给的两个矩形区域相交,深色区域为两个矩形的交集部分.

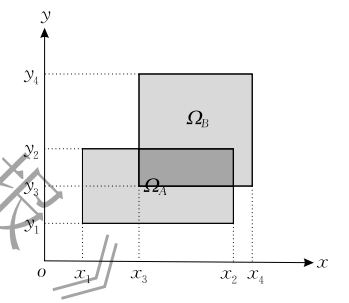


图 9　两个矩形区域位置关系(相交情形)

(3) 保密判断两个角形无限区域的位置关系

问题具体描述如下:Alice 和 Bob 分别有一个私密的角形区域(一个角形区域是由两条过原点的射线所夹的区域),需要保密判定两个区域是否相交,相离或具有某种包含关系. 假设 Alice 和 Bob 的区域分别由过原点的射线 L_1与 L_2以及 L_3与 L_4构成,而 L_i与 x 轴正向夹角分别为α_i($i=1,2,3,4$),保密判定两个区域相交,相离或具有某种包含关系可以转化为两个区间$[\alpha_1, \alpha_2]$与$[\alpha_3, \alpha_4]$的位置关系问题. 图 10 所示情形表示所给的两个角形区域相交,深色部分表示两个区域的重叠部分.

该问题的解决思想还可以推广解决下面关于多边形和角形区域位置关系问题:Alice 有一个保密的角形区域,其过原点的两条射线为 L_1与 L_2,Bob 有一个保密多边形 Ω,Bob 将多边形的每个顶点与

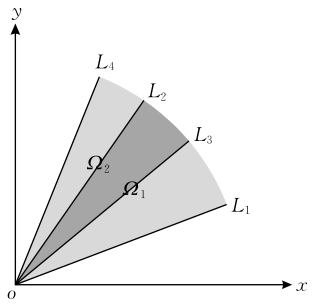


图 10 两个角形区域位置关系(相交情形)

原点相连得到若干条射线,其中将与 x 轴正向夹角最小及最大者分别记为 L_3,L_4. 如果将 L_i 与 x 轴正向夹角记为 α_i,于是,Bob 的保密多边形包含在角形区域内当且仅当 $[\alpha_3,\alpha_4]\subseteq[\alpha_1,\alpha_2]$. 图 11 所示情形表示所给多边形完全含于角形区域内.

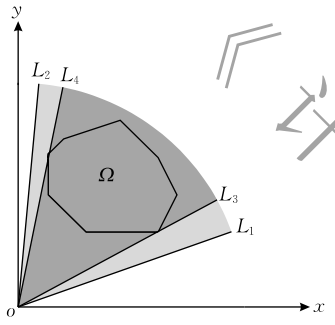


图 11 不规则多边形完全含于角形区域

8.2 商品交易及约会安排中的应用

商品交易中的应用. 商品交易中的价格谈判是非常重要的. 要使谈判有意义,谈判双方首先应该设立清晰的价格范围:底价(盈亏平衡点)和目标价,即交易双方应各自确立自己的价格区间,毫无疑问价格区间属于交易双方的商业秘密. 一般在谈判前,双方需要摸清对方的底线,预先了解交易成交的可能性,可对双方的报价进行预评估,即对双方所确定的价格区间的关系进行保密比较. 如果双方的价格区间不相交,表明双方的价格范围差异较大,即可认为交易没有成交的可能,这样就没有必要花费精力准备谈判细节. 如果双方的价格区间相交,即可认为交易有成交的可能性,这种情况下则需要花费足够的精力认真准备谈判细节. 因此对交易双方达成交易的可能性进行保密评估能够节省时间和交易成本.

在引言部分所述的商品交易问题的实例中,如果商家 B 的购买价格确定在区间[500,1000](或[200,600])内,公司 A 的商品定价区间为[800,1200]. A 和 B 需要利用协议 2 进行保密比较以决定是否应该继续磋商. 如果 B 的购买价格区间为[500,1000],由于该区间和 A 的价格区间相交,他们就可以通过进一步谈判达成交易;如果 B 的购买价格区间为[200,600],该区间和 A 的价格区间相离,A 可以选择放弃与 B 进行交易(一般来说交易双方开价都会大胆一些,两区间相离基本可以认为属于买家出价低于卖家定价的情形).

时间安排中的应用. 在实际生活中经常会遇到约会时间安排或其他活动的时间安排问题,这些问题常需要转化为区间位置关系保密判定问题来解决. 比如考虑这样的问题:某行业在某地举行峰会,届时业内重要人士将汇聚于此地,各巨头在此期间都会有一些秘密磋商的活动安排. 假如 Alice 和 Bob 有意进行一次会谈,两人对此会谈都有自己选择的时间安排,商谈之前需要保密地判定两方各自所选择的时间段是否有重叠. 如果有重叠则可进一步讨论会谈事宜;如两方给出的时间段不相交,可能意味着会谈无法举行,将无需为会谈作进一步的准备工作. 如果应用所设计的区间关系保密判定协议,实现保密判定时间安排是否相交问题,可以保护双方的商业机密又可节约会谈准备成本. 再比如,假如 Alice 和 Bob 在某一时间段内需要使用同一个资源(比如会场,或邀请某领导作报告等),由于该资源不能同时为他们所用,如果两方所选择的时间区间属于各自的秘密,那么也可应用协议 2 保密判断两方选择的时间区间是否有冲突.

9 结 论

本文用多项式表示区间从而将一个有理数与一个有理区间的位置关系问题转化为整数集上两向量的内积符号判定问题,进一步应用具有加法同态性的 Paillier 加密方案进行保密计算. 我们首先设计了有理数与有理区间位置关系保密判定协议(协议 1). 根据协议 1 的设计,两方根据其所具有的私密有理数与私密区间分别构造相应的保密向量,进而保密判定两向量内积的符号即可. 以协议 1 的设计思想为基础,进一步设计构造了两个有理区间位置关系保密判定协议(协议 2),在协议 2 的设计中,为防止额外的信息泄露,在协议 1 设计原理的基础上需要将一方参与者区间的两个端点与另一方区间的位置关系同时(混合)判定,以保证协议的安全性. 本文最后还设计了有理数域内百万富翁问题新的高效解决方案.

本文所研究的问题属于安全多方计算中的重要

问题，在保密的计算几何以及商品价格商议等方面有重要的应用前景. 目前关于这类问题的研究结果还很少，我们应用新的方法和技巧设计了关于这些问题的解决方案，详细的理论分析及具体的实例验证都表明本文的协议具有较高的计算效率，并且协议设计安全简洁，有重要的理论意义及实际应用价值.

参 考 文 献

[1] Kiayias A, Zhou H S, Zikas V. Fair and robust multi-party computation using a global transaction ledger//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Vienna, Austria, 2016: 705-734

[2] Garay J, Ishai Y, Ostrovsky R, et al. The price of low communication in secure multi-party computation//Proceedings of the 37th Annual International Cryptology Conference. Santa Barbara, USA, 2017: 420-446

[3] Yao A C. Protocols for secure computations//Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science. Chicago, USA, 1982: 160-164

[4] Goldwasser S. Multi-party computations: Past and present//Proceedings of the 16th Annual ACM Symposium on Principles of Distributed Computing. Santa Barbara, USA, 1997: 1-6

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

[6] Goldreich O, Micali S, Wigderson A. How to play any mental game//Proceedings of the 19th Annual ACM Symposium on Theory of Computing, New York, USA, 1987: 218-229

[7] Goldreich O. The Fundamental of Cryptography: Basic Applications. London, UK: Cambridge University Press, 2009

[8] Fagin R, Naor M, Winklery P. Comparing information without leaking it. Communications of the ACM, 1996, 39(4): 77-85

[9] Lin H Y, Tzeng W G. An efficient solution to the millionaires' problem based on homomorphic encryption. Applied Cryptography and Network Security, 2005, 5: 456-466

[10] Li S D, Guo Y M, Zhou S F, et al. Efficient protocols for the general millionaires' problem. Chinese Journal of Electronics, 2017, 26(4): 696-702

[11] Li S D, Wang D S, Dai Y Q, et al. Symmetric cryptographic solution to Yao's millionaires' problem and an evaluation of secure multiparty computations. Information Sciences, 2008, 178(1): 244-255

[12] Goethals B, Laur S, Lipmaa H, et al. On private scalar product computation for privacy-preserving data mining//Proceedings of the Information Security and Cryptology—ICISC 2004. Seoul, Korea, 2004: 104-120

[13] Amirbekyan A, Estivill-Castro V. A new efficient privacy-preserving scalar product protocol//Proceedings of the 6th Australasian Data Mining Conference (AusDM 2007), Queensland, Australia, 2007: 209-214

[14] Fang L, Ng W K, Zhang W. Encrypted scalar product protocol for outsourced data mining//Proceedings of the 2014 IEEE 7th International Conference on Cloud Computing. Anchorage, USA, 2014: 336-343

[15] Li S D, Wu C Y, Wang D S, et al. Secure multiparty computation of solid geometric problems and their applications. Information Sciences, 2014, 282: 401-413

[16] Atallah M J, Du W. Secure multi-party computational geometry//Proceedings of the 7th International Workshop on Algorithms and Data Structures (WADS 2001). Rhode Island, USA, 2001: 165-179

[17] Luo Yong-Long, Huang Liu-Sheng, Xu Wei-Jiang, et al. A protocol for privacy-preserving intersect-determination of two polygons. Acta Electronica Sinica, 2007, 35(4): 685-691(in Chinese)
(罗永龙，黄刘生，徐维江等. 一个保护私有信息的多边形相交判定协议. 电子学报，2007，35(4)：685-691)

[18] Freedman M J, Hazay C, Nissim K, et al. Efficient set intersection with simulation-based security. Journal of Cryptology, 2016, 29(1): 115-155

[19] Zhou Su-Fang, Li Shun-Dong, Guo Yi-Min, et al. Efficient secure set intersection problem computation. Chinese Journal of Computers, 2018, 41(2): 464-480(in Chinese)
(周素芳，李顺东，郭奕旻等. 保密集合相交问题的高效计算. 计算机学报，2018，41(2)：464-480)

[20] Soled D D, Malkin T, Raykova M, et al. Efficient robust private set intersection. International Journal of Applied Cryptography, 2012, 2(4): 289-303

[21] Nishide T, Ohta K. Multiparty computation for interval, equality, and comparison without bit-decomposition protocol//Proceedings of the 10th International Conference on Practice and Theory in Public-Key Cryptography. Berlin, Germany, 2007: 343-360

[22] Li S D, Wang D S, Dai Y Q. Symmetric cryptographic protocols for extended millionaires' problem. Science in China, 2009, 52(6): 974-982

[23] Zuo Xiang-Jian, Yang Xiao-Li, Li Shun-Dong. Privately determining protocol on three points are collinear and its application. Journal of Cryptologic Research, 2016, 3(3): 238-248(in Chinese)
(左祥建，杨晓莉，李顺东. 三点共线的保密判断问题及应用. 密码学报，2016，3(3)：238-248)

[24] Guo Yi-Min, Zhou Su-Fang, Dou Jia-Wei, et al. Efficient privacy-preserving interval computation and its applications. Chinese Journal of Computers, 2017, 40(7): 1664-1679(in Chinese)
(郭奕旻，周素芳，窦家维等. 高效的区间保密计算及应用. 计算机学报，2017，40(7)：1664-1679)

[25] Paillier P. Public-key cryptosystems based on composite degree residuosity classes//Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques. Prague, Czech Republic, 1999: 223-238

[26] Armknecht F, Katzenbeisser S, Peter A. Group homomorphic encryption: Characterizations, impossibility results, and applications. Designs, Codes and Cryptography, 2013, 67(2): 209-232

[27] Bellare M. A note on negligible functions. Journal of Cryptology, 2002, 15(4): 271-284

[28] Xia Z, Yang X, Xiao M, et al. Provably secure threshold Paillier encryption based on hyperplane geometry//Proceedings of the 21st Australasian Conference on Information Security and Privacy (ACISP 2016). Melbourne, Australia, 2016: 73-86

[29] Cramer R, Damgård I, Nielsen J B. Multiparty computation from threshold homomorphic encryption//Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques. Innsbruck, Austria, 2001: 280-300

DOU Jia-Wei, Ph. D., associate professor. Her main research interests include applied mathematics and applied cryptography.

WANG Wen-Li, M. S. candidate. Her main research interests include applied mathematics and applied cryptography.

LI Shun-Dong, Ph. D., professor, Ph. D. supervisor. His research interests include cryptography and information security.

Background

Our society has entered into information times. We are living in the information age. Internet and IoT have been greatly affected all aspects of our life, and produce mass data at all times. It needs great computing capability to process the data to help us to improve the efficiency of economic activities, to improve social management, to benefit mankind etc. Almost no entities are capable of processing their data promptly. Therefore, cloud computing, outsourced computing and cooperative computing are increasingly popular. But these computing modes pose great challenge to the privacy of their data. How to protect the privacy of the data is a key barrier to popularize these computing modes. Secure multiparty computation is crucial technology to protect data privacy in network world and in these cooperative computing processes. It can be widely used to protect privacy in electronic commerce, data-mining, scientific computing, social management etc.

Secure multiparty computation is a research focus in the international cryptographic community in recent years. There are many papers of secure multiparty computation at the three top international cryptographic conferences. We have studied this subject for more than ten years, and solved many practical secure multiparty computation problems. Our study has won the support of the National Natural Science Foundation of China.

In this paper, we study how to perform private computations on private rational numbers, mainly on how to privately determine the relation between a rational number and a rational interval, and the relation between two rational intervals. The second problem is a completely new secure multiparty scientific computation problem. To the best of our knowledge, it has not been investigated. Representing an interval as a polynomial, we present efficient protocols for these two problems involving rational interval. We prove that all our protocols are secure in the semi-honest model. We show the applications of the rational interval protocol, compare our protocols with related results theoretically and experimentally. Theoretical analysis and the simulation results show that our protocols are efficient. We will study protocols for malicious parties for these problems in future research.

The study is supported by the National Natural Science Foundation of China under Grant No. 61272435. The purpose of this project is to solve all kinds of confidential problems in field of cryptography. Our team has been devoted to exploring and analyzing cryptographic protocols for over 10 years, such as SMC, SMC geometry, 1-out-of-m oblivious transfer, zero knowledge proof. We have published over 60 papers, of which over 30 have been indexed by SCI.