高效的区间保密计算及应用

郭奕旻[1),2)] 周素芳[1)] 窦家维[3)] 李顺东[1)] 王道顺[4)]

[1)](陕西师范大学计算机科学学院 西安 710119)

[2)](中国科学院软件研究所可信计算与信息保障实验室 北京 100190)

[3)](陕西师范大学数学与信息科学学院 西安 710119)

[4)](清华大学计算机科学与技术系 北京 100084)

摘 要 多方保密计算是目前国际密码学界的研究热点,是网络空间隐私保护与信息安全的关键技术.密码学者已经研究了很多多方保密计算问题,但更多的多方保密计算问题还有待研究.文中研究一个重要的多方保密计算问题——有理数的区间的保密计算,即保密地计算一个保密的有理数在不在另一个保密的有理数区间内.该问题在密码学中有重要的理论意义,在其他多方保密计算协议的构造中有重要的实际意义,在隐私保护方面有广泛的应用.其中包括计算几何上的点与圆环的包含问题,点与无限区域的包含问题,点与线段的包含问题等.甚至在现实的商品交易中,运用该问题的解决方案能够减少交易成本.文中基于 Paillier 同态加密方案,以百万富翁协议为基本思想,利用计算几何理论,将有理数区间保密计算问题输入的有理数看成过原点的直线的斜率,将区间保密计算问题归约为直线之间的位置关系,根据平面直角坐标系上三点定义的三角形面积计算公式,设计了一个高效的有理数区间保密计算协议;采用基本算术知识,将有理数的大小比较归约到算术不等式的判定,调用对称密码整数集百万富翁协议,设计了另一个高效的有理数区间保密计算协议;用模拟范例证明了两个协议的安全性;通过理论和实际编程分析了协议的效率;分析表明两个协议是正确高效的;最后给出了协议在解决其他多方保密计算问题中的应用实例.

关键词 密码学;多方保密计算;区间保密计算;同态加密

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2017.01664

Efficient Privacy-Preserving Interval Computation and Its Applications

GUO Yi-Min[1),2)] ZHOU Su-Fang[1)] DOU Jia-Wei[3)] LI Shun-Dong[1)] WANG Dao-Shun[4)]

[1)](*School of Computer Science, Shaanxi Normal University, Xi'an* 710119)

[2)](*Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing* 100190)

[3)](*School of Mathematics and Information Science, Shaanxi Normal University, Xi'an* 710119)

[4)](*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084)

Abstract Secure multiparty computation (SMC) is presently a research focus in the international cryptographic community and a key technology of privacy preserving and information security in cyberspace. This paper investigates an important SMC problem, specific privacy-preserving rational interval computation (PIC). PIC attempts to securely determine whether one private rational number belongs to a private rational interval. This problem is of theoretical cryptographic importance, has practical importance in constructing other SMC protocols, and has many PIC-related applications, such as the inclusion problems between point and ring, point and infinite region, point and segment, and so on, even is able to reduce the cost in real commodity transaction.

收稿日期:2015-05-19;在线出版日期:2016-04-24.本课题得到国家自然科学基金(61272435,61373020,U1536102,U1536116)和中央高校基本科研业务费专项资金(GK201504017)资助.**郭奕旻**,女,1992 年生,博士研究生,主要研究方向为信息安全与密码学.E-mail:yiminguo@snnu.edu.cn.**周素芳**,女,1990 年生,博士研究生,主要研究方向为信息安全与密码学.**窦家维**(通信作者),女,1963 年生,博士,副教授,主要研究方向为应用数学与应用密码学.E-mail:jiawei@snnu.edu.cn.**李顺东**,男,1963 年生,博士,教授,博士生导师,主要从事密码学与信息安全研究.**王道顺**,男,1964 年生,博士,副教授,博士生导师,主要研究领域为密钥管理、数字水印与多媒体安全.

Based on Paillier's homomorphic encryption and the ideas in the millionaire's methods, firstly, we study the PIC problem from the viewpoint of geometry, where we consider that the private inputs as the slopes of lines that pass through the origin of the coordinates. Thus, the PIC problem can be reduced to the relationship between those lines. Then, we use the formula for computing the area of a triangle formed by three points to construct an efficient rational PIC protocol. Secondly, we regard the comparison as arithmetic inequalities and call an integral millionaire's approach based on symmetric cryptography, propose another efficient rational PIC protocol. Thirdly, we prove the privacy-preserving properties of these two protocols by using simulation paradigm and analyze their theoretical and practical efficiency. Analysis shows that these protocols are efficient. Finally, we demonstrate applications of these two PIC protocols.

Keywords　cryptography; secure multiparty computation; privacy-preserving interval evaluation; homomorphic encryption

1　引　言

多方保密计算(secure multiparty computation)的概念首先由 Yao[1] 以百万富翁问题提出，是国际密码学界近年来的研究热点，是网络空间隐私保护与信息安全的关键技术. 利用多方保密计算，两方或者多方可以在不泄露他们私有数据信息的情况下，利用隐私信息合作进行有社会、经济、科学与技术意义的计算，挖掘私有数据的价值，更好地发挥私有数据对于社会、经济、科学与技术的积极作用. 在密码学与信息安全中具有重要的理论与实际意义.

多方保密计算概念提出后，许多学者对多方保密计算进行了深入研究，推进了多方保密计算研究的发展. Yao 利用混淆电路(garbled circuit)证明了一般的多方保密计算问题都是可解的. 一些两方保密计算协议提出以后，Goldreich 等人[2-3] 进一步将两方保密计算推广到多方，定义了多方保密计算协议的安全性，提出了安全性证明的模拟范例，并通过将一般的多方保密计算问题归约到智力游戏(mental game)，证明了理论上所有多方保密计算问题均可解. 但因为效率的问题，用电路方法和智力游戏的方法解决一般的多方保密计算问题都是不实际的. 因此 Goldreich 指出：对于具体的问题，需要研究具体的解决方案，利用具体问题的条件，可以设计出高效的解决方案. Goldreich 对多方保密计算还有一个重要贡献[3]，他设计了一个编译器，给定一个半诚实模型下保密计算函数 f 的多方保密计算协议 π，编译器可以自动生成一个在恶意模型下保密计算 f 的多方保密计算协议 Π，从而证明了如果一个多方保密计算问题在半诚实参与者模型下可以解决，那么它在恶意参与者模型下也是可解的. 随后，Franklin 等人[4] 和 Gennaro 等人[5] 对多方保密计算作了形式化定义. 这些成果为多方保密计算研究奠定了基础.

作为密码学领域的热门研究方向，在以上研究成果的理论指引下，其他学者研究了许多具体的多方保密计算问题，包括保密信息比较[6-7]、保密几何计算[8-9]、保密数据挖掘[10]、隐私入侵检测[11]、百万富翁问题[1,12-20]、理性多方保密计算[21]、保密竞拍[22-23] 等，这些协议已经作为密码学其他研究领域的基本模块，广泛地应用于秘密共享[24-25]、外包计算[26]、电子商务[27] 和保密数据结构[28] 等.

区间保密计算是一个新的多方保密计算问题，具体可以描述为参与者需要保密地判断一个私密有理数 p 是否在一个私密有理数区间 $[m,n]$ 内. 从目前的研究来看，曾有学者研究过隐私数与有限集合的包含问题[20]，但其协议并不适用于解决有理数区间(无限集合)包含问题，也有学者设计了一个基于秘密共享的比特分解协议[29]，并将区间保密计算作为该协议的一个应用给出了解决方案，可是该文献并未对区间保密计算问题进行深入的理解和分析，其解决方案也存在不足. 事实上，区间保密计算的协议设计需要考虑许多安全因素，没有完整的理论安全分析和应用分析，并不能体现出区间保密计算问题存在的价值.

区间保密计算在密码学问题中具有理论研究意义，在隐私保护方面也有广泛的应用，其中包括计算几何上的点与圆环的包含问题，点与无限区域的包含问题，点与线段的包含问题等(具体内容在本文第

6 节进行了详细的描述),甚至在现实的商品交易中,运用该问题的解决方案能够减少交易成本.

根据区间保密计算问题的含义可知其解决方案涉及隐私的数与数之间比较问题,因此区间保密计算也可看作是百万富翁问题的延伸,但安全性要求比百万富翁问题更多.在其协议的设计上,需要参考百万富翁协议的主要思想.除此之外,还需要考虑特定条件下的安全性问题.目前百万富翁问题的研究情况如下:

百万富翁问题最早由 Yao 在文献[1]中提出,自提出以来已有许多有效的解决方案.其问题可以简单描述为:两个百万富翁 Alice 和 Bob 希望知道谁的财产更多,但是双方都不想向对方暴露自己的财产值,所以需要设计一个保密协议能够在不泄露双方保密值的情况下得到双方保密值的大小关系.Yao 在文献[1]中设计出了一个协议,但是该协议的效率比较低.Yao 提出的这个百万富翁问题很快引发了密码学研究者们的热情,目前,已有许多成果.这些研究对多方保密计算的发展起到了促进作用.

Boudot 等人[12]设计了一个解决社会百万富翁问题的公平协议,在离散对数和 Diffie-Hellman (DDH)困难性假设前提下,该协议在公平模式下的计算复杂度为 $O(k)$(k 是安全性参数).作为社会主义百万富翁问题的解决方案,该协议只能保密地判断两个数是否相等.Fischlin[13]提出了一个基于 Goldwasser-Micali 概率加密方案的非交互式百万富翁协议.在半诚实参与者模型下,每个参与者需要进行的模乘运算与输入的保密数长度成正比.该协议只能判断两个保密数的关系是大于还是小于等于,不能区分小于和等于的关系.Ioannidis 等人[14]提出了一个 OT_2^1不经意传输的百万富翁协议,该协议需要并行调用不经意传输 n 次(n 代表保密输入的长度,并会受到不经意传输安全参数的限制),其时间复杂度为 $O(n)$.

文献[15]构造了一个基于特殊的函数和 OT_m^1 不经意传输的百万富翁协议,虽然与 Yao 的协议相比,该协议的效率有很大的提升,但该协议仍然存在计算冗余.Lin 等人[16]通过设计一种创意的 0-1 编码,将百万富翁问题通过编码转换成一个集合相交问题,然后根据 ElGamal 乘法同态加密算法,提出了一种基于 0-1 编码的百万富翁协议.然而该协议的计算消耗仍然会随着保密输入长度的扩大而增加.Garay 等人[17]提出了两种分别需要对数轮和常数轮通信复杂度的百万富翁协议,这两种协议只能解决整数集的百万富翁问题.文献[18]设计了一个新的 0-1 编码方案,将百万富翁问题归约到向量的部分标量积的计算,然后利用 Paillier 加法同态加密体制,构造了一个高效的百万富翁协议.在假定保密输入且 $|U|=m$ 的情况下,该协议的计算复杂性为 $O(m)$.Gordon 等人[19]利用 *ShareGen* 函数和一个下三角矩阵定义了一个新的函数表达,并通过该函数设计了一个特殊的完全公平的百万富翁协议.该协议同样只能判断两个保密数的关系是大于还是小于等于,不能区分小于和等于的关系.

不同于以上介绍的基于公钥密码系统设计出的协议,Li 等人在文献[20]中将百万富翁问题归约成一个有限集合包含问题,设计出了一种基于对称密码学的百万富翁协议,这也是目前的研究成果中检索到的唯一基于对称密码算法的百万富翁协议.该协议不采用公钥密码系统的模指数运算,因此降低了协议的时间复杂度.但该协议不能完全判断两个保密数的大于和等于的关系.有限集合包含问题具体可以描述为判断一个非负整数 x 是否属于一个非负整数集合 $X=\{x_1,x_2,\cdots,x_n\}$,可以看作是区间保密计算的一个特殊情况,而非完整意义上的区间保密计算概念.因为非负整数集合 $X=\{x_1,x_2,\cdots,x_n\}$ 是有限集合,随着集合元素的增多,协议的耗时将会线性增长,而有理数区间是无限集合,在集合元素无限的情况下,有限集合包含协议将会变得不实用.

区间保密计算协议首次由 Nishide 等人在文献[29]中提出,不过区间保密计算并不是该文献的主要研究对象.该文献提出了一个改进的基于秘密共享的比特分解协议,并为该协议设计了 3 个应用协议,其中就包括区间保密计算协议.基于秘密共享的比特分解协议是一类将计算电路和布尔电路结合起来的比特协议,它的特点是将多项式的秘密 a 转换成比特后再进行共享,能够进行有效的面向比特操作.从 Nishide 等人提出的区间保密计算协议主要思想上来看,比特分解协议具有重要的理论意义,但是对于区间保密计算问题而言的实际意义十分有限,考虑到输入比特转换和计算过程的计算复杂度和通信复杂度,用这类思想设计高效的区间保密计算协议是不实际的.从协议本身来看,该协议并不能完美解决问题.首先,对于一个私密区间$[m,n]$,该协议不能判断出私密数 p 与右边界 n 的大于或等于关系,即当 $p=n$ 时,应该输出 $p\in[m,n]$,而协议输出错误;其次,该协议的所定义的区间只是基于整数集而非有理数域,其本质上也只是一个有限的集

合包含协议.

从定义上来看，区间保密计算的直观解决思路是执行两次百万富翁协议，但实际上这个思想存在问题，我们在第 3 节里会详细分析并加以解决. 由此可以看出，百万富翁协议是区间保密计算一个重要研究前提.

目前已有的百万富翁协议均是基于整数集上的协议，如果采用类似直观思想，区间保密计算的应用范围也将局限于整数集，就会成为一个有限集合问题，这样也会降低区间保密计算的研究意义和应用场景. 若将区间保密计算定义域扩展到有理数域，由于区间里存在无穷多个有理数，区间保密计算也可以描述为一个保密有理数和一个保密无限有理数区间的包含关系判定问题，将问题从有限领域扩展到无限领域本身就具有重大的研究价值. 所以研究区间保密计算既要参考现有的百万富翁协议思想，也需要在此思想上加以创新和变更，才能使区间保密计算协议具有更多的实际意义和应用场景.

本文以百万富翁协议为基本思想，利用计算几何定理，将有理数区间保密计算问题输入的有理数看成几何中直线的斜率，根据平面直角坐标系上三点定义的三角形面积计算公式，设计了一个高效的有理数区间保密计算协议. 然后采用基本算术知识，调用对称密码整数集百万富翁协议，设计了另一个高效的有理数区间保密计算协议.

本文的贡献如下：

(1) 对区间保密计算问题进行了完整的理论和实际分析.

(2) 利用计算几何定理和基本算术知识设计了两个高效的有理数区间保密计算协议，并证明了方案的安全性.

(3) 给出了区间保密计算协议的应用实例，扩大了多方保密计算的研究领域与实际应用范围.

本文第 2 节介绍预备知识、安全性定义和设计区间保密计算协议需要用到的基本模块；第 3 节提出两个有理数区间保密计算的解决方案；第 4 节证明以上协议的安全性；第 5 节分析协议的效率；第 6 节介绍区间保密计算的应用场景；第 7 节给出本文的总结.

2　预备知识

2.1　安全性定义

(1) 双方计算

双方计算是一个把随机的输入对映射成为输出对的随机计算过程，用函数表示为

$$f:\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^*\times\{0,1\}^*.$$

该函数表示对于任意的输入对(x,y)，会输出一个随机变量$(f_1(x,y),f_2(x,y))$. 一个参与方输入 x，希望通过保密计算得到 $f_1(x,y)$，另一个参与方输入 y，希望通过保密计算得到 $f_2(x,y)$，变量的范围是一对字符串. 这样的函数又可以记为

$$(x,y)\to(f_1(x,y),f_2(x,y)).$$

(2) 理想双方保密协议

理想的双方保密计算协议是假定存在一个正直可信的第三方(Trust Third Party，TTP)，他不会透露隐私信息也不会传递虚假信息. 因此在拥有可信第三方的基础上，参与者 Alice 和 Bob 分别把自己拥有的秘密数 x,y 告诉 TTP，由 TTP 单独计算出 $f(x,y)$，然后将该结果分发给 Alice 和 Bob 而不透露其他任何信息，参与者 Alice 和 Bob 也不能从获得的结果中得到任何其他信息. 这种理想的协议是双方保密计算协议中安全性最高的，任何实际协议在任何情况下计算 $f(x,y)$的安全性都不会高于理想保密协议. 但在现实的复杂网络中，参与者双方都信任的第三方是不存在的，因此需要设计在没有可信第三方的情况下安全保密的协议，并通过和理想保密计算模型的比较来检验其安全性.

(3) 半诚实与恶意参与者模型

本文提出的协议和安全性均适用于半诚实参与者. 半诚实参与者在参与协议的过程中完全按照协议的规定执行，不会欺骗和泄露消息，但是可能会收集和保留在执行协议中获得的一切数据，并试图从这些数据中推断出额外的信息，因此也称这种参与者为被动参与者或诚实但好奇参与者(honest-but-curious). 多方保密计算新问题的初期研究基本上都是以半诚实模型为基础.

恶意参与者在参与协议的过程中不会完全按照协议来执行，他们以破坏协议正确性或以获取其他参与者的隐私输入为目的，在协议中甚至可以控制其他参与者来按照自己设计的方式来参与协议，因此也称这类参与者为主动攻击者. 在对某个多方保密计算问题深入研究后，部分的学者会转向研究恶意模型下安全多方计算协议[30-33].

但到目前为止，研究最多的还是半诚实模型下安全多方计算协议，这是因为[3]：① 多方保密计算的参与者大多数是半诚实的；② 研究半诚实模型下的多方保密计算是研究恶意模型下多方保密计算的基础. 有了半诚实模型下安全的协议，才可以针对协议中可能发现的恶意行为进行改进从而成为恶意模

型下安全的协议[34],也可以利用 Goldreich 的编译器自动生成一个恶意模型下安全的多方保密计算协议.这基本上是设计多方保密计算协议的方法论.

(4)隐私的模拟范例

模拟范例是由 Goldreich 提出的,在安全多方计算协议安全性证明中广泛使用的证明方法.相比于其他安全性证明方法,模拟范例更为简便.它可以模拟协议参与者执行协议的过程.其证明原理为:如果参与者都将自己的输入提交给一个可信的第三方,得到自己的输出.每个参与者利用自己的输入和输出单独模拟协议的执行过程,能得到安全多方计算协议中他能得到的任何信息,就说明参与者不能从实际多方保密计算协议中得到比理想多方保密计算协议更多的信息,即证明协议的计算过程是保密的.

模拟范例的具体描述如下:假设有两个参与方 Alice 和 Bob 需要进行保密的双方计算,设

$$f=(f_1,f_2):\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^*\times\{0,1\}^*$$

是一个概率多项式时间函数,π 代表函数 f 的双方协议.在输入为(x,y)的情况下,执行协议 π 时获得信息序列可以表示为

$$view_i^{\pi}(x,y)=(x,r^i,m_1^i,\cdots,m_t^i),$$

其中 i 代表第 i 参与方,r^i 代表参与方 i 产生的随机数,m_j^i 代表参与方 i 收到的第 j 个消息;参与者的输出可表示为

$$output_i^{\pi}(x,y),\ i=1,2.$$

定义 1[3]. 对于协议 π 和函数 $f(x,y)$,如果存在概率多项式时间算法 S_1 和 S_2 使得

$$\{S_A(x,f_1(x,y)),f_2(x,y)\}_{x,y}\overset{c}{\equiv}\{view_1^{\pi}(x,y),output_2^{\pi}(x,y)\}_{x,y} \quad (1)$$

$$\{f_1(x,y),S_B(x,f_2(x,y))\}_{x,y}\overset{c}{\equiv}\{output_1^{\pi}(x,y),view_2^{\pi}(x,y)\}_{x,y} \quad (2)$$

成立,则协议 π 保密地计算 $f(x,y)$,其中$\overset{c}{\equiv}$代表在计算上是不可区分的.

2.2 同态加密

同态加密能够在保证明文机密性的前提下,通过对密文进行运算来代替对明文的运算,获得相应的密文.同态加密不仅在多方保密计算领域,在其他安全领域也起着重要的作用.这个概念首次在文献[35]中提出,如今同态加密研究已经成为密码学界的研究热点.加法同态和乘法同态是目前比较流行的两类同态加密方案.

Paillier 在文献[36]中提出了一个加法同态加密方案满足下列性质:

$$E(x+y)=E(x)\cdot E(y),$$

$$E(x\cdot y)=(E(x))^y.$$

Paillier 方案具体过程如下:

准备:设 $N=pq$,p 和 q 是两个大素数;

$$\lambda(N)=lcm(p-1,q-1);$$

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

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

$$L(u)=\frac{u-1}{N}(aDu\in S_N);$$

$g\in B$ 为公钥;λ 为私钥.

加密:选择一个随机数 $r<N$,明文 $m<N$,加密过程为

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

解密:密文 $c<N^2$,解密计算为

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

2.3 三角形面积公式

平面解析几何学中给出了计算三角形面积的公式.假设有一个由 $P_1(x_1,y_1)$,$P_2(x_2,y_2)$ 和 $P_3(x_3,y_3)$构成的三角形$\triangle P_1P_2P_3$,它的面积计算公式可以表示为

$$S_{\triangle P_1P_2P_3}=\frac{1}{2}\begin{vmatrix}x_1&y_1&1\\x_2&y_2&1\\x_3&y_3&1\end{vmatrix}=\frac{1}{2}[y_1(x_3-x_2)+x_1(y_2-y_3)+x_2y_3-x_3y_2] \quad (3)$$

值得注意的是,式(3)计算出的三角形面积的符号是根据点 $P_1(x_1,y_1)$,$P_2(x_2,y_2)$ 和 $P_3(x_3,y_3)$的方向排列确定的,若点 $P_1(x_1,y_1)$,$P_2(x_2,y_2)$ 和 $P_3(x_3,y_3)$呈逆时针方向排列,根据式(3)计算出的三角形面积结果为正值,若点 $P_1(x_1,y_1)$,$P_2(x_2,y_2)$ 和 $P_3(x_3,y_3)$呈顺时针方向排列,计算出的三角形面积结果为负值.

2.4 基于对称密码学的百万富翁解决方案

百万富翁问题具体可以描述成两个百万富翁 Alice 和 Bob 想在不泄露各自财富值的情况下,比较两人谁的财富更多.该问题的数学表达为:Alice 有保密数 x,Bob 有保密数 y,如何保密地比较 $x>y$ 或 $x<y$ 或 $x=y$?

在文献[20]中,Li 等人提出了一个基于对称密码学的安全协议来解决百万富翁问题.由于在不失一般性的情况下,比特异或运算相对于模指数运算

是可以被忽略的[37]，即对称加密的计算复杂度远小于公钥加密运算，所以 Li 的协议是高效的. 作为百万富翁协议，其局限之处在于该协议只能判断 $x<y$ 或 $x\geq y$ 这两种大小关系，而不能区分 $x=y$ 或 $x>y$. 我们利用其性质将该协议作为基本模块来设计第 3 节提出的协议 3. Li 的协议的具体步骤如下：

协议 1.　基于对称密码学的百万富翁解决方案.

输入：Alice 的保密数为 x，Bob 的保密数为 y

输出：$x<y$ 或 $x\geq y$

准备：假设 $x,y\in U$，Bob 准备工作如下：

(1) 产生一个集合 $X=\{1,2,\cdots,y-1\}$，并计算 $\overline{X}$，使得

$$X\cup\overline{X}=U,\ |U|=t.$$

(2) 从 $\{X,\overline{X}\}$ 中选择一个集合

$$A=\{a_1,a_2,\cdots,a_k\},\ |A|<|U|/2.$$

(3) 基于集合 A，构造一个新的集合

$$B=\{b_1,b_2,\cdots,b_k,b_{k+1},\cdots,b_t\},$$

使得 $b_i=a_i(1\leq i\leq k)$，$b_i\notin U(k+1\leq i\leq t)$.

1. Alice 和 Bob 分别产生一个伪随机序列

$$R=\{r_1,r_2,\cdots,r_t\},$$
$$S=\{s_1,s_2,\cdots,s_t\}.$$

Alice 将

$$C=x\oplus R=\{x\oplus r_1,x\oplus r_2,\cdots,x\oplus r_t\}=\{c_1,c_2,\cdots,c_t\}$$

发送给 Bob.

2. Bob 计算

$$D=B\oplus S=\{b_1\oplus s_1,b_2\oplus s_2,\cdots,b_t\oplus s_t\}=\{d_1,d_2,\cdots,d_t\},$$
$$E=C\oplus S=\{c_1\oplus s_1,\cdots,c_t\oplus s_t\}=\{x\oplus r_1\oplus s_1,\cdots,x\oplus r_t\oplus s_t\}=\{e_1,e_2,\cdots,e_t\},$$

并对 E 生成一个伪随机置换

$$\psi(E)=\{e_{\psi(1)},e_{\psi(2)},\cdots,e_{\psi(t)}\}.$$

Bob 将 D 和 $\psi(E)$ 发送给 Alice.

3. Alice 计算

$$G=D\oplus R=\{b_1\oplus s_1\oplus r_1,\cdots,b_t\oplus s_t\oplus r_t\},$$

并发送 $|\psi(E)\cap G|$ 给 Bob.

4. Bob 首先判断

$$|\psi(E)\cap G|=1\Rightarrow x\in B;\ \text{否则 } x\notin B.$$

然后判断

$$(x\in B)\wedge(A=X)\Rightarrow x\in X\Rightarrow x<y;$$
$$\text{否则 } x\notin X\Rightarrow x\geq y,$$
$$(x\notin B)\wedge(A=\overline{X})\Rightarrow x\in X\Rightarrow x<y;$$
$$\text{否则 } x\notin X\Rightarrow x\geq y.$$

Bob 把结果告诉 Alice.

3　高效的有理数区间保密计算协议

不同于普通的百万富翁问题只是比较两个具体私密数值的大小，区间保密计算可以用来保密判断一个私密数是否在一个私密区间内，这类协议可以广泛应用在商品交易中减少一定的交易时间和成本. 例如，Bob 想要从 Alice 那儿购买某种大宗商品，Bob 对于这件商品能支付的单价在 500 元到 1000 元之间，但又不想告知 Alice 自己的出价范围，因为若 Alice 知道了，就会开出 Bob 所能承受的最高价以谋取更高的利益. 同样，Alice 对于自己的商品定价为 800 元，但不想告知 Bob 自己的定价，却想判断 Bob 是否能够负担得起. 因此 Alice 和 Bob 都需要进行一次保密比较来决定是否应该继续磋商并达成合理的价格. 如果 Bob 的价位低于 Alice 的定价，Alice 可以选择放弃与 Bob 的交易而寻找出价更高的买家. 如果 Bob 的价格范围包含 Alice 的定价，他们就可以通过谈判达成交易. 于是，这里就需要设计一个安全协议，作为 Alice 和 Bob 预备交易的条件，来保密地比较 Alice 的定价 800 是否在 Bob 的价位区间[500,1000]内. 在如今飞速发展的经济贸易时代，商品交易现象数不胜数，如果能够设计出这样一个协议，来对交易双方的交易价格进行一个预先的比较估计，对于交易双方来说，都能节省不少的时间和交易成本. 因此，区间保密计算协议具有实际意义.

为了方便设计区间保密计算协议，我们先将该问题抽象为：Alice 拥有保密值 p，Bob 拥有保密区间$[m,n]$，如何保密地判断 p 是否属于区间$[m,n]$？值得注意的是，区间保密计算协议的安全性要求如果保密值 p 不在保密区间$[m,n]$中，Alice 与 Bob 都不应该知道 $p<m$ 或 $p>n$.

仅研究出在整数集的区间保密计算协议还远不能应用于实际，这样区间保密计算问题只会成为一个特殊的有限集合问题，大大降低了研究意义和应用场景. 研究有理数域的区间保密计算问题，不仅将问题从有限领域扩展到无限领域，扩大了研究价值，也在实际中拥有更广阔的应用场景，这是因为在现实的商品交易过程中，p，m 和 n 更有可能是有理数，例如 Alice 拥有保密值 532.8，Bob 拥有保密区间[489.6,1102.9]. 所以有理数域上的区间保密计算协议是本文的研究创新.

直观上考虑，设计有理数域上的区间保密计算协议涉及到有理数的比较问题. 我们曾考虑过直接并行执行两次百万富翁协议来达到最终目的，但遇到了下面 3 个问题：

(1) 从目前已有的百万富翁协议来看，只能解

决整数集上的百万富翁比较.

(2)执行两次百万富翁协议会暴露除 $p\in[m,n]$ 或 $p\notin[m,n]$外的额外信息,如 $p<m$ 或 $p>n$.

(3)用同一个隐私数 p 执行两次百万富翁协议不符合多方保密计算的安全定义,且可能导致信息泄露.

我们还考虑过直接将有理数编码成 0,1 比特串,再利用整数集上的百万富翁问题协议进行比较处理,但又遇到下面 4 个问题:

(1)如果考虑小数点,那么只能将整数部分和分数部分分别应用百万富翁协议进行比较.这必然泄露这两个数是在整数部分就分出大小还是在小数部分分出大小(至少一个参与者能获得这些信息).

(2)如果不考虑小数点,也就需要将参与协议的隐私数和隐私区间都扩大 2^n 倍,那么相应的整数范围就变得很大,不管采用哪个百万富翁协议,都会使计算复杂性大幅度增加.

(3)有的有理数用十进制分数表示的时候非常简洁,但如果用二进制比特串表示,比特串的长度可能很长,就好像无限循环小数一样.如果碰巧遇到这样的数,那么整数集上的百万富翁问题协议就完全无能为力.

(4)因为二进制数的小数部分是用 1/2+1/4+1/8+1/16+…的形式来表示,因此大多数的有理数都只能用二进制数近似表示.

通过以上问题可以分析出,设计有理数上的区间保密计算协议需要满足 4 个条件:

(1)需要以百万富翁协议思想为基本研究思想.

(2)协议只运行一次就能得出结果.

(3)协议不允许获得除 $p\in[m,n]$或 $p\notin[m,n]$外的额外信息,如 $p<m$ 或 $p>n$.

(4)协议应该避免用二进制比特串表示有理数.

3.1 节我们设计了两个区间保密计算协议.

3.1 两个有理数区间保密计算协议

3.1.1 第 1 个协议

我们受第 2.3 节中介绍的三角形面积公式的启发,提出了一个基于计算几何的区间保密计算协议,该协议能够保密地判断出一个隐私数是在区间外、区间内还是在区间的端点上.

方案的基本思想是,首先将 Alice 的隐私有理数与 Bob 的两个隐私有理数区间端点用分数的形式表示,并以它们为斜率分别在平面直角坐标系的第一象限上做三条过原点的直线.Bob 分别在自己的两条直线上任意取两个点 $P_2(x_2,y_2)$,$P_4(x_4,y_4)$和 $P_3(x_3,y_3)$,$P_5(x_5,y_5)$,Alice 在自己的直线上任意取两个点 $P_1(x_1,y_1)$,$P_6(x_6,y_6)$.Alice 和 Bob 保密地计算三角形 $P_1P_3P_5$ 和三角形 $P_6P_2P_4$ 的面积.根据计算三角形面积计算公式定义,若三角形的 3 个顺序固定的顶点呈逆时针方向排列,根据式(3)计算出的三角形面积结果为正值,若三角形的 3 个顺序固定的顶点呈顺时针方向排列,根据式(3)计算出的三角形面积结果为负值.根据解析几何知识可知,如果 Alice 的数在 Bob 的区间内,那么在第一象限内 Alice 的这条直线将处于 Bob 的两条直线之间,在点 P_2,P_4 和 P_3,P_5 的方向由 Bob 确定的情况下,若 $x_4>x_2$,$y_4>y_2$,$x_5>x_3$,$y_5>y_3$,三角形 $P_1P_3P_5$ 和三角形 $P_6P_2P_4$ 的面积符号必然相反,则它们面积的乘积必定小于等于 0;反之,不管 Alice 的数是在 Bob 区间外的左边还是右边,计算出的两个三角形的面积一定是符号相同的,则它们面积的乘积必定大于 0.协议具体数学描述如下:

假设 Alice 拥有一个保密正有理数 $p=\frac{v_1}{u_1}$,其中 $gcd(u_1,v_1)=1$,Bob 拥有一个保密正有理数区间 $[m,n]$,$m=\frac{v_2}{u_2}$,$n=\frac{v_3}{u_3}$,其中 $gcd(u_2,v_2)=1$,$gcd(u_3,v_3)=1$.在平面直角坐标系内,Alice 构造一条过原点,斜率为 p 的直线 L_1,Bob 构造两条过原点,斜率分别为 m 和 n 的直线 L_2 和 L_3,Alice 在直线 L_1 上任意选两个点 $P_1(x_1,y_1)$,$P_6(x_6,y_6)$,保证 x_1,y_1,x_6,y_6 为整数.Bob 在直线 L_2 上随机选两点 $P_2(x_2,y_2)$,$P_4(x_4,y_4)$,在直线 L_3 上随机选两点 $P_3(x_3,y_3)$,$P_5(x_5,y_5)$,保证 $x_2,y_2,x_3,y_3,x_4,y_4,x_5,y_5$ 为整数.为了达到更高的保密性,不需要保证 $x_4>x_2$,$y_4>y_2$ 或者 $x_5>x_3$,$y_5>y_3$.我们用点 P_6,P_2 和 P_4 构造一个三角形 $\triangle P_6P_2P_4$,点 P_1,P_3 和 P_5 构造一个三角形 $\triangle P_1P_3P_5$.如图 1 所示.

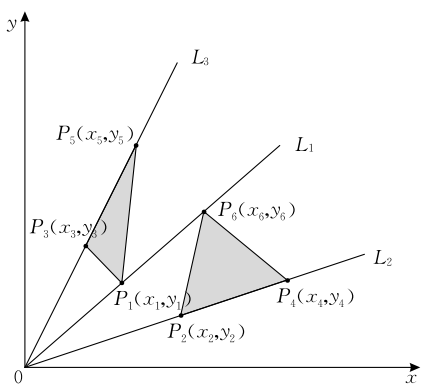

图 1 六点构造两个三角形 $\triangle P_6P_2P_4$ 和 $\triangle P_1P_3P_5$

根据式(3)，Alice 和 Bob 保密地计算出两个三角形$\triangle P_6P_2P_4$和$\triangle P_1P_3P_5$面积的乘积，通过判断

$$S_{\triangle P_6P_2P_4}\times S_{\triangle P_1P_3P_5}=\frac{1}{2}\begin{vmatrix}x_6 & y_6 & 1\\ x_2 & y_2 & 1\\ x_4 & y_4 & 1\end{vmatrix}\times\frac{1}{2}\begin{vmatrix}x_1 & y_1 & 1\\ x_3 & y_3 & 1\\ x_5 & y_5 & 1\end{vmatrix}$$

$$=\frac{1}{4}[y_6(x_4-x_2)+x_6(y_2-y_4)+x_2y_4-x_4y_2]\times$$

$$[y_1(x_5-x_3)+x_1(y_3-y_5)+x_3y_5-x_5y_3]$$

的符号，来判定 p 是否属于区间$[m,n]$. 具体协议方案如下.

协议 2.　区间保密计算问题的解决方案.

输入：Alice 的保密正有理数$p=\frac{v_1}{u_1}$，其中$gcd(u_1,v_1)=1$，Bob 的保密正有理数区间$[m,n]$，$m=\frac{v_2}{u_2}$，$n=\frac{v_3}{u_3}$，其中 $gcd(u_2,v_2)=1$，$gcd(u_3,v_3)=1$

输出：$T(p,[m,n])$

准备：基于 Paillier 的同态加密方案(G,E,D)，Bob 运行 $G(\tau)$生成同态加密的密钥对(p_k,s_k)，τ 是设定的安全参数.

1. 按照上述思想，Alice 和 Bob 构造点 P_1,P_2,P_3,P_4,P_5和 P_6，其中点 P_1和 P_6在直线 L_1上，点 P_2和 P_4在直线 L_2上，点 P_3和 P_5在直线 L_3上. Bob 做如下操作：

(1) 计算

$$a=x_4-x_2,b=y_2-y_4,c=x_2y_4-x_4y_2,$$
$$d=x_5-x_3,e=y_3-y_5,f=x_3y_5-x_5y_3.$$

根据定义可知，a 和 b，d 和 e 必定符号相异. 不失一般性，假设 $a>0,b<0,d>0,e<0$.

(2) 选择 4 个随机数 r_1,r_2,r_3和 r_4($r_1,r_2,r_3,r_4\in Z_n^*$)，使得

$$a_1=a+r_1>0,\ b_1=b+r_2>0,$$
$$d_1=d+r_3>0,\ e_1=e+r_4>0.$$

选择 4 个随机数是为了保证加密的数都是正整数和隐藏点 P_2和 P_4在直线 L_2的位置关系，点 P_3和 P_5在直线 L_3上的位置关系(如果只给小于 0 的数 b 加上随机数得到大于 0 的 b_1，Alice 通过计算 R，可以确定是 $b<0$ 而非 $a<0$)，从而保证Alice不能从最终结果中推出$p\notin[m,n]$且 $p<m$ 或者 $p>n$，达到更高的保密性，所以需要选择 4 个随机数. 为了方便描述，这里假设 $a>0,b<0,d>0,e<0$. 但是在实际运用协议的过程中，这些数的符号由 Bob 确定.

(3) 用生成的公钥 p_k对 a_1,b_1,d_1和 e_1进行加密，得到

$$E(a_1),E(b_1),E(d_1),E(e_1).$$

(4) 将 $E(a_1),E(b_1),E(d_1),E(e_1),r_1,r_2,r_3,r_4$一起发给Alice. 但不告诉Alice $E(a_1),E(b_1),E(d_1),E(e_1)$是属于哪一条直线.

2. Alice 选取两个随机数 r_5,r_6($r_5,r_6\in Z_n^*$)，并计算 $E(r_5),E(r_6)$和

$$E(S_1)=E(a_1y_6+b_1x_6+r_5)$$
$$=E(a_1)^{y_6}\cdot E(b_1)^{x_6}\cdot E(r_5),$$
$$E(S_2)=E(d_1y_1+e_1x_1+r_6)$$
$$=E(d_1)^{y_1}\cdot E(e_1)^{x_1}\cdot E(r_6),$$
$$R_1=r_1y_6+r_5,\ R_2=r_2x_6,$$
$$R_3=r_3y_1+r_6,\ R_4=r_4x_1,$$

并将 $E(S_1)$和 $E(S_2)$发送给 Bob.

3. Bob 用私钥解密 $E(S_1)$和 $E(S_2)$，并计算

$$S_3=S_1+c=a_1y_6+b_1x_6+c+r_5$$
$$=ay_6+bx_6+c+r_1y_6+r_2x_6+r_5,$$
$$S_4=S_2+f=d_1y_1+e_1x_1+f+r_6$$
$$=dy_1+ex_1+f+r_3y_1+r_4x_1+r_6.$$

Bob 将 S_3和 S_4发送给 Alice.

4. Alice 计算

$$S=\frac{1}{4}(S_3-R_1-R_2)(S_4-R_3-R_4)$$
$$=\frac{1}{4}(ay_6+bx_6+c)(dy_1+ex_1+f)$$
$$=\frac{1}{4}[y_6(x_4-x_2)+x_6(y_2-y_4)+x_2y_4-x_4y_2]\times$$
$$[y_1(x_5-x_3)+x_1(y_3-y_5)+x_3y_5-x_5y_3]$$
$$=S_{\triangle P_6P_2P_4}\times S_{\triangle P_1P_3P_5}.$$

通过 S 得出 $T(p,[m,n])$

$$T(p,[m,n])=\begin{cases}-1, & S<0\\ 0, & S=0\\ 1, & S>0\end{cases}.$$

Alice 将 $T(p,[m,n])$告诉 Bob.

5. Bob 根据自己确定的点 P_2,P_3和 P_4,P_5的位置关系，结合 $T(p,[m,n])$，判断 $p\in[m,n]$或 $p\notin[m,n]$，并将最终结果告诉 Alice.

例如，在 $a>0,b<0,d>0,e<0$ 的情况下，

$$\begin{cases}T(p,[m,n])=-1, & p\in[m,n]\\ T(p,[m,n])=1, & p\notin[m,n]\end{cases};$$

在 $a>0,b<0,d<0,e>0$ 的情况下，

$$\begin{cases}T(p,[m,n])=-1, & p\notin[m,n]\\ T(p,[m,n])=1, & p\in[m,n]\end{cases}.$$

该协议更适合于需要比较出 3 种关系的应用场景，即 $p\in[m,n]$，$p\notin[m,n]$和 $p=m$(或 $p=n$). $p=m$(或 $p=n$)是一种比较特殊情况，即 Alice 计算出来的 $T(p,[m,n])=0$，但 Alice 不知道 p 等于 m 还是等于 n，Alice 猜中的概率是 1/2. 但是在现实情况下，如实际商品交易过程中，如果计算出 $p=m$(或 $p=n$)这样的结果，Alice 很有可能会通过对商品的估值来增加猜中的概率. 这个问题可以用以下办法解决：由于协议中的保密数均为有理数，在没有限定保密数具体取值范围的情况下，出现 p 等于 m 或者

等于 n 的概率是比较小的.即使是在商品交易中,双方对某大宗商品都有一个比较确定的价格估计,Bob 可以通过对其价格区间的两边边界分别加上一个并不影响双方交易的极小的随机有理数(如取自区间$[0,1]$),如此来避免出现保密数与区间边界相等的情况.因此,可以说出现 $T(p,[m,n])=0$ 的情况是一个小概率事件.在密码学的定义中,如果某事件的发生概率极小,就可以称该事件是可以忽略的[38].

(1)正确性

由于每个有理数均可以用分数来表示,根据式(3),三角形$\triangle P_6P_2P_4$的面积可以用三点 P_6,P_2 和 P_4的坐标来计算,三角形$\triangle P_1P_3P_5$的面积可以用三点 P_1,P_3 和 P_5 的坐标来计算,那么由三角形$\triangle P_6P_2P_4$和$\triangle P_1P_3P_5$面积相乘的符号可以判断出点 P_1与直线 L_2,L_3的位置关系,即 p 和区间$[m,n]$的包含关系.所以协议 2 是正确的.

(2)隐私性

为了分析协议 2 的安全性,需要考察在执行协议的过程中,每个参与者是否能够得到其他参与者的隐私信息.

对于 Alice 而言,Alice 能够在协议过程中获得 4 个包含有 Bob 隐私数的密文$E(a_1)$,$E(b_1)$,$E(d_1)$,$E(e_1)$与两个明文 S_3,S_4.基于同态加密的安全性,在不知道私钥的情况下,解密密文是困难的,Alice 得不到 Bob 的保密数 a_1,b_1,d_1和 e_1.由于

$$\begin{aligned}S_3&=S_1+c=a_1y_6+b_1x_6+c+r_5\\&=ay_6+bx_6+c+r_1y_6+r_2x_6+r_5,\\S_4&=S_2+f=d_1y_1+e_1x_1+f+r_6\\&=dy_1+ex_1+f+r_3y_1+r_4x_1+r_6.\end{aligned}$$

在这两个等式中,x_1,y_1,x_6,y_6,r_5和 r_6是 Alice 自己的保密数和随机数,r_1,r_2,r_3和 r_4是从 Bob 那得知的随机数,a,b,c,d 和 f 是 5 个未知变量.根据数学知识,包含两个方程 5 个未知数的方程组也被称为自由度为 3 的不定方程组,不能利用这个方程组确定 5 个变量的值.Alice 从协议过程中得不到任何 Bob 保密数的相关信息.

对于 Bob 而言,他能够得到包含 Alice 保密数的明文 S_1,S_2,且

$$\begin{cases}S_1=a_1y_6+b_1x_6+r_5\\S_2=d_1y_1+e_1x_1+r_6\end{cases}.$$

在这两个等式中,a_1,b_1,d_1和 e_1是 Bob 自己的保密数,x_1,y_1,x_6,y_6,r_5和 r_6是 6 个未知变量.根据数学知识,包含两个方程 6 个未知数的方程组也被称为自由度为 4 的不定方程组,不能通过这个不定方程组确定 6 个变量的值.Bob 从协议过程中得不到任何 Alice 保密数的相关信息.因此协议 2 具有隐私性.

我们在第 4 节对协议 2 进行了详细的模拟范例安全性证明.

3.1.2 第 2 个协议

本小节以协议 1 作为基本模块,提出一个基于算术的区间保密计算协议,该协议适合于需要比较出两种关系的应用场景,即隐私数在区间内,还是不在区间内,而不泄露是否在区间的边界这样的信息.协议具体数学描述如下:

假设 Alice 拥有一个保密正有理数 $p=\frac{y}{x}$,其中 $gcd(x,y)=1$,Bob 拥有一个保密正有理数区间$[m,n]$,$m=\frac{y_1}{x_1}$,$n=\frac{y_2}{x_2}$,其中 $gcd(x_1,y_1)=1$,$gcd(x_2,y_2)=1$.若 $p\in[m,n]$,根据数学定义可以构成两个不等式

$$\begin{cases}\frac{y_2}{x_2}-\frac{y}{x}=\frac{xy_2-x_2y}{xx_2}\geq0\\\frac{y}{x}-\frac{y_1}{x_1}=\frac{x_1y-xy_1}{xx_1}\geq0\end{cases},$$

由于 xx_2与 xx_1均为正整数,所以有

$$\begin{cases}xy_2-x_2y\geq0\\x_1y-xy_1\geq0\end{cases},$$

由于两个非负整数相乘结果必定非负.因此

$$\begin{aligned}&(xy_2-x_2y)(x_1y-xy_1)\\&=xx_1yy_2-x^2y_1y_2-x_1x_2y^2+xx_2yy_1\\&=xy(x_1y_2+x_2y_1)-(x^2y_1y_2+x_1x_2y^2)\geq0,\end{aligned}$$

若 $p\notin[m,n]$,根据数学定义可得

(1)当 $p<m$ 时,

$$\begin{cases}xy_2-x_2y>0\\x_1y-xy_1<0\end{cases};$$

(2)当 $p>n$ 时,

$$\begin{cases}xy_2-x_2y<0\\x_1y-xy_1>0\end{cases}.$$

在这两种情况下,都有

$$(xy_2-x_2y)(x_1y-xy_1)<0.$$

此外,因为不可能出现 $xy_2-x_2y<0$,$x_1y-xy_1<0$ 的情况,所以 $p\in[m,n]\Leftrightarrow xy_2-x_2y>0$,$x_1y-xy_1>0$.因此,我们可以通过判断$(xy_2-x_2y)(x_1y-xy_1)$的符号来判断 p 是否属于区间$[m,n]$.协议的原理就是用 Paillier 的同态加密算法实现保密地计算$(xy_2-x_2y)(x_1y-xy_1)$的符号,从而保密地判断 p

是否属于区间$[m,n]$. 具体协议如下.

协议 3.　区间保密计算问题的解决方案.

输入：Alice 的保密正有理数 $p=\frac{y}{x}$，其中 $gcd(x,y)=1$，

Bob 的保密正有理数区间$[m,n]$，$m=\frac{y_1}{x_1}$，$n=\frac{y_2}{x_2}$，

其中. $gcd(x_1,y_1)=1$，$gcd(x_2,y_2)=1$

输出：$T(p,[m,n])$

准备：基于 Paillier 的同态加密方案(G,E,D)，Bob 运行 $G(\tau)$生成同态加密的密钥对(p_k,s_k)，τ 是设定的安全参数.

1. 根据上述思想，Bob 用生成的公钥 p_k进行如下加密：

$$E(a)=E(x_1y_2+x_2y_1),$$
$$E(b)=E(y_1y_2),$$
$$E(c)=E(x_1x_2),$$

Bob 将 $E(a)$，$E(b)$，$E(c)$和公钥 p_k一起发给 Alice.

2. Alice 选取一个足够大的随机数 R，保证 $axy-bx^2-cy^2+R>0$，并计算 $E(R)$和

$$E(T)=E(axy-bx^2-cy^2+R)$$
$$=E(a)^{xy}\cdot E(b)^{-x^2}\cdot E(c)^{-y^2}\cdot E(R),$$

并将 $E(T)$发送给 Bob.

3. Bob 用私钥解密 $E(T)$得到

$$T=axy-bx^2-cy^2+R$$
$$=xy(x_1y_2+x_2y_1)-(x^2y_1y_2+x_1x_2y^2)+R.$$

4. Alice 和 Bob 调用协议 1 保密判断 T 和 R 的大小关系，并以此确定保密数 p 和区间$[m,n]$的关系：

(1) 如果 $T<R$，则 $xy(x_1y_2+x_2y_1)-(x^2y_1y_2+x_1x_2y^2)<0$，$p\notin[m,n]$.

(2) 如果 $T\geq R$，则 $xy(x_1y_2+x_2y_1)-(x^2y_1y_2+x_1x_2y^2)\geq 0$，$p\in[m,n]$.

(1) 正确性

由于每个有理数均可以用分数来表示，根据数学知识，无论 $p\in[m,n]$或 $p\notin[m,n]$，均可以列出两个关于 p 与 m 和 p 与 n 的不等式. 又由于非负整数与非负整数相乘结果一定非负，正整数与负整数相乘一定为负，因此可以通过判断两个不等式乘积的符号来判断区间保密计算问题. 所以协议 3 是正确的.

(2) 隐私性

协议 3 的第 2 步 Alice 选取的足够大的随机数 R，是为了保证 $xy(x_1y_2+x_2y_1)-(x^2y_1y_2+x_1x_2y^2)+R$ 是大于 0 的，这样 Alice 和 Bob 才能够调用基于自然数的百万富翁协议 1.

为了分析协议 3 的安全性，需要考察在执行协议的过程中每个参与者是否能够得到其他参与者的隐私信息，由于协议 1 的安全性已经在文献[20]中进行了证明，因此这里只对协议 3 第 4 步之前的交互进行分析.

对于 Alice 而言，Alice 能够在协议过程中获得 3 个包含有 Bob 隐私数的密文 $E(a)$，$E(b)$，$E(c)$. 基于同态加密的安全性，在不知道私钥的情况下，解密密文是困难的，Alice 从协议过程中得不到任何 Bob 保密数的相关信息.

对于 Bob 而言，他能够得到包含 Alice 保密数的一个明文

$$T=axy-bx^2-cy^2+R.$$

在这个等式中，a，b 和 c 是 Bob 自己的保密数，x，y，R 是 3 个未知变量. 根据数学知识，一个方程不能解出 3 个未知数. Bob 从协议过程中得不到任何 Alice 保密数的相关信息. 因此，协议 3 具有隐私性.

我们在附录对协议 3 进行了详细的模拟范例安全性证明.

4　安全性分析

模拟范例是多方保密计算协议的安全性证明中一种被广泛使用的、较为简便的证明方法. 本节用模拟范例来证明协议 2 的安全性.

定理 1.　协议 2 能够保密地计算有理数域上的区间计算问题.

证明.　首先为 Alice 和 Bob 分别构造满足式(1)和(2)的模拟器 S_A 和 S_B.

接收到输入$(p,T(p,[m,n]))$后，S_A 做如下模拟：

(1) 选择两个随机数 $m'=\frac{v_2'}{u_2'}$，$n'=\frac{v_3'}{u_3'}$，使得 $T(p,[m',n'])=T(p,[m,n])$在有理数域成立.

(2) 随机选择 4 个点 $P_2'(x_2',y_2')$，$P_3'(x_3',y_3')$，$P_4'(x_4',y_4')$和 $P_5'(x_5',y_5')$，保证 x_2'，y_2'，x_3'，y_3'，x_4'，y_4'，x_5'，y_5'为整数.

(3) 计算

$$a'=x_4'-x_2',\ b'=y_2'-y_4',\ c'=x_2'y_4'-x_4'y_2',$$
$$d'=x_5'-x_3',\ e'=y_3'-y_5',\ f'=x_3'y_5'-x_5'y_3'.$$

并选择 4 个随机数 r_1'，r_2'，r_3'和 $r_4'(r_1',r_2',r_3',r_4'\in Z_n^*)$，使得

$$a_1'=a'+r_1'>0,\ b_1'=b'+r_2'>0,$$
$$d_1'=d'+r_3'>0,\ e_1'=e'+r_4'>0.$$

(不失一般性，假设 $a'>0$ 和 $b'<0$. 并且，在模拟范例中，随机数是不需要在整个定义域里面随机分布的)

(4) 选择两个随机数 r_5 和 $r_6(r_5,r_6\in Z_n^*)$，加密

$E(a_1')$,$E(b_1')$,$E(d_1')$,$E(e_1')$,$E(r_5)$,$E(r_6)$,并计算

$$E(S_1')=E(a_1'y_6+b_1'x_6+r_5)$$
$$=E(a_1')^{y_6}\cdot E(b_1')^{x_6}\cdot E(r_5),$$
$$E(S_2')=E(d_1'y_1+e_1'x_1+r_6)$$
$$=E(d_1')^{y_1}\cdot E(e_1')^{x_1}\cdot E(r_6),$$
$$R_1'=r_1'y_6+r_5,R_2'=r_2'x_6,$$
$$R_3'=r_3'y_1+r_6,R_4'=r_4'x_1.$$

(5) 计算

$$S_3'=S_1'+c'=a_1'y_6+b_1'x_6+c'+r_5$$
$$=a'y_6+b'x_6+c'+r_1'y_6+r_2'x_6+r_5,$$
$$S_4'=S_2'+f'=d_1'y_1+e_1'x_1+f'+r_6$$
$$=d'y_1+e'x_1+f'+r_3'y_1+r_4'x_1+r_6.$$

(6) 计算

$$S'=\frac{1}{4}(S_3'-R_1'-R_2')(S_4'-R_3'-R_4')$$
$$=\frac{1}{4}(a'y_6+b'x_6+c')(d'y_1+e'x_1+f')$$
$$=\frac{1}{4}[y_6(x_4'-x_2')+x_6(y_2'-y_4')+x_2'y_4'-x_4'y_2']\times$$
$$[y_1(x_5'-x_3')+x_1(y_3'-y_5')+x_3'y_5'-x_5'y_3'].$$

(7) 得到结果 $T(p,[m',n'])$.

令

$$S_A(p,T(p,[m,n]))=\{(u_1,v_1),r^A,E(S_1'),E(S_2'),$$
$$R_1',R_2',R_3',R_4',S',T(p,[m',n'])\}.$$

由于在协议 2 中

$$T(p,[m,n])=T(p,[m',n']),$$
$$output_1^{\pi}(p,[m,n])=output_2^{\pi}(p,[m,n])$$
$$=T(p,[m,n]),$$
$$view_1(p,[m,n])=\{(u_1,v_1),r^1,E(S_1),E(S_2)$$
$$R_1,R_2,R_3,R_4,S,T(p,[m,n])\},$$

根据定义和同态加密的语义安全性可知,

$$r^1\overset{c}{\equiv}r^A,\ E(S_1)\overset{c}{\equiv}E(S_1'),\ E(S_2)\overset{c}{\equiv}E(S_2'),$$
$$R_1\overset{c}{\equiv}R_1',\ R_2\overset{c}{\equiv}R_2',\ R_3\overset{c}{\equiv}R_3',\ R_4\overset{c}{\equiv}R_4',\ S\overset{c}{\equiv}S'.$$

因此,

$$\{S_A(p,T(p,[m,n])),T(p,[m,n])\}_{p,[m,n]}\overset{c}{\equiv}$$
$$\{view_1^{\pi}(p,[m,n]),output_2^{\pi}(p,[m,n])\}_{p,[m,n]}.$$

同理,模拟器 S_B 可以用类似的方法构造

$$\{T(p,[m,n]),S_B(p,T([m,n]))\}_{p,[m,n]}\overset{c}{\equiv}$$
$$\{output_1^{\pi}(p,[m,n]),view_2^{\pi}(p,[m,n])\}_{p,[m,n]}.$$

证毕.

用证明定理 1 的方法同样可以证明下面的推论 1. 我们在附录中给出了推论 1 的详细证明.

推论 1. 协议 3 能够保密地计算有理数域上的百万富翁问题.

5 效率分析

目前没有任何基于有理数的区间保密计算协议,由于 Nishide 等人[29]的协议在本质上只是一个有限集合包含协议,在方法上与本文提出的协议没有可比性,因此本节只对协议 2 和协议 3 进行效率分析和实验验证,并以 2013 年的文献[18]中所提出的一种同样使用 Paillier 加密算法的高效百万富翁协议(又名 SP 协议)的效率为参考. Paillier 同态加密协议中进行一次加密运算或解密运算都需做两次模指数运算,每进行一次密文模指数运算均算一次模指数运算. 在这个前提下,为了方便分析,忽略准备工作、随机数选取和比特异或运算的计算消耗,只分析协议的模指数运算次数和实验耗时.

在 SP 协议中,假定保密的输入为 $x,y\in U$,并且 $|U|=m$. Alice 需要进行 m 次加密运算,1 次解密运算,但由于其加密的明文均为 1 或 0,即 Alice 加密的公式为 $E(a_i)=g^1r^N \bmod N^2$ 或 $E(a_i)=g^0r^N \bmod N^2$,所以 Alice 一共需要做 $m+2$ 次模指数运算. Bob 需要进行 1 次密文运算 $E(v)=r^N\prod_{i=1}^{l}(E(a_i)^{b_i}) \bmod N^2$,根据协议设计,该运算可以简化为 $E(v)=r^NE(a_i)^l \bmod N^2$,所以 Bob 一共需要做 2 次模指数运算. 因此 SP 协议一共需要进行 $m+4$ 次模指数运算,并且会随着保密数据的长度增加而增加.

在协议 2 中,Alice 需要进行 2 次加密运算和 2 次密文运算 $E(S_1)=E(a_1)^{y_6}\cdot E(b_1)^{x_6}\cdot E(r_5)$,$E(S_2)=E(d_1)^{y_1}\cdot E(e_1)^{x_1}\cdot E(r_6)$,其中密文模指数运算 4 次,所以 Alice 一共需要做 8 次模指数运算. Bob 需要进行 4 次加密运算,2 次解密运算,共需要做 12 次模指数运算. 因此协议 2 一共需要进行 20 次模指数运算.

在协议 3 中,Alice 需要进行 1 次加密运算和 1 次密文运算 $E(T)=E(a)^{xy}\cdot E(b)^{-x^2}\cdot E(c)^{-y^2}\cdot E(R)$,其中密文模指数运算 3 次,所以 Alice 一共需要做 5 次模指数运算. Bob 需要进行 3 次加密运算,1 次解密运算,共需要做 8 次模指数运算. 虽然在协议 3 的第 4 步调用了协议 1,在假定 $0<T,R<n$ 的前提下,需要进行 $2n$ 次比特异或运算,但是在不失一般性的情况下,比特异或运算相对于模指数运算是可以忽略的[37]. 因此协议 3 一共需要进行 13 次模指数运算.

通过分析，协议 2、3 只需要较少而确定的模指数运算次数就可以完美地解决问题，并且不需要考虑保密数据的长度增长问题. 分析结果如表 1 所示.

表 1　3 种协议的模指数运算次数分析

	性能		
	Alice 的模指数运算次数	Bob 的模指数运算次数	总模指数运算次数
SP 协议	$m+2$	2	$m+4$
协议 2	8	12	20
协议 3	5	8	13

为了进一步对协议进行验证，我们采用 Java 编程语言对 3 种协议分别进行了编程实现，计算机配置如下：操作系统为 Windows 7 旗舰版，CPU 为 Inter Core i3-2100 3.10 GHz，内存为 4.00 GB. 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，并统一保密数的范围为[0，20]. 我们分别对 SP 协议、协议 2 和协议 3 进行实现，并对每种协议的实验结果（未预处理）随机抽取 31 组数据求得时间平均值，结果如表 2 所示.

表 2　未预处理的 3 种协议实验结果分析

	性能		
	Alice 的运算耗时/ms	Bob 的运算耗时/ms	总运算耗时/ms
SP 协议	70.226	3.289	73.515
协议 2	6.467	31.774	38.241
协议 3	18.259	19.677	37.936

实际上，通过对 Paillier 解密公式的分析可以发现，一个协议在实现解密计算的过程中，参与运算的 $L(g^{\lambda} \bmod N^2)$ 是可以被预处理的，因为 g，λ 和 N 均是在协议的准备工作里产生的，如果将 $L(g^{\lambda} \bmod N^2)$ 预先计算好，那么在进行解密运算时，可以直接调用，从而减少一次模指数运算. 我们对 $L(g^{\lambda} \bmod N^2)$ 进行预处理后，分别对 SP 协议、协议 2 和协议 3 进行实现，并对每种协议的实验结果随机抽取 31 组数据求得时间平均值，结果如表 3 所示.

表 3　预处理的 3 种协议实验结果分析

	性能		
	Alice 的运算耗时/ms	Bob 的运算耗时/ms	总运算耗时/ms
SP 协议	62.881	3.289	66.170
协议 2	6.467	20.258	26.725
协议 3	18.259	13.258	31.517

实验结果显示，经过预处理的一次解密运算普遍比未预处理运算减少约 6 ms. 表 3 数据显示，解决整数百万富翁问题的协议 SP，在限定保密数范围的情况下，需要的运算时间远大于另外 2 个协议. 在理论上分析协议 3 中 Alice 的模指数运算次数小于协议 2，但协议 3 的实验耗时比协议 2 多，这是由于协议 3 中 Alice 的模指数运算 $E(T)=E(a)^{xy} \cdot E(b)^{-x^2} \cdot E(c)^{-y^2} \cdot E(R)$ 所计算的指数 x^2 和 y^2，大于协议 2 的模指数运算 $E(S_2)=E(d_1)^{y_1} \cdot E(e_1)^{x_1} \cdot E(r_6)$ 的指数 x_1 和 y_1. 实验结果显示协议 2 和协议 3 是高效的.

6　区间保密计算的应用

除了能够在商品交易中节约成本和时间，研究区间保密计算在计算几何和代数计算上都具有应用价值. 为了更详细地阐明设计区间保密计算协议的意义，主要介绍 4 种有趣的应用.

(1) 保密几何中的点与圆环的包含问题

在目前已有的保密计算几何的研究中，有保密判断点与圆的包含问题、保密判断点与凸多边形的包含问题、保密判断点与凹多边形的包含问题等，但是还没有解决保密判断点与圆环的包含问题. 假设 Alice 拥有一个保密点 $P_1(x_1, y_1)$，Bob 拥有一个保密的圆环，内圈半径为 r，外圈半径为 R，由于圆环上所有的点满足不等式 $r^2 \le x^2+y^2 \le R^2$，如图 2 所示. 于是保密判断点与圆环的包含问题可以转换为保密判断数 $x_1^2+y_1^2$ 在不在区间 $[r^2, R^2]$ 内的问题，即可调用协议 2 或协议 3 来进行保密地判断.

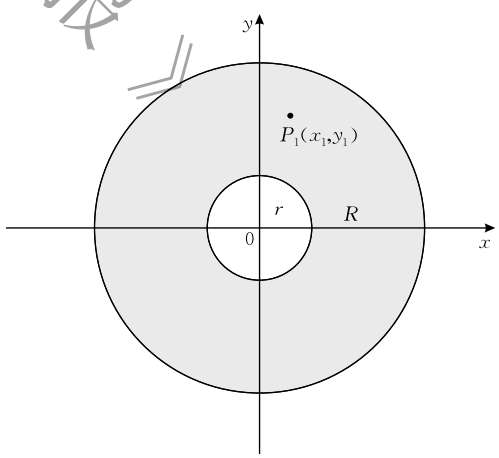

图 2　保密点与圆环的包含问题

该应用还可以做另外一个引申，即保密地判断点与不规则图形的包含问题. 这里的不规则图形可以描述为：在第一象限，任意两条过原点、斜率能够确定的直线与圆心在原点的圆环围出的不规则区域. 如图 3 所示. 通过协议 2 或协议 3 也可以保密地判断一个点与这种不规则图形的包含关系.

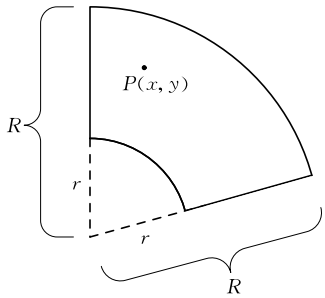

图 3 保密点与不规则图形的包含问题

(2)保密几何中的点与无限区域的包含问题

从目前的保密几何研究来看,与保密点有关的判断协议,均是将点与确定的几何图形进行比较.区间保密计算可以解决保密点与无限区域的包含问题:假设在平面直角坐标系的第一象限中,Alice 有一个保密点 $P_1(x_1,y_1)$,Bob 有两条过原点的保密直线 L_1 和 L_2,它们的斜率分别为 p 和 q,如何保密地判断点 $P_1(x_1,y_1)$是否在以两条直线为边界的无限区域内?首先过原点和点 $P_1(x_1,y_1)$做一条直线 L,其斜率 $a=\frac{y_1}{x_1}$,如图 4 所示.利用协议 2 或协议 3 来保密判断数 a 是否在区域$[p,q]$内,即可以保密地比较出点与以两条直线为边界的无限区域的包含关系.

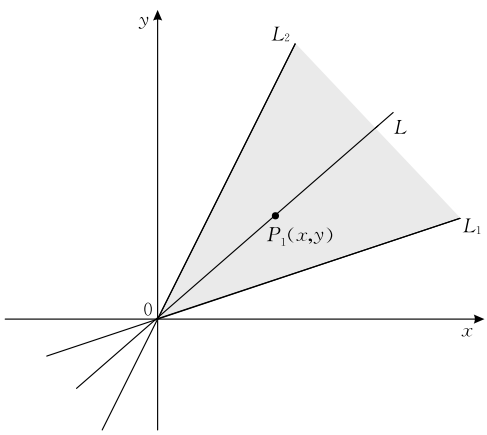

图 4 保密点与无限区域的包含问题

该应用还可以做另外一个引申,即保密地判断一个几何图形与无限区域的包含问题:假设在平面直角坐标系的第一象限中,Alice 有一个保密几何图形,Bob 有两条过原点保密的直线 L_1 和 L_2,它们的斜率分别为 p 和q,如何判断 Alice 的保密几何图形是否在 Bob 以两条直线为边界的无限区域内?可以先找出 Alice 图形上的两个点,分别满足其与原点所连的直线与 x 轴呈最大和最小夹角,然后用协议 2 或协议 3 判断这两个点和 Bob 的区间关系,如果这两个点都在区间内,那么整个几何图形也包含在无限区域内,如图 5 所示.

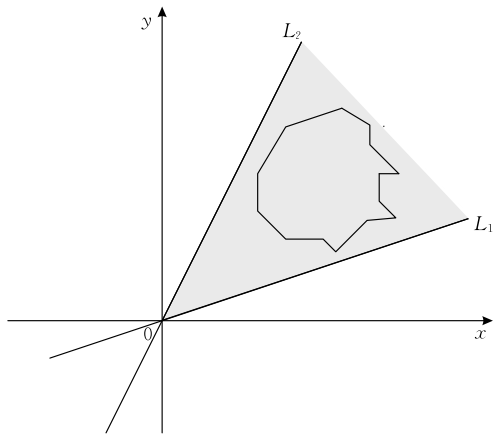

图 5 保密几何图形与无限区域的包含问题

(3)计算几何中点与线段的包含问题

将保密线段的两个端点看作一个区间的两个端点,协议 2 或协议 3 可以判断一个保密点是否在一条线段内.该问题可以描述为:假设在平面直角坐标系的第一象限中,Alice 有一个保密点 $P_1(x_1,y_1)$,Bob 有一条端点分别为 $P_2(x_2,y_2)$和 $P_3(x_3,y_3)$的线段 P_2P_3,如图 6 所示.如何保密地判断 P_1 是否在线段 P_2P_3 上?

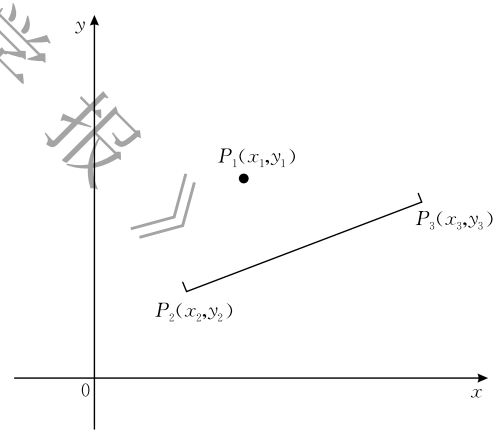

图 6 保密点与线段的包含问题

首先保密计算$\triangle P_1P_2P_3$的面积,若面积不等于 0,直接判定点 P_1 不在线段 P_2P_3,若面积等于 0,则说明点 P_1 在线段 P_2P_3 所在的直线上,然后调用协议 2 或者协议 3 可以判断出点 P_1 是在线段 P_2P_3 内还是在线段 P_2P_3 外.

(4)无限集合的包含问题

区间可以看成一个包含无限有理数的无限集合,假设 Alice 拥有一个保密数 x,Bob 拥有一个无限保密集合 $B=\{b_1,b_2,\cdots,\infty\}$,且 $b_i\in[m,n](1\leq i\leq\infty)$,调用协议 2 或协议 3 可以判断保密数 x 是

否属于无限集合 $B=\{b_1,b_2,\cdots,\infty\}$. 这个问题用现有的集合包含协议是无法解决的.

7 结　论

区间保密计算在多方保密计算协议的构造中有实际研究意义，在隐私保护方面有广泛的应用，它可以作为许多多方保密计算协议的基础模块，也可以解决保密计算几何的新问题，甚至能广泛应用于现实交易，达到减少交易成本的目的. 本文详细分析了区间保密计算问题的理论概念，结合计算几何和基本代数计算，基于 Paillier 加密算法，设计了两个高效的有理数区间保密计算协议，并证明了它们的安全性. 除文中提到的应用场景以外，区间保密计算的其他应用在将来的研究中也有待发掘. 当然，如何高效地将区间保密计算协议扩大到更大的适用范围，也是今后值得研究的一个方向.

参 考 文 献

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

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

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

[4] Franklin M, Yung M. Communication complexity of secure computation//Proceedings of the 24th Annual ACM Symposium on Theory of Computing. New York, USA, 1992: 699-710

[5] Gennaro R, Rabin M O, Rabin T. Simplified VSS and fast-track multiparty computations with applications to threshold cryptography//Proceedings of the 17th Annual ACM Symposium on Principles of Distributed Computing. New York, USA, 1998: 101-111

[6] Tang C M, Shi G H, Yao Z A. Secure multi-party computation protocol for sequencing problem. Science China Information Sciences, 2011, 54(8): 1654-1662

[7] Toft T. Sub-linear, secure comparison with two non-colluding parties//Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography. Taormina, Italy, 2011: 174-191

[8] 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

[9] Li S D, Wang D S, Dai Y Q. Efficient secure multiparty computational geometry. Chinese Journal of Electronics, 2010, 19(2): 324-328

[10] Fong P K, Weber-Jahnke J H. Privacy preserving decision tree learning using unrealized data sets. IEEE Transactions on Knowledge and Data Engineering, 2012, 24(2): 353-364

[11] Niksefat S, Sadeghiyan B, Mohassel P, et al. ZIDS: A privacy-preserving intrusion detection system using secure two-party computation protocols. Computer Journal, 2014, 57(4): 494-509

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

[13] Fischlin M. A cost-effective pay-per-multiplication comparison method for millionaires//Proceedings of the 2001 Conference on Topics in Cryptology: The Cryptographer's Track at RSA. San Francisco, USA, 2001: 457-471

[14] Ioannidis I, Grama A. An efficient protocol for Yao's millionaires' problem//Proceedings of the 36th Annual Hawaii International Conference on IEEE in System Sciences. Hawaii, USA, 2003: 6-10

[15] Li Shun-Dong, Dai Yi-Qi, You Qi-You. An efficient solution to Yao's millionaires' problem. Acta Electronica Sinica, 2005, 33(5): 769-773(in Chinese)
(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] Lin H Y, Tzeng W G. An efficient solution to the millionaires' problem based on homomorphic encryption//Proceedings of the 3rd International Conference on Applied Cryptography and Network Security. New York, USA, 2005: 456-466

[17] Garay J, Schoenmakers B, Villegas J. Practical and secure solutions for integer comparison//Proceedings of the 10th International Conference on Practice and Theory in Public-Key Cryptography. Berlin, Germany, 2007: 330-342

[18] Li Shun-Dong, Wang Dao-Shun. Efficient secure multiparty computation based on homomorphic encryption. Acta Electronica Sinica, 2013, 41(4): 798-803(in Chinese)
(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)

[19] Gordon S D, Hazay C, Katz J, et al. Complete fairness in secure two-party computation. Journal of the ACM, 2011, 58(6): 24

[20] 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

[21] Wang Y, Liu Z, Wang H, et al. Social rational secure multi-party computation. Concurrency and Computation: Practice and Experience, 2014, 26(5): 1067-1083

[22] Huang H, Li X Y, Sun Y, et al. PPS: Privacy-preserving strategyproof social-efficient spectrum auction mechanisms. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(5): 1393-1404

[23] Li M J, Juan J S T, Tsai J H C. Practical electronic auction scheme with strong anonymity and bidding privacy. Information Sciences, 2011, 181(12): 2576-2586

[24] Cramer R, Damgard I, Maurer U. General secure multi-party computation from any linear secret-sharing scheme//Proceedings of the 19th International Conference on Theory and Application of Cryptographic Techniques. Berlin, Germany, 2000: 316-334

[25] Liu Q, Wang G, Wu J. Time-based proxy re-encryption scheme for secure data sharing in a cloud environment. Information Sciences, 2014, 258: 355-370

[26] Atallah M J, Frikken K B. Securely outsourcing linear algebra computations//Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. New York, USA, 2010: 48-59

[27] Choi S G, Hwang K W, Katz J, et al. Secure multi-party computation of Boolean circuits with applications to privacy in on-line marketplaces//Proceedings of the 12th Conference on Topics in Cryptology. Berlin, Germany, 2012: 416-432

[28] Toft T. Secure data structures based on multi-party computation//Proceedings of the 30th Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing. New York, USA, 2011: 291-292

[29] 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

[30] Asharov G, Lindell Y, Schneider T, et al. More efficient oblivious transfer extensions with security for malicious adversaries//Oswald E, Fischlin M eds. Advances in Cryptology-EUROCRYPT 2015. Berlin, Germany: Springer, 2015: 673-701

[31] Lindell Y, Pinkas B. An efficient protocol for secure two-party computation in the presence of malicious adversaries. Journal of Cryptology, 2014, 28(2): 312-350

[32] Hazay C, Toft T. Computationally secure pattern matching in the presence of malicious adversaries. Journal of Cryptology, 2014, 27(2): 358-395

[33] Lindell Y. Fast cut-and-choose based protocols for malicious and covert adversaries//Canetti R, Garay J eds. Advances in Cryptology-CRYPTO 2013. Berlin, Germany: Springer, 2013: 1-17

[34] Freedman M J, Nissim K, Pinkas B. Efficient private matching and set intersection//Cachin C, Camenisch J eds. Advances in Cryptology-EURO CRYPT 2004. Berlin, Germany: Springer, 2004: 1-19

[35] Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms. Foundations of Secure Computation, 1978, 4(11): 169-180

[36] Paillier P. Public-key cryptosystems based on composite degree residuosity classes//Stern J ed. Advances in Cryptology-EUROCRYPT'99. Berlin, Germany: Springer, 1999: 223-238

[37] Bruce S. Applied Cryptography, Protocols, Algorithm and Source Code in C. Hoboken, USA: John Wiley & Sons, 1996

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

附录. 推论 1 的证明.

推论 1. 协议 3 能够保密地计算有理数域上的区间计算问题.

证明. 首先为 Alice 和 Bob 分别构造满足式(1)和(2)的模拟器 S_A 和 S_B.

接收到输入$(p,T(p,[m,n]))$后,S_A做如下模拟:

(1)选择两个随机数 $m'=\frac{y_1'}{x_1'}$, $n'=\frac{y_2'}{x_2'}$,使得 $T(p,[m',n'])=T(p,[m,n])$在有理数域成立.

(2)计算

$$E(a')=E(x_1'y_2'+x_2'y_1'),$$
$$E(b')=E(y_1'y_2'),$$
$$E(c')=E(x_1'x_2').$$

(3)随机选取一个足够大的随机数 R,保证 $a'xy-b'x^2-c'y^2+R>0$, 计算 $E(R)$和

$$E(T')=E(a'xy-b'x^2-c'y^2+R)$$
$$=E(a')^{xy}\cdot E(b')^{-x^2}\cdot E(c')^{-y^2}\cdot E(R),$$

并将 $E(T')$发送给 Bob.

(4)计算

$$T'=a'xy-b'x^2-c'y^2+R$$
$$=xy(x_1'y_2'+x_2'y_1')-(x^2y_1'y_2'+x_1'x_2'y^2)+R.$$

(5)调用协议 1 保密判断 T'和R'的大小关系,得到结果 $T(p,[m',n'])$.

令

$$S_A(p,T(p,[m,n]))=\{(x,y),r^A,E(T'),T(p,[m',n'])\},$$

由于在协议 3 中

$$T(p,[m,n])=T(p,[m',n']),$$
$$output_1^{\pi}(p,[m,n])=output_2^{\pi}(p,[m,n])=T(p,[m,n]),$$
$$view_1(p,[m,n])=\{(x,y),r^1,E(T),T(p,[m,n])\},$$

根据定义和同态加密的语义安全性可知,

$$r^1\overset{c}{\equiv}r^A,\ E(T)\overset{c}{\equiv}E(T'),$$

因此,

$$\{S_A(p,T(p,[m,n])),T(p,[m,n])\}_{p,[m,n]}\overset{c}{\equiv}$$
$$\{view_1^{\pi}(p,[m,n]),output_2^{\pi}(p,[m,n])\}_{p,[m,n]}.$$

同理,模拟器 S_B可以用类似的方法构造

$$\{T(p,[m,n]),S_B(p,T([m,n]))\}_{p,[m,n]}\overset{c}{\equiv}$$
$$\{output_1^{\pi}(p,[m,n]),view_2^{\pi}(p,[m,n])\}_{p,[m,n]}.$$

证毕.

GUO Yi-Min, born in 1992, Ph. D. candidate. Her main research interests include cryptography and information security.

ZHOU Su-Fang, born in 1990, Ph. D. candidate. Her main research interests include cryptography and information security.

DOU Jia-Wei, born in 1963, Ph. D., associate professor. Her main research interests include applied mathematics and applied cryptography.

LI Shun-Dong, born in 1963, Ph. D., professor, Ph. D. supervisor. His main research interests include cryptography and information security.

WANG Dao-Shun, born in 1964, Ph. D., associate professor, Ph. D. supervisor. His main research interests include key management, digital watermarking and multimedia security.

Background

Secure multiparty computation (SMC) was first introduced by Yao and is a current research focus in the international cryptographic community. SMC has become a crucial privacy-preserving technology in cyberspace. Since SMC was introduced, cryptographic scholars have studied many SMC problems that have arisen in various fields; however, many solutions to these problems are computationally inefficient. There are many new problems requiring study and many of those already addressed require further effort to develop more efficient solutions.

This study introduces a new SMC problem, privacy-preserving interval computation (PIC), which privately determines whether a private number belongs to a private interval. Although there are protocols for private-set member computation, which is a special case of private interval computation where the interval comprises finite natural numbers, the general private interval computation problem has not been studied. This problem is of theoretical cryptographic importance and has practical importance in SMC and other privacy-preserving computations.

The Millionaires' problem introduced by Yao compares two private numbers without disclosing them. Protocols for the Millionaires' problem are the main building blocks of various SMC schemes, including our PIC protocols. We use computational geometry theory and Paillier's homomorphic encryption scheme as building blocks to construct a new protocol for PIC problem that works even when the private numbers are rational ones and can determine three relationships between two private inputs, and then, using arithmetic theory as well as a symmetric millionaire's protocol to design an another PIC scheme. Furthermore, we prove that these two protocols are secure in the semi-honest model using the simulation paradigm. These protocols have many SMC applications.

Analyses indicate that these two protocols are computationally efficient. Examples of protocol application are provided in four examples showing how they can be used to construct other secure computational geometry protocols. Examples include privately determining (1) the relationship between a private point and a ring, (2) the relationship between a private point and some specific area, (3) the relationship between a private point and a line segment, and (4) the membership of an infinite set.

This study is sponsored by the National Natural Science Foundation of China under Grant Nos. 61272435, 61373020, U1536102 and U1536116. The aim of these projects is to address various privacy problems arising in cyberspace. Our team has been engaged in the design and analysis of cryptographic protocols, such as SMC, secret sharing, digital signature, and SMC geometry for over 10 years. We have published over 50 papers, of which over 20 have been indexed by SCI.