区间关系保密计算若干问题研究

窦家维,王颖囡,葛 雪
(陕西师范大学数学与信息科学学院,陕西西安 710062)

摘 要: 安全多方计算是密码学界的一个重要研究方向,本文主要研究区间的安全计算问题. 首先应用 Paillier 加密方案设计"点与区间"以及"区间与区间"关系两方保密计算基础协议,协议的特点是判定结果以密文形式输出. 将其推广为有理区间关系判定协议时,相比已有协议,本文协议更为安全与高效. 在此基础上,进一步研究多维度的"点与区间"以及"区间与区间"关系阈值判定这一类新问题. 由于基础协议的输出结果为密文,故以此为基础所设计的多维度问题协议更加安全. 最后,应用模拟范例方法严格证明了协议的安全性,并对协议进行了效率分析及模拟实验,理论分析及实验结果都说明本文协议是高效的.

关键词: 密码学; 两方安全计算; 点与区间关系; 区间与区间关系; 阈值问题
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112 (2021)01-0050-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.12263/DZXB.20191263

Some Research on Secure Interval Relation Computation

DOU Jia-wei, WANG Ying-nan, GE Xue
(*School of Mathematics and Information Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*)

Abstract: Secure multi-party computation (SMC) is an important research direction of cryptography. In this paper, we study the secure computation of intervals. Using the Paillier encryption scheme, we design the protocols of relationship between an interval and a point (or an interval). Firstly, the outputs of protocols are ciphertexts. If we extend it to rational intervals, the protocols are safer and more efficient than existing protocols. And then, we study the multi-dimensional problems, that is, the threshold problems of multiple points (or intervals) and intervals, which are new problems in SMC. Since the outputs of the basic protocols are ciphertexts, the multi-dimensional problem protocols are more secure. We strictly prove the security of the protocols using the simulation paradigm method, analyze and demonstrate the efficiency of the protocols through experiments, and compare with the related work to illustrate that the protocols are efficient.

Key words: cryptography; secure two-party computation; relationship between point and interval; relationship between interval and interval; threshold problem

1 引言

在实际应用中,很多问题都可以抽象为数据计算问题得到解决. 随着科技的进步与网络的发展,人们获取信息的手段不断增加,信息泄露更容易发生,这使得隐私保护下的数据计算成为研究热点. 安全多方计算作为密码学的一个重要研究方向,可以使参与者在保护自己数据隐私性的前提下,利用各方数据进行合作计算并得到所需结果. 安全两方计算问题最早由 Yao 提出[1],随后 Goldreich 等人[2,3]对安全多方计算问题进行深入研究,证明了所有安全多方计算问题都是可解的,并提出了通用的解决方案. 但通用方案解决具体问题时效率较低,因此需要针对具体问题寻求高效解决方案. 目前已有的安全多方计算协议主要包括保密的科学计算[4~6]、保密的计算几何[7~10]、保密的数据挖掘[11]、保密的集合运算[12,13]、保密的区间计算[14~21]以及其他安全多方计算应用问题.

关于区间的两方保密计算问题已有很多研究. 文献[14]中,Boneh 研究了区间查询问题,即判定一个点是否在一个区间内,所设计的协议仅保护了点的隐私. 文献[15~17]研究点与区间位置关系保密判定问题,其中文献[15]的判定结果由参与者共享,文献[16]所

收稿日期:2019-11-11;修回日期:2020-07-12;责任编辑:孙瑶
基金项目: 国家自然科学基金(No. 61272435)

设计协议同时保证了点与区间的隐私性. 在文献[17]中,当点不属于区间时,所设计协议会泄露点具体是位于区间的左侧或右侧的信息. 文献[18,19]将点与区间关系问题转化为判定多项式函数值的符号问题,并进一步解决了区间与区间位置关系的判定问题. 文献[20]研究重叠区间计算问题,所设计的区间与区间关系判定协议(协议 2)输出结果为密文,但复杂性较高.

考虑到在一些实际应用问题中,需要研究多维度"点与区间"或"区间与区间"关系阈值判定问题. 比如,在商品筛选中,用户希望通过输入一系列条件筛选出自己需要的商品. 将商品的属性抽象为若干个点(假设为 n 个),用户的要求范围抽象为 n 个对应区间,保密计算有多少个点属于对应的区间,并进一步判定具有这样性质的点的数目能否达到一个事先给定的阈值 $t(t\leqslant n)$(称这一问题为多维度"点与区间"关系阈值判定问题),来筛选出用户满意的商品(这些商品至少符合用户提出的 t 个条件). 类似地,许多实际问题可以抽象为保密计算两个区间列中有多少个对应区间是相交的,并判定具有相交性质的区间数目是否能达到一个给定的阈值 $t(t\leqslant n)$(称这一问题为多维度"区间与区间"关系阈值判定问题). 目前关于这类问题的研究结果还很少. 文献[21]对多维度"点与区间"关系判定问题(即 $t=n$ 的特殊情况)进行研究,其所设计的协议计算复杂性较高且有部分信息泄露. 由于研究这类问题有重要的实际意义,我们将设计更为安全高效的保密计算协议. 本文主要贡献如下:

(1)设计了"点与区间"以及"区间与区间"关系判定协议(协议 1 和协议 2),协议输出结果为密文,将其作为基础协议解决多维度"点与区间","区间与区间"关系判定问题以及区间的交并集等更复杂的保密计算问题时,能够保证中间结果的隐私性.

(2)提出并解决多维度"点与区间"以及"区间与区间"关系阈值保密判定新问题(协议 3 和协议 4). 当阈值 $t=n$ 时,协议 3 可解决文献[21]提出的问题,相比文献[21]的结果,本文协议 3 更为安全高效.

(3)所设计的协议对任何区间类型(开区间,闭区间或半开半闭区间)均适用,且区间端点可以是任意正有理数.

2　预备知识

2.1　计算模型及安全性定义

半诚实模型　半诚实参与者是指忠实履行协议的参与者,但在协议执行过程中,他们可能收集和保留获得的所有信息,并在协议执行后试图从中推算出其他参与者数据的额外信息. 若所有参与者均为半诚实参与者,则称这样的计算模型为半诚实模型.

协议的安全性　在安全多方计算中,普遍采用模拟范例方法证明协议的安全性,下面对其进行简单描述.

假设参与者为 P_1,P_2,两方合作计算概率多项式时间函数 $f:(x_1,x_2)\rightarrow(f_1(x_1,x_2),f_2(x_1,x_2))$,$P_i$ 的输入为 x_i. 假设 π 为计算函数 f 的一个两方协议,协议 π 执行中将 P_i 得到的信息序列记为 $view_i^{\pi}$:

$$view_i^{\pi}(x_1,x_2)=(x_i,r^i,m_1^i,\cdots,m_t^i,f_i(x_1,x_2))$$

其中 r^i 为 P_i 选择的随机数,m_k^i 为 P_i 收到的第 k 个信息,$f_i(x_1,x_2)$ 为 P_i 获得的输出结果.

如果存在概率多项式时间算法 S_1,S_2,使得对于 $i=1,2$,下面式子成立:

$$\{S_i(x_i,f_i(x_1,x_2))\}_{x_1,x_2}\overset{c}{\equiv}\{view_i^{\pi}(x_1,x_2)\}_{x_1,x_2}\quad(1)$$

则称协议 π 保密地计算了函数 f,其中 $\overset{c}{\equiv}$ 表示计算不可区分. 在证明两方计算协议安全性时,需要构造满足式(1)的 S_1 和 S_2.

2.2　Paillier 加密方案

Paillier 加密方案简要描述如下[22]:

密钥生成　给定安全参数 τ,运行密钥生成算法 $G(\tau)$:选取 τ 比特的素数 p,q,令 $N=pq,\lambda=\mathrm{lcm}(p-1,q-1)$;记 $L(x)=\dfrac{x-1}{N}$. 随机选取 $g\in Z_N^*$ 满足 $\gcd(L(g^{\lambda}\bmod N^2),N)=1$,则公钥为 $pk=(g,N)$,私钥为 $sk=\lambda$. 加密算法和解密算法分别记为 $E(\cdot)$ 和 $D(\cdot)$.

加密　对于明文 $m\in Z_N$,选择随机数 $r\in Z_N^*$,计算密文 $c=E(m)$:

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

解密　对于密文 $c\in Z_{N^2}^*$,解密得到明文 $m=D(c)$:

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

加法同态性　由于下面性质成立:

$$\begin{aligned}E(m_1)E(m_2)&=g^{m_1+m_2}(r_1r_2)^N \bmod N^2\\&=E(m_1+m_2\bmod N)\end{aligned}$$

因此 Paillier 加密方案具有加法同态性.

密文反转　假设 $E(m)$ 是应用公钥 pk 加密 $m(m\in\{0,1\})$得到的密文,定义 $T[E(m)]=E(1)E(m)^{N-1}$. 根据 Paillier 加密方案的加法同态性,$T[E(m)]=E(1-m)$. 因此,当 $m=0$ 时,$T[E(m)]=E(1)$;当 $m=1$ 时,$T[E(m)]=E(0)$. 称 $T[E(m)]$ 为密文反转运算.

2.3　基本命题

命题 1　任意整数 a,b,下面结论成立:

(a) $a>b$ 当且仅当 $2a>2b+1$;

(b) $a\leqslant b$ 当且仅当 $2a<2b+1$.

命题 1 将 a,b 三种大小关系 $a>b,a=b,a<b$ 合并为 $2a$ 与 $2b+1$ 的两种大小关系,在仅需判定 $a>b$ 是否

成立时应用命题 1 可防止额外信息泄露.

命题 2 在 Paillier 加密方案中,假设 a,b 在明文空间 Z_N 中取值. 令 $C=E(a)E(b)^{N-1}$ 以及 $w=D(C)$. 则有下面结论:

(a) $w=0$ 当且仅当 $a=b$;

(b) 如果 $-N/2<a-b<N/2$,则可知:$0<w<N/2$ 当且仅当 $a>b$;$N/2<w<N$ 当且仅当 $a<b$.

证明 由 Paillier 加密方案的加法同态性,$C=E(a)E(b)^{N-1}=E(a-b \bmod N)$,对 C 进行解密得 $w=D(C)=a-b \bmod N$.

(a) $w=a-b \bmod N=0$ 当且仅当存在整数 k,使得 $a-b=kN$. 根据 $a,b\in Z_N$,可知 $-N<a-b<N$,于是可知 $a-b=kN$ 成立当且仅当 $k=0$,即 $a=b$.

(b) 如果 $-N/2<a-b<N/2$,$w=a-b \bmod N\neq N/2$. 若 $a=b$,则 $w=0$;若 $a>b$,则 $0<a-b<N/2$,故 $0<w=a-b \bmod N=a-b<N/2$;若 $a<b$,则 $-N/2<a-b<0$,故 $N/2<w=a-b \bmod N=a-b+N<N$. 由于 $0\leqslant w<N$,仅可能为上述三种情况之一,故命题 2(b)得证. 综上,命题 2 是正确的.

3 区间关系保密判定基础协议

3.1 点与区间关系保密判定

问题描述:

假设 Alice 拥有区间 $I=(a,b)$,Bob 拥有点 e,$a<b$,其中 a,b,e 均为整数(称这样的区间 I 为整数区间),且 $a,e\geqslant 0$. Alice 和 Bob 要在不泄露自己数据信息的情况下合作计算 e 与 I 的位置关系函数 $F((a,b),e)$:如果 $e\in I$,定义 $F((a,b),e)=E(1)$,否则定义 $F((a,b),e)=E(0)$.

计算原理:

(ⅰ)由于 $e\in(a,b)$ 当且仅当 $e>a$ 与 $b>e$ 同时成立,应用命题 1 将判定 $e>a$(或 $b>e$)是否成立转化为判定 $2e>2a+1$(或 $2b>2e+1$)是否成立. 因此 $e\in(a,b)$ 当且仅当 $2e>2a+1$ 与 $2b>2e+1$ 同时成立.

(ⅱ) Alice 和 Bob 合作计算 $d_1=r_1(2a+1-2e)$,$d_2=r_2(2b-2e-1)$,使得 Alice 和 Bob 分别持有 d_1,d_2 和 r_1,r_2(r_1,r_2 为非零随机整数).

(ⅲ)由于 $d_1r_1=r_1^2(2a+1-2e)$,$d_2r_2=r_2^2(2b-2e-1)$. 故判定 $2e>2a+1$ 与 $2b>2e+1$ 是否同时成立即转化为判定 $d_1r_1<0$,$d_2r_2>0$ 是否同时成立. 由于 $d_1r_1>0$,$d_2r_2<0$ 不可能同时成立(否则与 $b>a$ 矛盾),故 $d_1r_1<0$,$d_2r_2>0$ 同时成立当且仅当 d_1r_1 与 d_2r_2 异号.

(ⅳ) Alice 和 Bob 根据 d_1,d_2 和 r_1,r_2 的符号,应用密文反转运算,合作计算 $F((a,b),e)$.

协议 1 点与区间位置关系函数保密计算协议.

输入: Alice 输入 $I=(a,b)$,Bob 输入 e.

输出:$F((a,b),e)$.

准备:设(G,E,D)是 Paillier 加密方案,τ 为安全参数,Alice 运行 $G(\tau)$生成公钥 $pk=(g,N)$和私钥 $sk=\lambda$,公布公钥(取 N 足够大,使得 $0<2e+1,2b<\sqrt{N/2}$).

step1 Alice 加密 a,b,发送密文 $E(a),E(b)$ 给 Bob.

step2 Bob 选择随机整数 r_1,r_2 满足 $-\sqrt{N/2}<r_1,r_2<\sqrt{N/2}$,计算 $W_1=[E(a)^2E(N+1-2e)]^{r_1}$,$W_2=[E(b)^2E(N-2e-1)]^{r_2}$,发送 W_1,W_2 给 Alice.

step3 Alice 解密得 $w_1=D(W_1)$,$w_2=D(W_2)$. 如果 w_1,w_2 同时小于 $N/2$ 或同时大于 $N/2$,令 $h=0$,否则令 $h=1$. 加密 h,发送密文 $E(h)$给 Bob.

step4 若 r_1,r_2 同号,Bob 计算 $H=E(h)E(0)$;否则计算 $H=T[E(h)]=E(1-h)$. 输出 H.

协议 1 的正确性:由 Paillier 加密方案的加法同态性可知,$w_1=r_1(2a+1-2e) \bmod N$,$w_2=r_2(2b-2e-1) \bmod N$. 由于 $2a+1<2b,2e+1,2b<\sqrt{N/2}$,$-\sqrt{N/2}<r_1,r_2<\sqrt{N/2}$,因此 $d_1=r_1(2a+1-2e)$,$d_2=r_2(2b-2e-1)$满足 $-N/2<d_1,d_2<N/2$,且 d_1,d_2 均不为零.

进一步对 w_1,w_2 的不同取值分析如下:

(ⅰ)如果 $w_1=r_1(2a+1-2e) \bmod N>N/2$,则必有 $d_1=w_1-N$,此时 $-N/2<d_1<0$.

(ⅱ)如果 $w_1=r_1(2a+1-2e) \bmod N<N/2$,则必有 $d_1=w_1$,此时 $0<d_1<N/2$.

同理,如果 $0<w_2<N/2$,则 $0<d_2<N/2$;如果 $N/2<w_2<N$,则 $-N/2<d_2<0$.

根据计算原理,$e\in(a,b)$ 当且仅当 d_1r_1 与 d_2r_2 异号. 而 d_1r_1 与 d_2r_2 异号当且仅当 d_1 与 d_2 同号且 r_1 与 r_2 异号,或 d_1 与 d_2 异号且 r_1 与 r_2 同号. 根据协议 1 第 3 步(b)及第 4 步,对于这两种情形均有 $H=E(1)$,而对于 d_1r_1 与 d_2r_2 同号的情形均有 $H=E(0)$.

综上,$e\in(a,b)$ 当且仅当 $H=E(1)$;$e\notin(a,b)$ 当且仅当 $H=E(0)$. 协议 1 是正确的.

协议 1 的安全性:通过模拟范例方法对协议 1 的安全性进行严格证明.

定理 1 半诚实模型下协议 1 是安全的.

证明 通过构造模拟器 S_1,S_2 严格证明定理 1. 首先构造 S_1. 接受输入$(a,b,F((a,b),e)=H)$后,S_1 按如下方式运行:

(ⅰ) S_1 任意选取 e',满足 $0<2e'+1<\sqrt{N/2}$且 $F((a,b),e')=F((a,b),e)$. 选择随机数 r_1',r_2'满足 $-\sqrt{N/2}<r_1',r_2'<\sqrt{N/2}$,计算 $W_1'=[E(a)^2E(N+1-2e')]^{r_1'}$,$W_2'=[E(b)^2E(N-2e'-1)]^{r_2'}$.

(ⅱ)S_1 分别解密 W_1',W_2',得到 w_1',w_2'. 如果 w_1',w_2'同时小于 $N/2$ 或同时大于 $N/2$,令 $h'=0$,否则令 $h'=1$.

加密 h' 得到 $E(h')$.

(ⅲ)若 r_1', r_2' 同号,计算 $H' = E(h')$;若 r_1', r_2' 异号,计算 $H' = T[E(h')] = E(1-h')$. 则有 $H' = F((a,b),e')$.

在协议执行中,$view_1^{\pi}((a,b),e) = \{a,b,W_1,W_2,F((a,b),e)\}$. 令 $S_1(a,b,F((a,b),e)) = \{a,b,W_1',W_2',F((a,b),e')\}$. Alice 对 W_1,W_2 解密后,得到 $w_1 = r_1(2a+1-2e) \bmod N$, $w_2 = r_2(2b-2e-1) \bmod N$,由于 r_1,r_2 为 Bob 选择的非零随机数,对于 Alice 来说,w_1,w_2 无异于随机数. 因此,$W_1 \overset{c}{\equiv} W_1'$, $W_2 \overset{c}{\equiv} W_2'$. 又 $F((a,b),e) = F((a,b),e')$,故 $\{S_1(a,b,F((a,b),e))\}_{a,b,e\in Z_N} \overset{c}{\equiv} \{view_1^{\pi}((a,b),e)\}_{a,b,e\in Z_N}$.

下面构造 S_2. 接受 $(e,F((a,b),e)=H)$ 后,S_2 按如下方式运行:

(ⅰ)S_2 任意选择区间 $I' = (a',b')$,满足 $0 \leqslant a' < b' < \sqrt{N/8}$ 且 $F((a,b),e) = F((a',b'),e)$. 加密 a',b' 得 $E(a'),E(b')$,选择随机数 r_1',r_2' 满足 $-\sqrt{N/2} < r_1', r_2' < \sqrt{N/2}$,计算 $W_1' = [E(a')^2 E(N+1-2e)]^{r_1'}$, $W_2' = [E(b')^2 E(N-2e-1)]^{r_2'}$.

(ⅱ)S_2 解密 W_1', W_2',得到 w_1', w_2'. 如果 w_1', w_2' 同时小于 $N/2$ 或同时大于 $N/2$,令 $h' = 0$,否则令 $h' = 1$. 加密 h' 得到 $E(h')$.

(ⅲ) 若 r_1', r_2' 同号,计算 $H' = E(h')$;若 r_1', r_2' 异号,计算 $H' = T[E(h')] = E(1-h')$. 则 $F((a',b'),e) = H'$.

在协议中,$view_2^{\pi}((a,b),e) = \{e,r_1,r_2,E(a),E(b),E(h),F((a,b),e)\}$. 令 $S_2(e,F((a,b),e)) = \{e,r_1',r_2',E(a'),E(b'),E(h'),F((a',b'),e)\}$.

由于随机数均是计算不可区分的,即有 $r_1 \overset{c}{\equiv} r_1'$, $r_2 \overset{c}{\equiv} r_2'$,由于 Bob 没有解密秘钥,故对 Bob 来说,$E(a) \overset{c}{\equiv} E(a')$, $E(b) \overset{c}{\equiv} E(b')$ 以及 $E(h) \overset{c}{\equiv} E(h')$;又因为 $F((a,b),e) = F((a',b'),e)$,故 $\{S_2(e,F((a,b),e))\}_{a,b,e\in Z_N} \overset{c}{\equiv} \{view_2^{\pi}((a,b),e)\}_{a,b,e\in Z_N}$.

因此,定理 1 得证.

注解 1　协议 1 对其他区间类型仍适用,若 $I = [a,b]$,则计算函数 $F((a-1,b+1),e)$ 即可. 若 $I = (a,b]$ (或 $I = [a,b)$),计算 $F((a,b+1),e)$ (或 $F((a-1,b),e)$) 即可.

3.2　两区间关系保密判定

问题描述:

假设 Alice 和 Bob 分别拥有整数区间 $I = (a,b)$, $J = (c,d)$,其中 $a,c \geqslant 0$. 希望在不泄露自己数据信息的情况下计算 I,J 的位置关系函数 $G(I,J)$:若 I,J 相交,定义 $G(I,J) = E(1)$,若 I,J 相离,定义 $G(I,J) = E(0)$.

计算原理:

区间 (a,b) 和 (c,d) 的所有位置关系如图 1 所示.

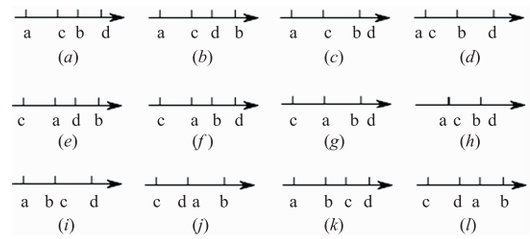

图1　两区间位置关系

由图 1 可知,(a,b), (c,d) 相交当且仅当 $d > a$ 与 $b > c$ 同时成立. 而 $d > a$ 与 $b > c$ 同时成立当且仅当 $2d > 2a+1$ 与 $2b > 2c+1$ 同时成立. 类似于协议 1 的计算原理,选择随机数 r_1,r_2,构造 $u_1 = r_1(2a+1-2d)$, $u_2 = r_2(2b-2c-1)$. 根据 u_1,u_2 和 r_1,r_2 的符号进行计算. 具体协议如下.

协议 2　两区间关系函数保密计算协议.

输入: Alice 和 Bob 分别输入 $I = (a,b)$, $J = (c,d)$,其中 $a,c \geqslant 0$.

输出:$G((a,b),(c,d))$.

准备:与协议 1 相同(取 N 足够大,使得 $0 < 2b, 2d < \sqrt{N/2}$).

step1　Alice 加密 a,b,发送 $E(a),E(b)$ 给 Bob.

step2　Bob 选择随机数 r_1,r_2 满足 $-\sqrt{N/2} < r_1, r_2 < \sqrt{N/2}$,计算 $V_1 = [E(a)^2 E(N+1-2d)]^{r_1}$, $V_2 = [E(b)^2 E(N-2c-1)]^{r_2}$,并发送给 Alice.

step3　Alice 解密得到 $v_1 = D(V_1)$, $v_2 = D(V_2)$. 如果 v_1,v_2 同时小于 $N/2$ 或同时大于 $N/2$,令 $l = 0$,否则令 $l = 1$. 加密 l,发送密文 $E(l)$ 给 Bob.

step4　若 r_1,r_2 同号,Bob 计算 $L = E(l)E(0)$;否则计算 $L = T[E(l)] = E(1-l)$. 输出 L.

协议 2 的正确性与安全性证明过程与协议 1 类似,此处不再赘述,仅给出下面定理.

定理 2　协议 2 是正确的,且在半诚实模型下是安全的.

注解 2　令 $I = [a,b]$, $J = [c,d]$,则图 1 中 (a) ~ (j) 表示 $[a,b]$, $[c,d]$ 相交,图 1(k)(l) 表示 $[a,b]$, $[c,d]$ 相离. 分析可知,$[a,b]$, $[c,d]$ 相交当且仅当 $a \leqslant d$, $b \geqslant c$ 同时成立,即 $2a < 2d+1$ 与 $2b+1 > 2c$ 同时成立. 类似于协议 2,可设计 I,J 为闭区间时的计算协议.

注解 3　在协议 1,2 中,若仅运行 1 ~ 3 步,则 Alice 持有解密数据,Bob 持有随机数,协议的运行结果由两方共享;若选取符号相同的随机数 r_1,r_2 (即 $r_1,r_2 > 0$ 或 $r_1,r_2 < 0$),可直接得到点与区间以及区间与区间的位

置关系(即协议输出结果为明文).

3.3 有理数域上区间问题保密计算

本节将第3.1节3.2节的问题扩展到有理数域上进行讨论,即点与区间端点都为有理数时的计算问题.

对正有理数 z,记其最简分数形式为:$z=\frac{z_1}{z_2}$,其中 z_1,z_2 为两个互素的正整数.

第3.1节问题解决方案

将 a,b 及 e 写成最简分式:$a=\frac{a_1}{a_2},b=\frac{b_1}{b_2}$及 $e=\frac{e_1}{e_2}$. 判定点 e 是否属于区间 (a,b),即判定 $e_1a_2>e_2a_1,e_1b_2<e_2b_1$ 是否同时成立. 令 $d_1=r_1(2e_1a_2-2e_2a_1-1),d_2=r_2(2e_1b_2+1-2e_2b_1)$. 类似于协议1,根据 r_1,r_2 与 d_1,d_2 的符号,计算得到 $F((a,b),e)$.

第3.2节问题解决方案

将 a,b 及 c,d 写成最简分式:$a=\frac{a_1}{a_2},b=\frac{b_1}{b_2}$及 $c=\frac{c_1}{c_2},d=\frac{d_1}{d_2}$. 此时仅需判定 $a<d$ 与 $b>c$ 是否同时成立,即判定 $a_1d_2<a_2d_1$ 与 $b_1c_2>b_2c_1$ 是否同时成立. 令 $u_1=r_1(2a_1d_2+1-2a_2d_1),u_2=r_2(2b_1c_2-2b_2c_1-1)$;类似于协议2,根据 r_1,r_2 及 u_1,u_2 的符号,计算得到 $G((a,b),(c,d))$.

4 多维度区间关系阈值问题保密计算

4.1 多维度"点与区间"关系阈值问题

问题描述:

假设 Alice 拥有 n 维区间序列 $I=\{I_1,\cdots,I_n\}$,Bob 拥有 n 维整数序列 $Q=\{e_1,\cdots,e_n\}$,其中 $I_k=(a_k,b_k)$ 为整数区间,且 $a_k,e_k\geqslant 0,k\in[n]=\{1,2,\cdots,n\}$. 在不泄露私密数据的情况下判定 $e_k\in I_k,k\in[n]$ 的区间个数(将其记为 s)是否达到阈值 t. 定义阈值函数 $S_t(I,Q)$ 如下:当 $s\geqslant t$ 时,令 $S_t(I,Q)=1$;当 $s<t$ 时,令 $S_t(I,Q)=0$. 多维度"点与区间"关系阈值保密判定即保密计算 $S_t(I,Q)$.

保密计算阈值函数 $S_t(I,Q)$ 有广泛的实际应用,例如:

(ⅰ)在贸易磋商时,Bob 向 Alice 推销自己的产品 C,假设该类产品有 n 项重要指标,Alice 对该类产品的性能指标有一定要求,如果 C 的 n 个性能指标中至少有 t 个符合要求,她才会考虑购买. 由于 Bob 的产品性能信息及 Alice 对产品的性能要求都属于商业机密,因此要在保护隐私的情况下进行磋商.

(ⅱ)在朋友推荐系统中,Alice 择友要求是对方至少满足自己所提 n 个条件中的 t 个. 系统根据这一要求结合所存储的候选人员信息进行朋友推荐. 由于系统储存的信息与 Alice 的要求都属于个人隐私,因此需要在保护隐私条件下进行朋友推荐.

在上述两个问题中,将 Alice 的要求抽象为区间序列 I,Bob 的产品性能参数(或推荐系统所存储候选人的信息)表示为点序列 Q,则问题转化为计算函数 $S_t(I,Q)$. 下面给出计算 $S_t(I,Q)$ 的具体方案.

计算原理:

调用协议1,计算点 e_k 与区间 $I_k=(a_k,b_k),k\in[n]$ 位置关系函数,得到 $H_k=F((a_k,b_k),e_k)$. 计算 $\prod_{k=1}^{n}H_k$,即 $e_k\in I_k,k\in[n]$ 的区间个数 s 对应的密文 $E(s)$. 根据命题1、2,保密比较 s 与 t 的大小关系.

协议3 多维度"点与区间"关系阈值问题保密判定协议.

输入: Alice 输入 $I=\{I_1,\cdots,I_n\}$,Bob 输入 $Q=\{e_1,\cdots,e_n\}$,其中 $I_k=(a_k,b_k)$ 为整数区间且 $a_k,e_k\geqslant 0,k\in[n]$;阈值 t.

输出:$S_t(I,Q)$.

准备:与协议1相同(取 N 足够大,使 $0<2e_k+1,2b_k<\sqrt{N/2}$ 且 $n<\sqrt{N/8}-1,k\in[n]$).

step1 Alice 与 Bob 分别输入 e_k 与 $I_k=(a_k,b_k),k\in[n]$. 调用协议1,Bob 得到输出 $H_k=F((a_k,b_k),e_k)$.

step2 Bob 选择随机数 $0<r<\sqrt{N/2}$,计算 $G=[(\prod_{k=1}^{n}H_k)^2E(N+1-2t)]^r$,发送 G 给 Alice.

step3 Alice 解密 G 得 $D(G)$,如果 $D(G)<N/2$,令 $\xi=1$,否则令 $\xi=0$. 输出 ξ.

协议3的正确性:由 Paillier 加密方案的加法同态性,$E(s)=\prod_{k=1}^{n}H_k$. 协议第3步解密得 $D(G)=r(2s+1-2t)\bmod N$. 由于 r 满足 $0<r<\sqrt{N/2}$,且有 $0<s,t<n<\sqrt{N/8}-1$,故 $0<r(2s+1),2rt<N/2$,于是可得 $-N/2<r(2s+1-2t)<N/2$. 根据命题1、2,$D(G)>N/2$ 当且仅当 $2s+1<2t$,即 $s<t$;$D(G)<N/2$ 当且仅当 $2s+1>2t$,即 $s\geqslant t$. 因此 $\xi=S_t(I,Q)$,故协议3是正确的.

协议3的安全性:协议3第1步为并行执行协议1的过程,第3步中 Alice 解密 G 得到 $D(G)=r(2s+1-2t)\bmod N$,由于 r 为 Bob 选择的随机数,Alice 解密仅得到 s,t 的大小关系,这是协议的输出结果,故协议3是安全的.

类似于协议1,可应用模拟范例方法证明协议安全性,在此省略,仅给出下面定理.

定理3 半诚实模型下协议3是安全的.

4.2 多维度"区间与区间"关系阈值问题

问题描述:

假设 Alice 和 Bob 分别拥有区间序列 $I=\{I_1,\cdots,$

$I_n\}$ 和 $J=\{J_1,\cdots,J_n\}$,其中 $I_k=(a_k,b_k)$,$J_k=(c_k,d_k)$,$k\in[n]$ 均为整数区间且 $a_k,c_k\geqslant 0$. 在不泄露数据隐私性的情况下判定 $I_k,J_k,k\in[n]$ 具有相交关系的区间个数 φ 是否达到给定的阈值 t. 定义阈值函数 $\Phi_t(I,J)$ 如下:如果 $\varphi\geqslant t$,定义 $\Phi_t(I,J)=1$,否则定义 $\Phi_t(I,J)=0$. 多维度"区间与区间"关系阈值判定问题即保密计算函数 $\Phi_t(I,J)$.

研究 $\Phi_t(I,J)$ 保密计算有广泛实际应用. 在进出口贸易谈判中,进口方 A 希望从出口方 B 处进口一批货物. 考虑到金额与需求等问题,A 对商品的进口量设置了上限与下限;相应地,B 根据库存和运输成本等问题对各种商品的出口量设置了上限与下限. 两方商定至少有 t 种商品进出口量能达成一致时才可能成交,否则就中止磋商. 由于对于 A(或 B)来说,上下限的设置在一定程度上反映了 A(或 B)方的购买力(或生产能力),如果不能成交则不希望泄露给对方. 将进口量与出口量分别表示为区间序列 I,J,计算阈值函数 $\Phi_t(I,J)$ 即可得到结果.

协议 4　多维度"区间与区间"关系阈值问题判定协议.

输入: Alice 和 Bob 分别输入 $I=\{I_1,\cdots,I_n\}$ 和 $J=\{J_1,\cdots,J_n\}$,其中 $I_k=(a_k,b_k)$,$J_k=(c_k,d_k)$ 为整数区间且 $a_k,c_k\geqslant 0$;阈值 t.

输出:$\Phi_t(I,J)$.

准备:与协议 1 相同(取 N 足够大,使得 $n<\sqrt{N/8}-1,0<2b_k,2d_k<\sqrt{N/2},k\in[n]$).

step1　Alice 和 Bob 分别输入 I_k 和 J_k,调用协议 2,使 Bob 得到输出 $L_k,k\in[n]$.

step2　Bob 选择随机数 r 满足 $0<r<\sqrt{N/2}$,计算 $X=[(\prod_{k=1}^{n}L_k)^2E(N+1-2t)]^r$,发送 X 给 Alice.

step3　Alice 解密 X,得到 $x=D(X)$. 如果 $x<N/2$,令 $y=1$,否则令 $y=0$. 输出 y.

协议 4 的正确性与安全性证明过程与协议 3 类似,不再赘述,仅给出下面定理.

定理 4　协议 4 是正确的,且在半诚实模型下是安全的.

5　效率分析

5.1　本文协议效率分析

计算复杂性分析:为便于分析与比较,我们仅考虑最耗时的模指数运算. 在 Paillier 加密方案中,加密(或解密)1 次需要进行 2 次(或 1 次)模指数运算.

协议 1、2 中,Alice 需 3 次加密与 2 次解密运算,共需 8 次模指数运算. Bob 需 3 次加密与 5 次模指数运算,共需 11 次模指数运算. 故协议 1、2 均需 19 次模指数运算.

协议 3、4 中,若区间序列维度为 n,Alice 需 $3n$ 次加密与 $2n+1$ 次解密,共 $8n+1$ 次模指数运算. Bob 最多需 $2n+2$ 次加密与 $5n+2$ 次模指数运算,共 $9n+6$ 次模指数运算. 因此协议 3、4 均需进行 $17n+7$ 次模指数运算.

通信复杂性分析:本文应用通信次数衡量协议通信复杂性. 协议 1、2 均需进行 3 次通信,协议 3、4 需 4 次通信.

5.2　与已有结果比较分析

文献[19]研究了点与区间,区间与区间关系判定问题,协议所得结果为明文. 其中协议 1 判定点与区间位置关系,需 11 次模指数运算与 3 次通信. 协议 2 研究两区间详细位置关系(包括相交、包含、端点重合、相离等多种位置关系),最多需 44 次模指数运算与 8 次通信,最少需 22 次模指数运算与 4 次通信. 本文协议 1、2 也可直接得到明文结果,协议 2 相比文献[19]协议 2 设计思想更为简单易行,且具有更低的计算复杂性与通信复杂性.

文献[20]设计输出结果为密文的区间关系判定协议(协议 2). 需要调用两次文献[23]中安全比较共享协议,假设数据取值范围为[0,m),此协议需 $2h$ 次加密与 h 次解密运算($h=\lceil\log_2^m\rceil+1$),即 $5h$ 次模指数运算;另外需调用一次文献[20]中协议 1,共 5 次加密与 7 次模指数运算,即 17 次模指数运算. 故文献[20]协议 2 共需 $10h+17$ 次模指数运算,需 5 次通信.

记点与区间关系判定问题为 PIR,区间与区间关系(相交与相离)判定问题以及详细关系判定问题分别为 IIR,IIRD. 本文协议与文献[19,20]协议对比分析如表 1.

表 1　效率对比分析

文献	解决问题	输出结果	模指数运算次数	通信次数
文献[19]协议 1	PIR	明文	11	3
本文协议 1	PIR	密文/明文	19	3
文献[19]协议 2	IIRD	明文	44	8
文献[20]协议 2	IIR	密文	$10h+17$	5
本文协议 2	IIR	密文/明文	19	3

文献[21]研究多维度"点与区间"关系判定问题,若 Alice(或 Bob)拥有的点(或开区间)个数为 n,文献[21]协议 1、2 研究问题与本文协议 3($t=n$ 时)研究问题相同. 文献[21]协议 1 需 $4n$ 次加密与 $2n$ 次解密运算,即 $10n$ 次模指数运算,需 $2n+2$ 次通信. 协议求得计算结果的同时,也泄露了有多少个点属于对应区间. 文献[21]中协议 2 为近似计算协议,若要提高精确性,协议的计算复杂性和通信复杂性都将升高. 因此,从计算

效率、安全性以及实际操作性几方面考虑,本文所设计的协议与文献[21]相比都有明显优势.

5.3 实验分析

实验测试环境: Windows 7 64 位(旗舰版)操作系统,内存 4.00GB,处理器 Intel(R) Core(TM) i3-3227UCPU@1.90GHz,用 java 语言在 MyEclipse 上运行实现.

实验方法:通过实验模拟协议运行过程,根据实验耗时验证协议执行效率.

本文协议 1、2 计算过程类似且所需模指数运算次数相同,文献[20]协议 2 与本文协议 2 研究问题相同.因此,分别对本文协议 2 与文献[20]协议 2 进行 1000 次模拟实验,并计算每次实验执行时间的平均值,可得协议耗时如图 2 所示. 由图 2 可知,文献[20]中协议 2 执行时间远远高于本文协议 2.

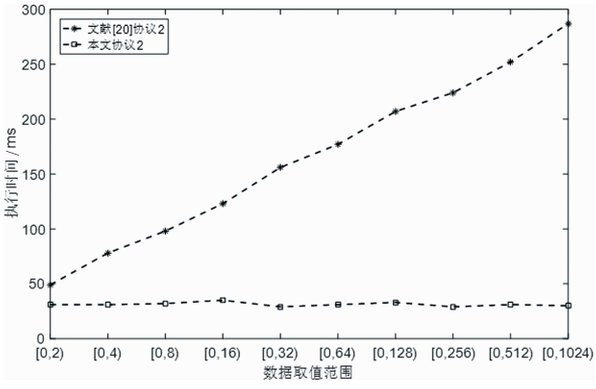

图2 本文协议2与文献[20]协议2执行时间

协议 3、4 计算过程类似,故仅对协议 3 进行实验分析. 在区间序列维度 n 分别为 5,10,…,40 时,对 n 的每个设定值进行 1000 次模拟实验,统计协议 3 执行时间平均值如图 3 所示.

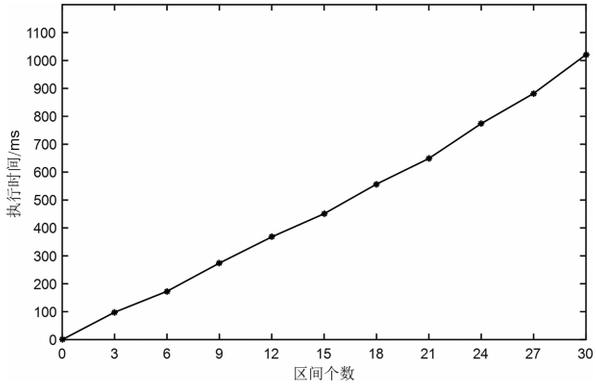

图3 协议3执行时间

6 总结与展望

本文研究“点与区间”与“区间与区间”关系保密判定问题,以及多维度“点与区间”与“区间与区间”关系阈值保密判定问题. 协议均是在半诚实模型下设计的,即参与者需严格按照协议要求执行协议. 考虑到在一些情况下,参与者可能基于某种目的而存在主动攻击行为,因此,研究恶意模型(即能够防止主动攻击行为的模型)下的区间关系安全计算协议将是我们下一步的研究工作.

参考文献

[1] YAO A C. Protocols for secure computations[A]. Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science[C]. Chicago:IEEE,1982. 160 – 164.

[2] GOLDREICH O, MICALI S, WIGDERSON A. How to play any mental game[A]. Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing[C]. New York:ACM,1987. 218 – 229.

[3] GOLDREIH O. Foundations of Cryptography: Volume 2, Basic Applications[M]. London: Cambridge University Press,2004. 599 – 764.

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

[5] GRIGORIEV D, SHPILRAIN V. Yao's millionaires' problem and decoy-based public key encryption by classical physics[J]. International Journal of Foundations of Computer Science,2014,25(04):409 – 417.

[6] LI S D, GUO Y M, ZHOU S F, et al. Efficient protocols for the general millionaires' problem[J]. Chinese Journal of Electronics,2017,26(4):696 – 702.

[7] YANG X Y, LI S D, Zuo X J. Secure multi-party geometry computation[J]. Journal of Cryptologic Research, 2016, 3(1):33 – 41.

[8] 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[J]. 电子学报,2007,35(4):685 – 691.
LUO Yong-long, HUANG Liu-sheng, XU Wei-jiang, et al. A protocol for privacy preserving intersect determination of two polygons[J]. Acta Electronica Sinica, 2007, 35(4): 685 – 691. (in Chinese)

[9] 李顺东,杨晓莉,左祥建,等. 保护私有信息的图形相似判定[J]. 电子学报,2017,45(9):2184 – 2189.
LI Shun-dong, YANG Xiao-li, ZUO Xiang-jian, et al. Privacy-preserving graphical similarity determination[J]. Acta Electronica Sinica,2017,45(9):2184 – 2189. (in Chinese)

[10] LIU L, CHEN X F, LOU W J. Secure three-party computational protocols for triangle area[J]. International Journal of Information Security,2016,15(1):1 – 13.

[11] LINDELL, PINKAS. Privacy preserving data mining[J]. Journal of Cryptology, 2008, 9(8): 616 – 621.
[12] EGERT R, FISCHLIN M, GENS D, et al. Privately computing set-union and set-intersection cardinality via bloom filters[J]. European Journal of Operational Research, 2015, 139(2): 371 – 389.
[13] 窦家维,陈明艳. 多重集的保密计算及应用[J]. 电子学报,2020,48(1):204 – 208.
DOU Jia-wei, CHEN Ming-yan. Secure multi-set operations and their applications[J]. Acta Electronica Sinica, 2020, 48(1): 204 – 208. (in Chinese)
[14] BONEH D, WATERS B. Conjunctive, subset, and range queries on encrypted data[A]. Proceedings of Theory of Cryptography Conference [C]. Berlin: Springer, 2007. 535 – 554.
[15] NISHIDE T, OHTA K. Multiparty computation for interval, equality, and comparison without bit-decomposition protocol[A]. Proceedings of the 10th International Conference on Practice and Theory in Public-Key Cryptography[C]. Berlin: Springer, 2007. 343 – 360.
[16] 郭奕旻,周素芳,窦家维,等. 高效的区间保密计算及应用[J]. 计算机学报,2017,41(7):1664 – 1679.
GUO Yi-min, ZHOU Su-fang, DOU Jia-wei, et al. Efficient privacy-preserving interval computation and its applications[J]. Chinese Journal of Computers, 2017, 41(7): 1664 – 1679. (in Chinese)
[17] 陈振华,李顺东,陈立朝,等. 点和区间关系的全隐私保密判定[J]. 中国科学:信息科学, 2018, 48(2): 187 – 204.
CHEN Zhen-hua, LI Shun-dong, CHEN Li-zhao, et al. Fully privacy-preserving determination of point-range relationship[J]. Scientia Sinica Informationis, 2018, 48(2): 187 – 204. (in Chinese)
[18] 窦家维,王文丽,刘旭红,等. 有理区间的安全多方计算与应用[J]. 电子学报,2018,46(9):11 – 16.
DOU Jia-wei, WANG Wen-li, LIU Xu-hong, et al. Secure multiparty computation of rational interval and its applications[J]. Acta Electronica Sinica, 2018, 46(9): 11 – 16. (in Chinese)
[19] 窦家维,王文丽,李顺东. 区间位置关系的保密判定[J]. 计算机学报,2019,42(5):1031 – 1044.
DOU Jia-wei, WANG Wen-li, LI Shun-dong. Privately determining interval location relation[J]. Chinese Journal of Computers, 2019, 42(5): 1031 – 1044. (in Chinese)
[20] STEFANA W, DANIELB M, FABIANB F, et al. Designing privacy-preserving interval operations based on homomorphic encryption and secret sharing techniques[J]. Journal of Computer Security, 2017, 25(1): 59 – 81.
[21] SHI L, LUO Y L, ZHANG C Y. Secure two-party multi-dimensional vector comparison protocol[A]. International Conference on Management and Service Science[C]. Wuhan: IEEE, 2009. 1 – 5.
[22] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[A]. Advances in Cryptology [C]. Czech Republic: Springer, 1999. 223 – 238.
[23] NERGIZ A E, NERGIZ M E, Pedersen T, et al. Practical and secure integer comparison and interval check[A]. 2010 IEEE Second International Conference on Social Computing[C]. Minneapolis: IEEE, 2010. 791 – 799.

作者简介

窦家维　女,1963 年出生,陕西西安人. 副教授、硕士生导师. 分别在陕西师范大学、西安交通大学获得硕士学位、博士学位. 主要研究方向为应用数学和密码学.
E-mail: jiawei@ snnu. edu. cn

王颖囡　女,1996 年出生,河南三门峡人. 现为陕西师范大学硕士生. 主要研究方向为应用数学和密码学.
E-mail: wangyingnan@ snnu. edu. cn

葛　雪　女,1995 年出生,山西运城人. 现为陕西师范大学硕士生. 主要研究方向为应用数学和密码学.