中国科学: 信息科学 2018 年 第 48 卷 第 2 期: 187–204
SCIENTIA SINICA Informationis
论文

点和区间关系的全隐私保密判定

陈振华[1,2,3*], 李顺东[4], 陈立朝[1], 黄琼[5], 张卫国[1]

1. 西安科技大学计算机科学与技术学院, 西安 710054
2. 中国科学院信息工程研究所信息安全国家重点实验室, 北京 100093
3. 桂林电子科技大学广西可信软件重点实验室, 桂林 541004
4. 陕西师范大学计算机科学学院, 西安 710062
5. 华南农业大学数学与信息学院, 广州 510642
* 通信作者. E-mail: chenzhenhua@snnu.edu.cn

收稿日期: 2017–6–13; 接受日期: 2017–9–13; 网络出版日期: 2018–01–08
国家自然科学基基金 (批准号: 61272435)、信息安全国家重点实验室开放课题基金 (批准号: 2016-MS-19)、广西可信软件重点实验室研究课题资助 (批准号: kx201614) 和陕西省自然科学基础研究计划面上项目 (批准号: 2017JM6069) 资助

摘要 点和区间关系的保密判定在范围查询中应用非常广泛, 但目前已存的解决方案大多只保护了一方的隐私, 而另一方的隐私并未得到保护. 此外, 已存方案给出的点和区间都是离散的整数 (或有理数) 范围. 针对这些问题, 本文利用安全多方计算的思想设计了保密判定点和区间关系的 2 种协议, 不但同时保护了两方的隐私, 而且将数域推广到连续的实数. 本文首先利用 0-1 编码并结合 Goldwasser-Micali 同态加密给出了全隐私判定一个整数点是否在一个离散整数区间上的协议 1; 然后利用函数的单调性和 Paillier 同态加密给出了全隐私判定一个实数点是否在一个连续实数区间的协议 2. 最后, 给出了本文协议的一个应用实例. 理论和实验分析显示: 本文的两个协议在取得较优通信效率的同时都取得了全隐私性. 此外, 协议 2 相比以往的方案, 第一次给出点和连续实数区间的判定方法, 在保持较优效率和良好性能的同时取得了通用性.

关键词 点和区间, 全隐私, 安全多方计算, 实数, 同态加密

1 引言

安全多方计算最早由 Yao [1] 提出, 是指在不泄漏各方的输入数据 (隐私性) 的条件下, 正确完成输入数据的函数计算 (正确性). 现实问题中涉及到保护隐私的合作计算都可以归结到安全多方计算的范围. 因此它在保护隐私的质量评估 [2]、定位查找 [3]、数据挖掘 [4]、数据查询 [5]、外包计算 [6] 等方面有着广泛的应用.

点和区间关系的保密判定, 是指在保护一方 (或两方) 隐私的情况下, 判断一方的点是否包含在另一方区间中. 这个问题是密文搜索中常需嵌入的属性关系问题, 在保护隐私的范围查询或定位搜索中

引用格式: 陈振华, 李顺东, 陈立朝, 等. 点和区间关系的全隐私保密判定. 中国科学: 信息科学, 2018, 48: 187–204, doi: 10.1360/N112017-00025
Chen Z H, Li S D, Chen L C, et al. Fully privacy-preserving determination of point-range relationship (in Chinese). Sci Sin Inform, 2018, 48: 187–204, doi: 10.1360/N112017-00025

有着非常广泛的应用. 例如, 2007 年, Boneh 等 [7] 提出了一种搜索加密方案, 只有满足一定大小关系的目标密文才可以被搜索到. 这个方案推广后可以进行区间查询, 即只有满足点和区间包含关系的目标密文才可以被搜索到, 从而进一步解密目标密文. 但这个方案中, 只有点的隐私得到了保护, 而区间隐私并没有得到保护. 2013 年, Wen 等 [8] 提出了一种可以直接进行区间查询的搜索方案, 应用在智能电网中. 这个方案中点和区间的隐私都得到了保护, 但却和 Boneh 等 [7] 的方案一样, 所判断的点和区间都是离散的整数.

若在以上方案中能进行点和区间关系的全隐私保密判定, 即在判定点和区间关系时, 两方 (点和区间) 的隐私都得到保护, 就能提高方案中用户的隐私性. 与此同时, 将点和区间的范围从离散的整数推广到连续的实数, 就能更好地扩大这些方案的应用, 从而丰富公钥密码学的体制和应用. 因此, 本文对点和区间关系进行全隐私的保密判定, 有着重要的研究意义.

点和区间关系的全隐私保密判定, 是指在不泄漏双方隐私的情况下, 保密地判断一方的点是否包含在另一方区间中. 这个问题的解决归属于安全多方计算的研究领域, 是安全多方计算问题的一个分支. 因此以安全多方计算的思想解决该问题, 恰好符合了两方, 即点和区间隐私都需要保护的要求. 本文正是基于这一点, 利用了安全多方计算的思想去研究这个问题.

1.1 相关工作

针对点和区间关系的保密判定问题, 目前的方案 [9~12] 大多利用了承诺或可验证加密的技术, 证明者给出了一个点在某个区间上的证据, 然后让验证者进行验证. 但这些方案只保护了点的隐私, 并且点和区间都是离散的整数. 2016 年, Guo 等 [13] 第一次利用安全多方计算的思想给出了点和区间关系的全隐私保密判定协议, 并且将数和区间的范围推广到有理数域上. 在该方案中, Guo 等 [13] 先将数和区间关系的判定问题转化为两个有理数比较大小问题, 然后将有理数化成两个整数的商, 并将此商和平面上直线的斜率对应, 从而将两个有理数比较大小问题进一步转化为平面上两条直线的位置关系问题, 最后基于同态加密解决了该问题. 这个方法非常巧妙, 解决了点和区间的全隐私判定问题, 但数和区间的取值范围却只能是离散的有理数.

本文的研究目的, 是不但要解决点和区间的全隐私判定问题, 还要将数和区间的取值范围从离散的整数 (或有理数) 扩展到连续的实数. 正如前文所述, 我们拟弥补类似于文献 [7,8] 这样的密文搜索方案中的不足, 推进公钥密码学的体制和应用, 然而已存方案 [9~13] 都不能解决这些问题, 均已失效.

1.2 本文贡献

针对以上方案的不足和本文的创作目的, 我们设计了新的点和区间关系的保密判定协议. 贡献如下:

(1) 提出了新的转化思路和技巧. 以 0-1 编码和级联异或的思想解决了整数域上的判定问题; 以实数化为整数和函数单调性的思想解决了实数域上的判定问题.

(2) 设计了两个新的协议. 构造了整数点和离散整数区间的全隐私保密判断定协议 1; 构造了实数点和连续实数区间的全隐私保密判定协议 2.

(3) 提高了效率. 本文的两个协议并没有利用循环语句调用百万富翁协议, 而是一次性保密判断了一个点是否在一个区间上.

(4) 通用性. 本文的协议 2 可以做为保密判断点和区间关系的通用协议.

表 1 $x \oplus y$

Table 1 $x \oplus y$

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

2 预备知识

2.1 级联异或

(1) 异或. 在二进制运算中, 其中有一种二元运算为异或运算, 用符号 $\oplus$ 表示. 令 $x = 0, 1$, $y = 0, 1$, 可得到 $x \oplus y$ 的运算结果如表 1.

由表 1 可以看出, 若 x 异或 0, 则异或结果保持不变仍为 x; 若 x 异或 1, 则异或结果反转, 即 x 变成相反的数 $\neg x$. 因此得到下面异或运算的性质 1.

性质1 任何数和 0 异或都不改变这个数; 而任何数和 1 异或都使得该数反转.

(2) 级联. 我们用 $\|$ 表示级联, 该运算是指将多个二进制字符串串联在一起成为更长的字符串. 字符串级联后仍然可以进行异或运算. 令 a, b, c, d 为等长的字符串, 将字符串 a, b 级联后得到 $a \| b$; 将 c, d 级联后得到 $c \| d$, 则得到以下性质 2.

性质2 异或后级联等价于级联后异或. 即 $(a \oplus c) \| (b \oplus d) = (a \| b) \oplus (c \| d)$. 其中 a, b, c, d 为等长的二进制字符串.

证明 我们从右式向左式证明. $(a \| b) \oplus (c \| d)$ 表示字符串 $a \| b$ 和另一个字符串 $c \| d$ 按位异或. 因为 a, b, c, d 等长, 则 a 和 c 按位进行异或得到 $a \oplus c$; b 和 d 按位进行异或得到 $b \oplus d$, 再将两者级联得到 $(a \oplus c) \| (b \oplus d)$, 该结果就为 $(a \| b) \oplus (c \| d)$ 的运算结果.

2.2 Paillier 的同态加密体制

Paillier 在文献 [14] 中提出了一种加密方案.

- 系统建立. 系统选取 $N = pq$, 其中 p, q 为两个大素数, $\lambda = \mathrm{lcm}(p-1,\ q-1)$, $g \in B$, $B = \cup_{\alpha=1}^{\lambda} B_\alpha$, $B_\alpha \subset Z_N^*$. 系统公钥为 $(g,\ N)$, 私钥为 λ.
- 加密过程. 明文 $m < N$, 任取随机数 $r \in Z_N^*$, 密文: $c = g^m r^N \mathrm{mod} N^2$.
- 解密过程. 密文 $c < N^2$, $L(u) = \frac{u-1}{N}$, $u < N^2$, 明文: $m = \frac{L(c^\lambda \mathrm{mod} N^2)}{L(g^\lambda \mathrm{mod} N^2)}$.

性质3 Paillier 加密方案具有加法同态性质.

证明 设 E 是一个加密算法, $c_1 = E(m_1, r_1)$ 是对 m_1 的加密, $c_2 = E(m_2, r_2)$ 是对 m_2 的加密, 若有 $c_1 c_2 = E(m_1 + m_2, r)$, 其中 r_1, r_2, r 是随机数, 则称 E 是一个加法同态加密算法. 在 Paillier 方案中, 令 $r_1 r_2 = r$, 则有

$$\begin{aligned} c_1 c_2 &= (g^{m_1} r_1^N \mathrm{mod} N^2)(g^{m_2} r_2^N \mathrm{mod} N^2) \\ &= g^{m_1+m_2} (r_1 r_2)^N \mathrm{mod} N^2 \\ &= g^{m_1+m_2} r^N \mathrm{mod} N^2, \end{aligned}$$

即有, $E(m_1)E(m_2) = E(m_1 + m_2, r)$. 因此, Paillier 加密方案具有加法同态性质.

2.3 Goldwasser-Micali 的同态加密体制

Goldwasser-Micali 在文献 [15] 中提出了一种加密方案.

- 系统建立. 系统选取 $N = pq$, 其中 p, q 为两个大素数, y 为模 N 的非二次剩余. 系统公钥为 $(N,\ y)$, 私钥为 $(p,\ q)$.
- 加密过程. 明文 $m \in \{0,1\}$, 任取随机数 $r \in Z_N^*$, 密文: $c = y^m r^2 \mathrm{mod} N$.
- 解密过程. 密文 $c < N$, 输入私钥 (p,q), 求 Jacobi 符号 $(\frac{c}{N}) = (\frac{c}{p})(\frac{c}{q})$, 明文

$$m = \begin{cases} 0, & 若\left(\left(\dfrac{c}{p}\right) = 1\right) \wedge \left(\left(\dfrac{c}{q}\right) = 1\right), \\ 1, & 若\left(\left(\dfrac{c}{p}\right) = -1\right) \vee \left(\left(\dfrac{c}{q}\right) = -1\right). \end{cases}$$

性质4 Goldwasser-Micali 加密方案具有异或同态性质.

证明 设 E 是一个加密算法, $c_1 = E(m_1, r_1)$ 是对 m_1 的加密, $c_2 = E(m_2, r_2)$ 是对 m_2 的加密, 若有 $c_1 c_2 = E(m_1 \oplus m_2, r)$, 其中 r_1, r_2, r 是随机数, $\oplus$ 表示异或, 则称 E 是一个异或同态加密算法. 在 Goldwasser-Micali 方案中, 令 $r_1 r_2 = r$, 则有

$$\begin{aligned} c_1 c_2 &= (g^{m_1} r_1^2 \mathrm{mod} N) g^{m_2} r_2^2 \mathrm{mod} N \\ &= g^{m_1 \oplus m_2} (r_1 r_2)^2 \mathrm{mod} N \\ &= g^{m_1 \oplus m_2} r^2 \mathrm{mod} N, \end{aligned}$$

即有, $E(m_1)E(m_2) = E(m_1 \oplus m_2, r)$. 因此, Goldwasser-Micali 加密方案具有异或同态性质.

性质5 Goldwasser-Micali 加密方案具有自盲性质和反转性质.

证明 根据异或运算的性质 1, 对 Goldwasser-Micali 加密体制进行异或同态操作时, 若令 $m_2 = 0$, 则有

$$\begin{aligned} c_1 c_2 &= g^{m_1} r_1^2 \mathrm{mod} N g^0 r_2^2 \mathrm{mod} N \\ &= g^{m_1 \oplus 0} (r_1 r_2)^2 \mathrm{mod} N \\ &= g^{m_1} r^2 \mathrm{mod} N, \end{aligned}$$

即异或 0 可使得密文 c_1 变成另一个密文 $c_1 c_2$, 但不影响解密的明文 m_1. 若令 $m_2 = 1$, 则有

$$\begin{aligned} c_1 c_2 &= g^{m_1} r_1^2 \mathrm{mod} N g^1 r_2^2 \mathrm{mod} N \\ &= g^{m_1 \oplus 1} (r_1 r_2)^2 \mathrm{mod} N \\ &= g^{\neg m_1} r^2 \mathrm{mod} N, \end{aligned}$$

即异或 1 可使得密文 c_1 变成另一个密文 $c_1 c_2$, 且使得原来的明文 m_1 反转为相反的明文 $\neg m_1$.

因此, 由以上推理可得到: 在 Goldwasser-Micali 加密方案中, 异或 0 具有自盲性质; 异或 1 具有反转性质.

2.4 安全多方计算的安全性

(1) 半诚实参与者. 安全多方计算的协议运行环境按照参与者可以分为半诚实模型和恶意模型 [16], 半诚实参与者指协议方将诚实地执行协议, 不会篡改输入和输出信息, 但可能会保留计算的中间结果, 试图推导出协议之外的信息或者他人的信息.

(2) 半诚实模型下的安全性定义. Goldreich [16] 利用比特承诺和零知识证明理论设计了一个编译器, 这个编译器可以将在半诚实参与者条件下保密计算函数 f 的协议 π 自动生成在恶意参与者条件下也能保密计算 f 的协议 π'. 新的协议 π' 可以迫使恶意参与者以半诚实方式参与协议的执行, 否则就会被发现. 因此大多数情况下, 只设计半诚实模型下的协议. 当设计出所需要的半诚实模型下的安全多方协议时, 只要按照 Goldreich [16] 的通用转化方法就可以将原协议转化为恶意模型下的新协议. 基于这一结论, 本文也只给出半诚实模型下的协议和相应的安全性模拟范例.

设 (x,y) 为概率多项式函数, π 是计算 f 的协议, 设 Alice 拥有 x, Bob 拥有 y, 他们要在不暴露 x,y 的前提下, 合作计算函数 $f(x,y)=(f_1(x,y),f_2(x,y))$. 计算的目的是为了让 Alice 和 Bob 分别得到函数 f 的两个分量 $f_1(x,y),f_2(x,y)$. Alice 在执行协议的过程中所得到的视图记为 $\mathrm{view}_1(x,y)$, 输出记作 $\mathrm{output}_1(x,y)$; 同理, Bob 的视图记为 $\mathrm{view}_2(x,y)$, 输出记作 $\mathrm{output}_2(x,y)$. Goldreich 在文献 [16] 中给出计算不可区分性的半诚实参与者的安全两方计算定义, 表述如下.

定义1 协议 π 保密地计算了 $f(x,y)$, 若存在概率多项式时间模拟器 S_1 与 S_2, 使得以下两式同时成立:

$$\{S_1(x,f_1(x,y)),f_2(x,y)\}\stackrel{c}{=}\{\mathrm{view}_1(x,y),\mathrm{output}_2(x,y)\},\tag{1}$$

$$\{f_1(x,y),S_2(y,f_2(x,y))\}\stackrel{c}{=}\{\mathrm{output}_1(x,y),\mathrm{view}_2(x,y)\},\tag{2}$$

其中 $\stackrel{c}{=}$ 表示计算不可区分.

此定义说明了任何一方参与者视图中的信息只能从自己输入和所获得的输出中得到, 即说明任何一方参与者视图中不包含额外的信息, 这样就保证了在协议执行过程中, 任何一方得不到其他方的私有信息. 因此要证明一个两方计算协议是保密的, 就必须构造使得式 (1) 和 (2) 成立的模拟器 S_1 与 S_2.

3 问题的描述和转化

3.1 问题的描述

问题 1. 整数点和离散整数区间的保密判定. 已知 U 为一个全集, Alice 拥有一个整数点 x , Bob 拥有一个离散的整数区间 $[y,y+l]=\{y,y+1,\ldots,y+l\}$, 其中 $x,y,y+l\in U$. 在不泄露点和区间任何信息的情况下, Alice 和 Bob 都想知道整数点 x 是否包含在离散的整数区间 $[y,y+l]$ 中, 即是否 $x\in[y,y+l]$.

问题 2. 实数点和连续实数区间的保密判定. 已知 Alice 拥有一个实数点 x, Bob 拥有一个的连续的实数区间 $[y_1,y_2]$, $x,y_1,y_2\in U$, 小数点位数精确到 k 位. 在不泄露点和区间任何信息的情况下, Alice 和 Bob 都想知道实数点 x 是否包含在连续的实数区间 $[y_1,y_2]$ 中, 即是否 $x\in[y_1,y_2]$.

3.2 问题的转化

为了将 3.1 小节的 2 个问题转化为我们能解决的问题, 本文利用了以下 4 个技巧.

(1) 0-1 编码. $U=\{x_1,x_2,\ldots,x_n\}$ 为一个全集, $|U|=n$. Alice 拥有整数点 x, 将 x 按规则 I 编码

表 2　0-1 编码

Table 2　0-1 coding

Original data	0-1 coding
$x=4$	$a=\{0,0,0,1,0,0,0\}$
$y=2$	$b=\{0,1,1,1,1,1,1\}$
$y+l=5$	$c=\{0,0,0,0,1,1,1\}$

表 3　异或级联

Table 3　xor concatenation

Original data	xor concatenation
$x=4$	$a=\{0,0,0,1,0,0,0\}$
$y=2$	$b=\{0,1,1,1,1,1,1\}$
$y+l=5$	$c=\{0,0,0,0,1,1,1\}$
$a\oplus b$	$\{0,1,1,0,1,1,1\}$
$a\oplus c$	$\{0,0,0,1,1,1,1\}$
$(a\oplus b)\parallel(a\oplus c)$	$\{0,1,1,0,1,1,1\parallel 0,0,0,1,1,1,1\}$
$b\parallel c$	$\{0,1,1,1,1,1,1\parallel 0,0,0,0,1,1,1\}$

为一个 n 长的 0-1 码 $\{c_1,c_2,\ldots,c_n\}$.

$$\text{规则 I:}\begin{cases} c_i=1, & \text{若} x=x_i,\\ c_i=0, & \text{若} x\neq x_i.\end{cases}$$

Bob 拥有离散整数区间 $[y,y+l]$, 将两个端点 $y,y+l$ 按规则 II 分别编码为 n 长的 0-1 码 $\{c'_1,c'_2,\ldots,c'_n\}$.

$$\text{规则 II:}\begin{cases} c'_i=1,\ldots,c'_n=1, & \text{若} y\geqslant x_i,\\ c'_1=0,\ldots,c'_{i-1}=0, & \text{若} y<x_i,\end{cases}\quad\begin{cases} c'_i=1,\ldots,c'_n=1, & \text{若} y+l\geqslant x_i,\\ c'_1=0,\ldots,c'_{i-1}=0, & \text{若} y+l<x_i.\end{cases}$$

为了清楚起见, 本文给出规则 I 和规则 II 编码的实例 1.

实例1　设全集 $U=\{1,2,3,4,5,6,7\}$, Alice 拥有整数点 $x=4$, Bob 拥有离散整数区间 $[y,y+l]=[2,5]$. Alice 按照规则 I 将 $x=4$ 编码为 7 长的 0-1 码, Bob 按照规则 II 将区间 $[y,y+l]=[2,5]$ 的两个端点 $y=2$, $y+l=5$ 分别编码为 7 长的 0-1 码, 所得的 3 个编码分别如表 2.

(2) 级联异或. 将实例 1 中给出的 0-1 编码先异或再级联, 得到异或级联运算后的结果, 如表 3.

利用 2.1 小节的性质 1: 任何数和 0 异或都不改变这个数, 而任何数和 1 异或都使得该数反转. 因此从表 3 可以看出, 如果 $x>y$, 即 $4>2$, 那么将 $a\oplus b=\{0,1,1,0,1,1,1\}$ 和 $b=\{0,1,1,1,1,1,1\}$ 进行对照, 可以发现 $a\oplus b$ 相比 b, 1 的个数减少了 1 个. 同理, 如果 $x<y+l$, 即 $4<5$, 那么将 $a\oplus c=\{0,0,0,1,1,1,1\}$ 和 $c=\{0,0,0,0,1,1,1\}$ 进行对照, 可以发现 $a\oplus c$ 相比 c, 1 的个数增多了 1 个. 综合这两种情况可以得出, 要判断是否 $x\in[y,y+l]$, 那么只需要将 $(a\oplus b)\parallel(a\oplus c)$ 和 $b\parallel c$ 进行对照, 观察两者 1 的总个数是否相同即可. 如果相同, 那么 $x\in[y,y+l]$; 否则 $x\notin[y,y+l]$. 又根据 2.1 小节的性质 2: 异或后级联等价于级联后异或, 即 $(a\oplus b)\parallel(a\oplus c)=(a\parallel a)\oplus(b\parallel c)$. 因此最终得到: 要判断是否 $x\in[y,y+l]$, 那么只需将 $(a\parallel a)\oplus(b\parallel c)$ 和 $b\parallel c$ 进行对照, 观察两者中 1 的总个数是否相同即可. 将以上方法应用到实例 1, 得到级联异或运算后的结果, 如表 4.

表 4 级联异或

Table 4 Concatenation xor

Original data	Concatenation xor
$x=4$	$a=\{0,0,0,1,0,0,0\}$
$y=2$	$b=\{0,1,1,1,1,1,1\}$
$y+l=5$	$c=\{0,0,0,0,1,1,1\}$
$a \parallel a$	$\{0,0,0,1,0,0,0 \parallel 0,0,0,1,0,0,0\}$
$b \parallel c$	$\{0,1,1,1,1,1,1 \parallel 0,0,0,0,1,1,1\}$
$(a \parallel a) \oplus (b \parallel c)$	$\{0,1,1,0,1,1,1 \parallel 0,0,0,1,1,1,1\}$

表 5 实数化为整数

Table 5 Transferring real into integer

Original data	Corresponding integer
$x=4.27$	$t=4270$
$y_1=3.348$	$t_1=3348$
$y_2=51.3$	$t_2=51300$

由表 4 可以看出, 将 $(a \parallel a) \oplus (b \parallel c)$ 和 $b \parallel c$ 中 1 的个数进行对照, 如果 1 的个数不变, 那么 $x \in [y, y+l]$; 否则 $x \notin [y, y+l]$.

(3) 实数化为整数. Alice 拥有实数点 x, Bob 拥有连续的实数区间 $[y_1, y_2]$, 其中 $x, y_1, y_2 \in U$, 小数点位数精确到 k 位. 由于实数的问题在密码学范畴内很难处理, 因此需要将实数化为整数处理, 即将 x, y_1, y_2 同时扩大 10^k 倍, 这样就去掉了 x, y_1, y_2 的小数点, 变成了整数 t, t_1, t_2. 由于本文采用 Paillier 加密体制要将数据 t, t_1, t_2 加密, 因此本文的数据都应小于 Paillier 的明文范围, 即模数 N. 一般情况下, Paillier 加密体制中模数 N 的大小为二进制 1024 位, 那么对应的十进制最多不超过 2^{1024}, 因此统一规定本文 x, y_1, y_2 的取值范围即使扩大 10^k 倍, 变成整数 t, t_1, t_2 后也应 $< 2^{1024}$. 若超出这范围, 则可将 Paillier 加密体制中模数 N 增大, 或选取其他更大模数的加法同态加密体制.

为了清楚起见, 本文给出实数化整数的实例 2.

实例2 设 Alice 拥有实数点 $x=4.27$, Bob 拥有连续实数区间 $[y_1, y_2]=[3.348,\ 51.3]$, 小数点位数精确到 $k=3$ 位. 因此将 $x,\ y_1,\ y_2$ 都统一乘以 10^3 倍, 变成整数 $t,\ t_1,\ t_2$, 分别如表 5 所示.

从表 5 可以得出, 要判断是否 $x \in [y_1, y_2]$, 即判断是否 $y_1 \leqslant x \leqslant y_2$. 只需判断将 $x,\ y_1,\ y_2$ 的小数点去掉后变成的整数 $t,\ t_1,\ t_2$ 是否满足 $t_1 \leqslant t \leqslant t_2$ 即可.

(4) 函数的单调性. Alice 拥有实数点 x, Bob 拥有连续的实数区间 $[y_1, y_2]$. 由 3.2 小节 (3) 的转化可知, 要判断 $x \in [y_1, y_2]$, 只需判断转化后的整数 $t_1 \leqslant t \leqslant t_2$ 即可. 而要判断 $t_1 \leqslant t \leqslant t_2$, 可利用函数的单调性. 为此, Bob 首先任选两个随机的整数点 $k,\ b$, 构造一条单调递增 (或者递减) 的直线 $f(x)=kx+b$. 然后求出 $t_1,\ t,\ t_2$ 在该直线上的纵坐标 $f(t_1), f(t), f(t_2)$, 如图 1 所示. 根据函数的单调递增性 (或递减性), 要判断 $t_1 \leqslant t \leqslant t_2$, 只需判断 $f(t_1) \leqslant f(t) \leqslant f(t_2)$ 即可.

由以上 4 个转化技巧可以得到, 对于问题 1, 整数点和离散整数区间的保密判定, 利用 0-1 编码和级联异或的技巧就可以解决. 对于问题 2, 实数点和连续实数区间的保密判定, 利用实数化为整数和函数单调性的技巧就可以解决.

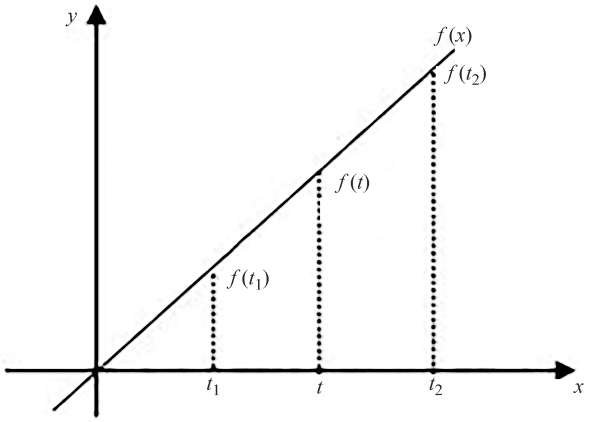

图 1　单调函数
Figure 1　Monotonous function

4　具体协议

以下协议假设所有的参与者都在半诚实模型下, 敌手具有多项式计算能力, 网络之间传输都是公开信道. 基于 3.2 小节的转化技巧, 本文给出了全隐私保密判定一个整数点和一个离散整数区间的协议 1; 全隐私保密判定一个实数点和一个连续实数区间的协议 2.

协议1　整数点和一个离散整数区间的保密判定.

输入: $U=\{x_1,x_2,\ldots,x_n\}$ 为一个全集, $x,\ y,\ y+l\in U,\ \ |U|=n$. Alice 保密输入整数点 x, Bob 保密输入离散的整数区间 $[y,y+l]$.

输出: Alice 和 Bob 都想知道点 x 是否包含在区间 $[y,y+l]$ 中, 即是否 $x\in[y,y+l]$.

(1) Bob 首先选取 2.3 小节 Goldwasser-Micali 的同态加密体制, 得到公钥为 $(N,\ y)$, 私钥为 $(p,\ q)$. 并利用 3.2 小节 (1) 中的 0-1 编码规则 II 将离散整数区间 $[y,y+l]$ 的两个端点 $y,y+l$ 分别编码为 n 长的 0-1 码:

$$b=\{0,0,\ldots,1,\ldots,1\}=\{m_1,m_2,\ldots,m_y,\ldots,m_n\},$$
$$c=\{0,0,\ldots,1,\ldots,1\}=\{m_1,m_2,\ldots,m_{y+l},\ldots,m_n\}.$$

将 b 和 c 级联得到 $2n$ 长编码: $b\parallel c=\{m_1,m_2,\ldots,m_{2n}\}$. 然后将 $b\parallel c$ 中的每一位加密得到 $2n$ 长密文: $E(b\parallel c)=\{E(m_1),E(m_2),\ldots,E(m_{2n})\}$, 将这 $2n$ 个密文发给 Alice.

(2) Alice 利用 3.2 小节 (1) 中的 0-1 编码规则 I 将整数点 x 表示成 n 长的 0-1 码:

$$a=\{0,0,\ldots,1,\ldots,0\}=\{m'_1,m'_2,\ldots,m'_x,\ldots,m'_n\}.$$

将 a 和 a 进行级联得到 $2n$ 长编码: $a\parallel a=\{m'_1,m'_2,\ldots,m'_x,\ldots,m'_{2n}\}$. 将 $a\parallel a$ 中的每一位加密得到 $2n$ 长密文: $E(a\parallel a)=\{E(m'_1),E(m'_2),\ldots,E(m'_{2n})\}$. 然后将收到的 $2n$ 个密文 $\{E(m_1),E(m_2),\ldots,E(m_{2n})\}$ 和 $\{E(m'_1),E(m'_2),\ldots,E(m'_{2n})\}$ 两两逐位相乘, 进行同态操作, 得到

$$E(b\parallel c)E(a\parallel a)$$
$$=\{E(m_1)E(m'_1),E(m_2)E(m'_2),\ldots,E(m_{2n})E(m'_{2n})\}$$

$$= \{E(m_1 \oplus m_1'), E(m_2 \oplus m_2'), \ldots, E(m_{2n} \oplus m_{2n}')\}$$
$$= E((b \parallel c) \oplus (a \parallel a)).$$

Alice 选取随机置换 T 将以上 $2n$ 个密文进行随机置换, 得到随机置换后的 $2n$ 个密文:

$$(E((b \parallel c) \oplus (a \parallel a)))^T = \{E(m_1 \oplus m_1'), E(m_2 \oplus m_2'), \ldots, E(m_{2n} \oplus m_{2n}')\}^T,$$

发回 Bob.

(3) Bob 收到置换后的 $2n$ 个密文后, 逐次解密, 得到

$$((b \parallel c) \oplus (a \parallel a))^T = \{(m_1 \oplus m_1'), (m_2 \oplus m_2'), \ldots, (m_{2n} \oplus m_{2n}')\}^T.$$

由于 $(b \parallel c) \oplus (a \parallel a)$ 置换后得到 $((b \parallel c) \oplus (a \parallel a))^T$, 两者序列中 1 的总个数不变, 因此根据 3.2 小节 (2) 中的级联异或, 将 $((b \parallel c) \oplus (a \parallel a))^T$ 和 $(b \parallel c)$ 中 1 的总个数做对比, 如果 1 的个数不变, 那么 $x \in [y, y+l]$; 否则 $x \notin [y, y+l]$.

(4) Bob 将结果告诉 Alice.

分析. 在协议 1 中, 由于 Bob 发送给 Alice 的是自己区间 $[y, y+l]$ 两个端点编码后的密文 $E(b \parallel c)$, 任何人不能解密, 因此不能从中得到 $y, y+l$ 的隐私. 另一方面, Alice 将自己的整数点 x 编码并加密得到密文 $E(a \parallel a)$, 两者相乘后得到 $E(b \parallel c)E(a \parallel a) = E((b \parallel c) \oplus (a \parallel a))$, 若直接将此密文发送给 Bob, 由于 Bob 可以解密得到 $(b \parallel c) \oplus (a \parallel a)$, 在这个基础上, 再取一次异或 $(b \parallel c) \oplus (a \parallel a) \oplus (b \parallel c)$, 就可以得到 $a \parallel a$, 从而得到 Alice 的隐私 x. 因此为了防止这种隐私泄露, Alice 将 $E((b \parallel c)E(a \parallel a))$ 随机置换得到 $(E(b \parallel c)E(a \parallel a))^T$, 这样使得 Bob 解密后只能得到 $((b \parallel c) \oplus (a \parallel a))^T$, 由于 Bob 不知道置换函数 T, 因此不能从中得到 $a \parallel a$, 从而保护了 Alice 的隐私.

协议2 实数点和一个连续实数区间的保密判定.

输入: Alice 保密输入实数点 x, Bob 保密输入连续的实数区间 $[y_1, y_2]$, 小数点位数精确到 k 位.

输出: Alice 和 Bob 都想知道点 x 是否包含在区间 $[y_1, y_2]$ 中, 即是否 $x \in [y_1, y_2]$.

(1) Alice 首先选取 2.2 小节 Paillier 的同态加密体制, 得到公钥为 $(N,\ g)$, 私钥为 λ, 然后利用 3.2 小节 (3) 中实数化整数的技术, 将自己的隐私点 x 变成整数 t, 并将 t 加密得到密文 $E(t)$ 发送给 Bob.

(2) 同理, Bob 利用 3.2 小节 (3) 中实数化整数的技术也将自己区间的两个端点 y_1, y_2 变成整数 t_1, t_2, 并任选两个随机的整数点 $k,\ b$, 构造一条单调递增 (或者递减) 的直线 $f(x) = kx + b$. 然后求出 $f(x) = kx + b$ 在该直线上的纵坐标 $f(t_1), f(t_2)$. 最后, Bob 做同态运算, 得到密文: $c = E(t)^k E(b) = E(kt + b)$. Bob 将纵坐标 $f(t_1), f(t_2)$ 和密文 c 发送给 Alice.

(3) Alice 收到 $f(t_1), f(t_2), c$ 后, 将 c 解密得到 $f(t)$, 然后比较 $f(t)$ 和 $f(t_1), f(t_2)$ 的大小. 根据 3.2 小节 (4) 中函数单调性的结论, 若 $f(t_1) \leqslant f(t) \leqslant f(t_2)$, 得到 $t_1 \leqslant t \leqslant t_2$, 即 $x \in [y_1, y_2]$; 否则 $x \notin [y_1, y_2]$.

(4) Alice 将结果告诉 Bob.

分析. 在协议 2 中, Alice 发送给 Bob 的是自己隐私点 x 转化为整数 t 后的密文 $E(t)$, 由于任何人不能解密得到 $E(t)$, 因此保护了 Alice 的隐私点 x. 另一方面, Alice 得到 Bob 发送的数据 $f(t_1), f(t_2), c$ 后, 虽然似乎可以求解一个方程 $f(x) = kx + b$, 但这个方程中却有 2 个未知数 $k,\ b$, 而 $f(t_1), f(t_2)$ 对解这个方程不起任何作用, 因此从这个方程解不出 $k,\ b$, 从而保护了 Bob 的隐私区间 $[y_1, y_2]$.

备注1 协议 2 中, Bob 将纵坐标 $f(t_1), f(t_2)$ 发送给 Alice 时, 不需要告诉 Alice 直线的单调性, 只需要将计算好的 $f(t_1), f(t_2)$ 发送给 Alice 即可, Alice 只要判断计算出 $f(t)$ 是否在 $f(t_1), f(t_2)$ 这个范围内就能得到结论. 否则, 若知道单调性, 当 $f(t)$ 不在 $f(t_1), f(t_2)$ 这个范围内时, Alice 会推出自己的点 $x < y_1$ 或 $x > y_2$, 而这是协议不许可的. 因为我们的输出结果是只让双方知道 $x \in [y_1, y_2]$ 还是 $x \notin [y_1, y_2]$, 其他应该一无所获.

备注2 协议 2 虽然给出的是实数点和连续实数区间的保密判定协议, 但仍然可以应用到整数点和离散的整数区间, 即协议 2 可以作为保密判断点和区间关系的通用协议.

备注3 在协议 1 中需要一个全集, 但这不是协议本身的缺陷, 相当于给双方给出了一个定义域. 同理, 在协议 2 中需要知道小数点精确位数, 相当于给双方给出了一个实数位数可以处理的范围, 这些额外的信息并不影响协议的正确性和隐私性. 关于这一点, Du 等在文献 [17] "A practical approach to solve secure multi-party computation problems" 一文中专门有论述: 在设计协议时, 如果在降低完美安全性 (即零信息泄露) 的程度上, 允许泄露的信息并不影响方案的有效性, 那么这就是可接受性安全. 而可接受性安全要根据具体问题, 具体设定.

5 安全性分析

本节应用 2.4 小节的安全性模拟范例给出本文 2 个协议的安全性证明.

定理1 协议 1 保密地判断了整数点和离散整数区间的关系.

证明 通过构造满足 2.4 小节式 (1) 和 (2) 的模拟器 S_1, S_2 来证明本定理. 在本协议中

$$f_1(X, Y) = f_2(X, Y) = (x \in [y, y + l]),$$

或者

$$f_1(X, Y) = f_2(X, Y) = (x \notin [y, y + l]).$$

假设 $f_1(X, Y) = f_2(X, Y) = (x \in [y, y + l])$, 构造模拟器 S_1. S_1 接受 $(X, f_1(X, Y))$ 作为输入, 按如下方式工作.

第 1 步: S_1 接受输入 $(X, f_1(X, Y)) = (x, x \in [y, y + l])$ 后, 首先随机选取一个离散的整数区间 $\overline{Y} = [\overline{y}, \overline{y} + \overline{l}]$, 使得 $f_1(X, Y) = f_1(X, \overline{Y})$. 然后用 $(X, \overline{Y}) = (X, [\overline{y}, \overline{y} + \overline{l}])$ 来模拟. 按照协议 1, S_1 将区间 $[\overline{y}, \overline{y} + \overline{l}]$ 的两个端点分别编码得到 $\overline{b}$, $\overline{c}$, 并将 $\overline{b}$, $\overline{c}$ 级联得到 $2n$ 长编码: $\overline{b} \parallel \overline{c} = \{\overline{m_1}, \overline{m_2}, \ldots, \overline{m_{2n}}\}$, 然后将 $\overline{b} \parallel \overline{c}$ 中的每一位加密得到 $2n$ 长密文:

$$E(\overline{b} \parallel \overline{c}) = \{E(\overline{m_1}), E(\overline{m_2}), \ldots, E(\overline{m_{2n}})\},$$

将以上 $2n$ 个密文记做 A'.

第 2 步: S_1 将点 x 编码得到 a, 并将 a 和 a 级联得到 $2n$ 长编码: $a \parallel a = \{m'_1, m'_2, \ldots, m'_{2n}\}$. 然后将 $a \parallel a$ 中的每一位加密得到 $2n$ 长密文: $E(a \parallel a) = \{E(m'_1), E(m'_2), \ldots, E(m'_{2n})\}$, 将这 $2n$ 个密文记做 B. 利用同态性, S_1 将 A' 和 B 两两逐次相乘, 进行同态操作, 得到

$$\begin{aligned}
&E(\overline{b} \parallel \overline{c})E(a \parallel a) \\
&= \{E(\overline{m_1})E(m'_1), E(\overline{m_2})E(m'_2), \ldots, E(\overline{m_{2n}})E(m'_{2n})\} \\
&= \{E(\overline{m_1} \oplus m'_1), E(\overline{m_2} \oplus m'_2), \ldots, E(\overline{m_{2n}} \oplus m'_{2n})\}
\end{aligned}$$

$$= E((\overline{b} \parallel \overline{c}) \oplus (a \parallel a)).$$

S_1 选取随机置换 T 将以上 $2n$ 个密文进行随机置换, 得到置换后的 $2n$ 个新密文:

$$(E((\overline{b} \parallel \overline{c}) \oplus (a \parallel a)))^T = \{E(\overline{m_1} \oplus m_1'), E(\overline{m_2} \oplus m_2'), \ldots, E(\overline{m_{2n}} \oplus m_{2n}')\}^T,$$

将以上 $2n$ 个新密文记作 C'.

第 3 步: 将这 $2n$ 个新密文 C' 逐次解密得到

$$((\overline{b} \parallel \overline{c}) \oplus (a \parallel a))^T = \{(\overline{m_1} \oplus m_1'), (\overline{m_2} \oplus m_2'), \ldots, (\overline{m_{2n}} \oplus m_{2n}')\}^T.$$

将 $((\overline{b} \parallel \overline{c}) \oplus (a \parallel a))^T$ 和 $(\overline{b} \parallel \overline{c})$ 中 1 的总个数做对比, 如果 1 的个数不变, 那么 $x \in [y, y+l]$; 否则 $x \notin [y, y+l]$. 将最后结果记为 R'.

在本协议中,

$$\text{view}_1(X, Y) = \{X, A, B, C, R\}, \quad S_1(X, \overline{Y}) = \{X, A', B, C', R'\}.$$

由于 $R = (x \in [y, y+l])$, $f_1(X, Y) = f_1(X, \overline{Y})$, 因此 $R' = (x \in [\overline{y}, \overline{y} + \overline{l}])$, $R = R'$. 由于

$$A = E(b \parallel c) = \{E(m_1), E(m_2), \ldots, E(m_{2n})\},$$
$$A' = E(\overline{b} \parallel \overline{c}) = \{E(\overline{m_1}), E(\overline{m_2}), \ldots, E(\overline{m_{2n}})\},$$

即 A 和 A' 都是同一概率性公钥算法加密结果, 因此 A 和 A' 计算不可区分, 即 $A \stackrel{c}{=} A'$. 由于

$$\begin{aligned} C &= (E((b \parallel c) \oplus (a \parallel a)))^T \\ &= \{E(m_1 \oplus m_1'), E(m_2 \oplus m_2'), \ldots, E(m_{2n} \oplus m_{2n}')\}^T \\ &= (AB)^T, \\ C' &= (E((\overline{b} \parallel \overline{c}) \oplus (a \parallel a)))^T \\ &= \{E(\overline{m_1} \oplus m_1'), E(\overline{m_2} \oplus m_2'), \ldots, E(\overline{m_{2n}} \oplus m_{2n}')\}^T \\ &= (A'B)^T. \end{aligned}$$

由于 $A \stackrel{c}{=} A'$, 而随机置换为同一置换 T, 因此 $(AB)^T \stackrel{c}{=} (A'B)^T$, 即 $C \stackrel{c}{=} C'$, 又因为

$$\text{output}_2(X, Y) = f_2(X, Y) = (x \in [y, y+l]),$$

因此有

$$\{S_1(x, f_1(x, y)), f_2(x, y)\} \stackrel{c}{=} \{\text{view}_1(x, y), \text{output}_2(x, y)\}.$$

同理, 用类似的方法可构造模拟器 S_2 使得

$$\{f_1(x, y), S_2(y, f_2(x, y))\} \stackrel{c}{=} \{\text{output}_1(x, y), \text{view}_2(x, y)\}.$$

定理2 协议 2 保密地判断了实数点和连续实数区间的关系.

证明 通过构造满足 2.4 小节式 (1) 和 (2) 的模拟器 S_1, S_2 来证明本定理. 在本协议中,

$$f_1(X, Y) = f_2(X, Y) = (x \in [y_1, y_2]),$$

或者

$$f_1(X,Y)=f_2(X,Y)=(x\notin[y_1,y_2]).$$

假设 $f_1(X,Y)=f_2(X,Y)=(x\in[y_1,y_2])$, 构造模拟器 S_1. S_1 接受 $(X,f_1(X,Y))$ 作为输入, 按如下方式工作.

第 1 步: S_1 接受输入 $(X,f_1(X,Y))=(x,x\in[y_1,y_2])$ 后, 首先随机选取一个离散的整数区间 $\overline{Y}=[\overline{y_1},\overline{y_2}]$, 使得 $f_1(X,Y)=f_1(X,\overline{Y})$. 然后用 $(X,\overline{Y})=(x,[\overline{y_1},\overline{y_2}])$ 来模拟. 按照协议 2, S_1 将点 x 转化为整数 t, 并将 t 加密得到 $E(t)$, 记做 A.

第 2 步: S_1 将区间 $[\overline{y_1},\overline{y_2}]$ 的两个端点 $\overline{y_1}$, $\overline{y_2}$ 变成等长的整数 $\overline{t_1}$, $\overline{t_2}$, 并任选两个随机的整数点 $\overline{k}$, $\overline{b}$, 构造一条单调递增 (或者递减) 的直线 $g(x)=\overline{k}x+\overline{b}$. 然后求出 $\overline{t_1}$, $\overline{t_2}$ 在该直线上的纵坐标 $g(\overline{t_1})$, $g(\overline{t_2})$, 并做同态运算, 得到密文: $\overline{c}=E(t)^{\overline{k}}E(\overline{b})=E(\overline{k}t+\overline{b})$.

第 3 步: S_1 将 $\overline{c}$ 解密得到 $\overline{k}t+\overline{b}=g(t)$. 然后比较 $g(t),g(\overline{t_1}),g(\overline{t_2})$ 的大小, 若 $g(\overline{t_1})\leqslant g(t)\leqslant g(\overline{t_2})$, 那么 $x\in[y_1,y_2]$; 否则 $x\notin[y_1,y_2]$. 将最后结果记为 R'.

在本协议中,

$$\mathrm{view}_1(X,Y)=\{X,f(t_1),f(t_2),C,R\},\quad S_1(X,\overline{Y})=\{X,g(\overline{t_1}),g(\overline{t_2}),\overline{C},R'\}.$$

由于 $R=(x\in[y_1,y_2])$, $f_1(X,Y)=f_1(X,\overline{Y})$, 因此 $R'=(x\in[\overline{y_1},\overline{y_2}])$, $R=R'$. 由于 $c=E(kt+b)$, $\overline{c}=E(\overline{k}t+\overline{b})$, 而 k, b, $\overline{k}$, $\overline{b}$ 为 4 个随机数, E 为概率性加密, 因此 $c\overset{c}{=}\overline{c}$. 由于

$$f(t_1)=kt_1+b,\quad f(t_2)=kt_2+b,$$
$$g(\overline{t_1})=\overline{k}\overline{t_1}+\overline{b},\quad g(\overline{t_2})=\overline{k}\overline{t_2}+\overline{b}.$$

同理, k, b, $\overline{k}$, $\overline{b}$ 为 4 个随机数, $\overline{t_1}$, $\overline{t_2}$ 也为 2 个随机数, t_1, t_2 为未知的 2 个数, 因此: $f(t_1)\overset{c}{=}g(\overline{t_1})$; $f(t_2)\overset{c}{=}g(\overline{t_2})$. 又因为

$$\mathrm{output}_2(X,Y)=f_2(X,Y)=(x\in[y_1,y_2]),$$

因此有

$$\{S_1(x,f_1(x,y)),f_2(x,y)\}\overset{c}{=}\{\mathrm{view}_1(x,y),\mathrm{output}_2(x,y)\}.$$

同理, 用类似的方法可构造模拟器 S_2 使得

$$\{f_1(x,y),S_2(y,f_2(x,y))\}\overset{c}{=}\{\mathrm{output}_1(x,y),\mathrm{view}_2(x,y)\}.$$

6 效率分析与比较

6.1 理论分析与比较

本节将本文的 2 个协议和引言的相关文献 [13] 的 2 个协议分别在计算开销、通信开销以及性能方面做出分析和比较.

计算开销. 由于文献 [13] 和本文的 2 个协议都利用了同态公钥加密, 因此以开销较大的模幂运算次数作为衡量计算开销的指标, 其他都忽略不计. 为了便于比较, 统一将文献 [13] 和本文协议 2 调用的 Paillier 公钥加密中的模幂运算记为 M_{N^2}; 将本文协议 1 调用的 Goldwasser-Micali 公钥加密中的

表 6 本文协议与现有文献 [13] 的效率比较

Table 6 Efficiency comparison between our protocols and the protocols in [13]

Protocol	Computation cost	Communication overhead
Protocol 1 in [13]	$12M_{N^2}$	5
Protocol 2 in [13]	$8M_{N^2}$	6
Protocol 1 in ours	$2nM_N$	3
Protocol 2 in ours	$4M_{N^2}$	3

表 7 本文协议与现有文献 [13] 的性能比较

Table 7 Performance comparison between our protocols and the protocols in [13]

Protocol	(I)	(II)	(III)	(IV)	(V)
Protocol 1 in [13]	✓	✓	✓	✓	×
Protocol 2 in [13]	×	✓	✓	✓	×
Protocol 1 in ours	✓	✓	✓	✓	×
Protocol 2 in ours	✓	✓	✓	✓	✓

模幂运算记为 M_N, $N^2 >> N$. 文献 [13] 中协议 1 两方共需要 12 个模幂运算, 即 $12M_{N^2}$; 协议 2 两方共需要 8 个模幂运算, 即 $8M_{N^2}$. 本文的协议 1 两方共需要 $2n$ 个模幂运算, 即 $2nM_N$; 协议 2 两方共需要 4 个模幂运算, 即 $4M_{N^2}$, 其中 n 为本文协议 1 中全集的势.

通信开销. 衡量通信复杂度的指标用协议交换信息的比特数, 或者用通信轮数 (round), 在安全多方计算中通常用轮数作为衡量通信开销的指标. 文献 [13] 的协议 1 需要交互 5 rounds; 协议 2 需要交互 6 rounds. 本文的协议 1 需要交互 3 rounds; 协议 2 需要交互 3 rounds.

性能. 以下 5 种功能作为衡量性能的指标. 用 "✓" 表示取得该性能, 用 "×" 表示未取得该性能.

(I) 无基础子协议: 协议过程不需要调用其他安全多方计算基础子协议;

(II) 一次性: 不需要调用循环语句执行协议;

(III) 完美安全性: 最后的输出结果除了得到判断结果外, 其他信息都不能得到;

(IV) 全隐私性: 协议同时保护了两方的隐私;

(V) 通用性: 协议适用于任何数和区间范围.

综合以上分析, 得到本文的协议 1, 协议 2 和文献 [13] 的协议 1, 协议 2 效率比较, 如表 6; 性能比较如表 7.

从表 6 可以看出, 本文设计的协议 2 计算效率远高于文献 [13] 的 2 个协议. 此外, 本文 2 个协议的通信成本都低于文献 [13] 的通信成本. 虽然文献 [13] 中 2 个协议的计算效率似乎都高于本文的协议 1, 但由于 $N^2 >> N$, 当全集的势 n 比较小, 即编码的长度比较短时, 由 6.2 小节的实验可以得到: 当全集的势 $n < 15$ 时, 本文协议 1 的效率仍然高于文献 [13] 中协议 1 的效率 (图 2). 从表 7 可以看出, 本文协议 2 所取得的性能是最全的, 同时取得了 5 种性能; 协议 1 少了一种性能, 不具有通用性, 即只能处理离散的整数. 而文献 [13] 的 2 个协议都不具有通用性, 即只能处理有理数. 此外, 文献 [13] 的协议 2 还少了一种性能, 需要调用一次 Li 等 [18] 设计的百万富翁基础子协议.

6.2 实验实现

为了更加直观地呈现表 6 中本文协议与文献 [13] 协议的效率比较, 我们在 java 语言环境下, 将表 6

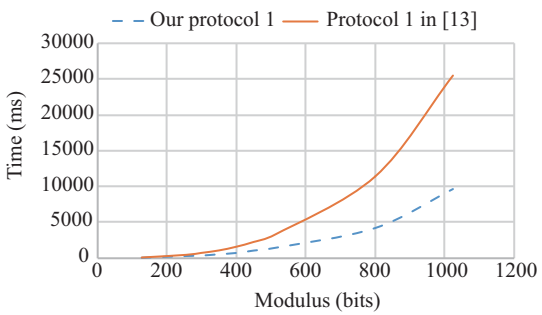

图 2 (网络版彩图) 本文协议 1 和文献 [13] 协议 1 的计算开销比较

Figure 2 (Color online) Comparison of computation cost between our protocol 1 and protocol 1 in [13]

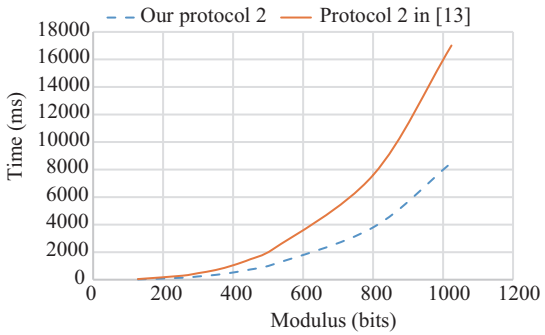

图 3 (网络版彩图) 本文协议 2 和文献 [13] 协议 2 的计算开销比较

Figure 3 (Color online) Comparison of computation cost between our protocol 2 and protocol 2 in [13]

表 8 不同模数下一个模幂运算的平均耗时

Table 8 Average time cost per modular exponentiation

p, q (bit)	M_N (ms)	M_{N^2} (ms)
128	1.847	5.857
256	14.000	36.857
300	16.857	59.571
350	26.142	88.000
400	35.142	131.142
450	51.857	186.857
512	71.000	273.142
800	209.429	949.714
1024	482.143	2126.429

中 4 个协议编程实现, 给出了本文协议和文献 [13] 协议的计算开销所需要的耗时 (ms). 实验采用的计算机配置如下: 操作系统为 Windows 7 旗舰版, CPU 为 AMD A6-3240M 1.5 GHz, 内存为 4.00 GB. 实验中 Pailler 和 Goldwasser-Micali 加密算法中的大素数 p 和 q 的位数相同, 分别取 p 和 q 为 128, 256, 300, 350, 400, 450, 512, 800, 1024 bit, 在这 9 组 p 和 q 下, 分别计算一个模幂运算 M_N, M_{N^2} 的平均耗时, 得到表 8. 其中表 8 的第 1 列表示 p 和 q 的位数 (bit), 第 2 列和第 3 列分别表示在不同模数下一个模幂运算 M_N, M_{N^2} 的平均耗时 (ms).

根据表 8 得到的每一个模幂运算 M_N 和 M_{N^2} 的平均耗时, 再由表 6, 可计算出 4 个协议所需要的模幂运算总时间. 这样可得到不同模数下本文协议 1 和文献 [13] 的协议 1; 本文协议 2 和文献 [13] 协议 2 的计算开销比较, 分别如图 2 和 3 所示. 横轴为不同的模数 (bits), 纵轴是不同的模数下协议所需要的总时间 (ms), 其中图 2 中我们处理的全集的势 n 比较小 ($n < 15$).

由图 3 的实验结果显示, 本文协议 2 的效率高于文献 [13] 的协议 2. 由图 2 的实验结果显示, 当全集的势 n ($n < 15$) 比较小, 即编码的长度较短时, 本文协议 1 的效率仍然高于文献 [13] 的协议 1, 但当 $n > 15$ 时, 因为本文协议 1 的计算开销和 n 有关, 因此从此刻开始, 我们的协议 1 效率低于 [13] 的协议 1.

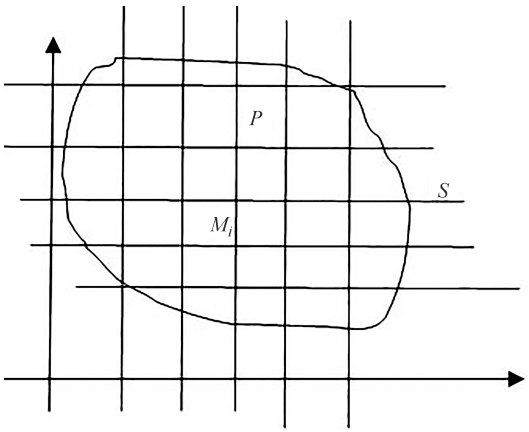

图 4 点 P 和不规则区域 S 的位置

Figure 4 Relationship between point P and irregular region S

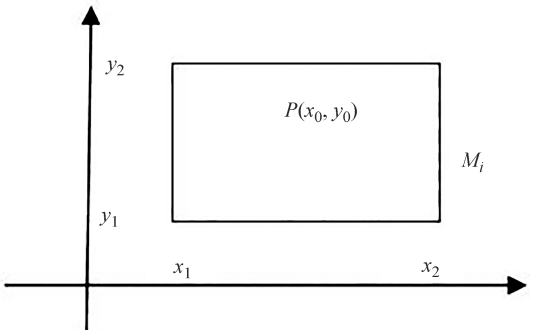

图 5 点 P 和矩形 M_i 的位置关系

Figure 5 Relationship between point P and matrix M_i

综合以上理论分析和实验分析, 可以得到本文设计的 2 个协议在保持较优通信效率的同时, 都取得了全隐私性. 尤其本文的协议 2, 第一次给出了实数点和连续实数区间的判断方法, 无论在计算效率、通信效率、性能方面相比以往的方案都达到了最优. 而本文的协议 1 在处理编码长度较短时, 效率也较高. 因此本文的 2 个协议较好地解决了引言里文献 [7,8] 中区间查询的全隐私问题和数的范围问题, 适合作为一种子模块嵌入到密文搜索体制中, 从而推广了公钥密码体制的体制和应用.

7 应用: 保密位置判断问题

7.1 问题描述

保密位置判断是保密定位查找中一个很重要的问题, 在军事, 商业中有着重要的应用. 例如, 要判断甲方的一个目标是否落在乙方的一个区域内, 以便做出下一步的决策. 而由于甲乙两方的信息都比较敏感或者为敌我关系, 双方都不可能向对方透露自己的信息, 那么如何保密判断两者的位置关系呢? 这样的保密判断问题往往可抽象成点和矩形的保密位置判断问题.

例如图 4 中, P 为甲方的一个目标, S 为乙方的一个不规则区域, 要保密判断是否 $P \in S$, 可以将 S 用平行于坐标轴的直线划分为若干矩形 M_i, $i = 1, 2, \ldots, n$, 对每个矩形 M_i, 只需判断是否存在某个 M_i, $P \in M_i$ 即可. 对于紧邻边界的区域, 可以将矩形不断细分, 这样最后都能划归为点和矩形的位置关系. (注意划分的时候, 不能让这些直线的各个交点超过 S 的边界)

7.2 问题的转化和解决

从图 4 及以上分析中可知, 要判断点 P 是否落在一个不规则区域 S, 只需判断 P 和分割后的某个矩形 M_i, 是否 $P \in M_i$ 即可. 为了清楚起见, 本文给出图 5. 图 5 中 M_i 的上下边界为 $[y_1, y_2]$, 左右边界为 $[x_1, x_2]$, P 的坐标为 $[x_0, y_0]$. 要判断是否 $P \in M_i$, 只需判断 $\begin{cases} x_i \leqslant x_0 \leqslant x_2 \\ y_i \leqslant y_0 \leqslant y_2 \end{cases}$ 是否同时满足即可. 若同时满足, 则 $P \in M_i$; 否则 $P \notin M_i$. 而要判断 $\begin{cases} x_i \leqslant x_0 \leqslant x_2 \\ y_i \leqslant y_0 \leqslant y_2 \end{cases}$ 的问题就变为了点和区间的保密判定问题.

由以上转化可以看出, 我们将保密位置判断问题最终转化为点和区间的保密判断问题, 这样就可连续调用两次本文协议 2 解决.

8 总结和开放问题

目前带有区间查询的密文搜索体制中, 大多其中一方的隐私并没有得到保护, 会造成安全隐患. 此外, 所查询的点和区间都只是整数范围. 虽然有针对该问题的已存方案, 但数的范围还不能推广到实数. 针对这些问题, 本文从安全多方计算的角度对点和区间的判定问题进行了研究. 本文利用 0-1 编码和级联异或的思想解决了整数点和离散的整数区间全隐私保密判定问题; 利用实数化为整数和函数单调性的思想解决了实数点和连续的实数区间全隐私保密判定问题. 最后的分析显示, 本文设计的 2 个协议, 确实取得了全隐私性, 并且第 2 个协议将数域推广到实数范围, 在保持较高效率的同时取得了通用性.

以本文设计的 2 个协议作为子模块, 将其嵌入到密文搜索体制中, 可设计出带有全隐私区间查询和扩大数域查询范围的新型密文搜索方案.

在密文搜索体制中, 为了便于搜索, 一般都有搜索陷门 (trapdoor) 或搜索令牌 (token). 在搜索时, 将产生的搜索陷门 (trapdoor) 或搜索令牌 (token) 和产生的密文 (ciphertext) 进行匹配, 如果匹配成功, 则说明该密文为搜索的目标密文. 这种场景大致分为两类, 一种是依靠参与方本身完成搜索过程; 一种是将密文 (ciphertext) 和搜索陷门 (trapdoor) 或搜索令牌 (token) 交给第三方, 让第三方服务器进行匹配运算. 如果是第 1 种场景, 那么利用本文设计的协议 1 或协议 2 就可以完成, 将一方数据加密后充当密文 (ciphertext), 另一方同态操作后的密文充当搜索陷门 (trapdoor), 再让一方进行匹配. 此过程两方的隐私都得到了保护, 因此可以称为全隐私的密文搜索方案, 但数据的通信过程比传统的密文搜索方案至少多了一轮. 反之, 如果是第 2 种场景, 由于第三方服务器不可信, 需要对参与匹配运算的第三方服务器保护隐私, 这其实是一个可公开匹配过程 (public match). 而本文的匹配, 即验证过程 (match) 是依靠参与方交互完成的, 并不能公开匹配. 因此若将本文的协议改造为第 2 种场景下的密文搜索方案, 需要在本文协议的基础上加入公开匹配的一些技术手段. 而如何完成这一点正是我们接下来进一步的工作.

参考文献

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

2 Freudiger J, Rane S, Brito A E, et al. Privacy preserving data quality assessment for high-fidelity data sharing. In: Proceedings of the ACM Workshop on Information Sharing and Collaborative Security. New York, 2014. 21–29

3 Li X Y, Jung T. Search me if you can: privacy-preserving location query service. In: Proceedings of IEEE INFOCOM, Turin, 2013. 2760–2768

4 Yang J, Zhao J S, Zhang J P. A privacy preservation method for high dimension data mining. Acta Electr Sin, 2013, 41: 2187–2192 [杨静, 赵家石, 张健沛. 一种面向高维数据挖掘的隐私保护方法. 电子学报, 2013, 41: 2187–2192]

5 Samanthula B K, Elmehdwi Y, Howser G, et al. A secure data sharing and query processing framework via federation of cloud computing. Inf Syst, 2015, 48: 196–212

6 Kerschbaum F. Privacy-preserving computation. In: Annual Privacy Forum. Berlin: Springer, 2014. 41–54

7 Boneh D, Waters B. Conjunctive, subset, and range queries on encrypted data. In: Proceedings of Theory of Cryptography Conference. Berlin: Springer, 2007. 535–554

8 Wen M, Lu R, Zhang K, et al. A privacy-preserving range query scheme over encrypted metering data for smart grid. IEEE Trans Emerg Top Comput, 2013, 1: 178–191

9 Cramer R, Damgard I, Schoenmakers B. Proofs of partial knowledge and simplified design of witness hiding protocols. In: Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, 1994. 174–187
10 Boudot F. Efficient proofs that a committed number lies in an interval. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, Bruges, 2000. 431–444
11 Camenisch J, Chaabouni R, Shelat A. Efficient protocols for set membership and range proofs. In: Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, 2008. 234–252
12 Chaabouni R, Lipmaa H, Zhang B. A non-interactive range proof with constant communication. In: Proceedings of International Conference on Financial Cryptography and Data Security, Kralendijk, 2012. 179–199
13 Guo Y M, Zhou S F, Dou J W, et al. Efficient privacy-preserving interval computation and its applications. Chinese J Comput, 2017, 40: 1664–1679 [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: 1664–1679]
14 Paillier P. Public-key cryptosystems based on composite degree residue classes. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, Prague, 1999. 223–238
15 Goldwasser S, Micali S. Probabilistic encryption. J Comput Syst Sci, 1984, 28: 270–299
16 Goldreich O. Foundations of Cryptography: Basic Applications. London: Cambridge University Press, 2004. 599–729
17 Du W, Zhan Z. A practical approach to solve secure multi-party computation problems. In: Proceedings of the 2002 Workshop on New Security Paradigms. New York: ACM, 2002. 127–135
18 Li S D, Wang D S, Dai Y Q, et al. Symmetric cryptographic solutionto Yao's millionaires' problem and an evaluation of secure multiparty computations. Inf Sci, 2008, 178: 244–255

Fully privacy-preserving determination of point-range relationship

Zhenhua CHEN[1,2,3*], Shundong LI[4], Lichao CHEN[1], Qiong HUANG[5] & Weiguo ZHANG[1]

1. *School of Computer Science and Technology, Xi'an University of Science and Technology, Xi'an* 710054*, China*;
2. *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China*;
3. *Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin* 541004*, China*;
4. *School of Computer Science, Shaanxi Normal University, Xi'an* 710062*, China*;
5. *College of Mathematics and Informatics, South China Agricultural University, Guangzhou* 510642*, China*
* Corresponding author. E-mail: chenzhenhua@snnu.edu.cn

Abstract The privacy-preserving determination of point-range relationship is widely applied to range queries. However, most existing solutions only protect one party's privacy but not the other party's; moreover, they only cover integers or rational numbers. Focusing on these problems, we design two protocols with the notion of secure multiparty computation. We first present the fully privacy-preserving protocol 1, which can determine whether an integer is in a discrete integer interval using the 0-1 coding in combination with the Goldwasser-Micali homomorphic encryption. Subsequently, we present the fully privacy-preserving protocol 2, which can determine whether a real number is in a continuous real number interval using the monotonic function in combination with Paillier's homomorphic encryption. Finally, we present a practical example based on our protocol. Theoretical and experiential analyses show that both of our protocols achieve a low communication cost, while preserving the full privacy of two parties. In addition, protocol 2 in this paper first gives a solution to privately determine whether a real number is in a continuous real number interval, while showing higher efficiency and better performance.

Keywords point-range, full privacy, secure multiparty computation, real number, homomorphic encryption

Zhenhua CHEN was born in 1976. She received her Ph.D. degree in computer software and science from Shaanxi Normal University, Xi'an, in 2014. Currently, she is an associate professor at Xi'an University of Science and Technology. Her research interests include secure multiparty computation and public-key encryption, etc.

Lichao CHEN was born in 1989. He received his Bachelor's degree in applied mathematics from Yan'an University, Yan'an, in 2015. Currently, he is studying for his Master's degree at Xi'an University of Science and Technology. His research interests include information security and secure multiparty computation, etc.

Shundong LI was born in 1963. He received his Ph.D. degree in computer software and science from Xi'an Jiaotong University, Xi'an, in 2003. Currently, he is a professor at Shaanxi Normal University professor. His research interests include information hiding and secure multiparty computation, etc.

Qiong HUANG was born in 1981. He received his Ph.D. degree in information security from City University of Hong Kong, Hong Kong, in 2010. Currently, he is a professor at South China Agricultural University and a member of the China Computer Federation and Chinese Association for Cryptologic Research. His main research interests include cryptography and information security, etc.