安全向量优势协议及其应用

李顺东,左祥建,杨晓莉,巩林明
(陕西师范大学计算机科学学院,陕西西安,710119)

摘 要: 百万富翁问题是安全多方计算研究的热点问题之一,也是其他安全多方计算协议的基本构成模块.安全向量优势统计问题是百万富翁问题的推广,用于两方在不泄漏自己保密向量信息的前提下统计出满足大于关系的分量的数目.本文基于同态加密算法,通过对保密的数据进行编码,设计了一个计算百万富翁问题的协议,并利用模拟范例对协议进行安全性证明.然后利用这个新的协议作为基本模块,设计了一个向量优势统计协议,通过效率分析显示我们的方案是简单、高效的.最后将向量优势统计协议应用到整除判定问题和点与若干直线关系判定问题.

关键词: 安全多方计算;百万富翁问题;同态加密;向量优势统计
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2017)05-1117-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.05.014

Secure Vector Dominance Protocol and Its Applications

LI Shun-dong, ZUO Xiang-jian, YANG Xiao-li, GONG Lin-ming
(*School of Computer Science, Shaanxi Normal University, Xi' an, Shaanxi* 710119, *China*)

Abstract: The millionaires´problem is an important problem in secure multiparty computation and a basic building block of secure multiparty computation protocols. Secure vector dominance statistic problem is a problem generalized for the millionaires´problem, which can be used to get the number of $y_i > x_i$ without leaking further information. In this paper, we first propose an encoding scheme to encode private numbers; then based the new encoding scheme and homomorphic encryption scheme, we design a protocol for millionaires´problem and prove that the protocol is secure in the semi-honest model using the simulation paradigm. Then, we utilize this scheme to propose a solution to secure vector dominance statistic problem. The performance analysis indicates that our protocol is simpler and more efficient than the others. Finally, we use the scheme to solve the integer division problem and privately determine the relation between point and lines.

Key words: secure multi-party computation; millionaires´problem; homomorphic encryption; vector dominance statistic problem

1 引言

安全多方计算(Secure Multi-party Computation, SMC)使拥有私有数据的多个参与者能够合作利用他们的私有数据进行计算,又不泄露各自私有数据,是密码学界研究的热点问题.该问题由 Yao 在文献[1]中提出,Goldreich 等人对其进行深入的研究[2,3],推动了安全多方计算的研究发展.

安全多方计算在隐私数据的计算、电子商务、数据挖掘、保密存储、计算外包、入侵检测等方面有着广泛的应用[4~8].密码研究学者对安全多方计算问题展开了深入的研究,这些问题可以归纳为几个大类:(1)保密的科学计算;(2)保密统计分析;(3)保密数据挖掘;(4)保密计算几何问题;(5)其他安全多方计算问题.在这些问题中百万富翁问题是最重要的问题之一,也是其他安全多方计算协议的基本构成模块.文献[2,9]设计了混淆电路,通过对双方的输入进行双重加密,借助不经意传输工具及输出转换表,给出了在半诚实模型下通用的安全多方计算协议.Ioannidis 等人在文献[10]中提出基于不经意传输,利用简单的异或运算解决百万富翁问题,但每次调用不经意传输协议需要多次公钥计算,计算复杂度和通信复杂度较高.秦在文献[11]中提出基于 Φ 隐藏假设,设计了一个安全的比较协议,但该协议需要茫然的第三方协助完成计算.另外一些协

收稿日期:2016-01-18;修回日期:2016-07-04;责任编辑:马兰英
基金项目:国家自然科学基金(No.61272435);陕西师范大学研究生培养创新基金(No.2015CX029)

议通过分析问题的特征,致力于提高协议的效率,没有考虑算法的简洁性与通用性[12~15]. Tzeng、李等人利用0-1编码解决两个数保密比较大小问题[16~17],这是很有创意的协议,但二者对如何区分两个数相等的问题,没有给出有效的方案. 人们在提出各种高效的百万富翁问题解决方案的同时,也将该问题引申为一系列的特殊的安全多方计算问题. 文献[18]将该问题引申为安全向量优势问题(Secure Vector Dominance Problem),多次调用百万富翁问题协议比较每一组数的大小,方案的效率较低. 文献[19]将上述问题扩展为安全向量优势统计问题(Secure Vector Dominance Statistic Problem),但协议需要借助茫然的第三方,增加了协议执行的通信轮数,降低了方案的安全性. 文献[20]基于置换协议设计无茫然第三方的安全两方向量优势统计协议,协议的计算复杂性较高. 本文首先对保密数据进行编码,设计了一个百万富翁协议,该协议不仅给出了两个数比较大小问题,也解决两个数是否相等问题,且设计的协议简单,效率更高,适用的范围更广. 然后利用这个新的协议作为基本模块,设计一个安全两方向量优势统计问题协议. 最后利用安全两方向量优势统计协议解决整除判定问题和点与若干直线关系判定问题.

2 预备知识

2.1 安全性定义

半诚实参与者在执行协议的过程中会忠实地履行协议,但他可能会保留所有中间结果,试图从中间结果推导出协议之外的信息.

设 $f=(f_1,f_2):\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^*\times\{0,1\}^*$ 是一个概率多项式函数,π 是计算函数 f 的双方协议. 协议的输入为 (x,y),执行协议 π 时第一个参与者 Alice 的 *view* 记作 $view_1^\pi(x,y)=(x,r^1,m_1^1,\cdots,m_t^1)$,其中 r^1 是 Alice 自己产生的随机数,m_i^1 是她收到的第 i 个消息,Alice 的输出记作 $output_1^\pi(x,y)$. 第二个参与者 Bob 的 $view_2^\pi(x,y)$ 和输出 $output_2^\pi(x,y)$ 可以类似地定义.

对于一个函数 f,如果存在概率多项式时间算法 S_1 与 S_2(也称这样的多项式时间算法为模拟器)使得

$$\{(S_1(x,f_1(x,y)),f_2(x,y))\}_{x,y}\overset{c}{\equiv}\{(view_1^\pi(x,y),output_2^\pi(x,y))\}_{x,y} \tag{1}$$

$$\{(f_2(x,y),S_2(y,f_2(x,y)))\}_{x,y}\overset{c}{\equiv}\{(output_1^\pi(x,y),view_2^\pi(x,y))\}_{x,y} \tag{2}$$

其中 $\overset{c}{\equiv}$ 表示计算上不可区分. 则认为 π 保密地计算 f. 要证明一个多方计算方案是保密的,就必须构造满足式(1)和式(2)的模拟器 S_1 与 S_2.

半诚实的参与者模型是一个重要的模型,Goldreich 在文献[3]中利用比特承诺和零知识证明理论设计了一个编译器,给定一个在半诚实参与者条件下保密计算 f 的协议 π,这个编译器能自动生成一个在恶意参与者条件下也能保密计算 f 的协议,这个新的协议可以迫使一个恶意的参与者以半诚实方式参与协议的执行,否则就会被发现. 另外,当人们研究恶意模型下安全的协议时,往往是先研究半诚实模型下安全的协议,然后研究恶意参与者会如何攻击这样的协议,找到防止恶意攻击的方法,并把防止的方法再添加到协议中,形成恶意参与者安全的协议. 所以研究半诚实模型下安全的协议有实际的意义. 本文假设协议的参与者都是半诚实的.

2.2 Paillier 同态加密方案

密钥生成:给定一个安全参数 k,选择两个素数 p,q,其中 $n=p\times q$,$\lambda=lcm(p-1,q-1)$ 是 $p-1$ 和 $q-1$ 的最小公倍数. 随机选择一个 $g\in Z_N^*$ 使得 $\gcd(L(g^\lambda \bmod N^2),N)=1$,定义为 $L(x)=\dfrac{x-1}{N}$. 算法的公钥为 (g,N),私钥为 λ.

加密:随机选择一个随机数 r,$r<N$,计算

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

解密:计算

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

Paillier 是概率加密算法,具有语义安全性,满足加法同态性[21]. 将密文 $E(m_1)=g^{m_1}r_1^n \bmod N^2$ 和和 $E(m_2)=g^{m_2}r_2^n \bmod N^2$ 相乘,可得:

$$\begin{aligned}E(m_1)\otimes E(m_2)&=g^{m_1}r_1^n\cdot g^{m_2}r_2^n \bmod N^2\\&=g^{m_1+m_2}(r_1r_2)^n \bmod N^2\\&=E(m_1+m_2)\end{aligned}$$

3 百万富翁问题高效的解决方案

3.1 问题描述

Alice 拥有数据 x,Bob 拥有数据 y. 双方想知道 x 和 y 的关系:$x>y$、$x<y$、$x=y$. 且不泄露 x 和 y 的信息. 本文首先将保密的数据编码成一个向量,该向量中的元素由0,1,2组成,在加法同态的基础上设计一个简单、高效的协议.

对保密数据的编码:设 $x,y\in\{z_1,z_2,\cdots,z_m\}=U$,其中 $z_1<z_2<\cdots<z_m$. 设 $x=z_k$,$y=z_l$ $(1\leqslant k,l\leqslant m)$,根据 x 和 U 构造一个新的向量 $\boldsymbol{A}=(a_1,a_2,\cdots,a_m)$. 构造规则如下:

$$a_i=\begin{cases}0, & i<k;\\1, & i>k;\\2, & i=k.\end{cases}$$

由数据 y 在集合 U 中的排列位置可知,如果 $x>y$,

即 $k>l$,那么数据 y 在向量 $\boldsymbol{A}$ 中对应的值为 0,即 $a_l=0$;如果 $x<y$,即 $k<l$,那么数据 y 在向量 $\boldsymbol{A}$ 中对应的值为 1,即 $a_l=1$;如果 $x=y$,即 $k=l$,那么数据 y 在向量 $\boldsymbol{A}$ 中对应的值为 2,即 $a_l=2$.

因此,保密的判断数据 x 和 y 的关系($x>y$,$x<y$,$x=y$)可以归约到保密计算 a_l 的值. Alice 用自己的公钥加密向量 $\boldsymbol{A}$,得到 $E(A)=(E(a_1),E(a_1),\cdots,E(a_m))$,并将 $E(\boldsymbol{A})$ 发送给 Bob,Bob 选择一个随机数 r_b,根据数据 y 在集合 U 中的排列位置,Bob 计算

$$E(v)=r_b^N E(a_l)\bmod N^2$$

将 $E(v)$ 发送给 Alice,Alice 用私钥进行解密得到 v 的值. 为了便于描述,定义判断数据 x 和 y 的关系的二元谓词如下:

$$P(x,y)=\begin{cases}0, & x<y;\\ 1, & x>y;\\ 2, & x=y.\end{cases}$$

3.2　协议设计

协议 1　百万富翁问题解决方案.

输入　Alice 输入秘密数 x,Bob 输入秘密数 y.

输出　$P(x,y)$.

(1)设 $x=z_k$,$y=z_l$,Alice 根据 x 和集合 U 构造一个新的向量 $A=(a_1,a_2,\cdots,a_m)$. 则

$$a_i=\begin{cases}0, & i<k;\\ 1, & i>k;\\ 2, & i=k.\end{cases}$$

(2)(G,D,E) 是 Pailler 同态加密方案,τ 是设定的安全参数,Alice 运行 $G(\tau)$ 生成同态加密的公钥和私钥,Alice 向 Bob 公布生成的公钥. Alice 用公钥加密向量 $\boldsymbol{A}$ 得到

$$E(\boldsymbol{A})=(E(a_1),E(a_2),\cdots,E(a_m))$$

Alice 将 $E(\boldsymbol{A})$ 发送给 Bob.

(3)Bob 选择一个随机数 r_b,根据数据 y 在集合 U 中的排列位置,作如下计算

$$E(v)=r_b^N E(a_l)\bmod N^2$$

将 $E(v)$ 发给 Alice.

(4)Alice 用自己的私钥对 $E(v)$ 进行解密得到 v,若 $v=0$,则 $x>y$;若 $v=1$,则 $x<y$;若 $v=2$,则 $x=y$.

3.3　协议的正确性

定理 1　协议 1 能正确求出保密数据 x 和 y 的大小关系.

证明　Alice 拥有的密文信息分别为

$$\begin{aligned}E(\boldsymbol{A})&=(c_1,c_2,\cdots,c_m)\\&=(g^{a_1}r_1^N\bmod N^2,g^{a_2}r_2^N\bmod N^2,\cdots,g^{a_m}r_m^N\bmod N^2)\end{aligned}$$

根据同态性有

$$\begin{aligned}E(v)&=r_b^N E(a_l)\bmod N^2\\&=g^{a_l}(r_l r_b)^N\bmod N^2\\&=E(a_l)\end{aligned}$$

因此,若 $v=0$,则 $x>y$;若 $v=1$,则 $x<y$;若 $v=2$,则 $x=y$.

3.4　协议的安全性

定理 2　在半诚实模型下,协议 1 是安全的.

证明　我们通过构造使得式(1)和式(2)成立的模拟器 S_1,S_2 来证明本定理,首先构造 S_1.

(1)S_1 接受输入$(x,P(x,y))$,根据 $P(x,y)$ 的值构造 y',使得 $P(x,y')=P(x,y)$,用 x',y 进行模拟. 首先按照协议构造向量 $\boldsymbol{A}=(a_1,a_2,\cdots,a_m)$.

(2)加密向量 $\boldsymbol{A}$ 得到

$$E(\boldsymbol{A})=(E(a_1),E(a_2),\cdots E(a_m))$$

(3)选择一个随机数 r'_b,作如下计算

$$E(v')=(r'_b)^N E(a_{l'})\bmod N^2$$

解密 $E(v')$ 得到 v'.

在本协议中

$$view_1^{\pi}(x,y)=\{\boldsymbol{A},E(\boldsymbol{A}),E(v),P(x,y)\}$$

令 $S_1(x,P(x,y))=\{A,E(A),E(v'),P(x,y')\}$. 因为 $P(x,y)=P(x,y')$,Paillier 同态加密算法是语义安全的,则 $E(v)_{x,y}\overset{c}{\equiv}E(v')_{x,y}$. 所以

$$\{(S_1(x,P(x,y)),P(x,y))\}_{x,y}\overset{c}{\equiv}\{view_1^{\pi}(x,y),output_2^{\pi}(x,y)\}_{x,y}$$

使

$$\{(P(x,y),S_2(y,P(x,y)))\}_{x,y}\overset{c}{\equiv}\{output_1^{\pi}(x,y),view_2^{\pi}(x,y)\}_{x,y}$$

成立的 S_2 也可以用类似的方法构造.

3.5　协议的效率分析

文献[16,17]和本文的方案都是对保密数据进行编码,利用同态加密算法解决百万富翁问题,基本运算都是模乘运算. 忽略方案中随机数选择的计算开销,文献[16]的模为 p,文献[17]方案和本文方案的模为 N^2,为了便于比较,统一模为 N.

计算复杂性　设 $x,y\in U$,其中 $|U|=m$,本文在协议 1 中 Alice 进行 m 次加密运算,1 次解密运算,本文协议基于 Paillier 加法同态加密算法解决百万富翁问题,在 Paillier 方案中每一次加密和解密运算需要 $2\log N$ 次模乘运算[16],本文协议 1 中 Alice 总共需要 $2(m+1)\log N$ 次模乘数运算. Bob 只需要 1 次模乘运算,所以协议 1 的总开销为 $2(m+1)\log N+1$ 次模乘运算.

通信复杂性　以通信轮数来衡量,本文的方案和文献[16,17]的方案都需要进行 3 轮通信. 具体的方案效率比较结果如表 1 所示.

表 1 计算复杂性与通信复杂性的比较

	本文协议 1	文献[17]	文献[16]
计算复杂性	$2(m+1)\log N+1$	$2(m+1)\log N+3l$	$5m\log N+4m-6$
通信复杂性	3	3	3
适用范围	$>,<,=$	$>,\leqslant$	$>,\leqslant$

4 向量优势统计问题

4.1 问题描述

向量优势统计问题 Alice 有 n 维向量 $\boldsymbol{X}=(x_1,\cdots,x_n)$,Bob 有 n 维向量 $\boldsymbol{Y}=(y_1,\cdots,y_n)$,双方希望在不泄漏各自保密向量信息的基础上统计出 $y_i>x_i(i=1,2,\cdots,n)$ 的数目 V,称这样的问题为安全向量优势统计问题. 若 $V=n$,则向量 $\boldsymbol{Y}$ 比向量 $\boldsymbol{X}$ 有优势,记作 $\boldsymbol{Y}>\boldsymbol{X}$;若 $V=0$,对每一对(x_i,y_i)都有 $y_i\leqslant x_i(i=1,2,\cdots,n)$.

对保密数据的编码 设向量 $\boldsymbol{X}$ 中的元素 $x_i\in\{z_1,z_2,\cdots,z_m\}=U$,向量 $\boldsymbol{Y}$ 中的元素 $y_i\in\{z_1,z_2,\cdots,z_m\}=U$,其中 $z_1<z_2<\cdots,z_m$. 向量 $\boldsymbol{X}$ 中的元素 x_i 位于集合 U 中的第 k_i 位,向量 $\boldsymbol{Y}$ 中的元素 y_i 位于集合 U 中的第 l_i 位. 根据 x_i 和 U 构造新的向量 $\boldsymbol{A}_i=(a_{i1},a_{i2},\cdots,,a_{im})$. 则有

$$a_{it}=\begin{cases}0, & Zt\leqslant k_i;\\ 1, & Zt>k_i.\end{cases}$$

其中 $1<i\leqslant n,1<t\leqslant m$.

由向量 $\boldsymbol{Y}$ 中的元素 y_i 在集合 U 中的排列位置可知,统计 $y_i>x_i(i=1,2,\cdots,,n)$ 的数目 V 可以等同于计算 $V=a_{1l_1}+a_{2l_2}+\cdots,+a_{nl_n}$. 因此保密统计 $y_i>x_i(i=1,2,\cdots,n)$ 的数目 V 的问题可以归约到保密计算 $V=a_{1l_1}+a_{2l_2}+\cdots,+a_{nl_n}$ 的值,用加法同态算法可以实现. Alice 对向量 $\boldsymbol{X}$ 中的每一个元素按照上述方式进行编码,生成 n 个向量 $\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_n$,即 $\boldsymbol{A}_i=(a_{i1},a_{i2},\cdots,a_{im})$. Alice 将这 n 个向量进行加密. 将 $E(\boldsymbol{A}_1),E(\boldsymbol{A}_2),\cdots,E(\boldsymbol{A}_n)$ 发给 Bob. Bob 选择一个随机数 r_b,根据向量 $\boldsymbol{Y}$ 中的元素 y_i 在集合 U 中的排列位置,利用加法同态性作如下计算

$$E(V)=r_b^N E(a_{1l_1})E(a_{2l_2})\cdots E(a_{nl_n})\bmod N^2$$

Bob 将 $E(V)$ 发给 Alice. Alice 解密得到 V;若 $V=r$,则 $y_i>x_i(i=1,2,\cdots,n)$ 的数目为 r;若 $V=0$,对每一对(x_i,y_i)都有 $y_i\leqslant x_i(i=1,2,\cdots,n)$;若 $V=n$,则 $\boldsymbol{Y}>\boldsymbol{X}$.

4.2 协议设计

协议 2 安全两方向量优势统计协议.

输入 Alice 输入 n 维向量 $\boldsymbol{X}=(x_1,\cdots,x_n)$,Bob 输入 n 维向量 $\boldsymbol{Y}=(y_1,\cdots,y_n)$.

输出 $y_i>x_i(i=1,2,\cdots,n)$ 的数目 V.

(1)设向量 $\boldsymbol{X}$ 中的元素 $x_i\in\{z_1,z_2,\cdots,z_m\}=U$,向量 $\boldsymbol{Y}$ 中的元素 $y_i\in\{z_1,z_2,\cdots,z_m\}=U$,其中 $z_1<z_2<\cdots,z_m$. 根据 x_i 和 U 构造新的向量 $\boldsymbol{A}_i=(a_{i1},a_{i2},\cdots,a_{im})$. 则有

$$a_{it}=\begin{cases}0, & Zt\leqslant k_i;\\ 1, & Zt>k_i\end{cases}$$

其中 $1<i\leqslant n,1<t\leqslant m$.

(2)(G,D,E) 是 Pailler 同态加密方案,τ 是设定的安全参数,Alice 运行 $G(\tau)$ 生成同态加密的公钥和私钥,Alice 向 Bob 公布生成的公钥. Alice 用公钥加密向量 A_i 得到

$$E(\boldsymbol{A}_i)=(E(a_{i1}),E(a_{i2}),\cdots,E(a_{im}))$$

Alice 将 $E(A_i)$ 发送给 Bob.

(3)Bob 选择随机数 r_b,根据向量 $\boldsymbol{Y}$ 中的元素 y_i 在集合 U 中的排列位置,利用加法同态性作如下计算

$$E(V)=r_b^N E(a_{1l_1})E(a_{2l_2})\cdots E(a_{nl_n})\bmod N^2$$

将 $E(V)$ 发给 Alice.

(4)Alice 用自己的私钥对 $E(V)$ 进行解密得到 V. 若 $V=r$,则 $y_i>x_i(i=1,2,\cdots,n)$ 的数目为 r;若 $V=n$,则 $\boldsymbol{Y}>\boldsymbol{X}$;若 $V=0$,对每一对(x_i,y_i)都有 $y_i\leqslant x_i(i=1,2,\cdots,n)$.

4.3 协议的安全性

定理 3 在半诚实模型下,协议 2 是安全的.

证明 我们通过构造使得式(1)和式(2)成立的模拟器 S_1,S_2 来证明本定理,首先构造 S_1.

(1)S_1 接受输入$(\boldsymbol{X},\boldsymbol{V})$,根据 V 的值构造 $\boldsymbol{Y}'$,使得 $V'=V$,用 $\boldsymbol{X},\boldsymbol{Y}'$进行模拟. 首先按照协议构造向量 $\boldsymbol{A}_i=(a_{i1},a_{i2},\cdots,a_{im})$.

(2)加密向量 $\boldsymbol{A}_i$ 得到

$$E(\boldsymbol{A}_i)=(E(a_{i1}),E(a_{i2}),\cdots,E(a_{im}))$$

(3)选择一个随机数 r'_b,作如下计算

$$E(V')=(r'_b)^N E(a_{1l'1})E(a_{2l'2})\cdots E(a_{nl'n})\bmod N^2$$

解密 $E(V')$得到 V'.

在本协议中 $view_1^{\pi}(\boldsymbol{X},\boldsymbol{Y})=\{\boldsymbol{A}_i,E(\boldsymbol{A}_i),E(V),V\}$. 令 $S_1(X,V)=\{\boldsymbol{A},E(\boldsymbol{A}),E(V'),V'\}$. 因为 $V=V'$,则 $E(V')_{X,Y}\overset{c}{\equiv}E(V)_{X,Y}$. 所以

$$\{(S_1(\boldsymbol{X},V),V)\}_{X,Y}\overset{c}{\equiv}\{view_1^{\pi}(\boldsymbol{X},\boldsymbol{Y}),output_2^{\pi}(\boldsymbol{X},\boldsymbol{Y})\}_{X,Y}$$

使

$$\{(V,S_2(\boldsymbol{Y},V))\}_{X,Y}\overset{c}{\equiv}\{output_1^{\pi}(\boldsymbol{X},\boldsymbol{Y}),view_2^{\pi}(X,Y)\}_{X,Y}$$

成立的 S_2 也可以用类似的方法构造. 定理 3 证明完毕.

4.4 协议的效率分析

文献[19,20]和本文的方案都是用同态加密算法解决向量优势统计问题,基本运算都是模乘运算,为了便于比较,统一向量的维数 n,数据的长度为 m.

计算复杂性 本文在协议 2 中 Alice 进行 mn 次加密运算,1 次解密运算,Alice 总共需要 $2(mn+1)\log N$ 次模乘数运算. Bob 只需要 n 次模乘运算,所以协议 2 的总开销为 $2(mn+1)\log N+n$ 次模乘运算.

通信复杂性　以通信轮数来衡量,本文中协议 2 方案需要进行 3 轮通信. 具体的方案效率比较结果如表 2 所示.

表 2　计算复杂性与通信复杂性的比较

	本文协议 2	文献[19]	文献[20]
计算复杂性	$2(mn+1)\log N+n$	$18mn\log N+\sum_{i=1}^{l}(u_i^1+u_i^2+2)$	$24mn\log N+8mn+4n$
通信复杂性	3	4	3
有无第三方	无	有	无

协议效率改进　用协议 2 解决判定性问题,即判定 $V=0$ 或 $V=n$ 时,Alice 需要进行 mn 次加密运算. 协议 2 可以经过简单改造减少加密次数. 若判定 $V=n$,Alice 对向量 A_i 进行加密,其中 $i=1,2,\cdots,n$,只需对向量 $\boldsymbol{A}_i$ 中元素 1 进行加密,对向量 $\boldsymbol{A}_i$ 中每一个元素 0 用不同的随机数 R 代替,其中随机数 R 和向量 $\boldsymbol{A}_i$ 中元素 1 的密文是不可区分的. 若判定 $V=0$,Alice 对向量 $\boldsymbol{A}_i$ 进行加密,只需对向量 $\boldsymbol{A}_i$ 中元素 0 进行加密,对向量 $\boldsymbol{A}_i$ 中每一个元素 1 用不同的随机数 R 代替,其中随机数 R 和向量 $\boldsymbol{A}_i$ 中元素 0 的密文是不可区分的. 因此 Alice 执行协议 2 平均需要进行$\frac{mn}{2}$次加密运算. 此时协议 2 的平均总开销为$(mn+1)\log N+n$ 次模乘运算.

5　向量优势统计问题的应用

本节我们将利用安全两方向量优势统计协议解决整除判定问题和点与直线关系判定问题.

5.1　整除问题

整除判定问题 设 x,y 是任意两个整数,其中 $y\neq 0$. 如果存在一个整数 r 使得等式 $x=ry$ 成立,就称 y 整除 x,记作 $y\mid x$,并把 y 叫做 x 的因数. 否者,就称 y 不能整除 x,记作 $y\nmid x$. Alice 有整数 x,Bob 有整数 y,且 $x,y\geqslant 1$. 他们想知道整数 y 是否为整数 x 的因数,且不能泄露各自的信息.

根据算术基本定理,任意整数都可以表示为素数的乘积,则整数 x,y 可以表示为

$$x=p_1^{e_1}p_2^{e_2}\cdots p_n^{e_n},y=p_1^{f_1}p_2^{f_2}\cdots p_n^{f_n}$$

其中 p_i 表示第 i 个素数,即 $p_1=2,p_2=3,\cdots$,令$[p]=\{p_1,p_2,\cdots,p_n\}$. 利用 x,y 和$[p]$构造向量 $\boldsymbol{X}=(e_1,e_2,\cdots,e_n)$和向量 $\boldsymbol{Y}=(f_1,f_2,\cdots,f_n)$. 若 $y\mid x$,则对每一对(f_i,e_i),都有$f_i\leqslant e_i(i=1,2,\cdots,n)$. 因此保密计算整数 y 是否为整数 x 的因数问题可以归约到计算向量优势统计问题. 利用协议 2 计算$f_i\leqslant e_i(i=1,2,\cdots,n)$的数目 V. 若 $V=0$,则对每一对(f_i,e_i),都有$f_i\leqslant e_i$,即 $y\mid x$;若 $V\neq 0$,则 $y\nmid x$.

5.1.1　协议设计

协议 3　安全两方整除判定问题协议.

输入　Alice、Bob 的机密数 x,y,集合$[p]=\{p_1,p_2,\cdots,p_n\}$.

输出　是否 $y\mid x$.

(1) Alice 利用整数 x 和集合$[p]$构造向量 $\boldsymbol{X}=(e_1,e_2,\cdots,e_n)$,Bob 利用整数 y 和集合$[p]$构造向量 $Y=(f_1,f_2,\cdots,f_n)$.

(2) Alice 和 Bob 调用协议 2,计算 $f_i\leqslant e_i(i=1,2,\cdots,n)$的数目 V. 若 $V=0$,则对每一对(f_i,e_i),都有$f_i\leqslant e_i$,即 $y\mid x$;若 $V\neq 0$,则 $y\nmid x$.

在协议 3 中最多需要$(mn+1)\log N+n$ 次模乘运算,Alice 和 Bob 之间需要进行 3 轮通信. 协议 3 的安全性依赖于安全两方向量优势统计协议的安全性,应用证明定理 3 所用的方法很容易证明协议 3 的安全性,本文在这里省略证明过程.

5.2　点与直线关系判定问题

点与若干直线关系判定问题 假设 Alice 的点为 $P(x_0,y_0)$,Bob 有 n 条直线,直线方程为 $L_i:a_ix+b_iy+c_i=0,(1\leqslant i\leqslant n)$. Alice 和 Bob 判断点 $P(x_0,y_0)$与 n 条直线的关系,即点 P 在所有直线的上方或下方. 且双方不想泄露点 P 和直线 L_i 的信息. 该问题在点包含于多边形判定问题上有重要应用. 判断点 P 是否包含在多边形 Q 中,找到多边形最左点和多边形最右点将多边形划分成上下两部分 Q_1,Q_2. 若点 P 在 Q_1 中所有边的下方,在 Q_2 中所有边的上方. 则点 P 包含在多边形 Q 中,解决该问题的数学模型就是点与若干直线关系判定问题.

如果点 P 在直线 L_i 的上方,则 $a_ix_0+b_iy_0+c_i>0$;如果点 P 在直线 L_i 的下方或直线上,则 $a_ix_0+b_iy_0+c_i\leqslant 0$. 本文将点 P 和直线方程 L_i 的系数 a_i,b_i 分别用向量表示,即$(x_0,y_0),(a_i,b_i)$. Alice 和 Bob 应用向量内积协议[20],Alice 得到 $u_i=a_ix_0+b_iy_0+r_i$,其中 r_i 是只有 Bob 知道的随机数. Alice 构造向量 $\boldsymbol{X}=(u_1,u_2,\cdots,u_n)$,Bob 构造向量 $\boldsymbol{Y}=(c_1+r_1,c_2+r_2,\cdots,c_n+r_n)$. 若点 P 在直线 L_i 的上方,则对每一对(u_i,c_i+r_i),都有 $u_i>c_i+r_i(i=1,2,\cdots,n)$;若点 P 在直线 L_i 的下方或直线上,则对每一对(u_i,c_i+r_i),都有 $u_i\leqslant c_i+r_i(i=1,2,\cdots,n)$. 因此保密计算点与直线关系判定问题可以归约到计算向量优势统计问题. 利用协议 2 计算 $u_i>c_i+r_i$ 的数目 V. 若 $V=n$,则对每一对(u_i,c_i+r_i),都有 $u_i>c_i+r_i(i=1,2,\cdots,n)$,点 P 在直线 L_i 的上方;若 $V=0$,则对每一对(u_i,c_i+r_i),都有 $u_i\leqslant c_i+r_i(i=1,2,\cdots,n)$,点 P 在直线 L_i 的下方或直线上.

5.2.1　协议设计

协议 4　点与直线关系判定问题.

输入　Alice 的顶点 $P(x_0,y_0)$,Bob 的直线方程为 $L_i:a_ix+b_iy+c_i=0,(1\leqslant i\leqslant n)$.

输出 V 的值.

(1) Alice 和 Bob 应用向量内积协议, Alice 得到 $u_i = a_i x_0 + b_i y_0 + r_i$, 其中 r_i 是只有 Bob 知道的随机数.

(2) Alice 构造向量 $X = (u_1, u_2, \cdots, u_n)$, Bob 构造向量 $Y = (c_1 + r_1, c_2 + r_2, \cdots, c_n + r_n)$.

(3) Alice 和 Bob 调用协议 2, 计算 $u_i > c_i + r_i$ 的数目 V. 若 $V = n$, 则对每一对 $(u_i, c_i + r_i)$, 都有 $u_i > c_i + r_i (i = 1, 2, \cdots, n)$, 点 P 在直线 L_i 的上方; 若 $V = 0$, 则对每一对 $(u_i, c_i + r_i)$, 都有 $u_i \leqslant c_i + r_i (i = 1, 2, \cdots, n)$, 点 P 在直线 L_i 的下方或直线上.

在协议 4 中最多需要 $(mn + 1)\log N + n$ 次模乘运算, Alice 和 Bob 之间需要进行 3 轮通信. 协议 4 的安全性依赖于安全两方向量优势统计协议的安全性, 应用证明定理 3 所用的方法很容易证明协议 4 的安全性, 本文在这里省略证明过程.

6 结论

本文利用同态加密算法和对保数据进行编码, 设计了一个简单计算百万富翁问题的协议. 然后利用这个协议作为基本模块, 设计一个无茫然的第三方的安全两方向量优势统计问题协议. 最后将安全两方向量优势统计协议应用到整除判定问题和点与若干直线关系判定问题. 在后面工作中, 我们将探讨恶意模型下向量优势统计问题.

参考文献

[1] C Yao. Protocols for secure computations[A]. Proceedings of the 23th IEEE Symposium on Foundations of Computer Science[C]. Chicago: IEEE Press, 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] Goldreich O. Foundations of Cryptography: Volume 2, Basic Applications[M]. London: Cambridge University Press, 2004. 599 – 764.

[4] Du W, Atallah M J. Privacy-preserving cooperative scientific computations[A]. Proceedings of the 14th IEEE workshop on Computer Security Foundations[C]. Canada: IEEE Computer Society, 2001. 273.

[5] 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[M]. Berlin: Springer Berlin Heidelberg, 2012. 416 – 432.

[6] Li Y, Chen M, Li Q, et al. Enabling multilevel trust in privacy preserving data mining[J]. Knowledge and Data Engineering, IEEE Transactions on, 2012, 24 (9): 1598 – 1612.

[7] Toft T. Secure data structures based on multi-party computation[A]. Proceedings of the 30th annual ACM SIGACT-SIGOPS symposium on Principles of distributed computing[C]. New York: ACM, 2011. 291 – 292.

[8] Loftus J, Smart N P. Secure Outsourced Computation[M]. Progress in Cryptology – AFRICACRYPT 2011. Berlin: Springer Berlin Heidelberg, 2011. 1 – 20.

[9] A C Yao. How to generate and exchange secrets[A]. Proceedings of 27th Annual Symposium on Foundations of Computer Science (FOCS86)[C]. Toronto: IEEE, 1986. 162 – 167.

[10] Ioannidis and A. Grama. An efficient protocol for Yao´s millionaires´problem[A]. Proceedings of the 36th Hawaii Interna-tional Conference on System Sciences[C]. Hawaii: IEEE, 2003. 6 – 9.

[11] 秦静, 张振峰, 冯登国, 李宝. 无信息泄漏的比较协议[J]. 软件学报, 2004, 15(3): 421 – 427.
Qin Jing, Zhang Zhen-feng, Feng Deng-guo, Li Bao. A protocol of comparing information without leaking[J]. Journal of Software, 2004, 15(3): 421 – 427. (in Chinese)

[12] Sheikh R, Mishra D K, Kumar B. Secure multiparty computation: from millionaires problem to anonymizer[J]. Information Security Journal: A Global Perspective, 2011, 20(1): 25 – 33.

[13] 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.

[14] Karimian Ardestani N. Efficient Non-Interactive Secure Two-Party Computation for Equality and Comparison[D]. Canada: University of Calgary, 2015.

[15] Lipmaa H, Toft T. Secure Equality and Greater-Than Tests with Sublinear Online Complexity[M]. Automata, Languages and Programming. Berlin: Springer Berlin Heidelberg, 2013. 645 – 656.

[16] Lin H Y, Tzeng W G. An efficient solution to the millionaires' problem based on homomorphic encryption[A]. Applied Cryptography and Network Security[C]. Berlin: Springer Berlin Heidelberg, 2005. 456 – 466.

[17] 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)

[18] Atallah M J, Du W. Secure Multi-Party Computational Geometry[M]. Algorithms and Data Structures. Berlin: Springer Berlin Heidelberg, 2001. 165 – 179.

[19] 刘文,罗守山,王永滨. 安全两方向量优势统计协议及其应用[J]. 电子学报,2010,38(11):2573 – 2577.
Liu Wen, Luo Shou-shan, Wang Yong-bin. Secure two-party vector dominance statistic protocol and Its application[J]. Acta Electronica Sinica, 2010, 38(11): 2573 – 2577. (in Chinese)

[20] 钱小强,仲红,石润华. 无茫然第三方的安全两方向量优势统计协议[J]. 计算机工程,2014,40(2):148 – 152.
Qian Xiao-qiang, Zhong Hong, Shi Run-hua. Secure two-party vector dominance statistic protocol without oblivious third party [J]. Computer Engineering, 2014, 40(2): 148 – 152. (in Chinese)

[21] Paillier P. Public-key cryptosystems based on composite degree residuosity classes[A]. Advances in cryptology—EUROCRYPT' 99[C]. Berlin: Springer Berlin Heidelberg, 1999. 223 – 238.

作者简介

李顺东　男,1963 年 12 月生,河南平顶山人. 2003 年在西安交通大学获计算机科学与技术工学博士学位. 陕西师范大学计算机科学学院教授、博士生导师. 主要从事密码学与信息安全研究.
E-mail:shundong @ snnu. edu. cn

左祥建　男,1990 年6 月生,湖北荆州人. 陕西师范大学硕士研究生,主要研究领域为密码学与信息安全.
E-mail:zuoxiangjian@ snnu. edu. cn