同态加密的百万富翁问题高效解决方案

左祥建,李顺东,杨晓莉

(陕西师范大学 计算机科学学院,西安 710062)
E-mail :shundong@ snnu. edu. cn

摘　要: 安全多方计算问题由图灵奖得主姚期智于上世纪八十年代首先提出,现在已经成为密码学的一个重要研究方向. 百万富翁问题是多方安全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,但现有的解决方案效率低下,因而会影响其他安全多方协议的效率. 基于同态加密算法,通过对保密的数据进行 0-1 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. 通过效率分析显示我们的方案是简单、高效的. 最后利用这个新的协议作为基本模块,设计了一个保密数据查询问题的协议,并给出了应用实例.

关 键 词: 多方安全计算;百万富翁问题;同态加密;安全查询
中图分类号: TP391　　**文献标识码:** A　　**文 章 编 号:** 1000-1220(2017)03-0455-05

An Efficient Homomorphic Encryption Based Solution to Millionaires′ Problem

ZUO Xiang-jian,LI Shun-dong,YANG Xiao-li
(School of Computer Science,Shaanxi Normal University,Xi′an 710062,China)

Abstract: Secure Multi-party Computation was first proposed by A. C. Yao in 1980s. Now,it is a new and important area of cryptography. The millionaires′ problem is an important problem in secure multiparty computation and a basic building block of secure multiparty computation protocol. But known solutions are not efficient enough and thus affect the efficiency of many secure multiparty computation protocols. In this paper,we first propose a 0-1 encoding scheme to encode private numbers;then based the new encoding scheme and a 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. The performance analysis indicates that our protocol is simpler and more efficient than the others. Finally,we utilize this scheme to propose a solution to privacy-preserving data querying problem and show an example of its applications.

Key words: secure multi-party computation;millionaires′ problem;homomorphic encryption;secure querying

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,同时又不泄露各自私有数据,是目前密码学界研究的热点问题. 这个问题最先由 Yao 在文献[1]中提出,Yao 提出了这样一个问题:两个百万富翁 Alice 和 Bob,他们想知道谁更富有,但都不想让对方知道自己财富的信息,这就是百万富翁问题. 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]. 目前,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. Yao 在文献[1]中提出解决方案,但复杂性非常高,计算复杂性为输入规模的指数级别. 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,并借助不经意传输工具及输出转换表,给出了一个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 隐藏假设以及同态公钥加密的语义安全性假设,设计了一个安全的两方比较协议,但该协议需要茫然的第三方协助完成计算. 另外的一些协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[12-14]. Tzeng 等人在文献[15]将自然数编码成一个集合,把比较大小问题规约到集合相交问题,李等人在此的基础上,将两个数的比较问题规约到向量的部分标量积的保密计算问题[16]. Tzeng、李等人都是巧妙的利用 0-1 编码解决保密比较两个数的大小问

收稿日期:2016-01-19　收修改稿日期:2016-05-13　基金项目:国家自然科学基金项目(61272435)资助;陕西师范大学研究生培养创新基金项目(2015CXS029)资助.　作者简介:**左祥建**,男,1990 年生,硕士研究生,研究方向为密码学与信息安全;**李顺东**(通信作者),男,1963 年生,博士,教授,研究方向为密码学与信息安全;**杨晓莉**,女,1989 年生,硕士研究生,研究方向为密码学与信息安全.

题. 这是很有创意的协议,但二者都只是解决 $x>y, x\leqslant y$ 的问题,如何区分两个数相等的问题,没有给出有效的方案. 本文在此基础上,巧妙利用 0-1 编码,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,设计一个协议保密查询数据在有序集合中的排序问题.

本文贡献如下:

1)提出一种新的 0-1 编码方法解决保密数据比较大小问题.

2)利用新的 0-1 编码方法和 Paillier 同态加法方案提出了一种高效的百万富翁问题解决方案,并证明了方案的正确性与安全性,与文献[15,16]中的方案相比,本文中的协议效率更高,方案适用的范围更广.

3)利用新的协议作为基本模块,无需对数据进行多次比较,一次性查询出数据在有序集合中的排序问题,协议简单、计算容易、具有很高的效率.

2 预备知识

2.1 安全性

理想保密计算协议 假设存在一个可信的第三者(Trusted Third Party,TTP),他在任何情况下都不撒谎,决不会泄露不该泄露的信息. 借助于 TTP,双方保密计算可以这样实施:Alice 将 x 告诉 TTP,Bob 将 y 告诉 TTP;TTP 自己计算 $f(x,y)$,然后将结果分别告诉 Alice 和 Bob. 因为 Alice 和 Bob 没有办法从协议中得到除 $f(x,y)$ 之外的额外信息,这样一个简单的协议是安全性最高的双方保密计算协议,任何一个计算 $f(x,y)$ 的实际双方保密计算协议的安全性都不可能超过这个协议.

半诚实参与者 不严格地说,一个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 $f=(f_1,f_2):\{0,1\}^*\times\{0,1\}^*\rightarrow\{0,1\}^*\times\{0,1\}^*$ 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 $view_1^{\pi}=(x,r^1,m_1^1,\cdots,m_1^t)$,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 $output_1^{\pi}$. 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

$$\begin{aligned}&\{(S_1(x,f_1(x,y)),f_2(x,y))\}_{x,y}\\ \overset{c}{\equiv}&\{(view_1^{\pi}(x,y),output_2^{\pi}(x,y))\}_{x,y} \qquad (1)\\ &\{(f_2(x,y),S_2(y,f_2(x,y)))\}_{x,y}\\ \overset{c}{\equiv}&\{(output_1^{\pi}(x,y),view_2^{\pi}(x,y))\}_{x,y} \qquad (2)\end{aligned}$$

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(1)和(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,这是因为:

1)在实际工作中许多参与者都是半诚实的,因此研究半诚实模型下的安全多方计算在许多情况下比较简单,也是符合实际的,也能解决许实际问题. 即使在这样的条件下仍有许多安全多方计算的问题没有解决,所以半诚实模型下的安全多方计算仍有许多问题有待研究;

2)Goldreic 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,形成对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 同态加密

同态加密的概念是由 Rivest 在文献[17]中提出来的,同态加密的特殊性质使我们在不解密密文的情况下直接对密文进行某种运算,对明文数据进行各种计算,还不会影响明文数据的机密性. Sander 在文献[18]中定义了整数环上的加法、乘法同态加密,确保数据在加密前后的计算结果相同. 同态加密在多方保密计算和云计算中起着重要的作用.

加法同态加密体制:假设加密算法为 $E(\cdot)$,解密算法为 $D(\cdot)$. 对于任意的消息 m_1 和 m_2,加密结果为 $E(m_1)$,$E(m_2)$. 如果满足

$$E(m_1)\otimes E(m_2)=E(m_1+m_2)$$
$$E(m_1\otimes m_2)=(E(m_1))^{m_2}$$

则称该加密算法具有加法同态性.

2.3 Paillier 加密方案

Paillier 加密算法是概率加密算法,该算法具有加法同态性[19].

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 $L(x)=\frac{x-1}{N}$. 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

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

3 百万富翁问题高效解决方案

3.1 问题描述

Alice 拥有数据 x,Bob 拥有数据 y. Alice 和 Bob 想知道数据 x 和 y 的关系:$x>y, x<y, x=y$. 他们不想泄露 x 和 y 的信息. 本文首先将保密的数据编码成一个向量,该向量中的元素由一个 1 和若干个 0 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 $x=z_k, y=z_l$,根据 x 和 U 构造一个新的向量 $A=(a_1,a_2,\cdots a_m)$. 则有

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

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 $v=\sum_{i=1}^{l-1}a_i+\sum_{i=1}^{l}a_i=2\sum_{i=1}^{l-1}a_i+a_l=0$;如果 $x=y$,即 $k=l$,那么 $v=\sum_{i=1}^{l-1}a_i+\sum_{i=1}^{l}a_i=2\sum_{i=1}^{l-1}a_i+a_l=1$;如果 $x<y$,即 $k<l$,那么 $v=\sum_{i=1}^{l-1}a_i+\sum_{i=1}^{l}a_i=2\sum_{i=1}^{l-1}a_i+a_l=2$.因此保密的判断数据 x 和 y 的关系($x>y,x<y,x=y$)可以规约到保密计算 $\sum_{i=1}^{l-1}a_i+\sum_{i=1}^{l}a_i$,用加法同态算法可以实现. Alice 用自己的公钥加密向量 A,得到 $E(A)=(E(a_1),E(a_2),\cdots,E(a_m))$,并将 $E(A)$发送给 Bob,Bob 利用同态加密算法性质计算

$$E(v)=(\prod_{i=1}^{l-1}E(a_i))^2E(a_l)\bmod N^2.$$

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:

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

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 $A=(a_1,a_2,\cdots a_m)$. 则有

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

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 A 得到

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

Alice 将 $E(A)$发送给 Bob.

3)Bob 选择一个随机数 r_b,其中 $r_b<N$,根据数据 y 在集合 U 中的排列位置,利用加法同态性作如下计算

$$E(v)=r_b^N(\prod_{i=1}^{l-1}E(a_i))^2E(a_l)\bmod N^2$$
$$=E(2\sum_{i=1}^{l-1}a_i+a_l).$$

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

$$E(A)=(c_1,\cdots,c_m)$$
$$=(g^{a_1}r_1^N\bmod N^2,\cdots,g^{a_m}r_m^N\bmod N^2)$$

Bob 收到 $E(A)$,选择随机数 r_b,利用加法同态性作如下计算

$$E(v)=r_b^N(\prod_{i=1}^{l-1}E(a_i))^2E(a_l)\bmod N^2$$
$$=g^{2\sum_{i=1}^{l-1}a_i+a_l}(r_1r_1r_2r_2\cdots r_{l-1}r_{l-1}r_lr_b)^N\bmod N^2$$
$$=E(2\sum_{i=1}^{l-1}a_i+a_l)$$

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 $x<y$.

在协议 1 中,$r_b^N(r_b<N)$对保护 y 的机密性有至关重要的作用,如果没有随机数 r_b^N,Alice 利用向量 $A=(a_1,a_2,\cdots a_m)$进行穷举计算,则

$$E(v'')=(\prod_{i=1}^{l''-1}E(a_i))^2E(a_{l''})\bmod N^2=E(2\sum_{i=1}^{l''}a_i+a_{l''})$$

若存在 $E(v'')=E(v)$,则 $l''=l$,这样就会泄露 y 的值. 乘上随机数 r_b^N 就能避免 Alice 进行穷举计算,且不影响正确解密. Alice 在解密的过程中只能得到 v 的值,通过 v 的值判断保密数据 x 和 y 的大小关系,整个过程中没有泄露对方的保密数据任何信息,并且完成了保密判断保密数据 x 和 y 的大小关系的计算,正确性得以证明.

3.4　协议的安全性

协议 1 的安全性以 Paillier 同态加密算法的安全性为基础,Paillier 同态加密算法具有语义安全性,本文应用模拟范例,可以证明协议 1 是安全的.

定理 2. 在半诚实模型下,协议 1 是安全的.

证明:我们通过构造两个模拟器 S_1,S_2 使得(1)式和(2)式成立来证明本定理,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 $A=(a_1,a_2,\cdots a_m)$.

2)加密向量 A 得到

$$E(A)=(E(a_1),E(a_2),\cdots E(a_m)).$$

3)选择一个随机数 r'_b,作如下计算

$$E(v)=(r'_b)^N(\prod_{i=1}^{l'-1}E(a_i))^2E(a'_l)\bmod N^2=E(2\sum_{i=1}^{l'-1}a_i+a'_l)$$

解密 $E(v')$得到 v'.

在本协议中 $view_1(x,y)=\{A,E(A),E(v),P(x,y)\}$. 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 $v=v'$,$(v)_{x,y}\overset{c}{\equiv}E(v')_{x,y}$. 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. 定理 2 证明完毕.

3.5　协议的效率分析

本文的方案效率与文献[15,16]中方案进行比较,文献[15]基于 ElGamal 乘法同态加密算法解决百万富翁问题,文献[16]基于 Paillier 加法同态加密算法解决百万富翁问题. 文献[15]、文献[16]和本文的方案都是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,对保密数据都进行编码. 忽略方案中随机数选择的计算开销和双方准备阶段的计

算开销,文献[15]的模为 p,文献[16]方案和本文方案的模为 N^2,为了便于比较,统一模为 N,数据的长度为 m.

计算复杂度: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[15],Alice 总共需要 $2(m+1)\log N$ 次模乘数运算. Bob 只需要 l 次模乘运算,所以协议 1 的总开销为 $2(m+1)\log N+l$ 次模乘运算.

通信复杂度: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,在多方安全计算研究中通常用轮数. 以通信轮数来衡量,本文的方案和文献[15,16]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比较

Table 1 Computation and communication complexity

协议	计算复杂性	通信复杂性
协议 1	$2(m+1)\log N+l$	3
文献[16]	$2(m+1)\log N+3l$	3
文献[15]	$5m\log N+4m-6$	3

由表 1 可知,本文协议 1 的计算复杂性低于文献[15]和文献[16]中协议的计算复杂性,通信复杂性与文献[15]和文献[16]中协议通信复杂性一样. 在适用范围方面,文献[15]、文献[16]的方案都只是解决保密比较数据大小的问题,但对于两个数是否相等的问题,没有给出有效的方案,本文的协议 1 不仅解决了两个数比较大小问题,也能区分两个数是否相等的问题.

4 保密的数据查询问题

4.1 问题描述

Alice 有数据集 $A=\{a_1,a_2,\cdots a_s\}$,Bob 有数据 b,Bob 想查询数据 b 在集合 A 中的排列位置 R_A,且不泄露任何关于集合 A 中的元素和数据 b 任何其他的信息. 此问题是多方安全计算在数据查询中的一个重要应用,有着广泛的应用前景. 例如,学生高考结束后,涉及到填报志愿的问题. 当大学录取结束时,总会有人落榜,原因多为志愿填报不当. 某考生想报考一所知名大学,但他不确定自己的高考成绩能被该学校录取,他可以向该学校招生处查询自己的高考成绩在已报考该学校考生中的排名情况,增加录取的机率. 在查询的过程中,该学校为了保护其他考生的隐私,不会让该同学获知其他考生的高考成绩,该考生也不想向该学校招生处透露自己的高考成绩. 该问题的数学模型就是保密的数据查询问题. 在执行协议前,本文约定对集合 A 中的元素已按照由小到大的顺序排列,即 $a_1<a_2<\cdots<a_s$. 本文用 0-1 编码将集合编码成一个向量,即向量中的元素由 0 和 1 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 0-1 编码:设集合 $A\subset\{z_1,z_2,\cdots,z_m\}=U$,数据 $b=z_l(1\leqslant l\leqslant m)$,其中 $z_1<z_2<\cdots<z_m$. 根据集合 A 和集合 U 构造一个新的向量 $X=(x_1,x_2,\cdots,x_m)$. 则有

$$x_i=\begin{cases}1, & z_i\in A;\\ 0, & z_i\notin A.\end{cases}$$

数据 b 在集合 A 中的排列位置 R_A 可以进行如下计算:

$$R_A=\sum_{i=i}^{l-1}x_i+1.$$

因此,计算数据 b 在集合 A 中的排列问题,可以规约到计算 $R_A=\sum_{i=i}^{l-1}x_i+1$. 该协议用加法同态算法实现. Alice 用自己的公钥加密向量 X,得到 $E(X)=(E(x_1),E(x_2),\cdots,E(x_m))$,并将 $E(X)$ 发送给 Bob,Bob 选择随机数 r,利用同态加密算法性质计算

$$E(R_{A_1})=\prod_{i=1}^{l-1}E(x_i)E(r)\bmod N^2$$

将 $E(R_{A_1})$ 发送给 Alice,Alice 用私钥进行解密得到 R_{A_1} 的值,将 R_{A_1} 发送给 Bob,Bob 去掉随机数 r 得到 $R_A=\sum_{i=i}^{l-1}x_i+1$.

4.2 协议设计

协议 2. 保密查询数据在有序集合中的排列问题.

输入:Alice 集合 $A=\{a_1,a_2,\cdots a_s\}$,Bob 输入数据 b,其中 $a_1<a_2<\cdots<a_s$.

输出:排列位置 R_A.

1)设集合 $A\subset\{z_1,z_2,\cdots,z_m\}=U$,数据 $b=z_l(1\leqslant l\leqslant m)$,其中 $z_1<z_2<\cdots<z_m$. 根据集合 A 和集合 U,Alice 构造向量 $X=(x_1,x_2,\cdots,x_m)$. 则有

$$x_i=\begin{cases}1, & z_i\in A;\\ 0, & z_i\notin A.\end{cases}$$

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 X 得到

$$E(X)=(E(x_1),E(x_2),\cdots E(x_m)),$$

Alice 将 $E(X)$发送给 Bob.

3)Bob 选择随机数 r_b 和 r,其中 $r_b<N$,根据数据 b 在集合 U 中的排列位置,利用加法同态性作如下计算

$$\begin{aligned}E(R_{A_1})&=r_b^N\prod_{i=1}^{l-1}E(x_i)E(r)\bmod N^2\\&=E\Big(\sum_{i=1}^{l-1}x_i+r\Big).\end{aligned}$$

将 $E(R_{A_1})$发给 Alice.

4)Alice 用自己的私钥对 $E(R_{A_1})$进行解密得到 R_{A_1},Alice 将 R_{A_1} 发送给 Bob.

5)Bob 收到 R_{A_1},去掉随机数 r,计算 $R_A=R_{A_1}-R+1=\sum_{i=1}^{l-1}x_i+1$.

在协议 2 中最多需要 $2(m+1)\log N+l$ 次模乘运算,Alice 和 Bob 之间需要进行 3 轮通信. 协议 2 经过简单的改造,也能计算两个集合间的排序问题. 协议 2 的安全性以 Paillier 同态加密算法的安全性为基础,该算法算法具有语义安全性. 应用证明定理 2 所用的方法很容易证明协议 2 的安全性,本文在这里省略证明过程.

5 总 结

百万富翁问题是安全多方计算研究的最重要问题之一,也是其他安全多方计算协议的基本构成模块. 目前这个问题解决的方法比较多,但不具有简洁,适用范围有限. 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、高效的计算百万富翁问题的协议,并证明了协议的正确性和安全性.最后,利用这个新的协议作为基本模块,设计了一个保密数据查询问题的协议,并给出了应用实例.本文的协议是在半诚实模型下进行的,在后面工作中,我们将探讨恶意模型下高效的百万富翁计算问题.

References:

[1] Yao A C. Protocols for secure computations[C]. Proceedings of the 23rd Annual Symposium on Foundations of Computer Science. Institute of Electrical and Electronics Engineers(IEEE) Computer Society,1982:160-164.

[2] Goldreich O,Micali S,Wigderson A. How to play any mental game [C]. Proceedings of the Nineteenth Annual Association for Computing Machinery(ACM) Symposium on Theory of Computing, Association for Computing Machinery (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[C]. Proceedings of the 14th Institute of Electrical and Electronics Engineers (IEEE) Workshop on Computer Security Foundations, Institute of Electrical and Electronics Engineers (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[C]. Proceedings of the 12th Conference on Topics in Cryptology,Springer Verlag,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,Institute of Electrical and Electronics Engineers(IEEE) Transactions on, 2012,24(9):1598-1612.

[7] Toft T. Secure data structures based on multi-party computation[C]. Proceedings of the 30th Annual Association for Computing Machinery (ACM) Sigact Sigops Symposium on Principles of Distributed Computing,Association for Computing Machinery,2011:291-292.

[8] Loftus J,Smart N P. Secure outsourced computation[C]. Proceedings of the 4th International Conference on Progress in Cryptology in Africa,Springer-Verlag,2011:1-20.

[9] Yao A C. How to generate and exchange secrets[C]. Proceedings of 27th Annual Symposium on Foundations of Computer Science (FOCS′86),Institute of Electrical and Electronics Engineers,1986: 162-167.

[10] Ioannidis I,Grama A. An efficient protocol for Yao′s mil-lionaires′ problem[C]. Proceedings of the 36th Hawaii Interna-tional Conference on System Sciences,Hawaii,USA,Jan,2003:6-9.

[11] Qin Jing,Zhang Zheng-feng,Feng Deng-guo,et al. A protocol of comparing information without leaking[J]. Journal of Software, 2004,15(3):421-427.

[12] Li Shun-dong,Dai Yi-qi,You Qi-you. An efficient solution to Yao′s millionaire s′problem[J]. Chinese Journal of Electronics,2005, 233(5):770-773.

[13] 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.

[14] Luo Y,Huang L,Yang W,et al. An efficient protocol for private comparison problem[J]. Chinese Journal of Electronics,2009,18 (2):205-209.

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

[16] Li Shun-dong,Wang Dao-shun. Efficient secure multiparty computation based on homomorphic encryption[J]. Chinese Journal of Electronics,2013,41(4):798-803.

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

[18] Sander T,Tschudin C F. Protecting mobile agents against malicious hosts[M]. Mobile Agents and Security,Springer Berlin Heidelberg,1998:44-60.

[19] Paillier P. Public-key cryptosystems based on composite degree residuosity classes[C]. Proceedings of the 17th International Conference on Theory and Application of Cryptographic Techniques, Springer-Verlag,1999:223-238.

附中文参考文献:

[11] 秦　静,张振峰,冯登国,等. 无信息泄漏的比较协议[J]. 软件学报,2004,15(3):421-427.

[12] 李顺东,戴一奇,尤启友. 姚氏百万富翁问题的高效解决方案[J]. 电子学报,2005,233(5):770-773.

[16] 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.