盲百万富翁问题的高效解决方案

李顺东 张萌雨
(陕西师范大学计算机科学学院 西安 710119)

摘 要 安全多方计算是密码学研究的一个重要领域，也是国际密码学研究的热点之一. 百万富翁问题是第一个安全多方计算问题，它研究的是 Alice 和 Bob 各拥有一个私有数据 x、y，保密比较 x、y 大小的问题. 研究人员提出了许多解决方案，并在其基础上拓展出了许多新的问题. 本文对百万富翁问题进行了新的拓展，提出这样的问题: Alice、Bob、Carol 和 Dove 各拥有保密数据 x、y、u、v，他们要保密判定 $x+y$ 和 $u+v$ 的大小关系，但是都不愿意泄露自己的保密数据. 在此情况下，没有人知道 $x+y$、$u+v$ 的具体数值. 我们称这个问题为盲百万富翁问题，其具有重要的理论与实际意义. 为解决此问题，我们利用概率加密算法的性质和移位寄存器的思想设计了新的保密移位添加方法. 然后在半诚实模型下设计了参与者为三方、四方和 n 方的三个不同盲百万富翁问题的解决方案，并应用模拟范例证明了方案的安全性，可以抵抗任意的合谋攻击. 最后，对协议进行了效率分析和实验测试，理论分析和实验结果都表明本文的协议是高效的、实用的. 保密移位添加方法不仅可用于解决本文的盲百万富翁问题，还可以作为基础模块去解决其它安全多方计算问题. 盲百万富翁问题也为安全多方计算提供了新的研究思路.

关键词 安全多方计算；百万富翁问题；盲百万富翁问题；概率加密
中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2020.01755

An Efficient Solution to the Blind Millionaires′ Problem

LI Shun-Dong ZHANG Meng-Yu
(*School of Computer Science, Shaanxi Normal University, Xi'an* 710119)

Abstract The study of secure multi-party computation started in 1986, by Andrew Yao, and quickly became an extremely active area of research in academic circles and a hot topic of international cryptographic community. The millionaires′ problem is the first secure multiparty computation problem and the most fundamental one in secure scientific computing. It studies how two parties, Alice and Bob with private numbers x and y, respectively to jointly determine which of x and y is bigger without disclosing any other information. It is an important building block of many other secure multiparty computation protocols. The researchers proposed many effective solutions to the millionaires′ problem and generalized a series of new secure multiparty computation problems including private maximum and minimum computation, secure vector dominance, secure sorting, and so on. The existing protocols only work when the participants know the plaintext of the private data, but in some scenarios, the protocol of millionaires′ problem may be used as a sub-protocol. In this case, the participants may not know the private data which are in the form of ciphertext, and therefore, no existing protocol works. How to address millionaires′ problem when the private data is not known. This problem has not been investigated in literature. This paper extends millionaires′ problem in a new direction. We propose the following problem: Alice, Bob, Carol, and Dove have private numbers x, y, u and v, respectively and they want to determine the relation between $x+y$ and

收稿日期：2019-09-16；在线发布日期：2020-02-07. 本课题得到国家自然科学基金面上项目（61272435）资助. **李顺东**(通信作者)，博士，教授，博士生导师，中国计算机学会（CCF）会员，主要研究领域为密码学与信息安全. E-mail: shundong@snnu.edu.cn. **张萌雨**，硕士研究生，主要研究方向为密码学与信息安全.

$u+v$ without disclosing x, y, u, v. No party knows the value of $x+y$, $u+v$ in this scenario. We call this problem the blind millionaires′ problem. It is of important theoretical and practical significance but cannot be solved or cannot be well solved using the existing solutions. It is necessary to design specific protocols for this problem. To solve this problem, we first use the randomization property of probabilistic encryption algorithm to securely substitute some ciphertexts. Then, we use secure substitution and the idea of shift register to propose a secret shift adding method. This method can be used to securely add, subtract and multiply on ciphertexts on the condition that the plaintext space is small. Based on the secret shift adding method, combining with threshold decryption probabilistic cryptosystem, we design secure comparison protocols for three comparing problems in small plaintext space. The participants of the three protocols are 3, 4 and n. Second, we use the simulation paradigm to prove that these protocols are secure in the semi-honest model. These protocols can resist collusion attack of n–1 parties. With different encoding method, different protocol is appropriate for different problem it solves. We analyzed and compared our protocols with the most similar literature we can find. We also tested the execution time of the protocols. Both theoretical analysis and experimental results show that the protocol proposed in this paper is efficient and practical. Furthermore, the secret shift adding method can also be used as a basic building block to solve other secure multiparty computation problems. And the questions raised in this paper also provide a new research direction for the readers.

Keywords secure multiparty computation; millionaires' problem; blind millionaires' problem; probabilistic encryption

1 引 言

1982 年 Andrew Yao 在文献[1]中首次提出百万富翁问题，这标志着安全多方计算的诞生. 安全多方计算（Secure Multi-party Computation, SMC）也称为安全计算、多方计算或保密计算，是密码学的一个关键领域. 安全多方计算被认为是各种现实隐私保护问题的实际解决方案，特别是那些只需要共享秘密且各方之间没有太多交互的问题，例如分布式投票、私人竞标和拍卖、共享签名或解密功能以及私人信息检索[2]等.

Goldreich 等人[3, 4]对安全多方计算进行了深入的研究，并给出了适用于所有安全多方计算问题的通用解决方案. 多年来,通用安全多方协议的概念成为孕育具体问题协议的沃土. 但通用方案在求解具体的安全多方计算问题时，仅是一个问题可解的理论性证明，目前还不具有实际的可行性，原因有以下两点：一方面，除简单的布尔运算外，将一般计算问题转化成电路计算的转化复杂性很高；另一方面，使用通用方案解决一般的实际问题所需要的存储和计算都太多,效率太低. 随着通用解决方案的不断改进和优化，未来通用解决方案也可能用于解决一些实际问题，但目前解决实际问题的主要途径是针对实际应用提出具体高效的解决方案.

所谓百万富翁问题是指百万富翁 Alice 和 Bob 分别拥有财富 x、y，他们想要保密判定 x 和 y 的大小关系. 这是第一个安全多方计算问题，也是保密科学计算[1],[5-11]研究中的一个最基础的问题. 研究人员提出了许多高效的解决方案[1],[12-20]. 文献[1,4]的方案只能比较两个数的大小，无法判定两个数是否相等. 秦静等人在文献[12]中基于 Φ隐藏假设和同态加密体制的语义安全性假设,给出了一个高效安全的无信息泄漏的比较相等协议；Luo 等人在文献[13]中利用计算几何中的叉积协议和同态加密体制设计了一个高效的秘密比较方案，该方案能够一次有效地判定数据的大小或相等关系；文献[14]应用算术编码的方法解决两方秘密比较问题,大大降低了协议的计算复杂度. 但文献[12-14]只适用于两方参与者，且参与者仅持有单个数据的情形. 文献[15-17]巧用 0-1 编码方法给出了判断两个数据大小关系的高效解决方案. Li 等人在文献[18]中使用三角性面积公式解决了有理数比较大小的问题. 文献[20]提出了一种使用现实中纸牌进行数据大小关系判定的协议，但是其适用于计算机不可使用的情况.

百万富翁问题不仅是最基本的安全多方计算问

题，还是解决其他安全多方计算问题的基础. 其还可以派生出许多其它重要的可以用于解决许多实际应用的问题. 这些派生问题包括: 参与者人数不变，但每个参与者持有的数据是隐私向量的安全向量优势问题[21]；多个参与者保密计算其隐私数据的最大（小）值问题[11]、计算平均值问题、计算第 k 个最大（小）值问题和多个保密数据排序问题[22, 23]等.

目前研究百万富翁问题的解决方案仅适用这样的场景: 参与者知道被比较的隐私数据. 但有的时候需要在参与者只知道隐私数据密文的情况下保密比较得出相应的明文数据的大小关系. 我们称这种情况下的比较问题为盲百万富翁问题，此类问题具有更广泛的应用背景和实际意义，例如下面的问题都属于盲百万富翁问题.

1. A 公司计划建一座大楼，B、C 两家公司分别负责大楼建设和后期装修. A 公司的预算资金为 a，B、C 两家公司的建设费用分别为 b、c. 在正式达成合作前，任何一方都不想泄露自己的建设费用. 要在不泄露各方建设费用的情况下，判断这三家单位有没有可能达成建设协议，就需要保密判定 a 是否大于 $b+c$. 这个问题可以抽象为在知道 x 不知道 y 的情况下，保密判定 x 和 y 的大小关系.

2. 在某次大型商业招标活动中，A 和 B、C 和 D 分别达成协议合作竞标. 其中，A、B、C、D 分别计划出资金额为 a、b、c、d. 他们都希望中标，但在中标前每一方都不想让任何一方(包括合作方和招标方)获知自己的报价. 这就需要在不知道 $a+b$ 和 $c+d$ 的情况下（泄露 $a+b$ 对于 A，B 来说就是泄露了 a，b），保密判定 $a+b$ 和 $c+d$ 的大小关系. 这个问题可以抽象为在不知道 x 和 y 的情况下，保密判定 x 和 y 的大小关系.

3. 有 A、B 两个备选方案，n 个人想要在不泄露自己对哪个方案偏好的情况下调查这两个方案哪个更受欢迎. 记参与者 P_i 对方案 A 的喜爱程度为 x_i，对方案 B 的喜爱程度为 y_i. 在这个场景下需要参与者在不知道 $\sum x_i$ 和 $\sum y_i$ 的情况下，保密判定 $\sum x_i$ 和 $\sum y_i$ 的大小关系. 这个问题同样可以抽象为在不知道 x 和 y 的情况下，保密判定 x 和 y 的大小关系.

这三个盲百万富翁问题与百万富翁问题既有相同之处，又有不同之处. 相同之处是本质上都是保密比较 x 和 y 的大小. 不同之处在于: (1)在百万富翁问题中有两个参与者属于双方安全计算，在盲百万富翁问题中有两个以上的参与者属于安全多方计算；(2) 在百万富翁问题中，两个参与者分别持有要比较的隐私数据 x 和 y 的明文. 而盲百万富翁问题逻辑上可以划分为两个子问题: 求和问题和密文比较大小问题. 参与者在合作求得 x_i 和的密文 $E(\sum x_i)$ 以及 y_i 和的密文 $E(\sum y_i)$ 后，保密比较 $E(\sum x_i)$ 和 $E(\sum y_i)$ 得到 $\sum x_i$ 和 $\sum y_i$ 的大小关系. 即在盲百万富翁问题中，所有参与者持有的都是要比较的隐私数据 $\sum x_i$ 和 $\sum y_i$ 的密文. 也正因为存在上述的两个本质上的区别，所以现有的百万富翁问题的解决方案都不能用于解决盲百万富翁问题.

密文比较大小这一问题鲜有研究. 目前我们仅知道文献[24]中的 SLT 协议（Secure Less than Protocol）使用 Paillier 公钥系统的性质解决了该问题. 又由于 Paillier 公钥系统具有加法同态性，可以解决求和问题. 所以，可以以文献[24]的 SLT 协议为基础构造盲百万富翁问题的解决方案. 但使用文献[24]所实现的解决方案存在两个方面的缺陷: 首先，Paillier 公钥系统难于构建门限密码系统，且即使构建了门限解密，由于存在一个密钥的分发者，使得协议的参与者之间不平等，只要分发者参与合谋，其他参与者的安全性就无法得到保证；其次，使用 Paillier 公钥系统的性质解决有严格的条件限制，其要求 $x, y, x-y, (x-y)\cdot r < N/2$. 其中，随机数 r 是保护 x-y 的值不泄露的关键，但由于 r 是随机数，所以 $(x-y)\cdot r < N/2$ 这一条件限制很难得到保证，进而在实际使用中可能会出现错误或信息泄露.

综上所述，现有的研究都不能或者不能很好地解决本文所提出的盲百万富翁问题，所以需要针对这一具体问题提出高效的解决方案.

为了解决该问题，本文设计了一种新的保密移位添加方法. 在该方法的基础上提出了三个不同类型盲百万富翁问题的解决方案，这三个方案适用于不同的应用场景，每一个方案都是实用和高效的，都不需要调用其它协议. 由于方案不需要加密系统具有任何同态性，所以可以选用效率高的概率加密系统实现.

本文的主要贡献如下：

(1) 对百万富翁问题进行推广，提出了新的盲百万富翁问题，该问题具有重要的理论与实际意义.

(2) 利用移位寄存器的思想和概率加密的性质提出了一种新的保密移位添加方法，该方法可以用于实现小数据的加减运算，可以作为一种新的安全多方计算方法去解决许多问题.

(3) 使用新的方法解决了盲百万富翁问题，并用模拟范例证明了协议在半诚实模型下是安全的，可以抵抗任意数量的合谋攻击.

(4) 对协议进行了效率分析和实验验证，理论

分析和实验结果都表明本文方案是高效的.

2 预备知识

2.1 安全性定义

半诚实模型：半诚实参与者[4]在协议执行过程中完全按照协议要求诚实地执行协议，但有可能会记录协议执行过程中所收集到的信息，并试图根据收集到的信息推算其他参与者的私有信息. 如果所有参与者都是半诚实的，则称这样的模型为半诚实模型. 本文所设计的协议都是半诚实模型下的安全多方计算协议.

设有 n 个参与者 $P_1,\cdots,P_n$，分别拥有私密数据 $x_1,\cdots,x_n$,记 $X=(x_1,\cdots,x_n)$. 他们利用协议 Π 保密地计算 $f(X)=(f_1(X),\cdots,f_n(X))$，其中 $f_i(X)(i\in[n]=\{1,\cdots,n\})$ 为参与者 P_i 得到的输出结果. 在协议执行过程中，P_i 得到的信息序列记为

$$view_i^{\Pi}(X)=(x_i,r_i,M_i^1,\cdots,M_i^t),$$

其中，$M_i^j(j=1,\cdots,t)$ 表示 P_i 收到的第 j 个信息. 对于部分参与者构成的子集 $I=\{P_{i_1},\cdots,P_{i_s}\}\subseteq\{P_1,\cdots,P_n\}$，记

$$view_I^{\Pi}(X)=(I,view_{i_1}^{\Pi}(X),\cdots,view_{i_s}^{\Pi}(X)).$$

定义 1（半诚实参与者的安全性[4]）. 在参与者都是半诚实的情况下，如果存在概率多项式时间算法 S，使得对于任意的 $I=\{P_{i_1},\cdots,P_{i_s}\}\subseteq\{P_1,\ \cdots,P_n\}$，均有下式成立:

$$\begin{aligned}&\{S(I,(x_{i_1},\cdots,x_{i_s})),f_I(X))\}_{X\in(\{0,1\}^*)^n}\\&\overset{c}{\equiv}\{view_I^{\Pi}(X)\}_{X\in(\{0,1\}^*)^n}\end{aligned}\tag{1}$$

其中 $\overset{c}{\equiv}$ 表示计算上不可区分，则称协议 Π 保密地计算了 n 元函数 $f(X)$.

如果对于任意 $n-1$ 个参与者构成的集合 I,都存在满足(1)式的 S，则称协议 Π 能够抵抗任意数量的合谋攻击.

半诚实模型是非常重要的一个研究模型. 一方面，许多实际的参与者都是半诚实的，且按照 Goldreich 的通用转化方法，可以将在半诚实参与者条件下保密计算函数 f 的协议 Π 转化为在恶意参与者条件下也能保密计算 f 的协议 Π'，新协议可以迫使恶意参与者以半诚实方式执行协议. 另一方面，对恶意模型的研究可以建立在对半诚实模型研究的基础上，通过分析恶意参与者可能存在的恶意行为，将阻止恶意行为的方法添加到协议中，从而使新协议对恶意参与者也是安全的. 基于上述两点可知，研究半诚实模型下安全的协议是具有实际意义的.

2.2 加密系统

2.2.1 概率加密

在给定明文和密钥的前提下，确定性加密方案总是产生相同的密文，这样在明文空间较小的应用中很容易受到选择明文攻击，例如经典的 RSA 加密系统. 针对确定性加密方案的这一缺陷，Shafi Goldwasser 和 Silvio Micali 在文献[25]中首次提出了概率加密的概念，并给出了第一个可证明安全的概率公钥加密方案. 常用的概率加密算法包括 ElGamal、Paillier 和随机预言机模型下的各种结构.

概率加密在加密算法中加入了随机数，因此加密相同的消息时，只要选取不同的随机数就会产生不同的密文. 实际上，为了保持语义安全，即隐藏有关明文的全部信息，加密算法必须是概率性的. 可以将概率公钥加密算法的加密过程简单表达为

$$c\leftarrow Encrypt_{\varepsilon}(pk,m,r).$$

其中，c 为 m 的密文,ε 表示公钥加密方案,pk 为公钥，m 为明文消息，r 为随机数.

2.2.2 门限解密

门限解密[26, 27]是抵抗合谋攻击的一个重要工具. 为了保证每个参与者数据的私有性，使协议能够抵抗任意数量的合谋攻击，就需要朴素的 (n,n) 门限密码系统: n 个参与者联合生成公钥，解密密钥由这 n 个参与者联合持有. 加密消息直接使用公钥，但解密需要 n 个参与者合作才能完成，少于 n 个人时得不到明文的任何信息. 下面以 ElGamal 公钥系统[28]为例构造门限密码系统如下:

联合生成密钥：n 个参与者选取 ElGamal 公钥系统的参数 g,p. 每个参与者 P_i 选取各自的私钥 k_i，并计算 $h_i=g^{k_i}\ mod\ p$. 所有参与者联合持有私钥 $sk=\sum_{i=1}^{n}k_i$，联合生成公钥 pk:

$$h=\prod_{i=1}^{n}h_i\ mod\ p=g^{\sum_{i=1}^{n}k_i}\ mod\ p.$$

加密：对于明文消息 m，参与者 P_i 随机选取一个随机数 r，按照下式计算密文 c.

$$c=(u,v)=(mh^r \bmod p,g^r \bmod p).$$

联合解密：参与者计算 $w_i=v^{k_i} \bmod p$ 并公布. 进一步计算可得明文消息 m.

$$m=u\left[\prod_{i=1}^{n}w_i\right]^{-1} \bmod p.$$

2.2.3 密文的自盲性

密文的自盲性[29]（Self-Blinding）也称为密文的重随机化，是指给定明文 m 的一个密文，任何人不

需解密就可以把它转换为 m 的另一个密文. 值得注意的是，重随机化后的密文 $E'(m)$ 与调用加密算法所得的密文 $E(m)$ 在计算上是不可区分的. 如何对密文进行重随机化与所选择的加密方案有关，下面以 ElGamal 公钥系统为例. 对消息 m 进行重随机化，选择随机正整数 r_1，计算

$$(u',v')=(uh^{r_1},vg^{r_1})=(mh^{r+r_1} \bmod p, g^{r+r_1} \bmod p).$$

简单来说，在原有密文 $E(m)$ 的基础上乘上 $E(1)$ 即可实现对原有密文的重随机化，这是因为 ElGamal 公钥系统具有乘法同态性，即 $E(m)\cdot E(1)=E(m\cdot 1)=E'(m)$. 下文所提到重随机化操作均由上述计算过程实现，并以 $E'(m)$ 代表重随机化后的 $E(m)$.

本文所设计的协议需要加密系统同时具有概率加密、门限解密和密文的自盲性这三个性质，为了便于后续对协议的描述和分析，下文将统一以门限解密的 ElGamal 公钥系统为例进行描述.

3　三方盲百万富翁问题的解决方案

3.1　协议的基本原理

问题描述 1. 假设 Alice、Bob 和 Carol 各自拥有一个私有数据 x,y,z. 其中 $1\leqslant x,y,z\leqslant m$. Alice 和 Bob 为互不信任的合作方. 他们三人希望联合进行保密比较得出 $x+y$ 和 z 之间的大小关系，但又不愿意泄露任何有关自己私有数据的信息.

编码方法 1. 由问题描述 1 可知，数据 x,y,z 的取值范围为 $[1,m]$，则 $2\leqslant x+y\leqslant 2m$，即 $x,y,z,x+y$ 均在 1 到 $2m$ 之间. 所以，可以使用如下编码方法将 $x,x+y$ 转化为一个与其唯一对应的 $2m$ 维向量. 以 x 为例，将其转化为向量 $\boldsymbol{A}=(a_1,\cdots,a_{2m})$，$a_1$ 到 a_{2m} 依次代表 1 到 $2m$ 之间的所有整数，其中，小于 x 的数所对应的分量为 1，等于 x 的数所对应的分量为 2，大于 x 的数所对应的分量为 3，即

$$a_i=\begin{cases}1, \text{姑}\ i<x;\\ 2, \text{姑}\ i=x;\\ 3, \text{姑}\ i>x.\end{cases}$$

原理描述 1. Alice 首先使用编码方法 1 构造一个 $2m$ 维向量 $\boldsymbol{A}=(a_1,\cdots,a_{2m})$，其中向量的前 $x-1$ 个分量为 1，第 x 个分量为 2，后 $2m-x$ 个分量为 3. x 编码为

$$\boldsymbol{A}=(\underbrace{1,\cdots,1}_{\text{x-1了}},2,\underbrace{3,\cdots,3}_{2m-x\text{了}})$$

Bob 根据自己的私有数据 y 的值将向量 $\boldsymbol{A}$ 右移 y 位去掉 $\boldsymbol{A}$ 的后 y 个分量. 然后，在第一个分量前添加 y 个为 1 的分量，即

$$(\underbrace{1,\cdots,1}_{\text{x-1了}},2,\underbrace{3,\cdots,3}_{2m-x-y\text{了}})$$

$$\downarrow$$

$$(\underbrace{1,\cdots,1}_{y\text{了}},\underbrace{1,\cdots,1}_{\text{x-1了}},2,\underbrace{3,\cdots,3}_{2m-x-y\text{了}})$$

$$\downarrow$$

$$(\underbrace{1,\cdots,1}_{\text{x+y-1了}},2,\underbrace{3,\cdots,3}_{2m-x-y\text{了}})$$

经过移位添加操作后的向量分量总数仍为 $2m$ 个，但为 1 的分量数为 $x+y-1$ 个，即求得了 $x+y$. 为了叙述方便，将表示 $x+y$ 的向量记为 $\boldsymbol{C}$，则

$$\boldsymbol{C}=(\underbrace{1,\cdots,1}_{\text{x+y-1了}},2,\underbrace{3,\cdots,3}_{2m-x-y\text{了}}).$$

Carol 根据自己私有数据 z 的值，选择向量 $\boldsymbol{C}$ 的第 z 个分量. 如果该分量为 1，则表示 $x+y>z$；如果该分量为 2，则表示 $x+y=z$；如果该分量为 3，则表示 $x+y<z$.

以上所述即为本文判断 $x+y$ 和 z 大小关系的原理，它还可以用于解决 $x+y-z$ 是否大于 0 的问题，但需要使用加密算法实现协议的保密性. 由于此方法不涉及任何同态性，利用具有自盲性的概率加密算法本身所具有的性质即可保证协议的安全性.

为了便于描述，定义判断数据 $x+y$ 和 z 大小关系的二元谓词如下:

$$P(x+y,z)=\begin{cases}1, x+y>z;\\ 2, x+y=z;\\ 3, x+y<z.\end{cases}$$

例 1. 设 $x=2,y=3,z=4$，选取 $m=6$. Alice 按照编码方法 1 构造向量 $\boldsymbol{A}$ 如下：

$$\boldsymbol{A}=(1,2,\underbrace{3,3,3,3,3,3,3,3,3,3}_{10\text{了}}).$$

Bob 将向量 $\boldsymbol{A}$ 右移 3 位去掉 $\boldsymbol{A}$ 的后 3 个分量后，在第一个分量前添加 3 个为 1 的分量，得到 $x+y$ 的和向量 $\boldsymbol{C}$.

$$\boldsymbol{C}=(\underbrace{1,1,1,1}_{4\text{了}},2,\underbrace{3,3,3,3,3,3,3}_{7\text{了}}).$$

Carol 选择向量 $\boldsymbol{C}$ 的第 4 个分量，该分量为 1，可得 $x+y>z$. 事实上，$x+y=5$ 显然大于 $z=4$.

3.2　协议设计

协议 1. 三方盲百万富翁问题的解决方案.

输入：Alice、Bob、Carol 分别输入数据 x,y,z.

输出：$P(x+y,z)$.

准备：Alice、Bob、Carol 首先选取 ElGamal 公钥系统的公开参数 g，p，然后分别选择各自的私钥

k_i，联合生成公钥:

$$h=\prod_{i=1}^{3}h_i \bmod p=g^{\sum_{i=1}^{3}k_i} \bmod p.$$

1. Alice 使用编码方法 1 将数据 x 转化为向量 $\boldsymbol{A}=(a_1,\cdots,a_{2m})$，加密 $\boldsymbol{A}$ 发送给 Bob，即将

$$E(\boldsymbol{A})=(E(a_1),\cdots,E(a_{2m})).$$

发送给 Bob.

2. 设 $y=j$，Bob 将 $E(\boldsymbol{A})$ 右移 j 位去掉后 j 位密文，重随机化后在密文 $E'(a_1)$ 前添加 j 个 1 的密文，得到 $x+y$ 的密文. 记 $x+y=c$，Bob 将 $E(\boldsymbol{C})$ 发送给 Carol. $E(\boldsymbol{C})$ 每个分量的计算过程如下所示：

FOR i=1 TO $2m$

IF $i\leqslant j$

$E(c_i)\leftarrow E(1)$

EISE

$E(c_i)\leftarrow E'(a_{i-j})$

END

3. 设 $z=s$，Carol 选择 $E(\boldsymbol{C})$ 的第 s 个分量，记为 $E(q)=(u,v)$.

4. Alice、Bob、Carol 分别计算 $w_i=v^{k_i} \bmod p$ 并公布，然后进一步计算解密得到

$$q=u\left[\prod_{i=1}^{3}w_i\right]^{-1} \bmod p.$$

如果 $q=1$，则表示 $x+y>z$；如果 $q=2$，则表示 $x+y=z$；如果 $q=3$，则表示 $x+y<z$.

3.3 方案分析

正确性分析 本文协议 1 解决的是判断 $x+y$ 和 z 大小关系的问题. 根据编码方法 1 可知，求得的 $x+y$ 的编码 $\boldsymbol{C}$ 一共有 $2m$ 个分量，c_1 到 c_{2m} 依次代表 1 到 $2m$ 之间的所有整数，小于 $x+y$ 的数所对应的分量为 1，等于 $x+y$ 的数所对应的分量为 2，大于 $x+y$ 的数所对应的分量为 3. $1\leqslant z\leqslant m$，$\boldsymbol{C}$ 中第 z 个分量表示 z. 如果该分量为 1，表示 $x+y>z$；如果该分量为 2，表示 $x+y=z$；如果该分量为 3，表示 $x+y<z$. 下面对求解 $x+y$ 的编码 $\boldsymbol{C}$ 的正确性进行详细证明.

命题 1. 使用移位添加方法能够由 x 的编码 $\boldsymbol{A}$ 得到正确的 $x+y$ 的编码 $\boldsymbol{C}$.

$$\boldsymbol{A}=(\underbrace{1,\cdots,1}^{1\ \cdots\ x-1}_{x-1\text{了}},2,\underbrace{3,\cdots,3}^{x+1\ \cdots\ 2m}_{2m-x\text{了}}),$$

$$\boldsymbol{C}=(\underbrace{1,\cdots,1}^{1\ \cdots\ x+y-1}_{x+y-1\text{了}},2,\underbrace{3,\cdots,3}^{x+y+1\ \cdots\ 2m}_{2m-x-y\text{了}}).$$

下面用数学归纳法证明这个命题.

证明. (1) 当 $y=1$时，$x+y=x+1$，将 $\boldsymbol{A}$ 右移位 1 位去掉 $\boldsymbol{A}$ 的最后一个分量后，在第一个分量前添加一个为 1 的分量，可得

$$\boldsymbol{A}=(\underbrace{1,\cdots,1}^{1\ \cdots\ x-1}_{x-1\text{了}},2,\underbrace{3,\cdots,3}^{x+1\ \cdots\ 2m}_{2m-x\text{了}})\xrightarrow{\text{听穗1佥}}(\underbrace{1,\cdots,1}^{1\ \cdots\ x-1}_{x-1\text{了}},2,\underbrace{3,\cdots,3}^{x+1\ \cdots\ 2m-1}_{2m-x-1\text{了}})$$

$$\xrightarrow{\text{澍匀1}}(1,\underbrace{1,\cdots,1}^{1\ 2\ \cdots\ x}_{x-1\text{了}},2,\underbrace{3,\cdots,3}^{x+1\ x+2\ \cdots\ 2m}_{2m-x-1\text{了}})=(\underbrace{1,\cdots,1}^{1\ \cdots\ x}_{x\text{了}},2,\underbrace{3,\cdots,3}^{x+1\ x+2\ \cdots\ 2m}_{2m-x-1\text{了}})$$

$$\Leftrightarrow(\underbrace{1,\cdots,1}^{y=1\ 1\ \cdots\ x+y-1}_{x+y-1\text{了}},2,\underbrace{3,\cdots,3}^{x+y\ x+y+1\ \cdots\ 2m}_{2m-x-y\text{了}})=\boldsymbol{C}.$$

(2) 设当 $y=k(1\leqslant k\leqslant m-1)$ 时，$x+y=x+k$，将 $\boldsymbol{A}$ 右移位 k 位去掉 $\boldsymbol{A}$ 的后 k 个分量后，在第一个分量前添加 k 个为 1 的分量，记所求的编码为 $\boldsymbol{A}_{x+k}$.

$$\boldsymbol{A}=(\underbrace{1,\cdots,1}^{1\ \cdots\ x-1}_{x-1\text{了}},2,\underbrace{3,\cdots,3}^{x+1\ \cdots\ 2m}_{2m-x\text{了}})\xrightarrow{\text{听穗}k\text{佥}}(\underbrace{1,\cdots,1}^{1\ \cdots\ x-1}_{x-1\text{了}},2,\underbrace{3,\cdots,3}^{x+1\ \cdots\ 2m-k}_{2m-x-k\text{了}})$$

$$\xrightarrow{\text{澍匀1}}(\underbrace{1,\cdots,1}^{1\ 1\ \cdots\ k}_{k\text{了}},\underbrace{1,\cdots,1}^{k+1\ \cdots\ x+k-1}_{x-1\text{了}},2,\underbrace{3,\cdots,3}^{x+k\ x+k+1\ \cdots\ 2m}_{2m-x-k\text{了}})$$

$$=(\underbrace{1,\cdots,1}^{1\ \cdots\ x+k-1}_{x+k-1\text{了}},2,\underbrace{3,\cdots,3}^{x+k\ x+k+1\ \cdots\ 2m}_{2m-x-k\text{了}})=\boldsymbol{A}_{x+k}.$$

则当 $y=k+1$时，$x+y=x+k+1$，将 $\boldsymbol{A}_{x+k}$ 右移去掉 $\boldsymbol{A}_{x+k}$ 的最后一个分量后，在第一个分量前添加添加 1 个为 1 的分量，可得

$$\boldsymbol{A}_{x+k}=(\underbrace{1,\cdots,1}^{1\ \cdots\ x+k-1}_{x+k-1\text{了}},2,\underbrace{3,\cdots,3}^{x+k\ x+k+1\ \cdots\ 2m}_{2m-x-k\text{了}})$$

$$\xrightarrow{\text{听穗1佥}}(\underbrace{1,\cdots,1}^{1\ \cdots\ x+k-1}_{x+k-1\text{了}},2,\underbrace{3,\cdots,3}^{x+k\ x+k\ \cdots\ 2m-1}_{2m-x-k-1\text{了}})$$

$$\xrightarrow{\text{澍匀1}}(1,\underbrace{1,\cdots,1}^{1\ 2\ \cdots\ x+k}_{x+k-1\text{了}},2,\underbrace{3,\cdots,3}^{x+k+1\ x+k+2\ \cdots\ 2m}_{2m-x-k-1\text{了}})$$

$$=(\underbrace{1,\cdots,1}^{1\ \cdots\ x+k}_{x+k\text{了}},2,\underbrace{3,\cdots,3}^{x+k+1\ x+k+2\ \cdots\ 2m}_{2m-x-k-1\text{了}})$$

$$\Leftrightarrow(\underbrace{1,\cdots,1}^{y=k+1\ 1\ \cdots\ x+y-1}_{x+y-1\text{了}},2,\underbrace{3,\cdots,3}^{x+y\ x+y+1\ \cdots\ 2m}_{2m-x-y\text{了}})=\boldsymbol{C}.$$

综上所述，使用移位添加方法可以由 x 的编码 $\boldsymbol{A}$ 正确求解 $x+y$ 的编码 $\boldsymbol{C}$.

证毕.

安全性分析 协议 1 的安全性是基于门限解密的 ElGamal 公钥系统安全性的. 在计算过程中，Alice、Bob 和 Carol 三个人收或发的消息都是密文. Alice 仅发送编码的密文消息，Bob 和 Carol 两人无法通过所收到的密文获知任何的额外信息，原因有以下两点: 首先，协议 1 是门限解密的，每个人都只拥有私钥的一部分，只要有一个人不参与解密，就无法获知有关密文的任何信息. 其次，ElGamal

公钥系统是语义安全的，随机数和密文是计算不可区分的. 在解密过程中，Alice、Bob 和 Carol 分别计算并公布了 $w_i = v^{k_i} \bmod p$. 私钥 k_i 的安全性基于离散对数假设，不存在多项式时间算法 A 在接受输入 (w_i, v, p) 后可以输出 k_i. 因此，在协议的整个执行过程中，Alice、Bob 和 Carol 的数据 x、y、z 都是完全保密的. 协议 1 是使用 (3,3) 门限密码系统实现的，可以抵抗任意 2 个参与者的合谋攻击. 下面我们使用模拟范例对协议进行详细证明.

定理 1. 协议 1 在半诚实模型下是安全的，且可以抵抗任意数量的合谋攻击.

证明. (1) 在 Alice 不参与合谋的情况下

$$I = \{Bob, Carol\}, X = \{x, y, z\},$$
$$f(X) = f_I(X) = P(x+y, z),$$
$$\{view_I^{\Pi}(X)\}_{X \in (\{0,1\}^*)^n}$$
$$= (I, view_2^{\Pi}(X), view_3^{\Pi}(X))$$
$$= \{I, y, r_2, E(\boldsymbol{A}), z, r_3, E(\boldsymbol{C}), f_I(X)\}.$$

给定输入 $(I,(y,z), f_I(X))$，S 随机选择 $1 \leqslant x' \leqslant m$ 使得

$$f(X') = f_I(x', y, z) = P(x'+y, z)$$
$$= f_I(X) = f(x, y, z) = P(x+y, z),$$

用 x'、y、z 进行模拟，模拟器 S 工作过程如下：

首先，S 按照协议要求构造向量 $\boldsymbol{A}'$，

$$\boldsymbol{A}' = (\underbrace{1,\cdots,1}_{x'-1\text{个}}, \overset{1\cdots x'-1 \quad x' \quad x'+1\cdots 2m}{2}, \underbrace{3,\cdots,3}_{2m-x'\text{个}}).$$

加密 $\boldsymbol{A}'$ 得到

$$E(\boldsymbol{A}') = (E(a_1'), \cdots, E(a_{2m}')).$$

然后，S 根据 y 的值按照协议要求进行保密移位添加和重随机化操作，得到

$$E(\boldsymbol{C}') = (E(c_1'), \cdots, E(c_{2m}')).$$

最后，S 根据 z 的值选取 $E(\boldsymbol{C}')$ 中对应分量 $E(q')$，解密 $E(q')$ 得到

$$f_I(X') = f_I(x', y, z) = P(x'+y, z).$$

令

$$S(I,(y,z), f_I(X))$$
$$= \{I, y, r_2, E(\boldsymbol{A}'), z, r_3, E(\boldsymbol{C}'), f_I(X')\}.$$

因为 ElGamal 公钥系统是语义安全的概率加密方案，所以 $E(\boldsymbol{A})$ 与 $E(\boldsymbol{A}')$、$E(\boldsymbol{C})$ 与 $E(\boldsymbol{C}')$ 在计算上是不可区分的. 又因为 $f_I(X) = f_I(X')$，以及其他所有参数都是相等的，所以

$$\{S(I,(y,z), f_I(X))\}_{X \in (\{0,1\}^*)^n} \overset{c}{\equiv} \{view_I^{\Pi}(X)\}_{X \in (\{0,1\}^*)^n},$$

因此，协议 1 对于 x 是安全的.

(2) 由于 Alice 和 Bob（或 Carol）合谋的证明可以由(1)中的证明类似模拟得到，所以下面我们仅给出证明的思路. 由于 ElGamal 公钥系统是语义安全的，所以参与者在协议过程中所得的 $2m$ 个密文与 $2m$ 个随机数是计算不可区分的. 所获得的 *view* 与用满足谓词 $P(x+y, z)$ 的任意一组输入进行模拟所得到的信息序列也是计算不可区分的. 所以很容易得出结论：在 Bob 或 Carol 不参与合谋的情况下，协议 1 也是安全的，即协议对 Bob（或 Carol）的数据 y（或 z）也是安全的.

综上所述，协议 1 对于半诚实参与者是安全的，且可以抵抗任意数量的合谋攻击.

证毕.

4　四方盲百万富翁问题的解决方案

4.1　协议的基本原理

问题描述 2. 假设有四个参与者 Alice、Bob、Carol、Dove，他们各拥有一个私有数据 x、y、u、v. 其中 $1 \leqslant x, y, u, v \leqslant m$. Alice 和 Bob、Carol 和 Dove 分别为两组互不信任的合作方. 他们四人希望联合进行保密比较得出 $x+y$ 和 $u+v$ 之间的大小关系，但又不愿意泄露任何有关自己私有数据的信息.

编码方法 2. 由问题描述 2 可知，数据 x, y, u, v 的取值范围为 $[1, m]$，则 $2 \leqslant x+y \leqslant 2m$，$2-m \leqslant x+y-u \leqslant 2m-1$，即 $x, x+y, x+y-u$ 在 $-m$ 到 $2m$ 之间. 所以，可将 $x, x+y, x+y-u$ 转化为一个与其唯一对应的 $3m+1$ 维向量，向量的第 1 维到第 $3m+1$ 维依次代表 $-m$ 到 $2m$ 之间的所有整数. 其中，小于 $x, x+y, x+y-u$ 的数所对应的分量为 1，等于 $x, x+y, x+y-u$ 的数所对应的分量为 2，大于 $x, x+y, x+y-u$ 的数所对应的分量为 3.

又由于 $1 \leqslant v \leqslant m$，在下文原理描述 2 中 Dove 根据 v 进行分量选择时，不会使用到 $-m$ 到 -1 之间的数所对应的分量，所以可将向量维数减至 $2m+1$ 维. 以 x 为例，将其转化为向量 $\boldsymbol{A} = (a_1, \cdots, a_{2m+1})$，$a_1$ 到 a_{2m+1} 依次代表 0 到 $2m$ 之间的所有整数，其中，小于 x 的数所对应的分量为 1，等于 x 的数所对应的分量为 2，大于 x 的数所对应的分量为 3，即

$$a_i = \begin{cases} 1, \text{姑}\text{且}i < x+1; \\ 2, \text{姑}\text{且}i = x+1; \\ 3, \text{姑}\text{且}i > x+1. \end{cases}$$

原理描述 2. 因为 $x+y > u+v \Leftrightarrow x+y-u > v$，所以可以将判断 $x+y$ 和 $u+v$ 大小关系的问题转化为判断 $x+y-u$ 和 v 大小关系的问题. 具体的求解原理如下所述：

Alice 首先使用编码方法 2 构造一个 $2m+1$ 维向量 $\boldsymbol{A}=(a_1,\cdots,a_{2m+1})$，其中向量的前 x 个分量为 1，第 $x+1$ 个分量为 2，后 $2m-x$ 个分量为 3. x 编码为

$$\boldsymbol{A}=(\underbrace{1,\cdots,1}_{x\text{个}},2,\underbrace{3,\cdots,3}_{2m-x\text{个}})$$

Bob 根据自己私有数据 y 的值将向量 $\boldsymbol{A}$ 右移 y 位去掉 $\boldsymbol{A}$ 的后 y 个分量. 然后，在第一个分量前添加 y 个为 1 的分量，即

$$(\underbrace{1,\cdots,1}_{x\text{个}},2,\underbrace{3,\cdots,3}_{2m-x-y\text{个}})$$

$$\downarrow$$

$$(\underbrace{1,\cdots,1}_{y\text{个}},\underbrace{1,\cdots,1}_{x\text{个}},2,\underbrace{3,\cdots,3}_{2m-x-y\text{个}})$$

$$\downarrow$$

$$(\underbrace{1,\cdots,1}_{x+y\text{个}},2,\underbrace{3,\cdots,3}_{2m-x-y\text{个}})$$

经过移位添加操作后的向量分量总数仍为 $2m+1$ 个，但为 1 的分量数为 $x+y$ 个，即求得了 $x+y$. 为了叙述方便，将表示 $x+y$ 的向量记为 $\boldsymbol{C}$，则

$$\boldsymbol{C}=(\underbrace{1,\cdots,1}_{x+y\text{个}},2,\underbrace{3,\cdots,3}_{2m-x-y\text{个}}).$$

Carol 根据自己私有数据 u 的值将向量 $\boldsymbol{C}$ 左移 u 位去掉 $\boldsymbol{C}$ 的前 u 个分量. 然后，在最后一个分量后添加 u 个为 3 的分量，即

$$(\underbrace{1,\cdots,1}_{x+y-u\text{个}},2,\underbrace{3,\cdots,3}_{2m-x-y\text{个}})$$

$$\downarrow$$

$$(\underbrace{1,\cdots,1}_{x+y-u\text{个}},2,\underbrace{3,\cdots,3}_{2m-x-y\text{个}},\underbrace{3,\cdots,3}_{u\text{个}})$$

$$\downarrow$$

$$(\underbrace{1,\cdots,1}_{x+y-u\text{个}},2,\underbrace{3,\cdots,3}_{2m-x-y+u\text{个}})$$

经过移位添加操作后的向量分量总数仍为 $2m+1$ 个，但为 1 的分量数为 $x+y-u$ 个，即求得了 $x+y-u$. 为了叙述方便，将表示 $x+y-u$ 的向量记为 $\boldsymbol{D}$，则

$$\boldsymbol{D}=(\underbrace{1,\cdots,1}_{x+y-u\text{个}},2,\underbrace{3,\cdots,3}_{2m-x-y+u\text{个}}).$$

Dove 根据自己私有数据 v 的值，选择向量 $\boldsymbol{D}$ 的第 $v+1$ 个分量. 如果所选分量为 1，表示 $x+y-u>v$，即 $x+y>u+v$；如果所选分量为 2，表示 $x+y-u=v$，即 $x+y=u+v$；如果所选分量为 3，表示 $x+y-u<v$，即 $x+y<u+v$.

以上所述即为本文判断 $x+y$ 和 $u+v$ 大小关系的原理，其还可以用于判定 $x-u$ 与 $v-y$ 之间的大小关系，以及其它类似的四方数据做加减运算的比较问题，但需要使用加密系统实现协议的保密. 由于此方法不涉及任何同态性，利用具有自盲性的概率加密算法本身所具有的性质即可保证协议的安全性.

为了便于描述，定义判断数据 $x+y$ 和 $u+v$ 大小关系的二元谓词如下：

$$P(x+y,u+v)=\begin{cases}1, x+y>u+v;\\ 2, x+y=u+v;\\ 3, x+y<u+v.\end{cases}$$

例 2. 设 $x=2,y=3,u=5,v=1$，选取 $m=6$. Alice 按照编码方法 2 构造向量 $\boldsymbol{A}$ 如下：

$$\boldsymbol{A}=(\underbrace{1,1}_{2\text{个}},2,\underbrace{3,3,3,3,3,3,3,3,3,3}_{10\text{个}}).$$

Bob 将向量 A 右移 3 位去掉 A 的后 3 个分量后，在第一个分量前添加 3 个为 1 的分量，得到 $x+y$ 的和向量 $\boldsymbol{C}$：

$$\boldsymbol{C}=(\underbrace{1,1,1,1,1}_{5\text{个}},2,\underbrace{3,3,3,3,3,3,3}_{7\text{个}}).$$

Carol 将向量 $\boldsymbol{C}$ 左移 5 位去掉 $\boldsymbol{C}$ 的前 5 个分量后，在最后一个分量后添加 5 个为 3 的分量，得到 $x+y-u$ 的和向量 $\boldsymbol{D}$：

$$\boldsymbol{D}=(2,\underbrace{3,3,3,3,3,3,3,3,3,3,3,3}_{12\text{个}}).$$

Dove 选择向量 $\boldsymbol{D}$ 的第 2 个分量，该分量为 3，可得 $x+y<u+v$. 事实上，$x+y=5$ 显然小于 $u+v=6$.

4.2 协议设计

协议 2. 四方盲百万富翁问题的解决方案.

输入：Alice、Bob、Carol、Dove 分别输入数据 x,y,u,v.

输出：$P(x+y,u+v)$.

准备：Alice、Bob、Carol、Dove 首先选取 ElGamal 公钥系统的公开参数 g，p，然后分别选择各自的私钥 k_i，联合生成公钥：

$$h=\prod_{i=1}^{4}h_i \bmod p=g^{\sum_{i=1}^{4}k_i} \bmod p.$$

1. Alice 使用编码方法 2 将数据 x 转化为向量 $\boldsymbol{A}=(a_1,\cdots,a_{2m+1})$，加密 A 发送给 Bob，即将

$$E(\boldsymbol{A})=(E(a_1),\cdots,E(a_{2m+1})).$$

发送给 Bob.

2. 设 $y=j$，Bob 将 $E(\boldsymbol{A})$ 右移 j 位去掉后 j 个密文，重随机化后在密文 $E'(a_1)$ 前添加 j 个 1 的密

文，得到 $x+y$ 的密文. 记 $x+y=c$，Bob 将 $E(\boldsymbol{C})$ 发送给 Carol. $E(\boldsymbol{C})$ 每个分量的计算过程如下所示：

FOR　i=1　TO　$2m$+1
　　IF　$i \leqslant j$
　　$E(c_i) \leftarrow E(1)$
　　EISE
　　$E(c_i) \leftarrow E'(a_{i-j})$
END

3. 设 $u=t$，Carol 将 $E(\boldsymbol{C})$ 左移 t 位去掉前 t 个密文，重随机化后在密文 $E'(c_{2m+1})$ 后添加 t 个 3 的密文，得到 $x+y-u$ 的密文. 记 $x+y-u=d$，Bob 将 $E(\boldsymbol{D})$ 发送给 Dove. $E(\boldsymbol{D})$ 每个分量的计算过程如下所示：

FOR　i=1　TO　$2m$+1
　　IF　$i \leqslant 2m-t+1$
　　$E(d_i) \leftarrow E'(c_{t+i})$
　　EISE
　　$E(d_i) \leftarrow E(3)$
END

4. 设 $v=q$，Dove 选择 $E(\boldsymbol{D})$ 的第 $q+1$ 个分量，记为 $E(s)=(u,v)$.

5. Alice、Bob、Carol、Dove 分别计算 $w_i=v^{k_i} \bmod p$ 并公布，然后进一步计算解密得到

$$s=u\left[\prod_{i=1}^{4} w_i\right]^{-1} \bmod p.$$

如果 $s=1$，表示 $x+y>u+v$；如果 $s=2$，表示 $x+y=u+v$；如果 $s=3$，表示 $x+y<u+v$.

4.3　方案分析

正确性分析　本文协议 2 解决的是判断 $x+y$ 和 $u+v$ 大小关系的问题. 由原理描述 2 可知，本文将其转化为判断 $x+y-u$ 和 v 大小关系的问题进行解决.使用移位添加方法由 x 的编码 $\boldsymbol{A}$ 求解 $x+y-u$ 的编码 $\boldsymbol{D}$ 的正确性证明与 3.3 节正确性分析中所给出的证明类似，这里不再详细描述. 根据编码方法 2 可知，求得的 $x+y-u$ 的编码 $\boldsymbol{D}$ 一共有 $2m+1$ 个分量，d_1 到 d_{2m+1} 依次代表 0 到 $2m$ 之间的所有整数，小于 $x+y-u$ 的数所对应的分量为 1，等于 $x+y-u$ 的数所对应的分量为 2，大于 $x+y-u$ 的数所对应的分量为 3. $1 \leqslant v \leqslant m$，$\boldsymbol{D}$ 中第 $v+1$ 个分量代表 v. 如果该分量为 1，表示 $x+y>u+v$；如果该分量为 2，表示 $x+y=u+v$；如果该分量为 3，表示 $x+y<u+v$.

安全性分析　协议 2 的安全性是基于门限解密的 ElGamal 公钥系统的安全性的. 在计算过程中，Alice、Bob、Carol 和 Dove 四个人收或发的消息都处在密文状态下. Alice 仅发送编码的密文消息，Bob、Carol 和 Dove 三人无法通过所收到的密文获知任何的额外信息，原因与前面对协议 1 的分析相同. 协议 2 是使用 (4,4) 门限密码系统实现的，可以抵抗任意 3 个参与者的合谋攻击. 因为与协议 1 的证明过程类似，所以下面不再详细加以证明，只给出证明的思路.

定理 2. 协议 2 在半诚实模型下是安全的，且可以抵抗任意数量的合谋攻击.

由于 ElGamal 公钥系统是语义安全的，所以参与者在协议过程中所得的 $2m+1$ 个密文与 $2m+1$ 个随机数是计算不可区分的. 进而其所获得的 *view* 与用满足谓词 $P(x+y,u+v)$ 的任意一组输入进行模拟所得到的信息序列也是计算不可区分的. 所以，可以很容易的得出结论：协议 2 对 Alice、Bob、Carol 和 Dove 的数据 x、y、u、v 是安全的.

5　N 盲百万富翁问题的解决方案

5.1　协议的基本原理

问题描述 3.　假设有 n 个参与者 $P_1,\cdots,P_n$，他们每个人拥有两个保密数据 x_i、y_i，其中 $x_i,y_i \in \{0,1\}$. 他们希望合作判定 $\sum_{i=1}^{n} x_i$，$\sum_{i=1}^{n} y_i$ 之间的大小关系，且不泄露任何其它信息.

编码方法 3.　由问题描述 3 可知，数据 x_i,y_i 的取值为 0 或 1，则 $-j \leqslant \sum_{i=1}^{j} x_i - \sum_{i=1}^{j} y_i \leqslant j (j=1,\cdots,n-1)$，即 $\sum_{i=1}^{j}(x_i-y_i)(j=1,\cdots,n-1)$ 均在 $-n$ 到 n 之间. 进而，可以使用如下编码方法将 $\sum_{i=1}^{j}(x_i-y_i)$ 转化为一个与其唯一对应的 $2n+1$ 维向量. 以 x_1-y_1 为例，将其转化为向量 $\boldsymbol{A}=(a_1,\cdots,a_{2n+1})$，$a_1$ 到 a_{2n+1} 依次代表 $-n$ 到 n 之间的所有整数. 其中，小于 x_1-y_1 的数所对应的分量为 1，等于 x_1-y_1 的数所对应的分量为 2，大于 x_1-y_1 的数所对应的分量为 3，即

$$a_i=\begin{cases}1, \text{姑柾} i < n+x_1-y_1+1;\\ 2, \text{姑柾} i = n+x_1-y_1+1;\\ 3, \text{姑柾} i > n+x_1-y_1+1.\end{cases}$$

原理描述 3.　因为 $\sum_{i=1}^{n} x_i > \sum_{i=1}^{n} y_i \Leftrightarrow \sum_{i=1}^{n-1}(x_i-y_i) > y_n - x_n$，所以可以将判断 $\sum_{i=1}^{n} x_i$ 和 $\sum_{i=1}^{n} y_i$ 大小关系的问题转化为判断 $\sum_{i=1}^{n-1}(x_i-y_i)$ 与 y_n-x_n 大小关系的问题. 具体的求解原理如下所述:

P_1 首先使用编码方法 3 构造一个 $2n+1$ 维向量 $\boldsymbol{A}=(a_1,\cdots,a_{2n+1})$，其中向量的前 $n+x_1-y_1$ 个分量为 1，第 $n+x_1-y_1+1$ 个分量为 2，后 $n-x_1+y_1$ 个分量为 3. x_1-y_1 编码为

$$\boldsymbol{A}_1=(\underbrace{1,\cdots,1}_{n+x_1-y_1\text{个}},\ 2,\ \underbrace{3,\cdots,3}_{n-x_1+y_1\text{个}})$$

若要比较 $x_1+x_2+x_3$ 和 $y_1+y_2+y_3$ 之间的大小关系，首先，P_2 根据 x_2-y_2 的值对 $\boldsymbol{A}_1$ 进行相应的左移 $(x_2-y_2<0)$ 或右移 $(x_2-y_2>0)$ 操作得到 $x_1+x_2-(y_1+y_2)$ 的密文向量 $\boldsymbol{A}_2$(注：当 $x_2-y_2=0$ 时，不进行操作).

不失一般性地假设 $x_2-y_2>0$，具体的操作如下：

P_2 根据 x_2-y_2 的值将向量 $\boldsymbol{A}_1$ 右移 x_2-y_2 位去掉 $\boldsymbol{A}_1$ 的后 x_2-y_2 个分量，然后，在第一个分量前添加 x_2-y_2 个为 1 的分量，即

$$(\underbrace{1,\cdots,1}_{n+x_1-y_1\text{个}},\ 2,\ \underbrace{3,\cdots,3}_{n-x_1+y_1-x_2+y_2\text{个}})$$

$$\downarrow$$

$$(\underbrace{1,\cdots,1}_{x_2-y_2\text{个}},\underbrace{1,\cdots,1}_{n+x_1-y_1\text{个}},2,\underbrace{3,\cdots,3}_{n-x_1+y_1-x_2+y_2\text{个}})$$

$$\downarrow$$

$$(\underbrace{1,\cdots,1}_{n+x_1+x_2-y_1-y_2\text{个}},\ 2\ ,\ \underbrace{3,\cdots,3}_{n-x_1-x_2+y_1+y_2\text{个}})$$

经过移位添加操作后的向量分量总数仍为 $2n+1$个，但为 1 的分量数为 $n+(x_1+x_2-(y_1+y_2))$ 个，即求得了 $x_1+x_2-(y_1+y_2)$. 为了叙述方便，将表示 $x_1+x_2-(y_1+y_2)$ 的向量记为 $\boldsymbol{A}_2$.

P_3 根据 y_3-x_3 的值选择向量 $\boldsymbol{A}_2$ 的对应分量即可得出 $x_1+x_2+x_3$ 和 $y_1+y_2+y_3$ 之间的大小关系. $y_3-x_3\in\{-1,0,1\}$，$\boldsymbol{A}_2$ 中第 $n+1+y_3-x_3$ 个分量代表 y_3-x_3. 如果该分量为 1，可得 $x_1+x_2-(y_1+y_2)>y_3-x_3$，即 $x_1+x_2+x_3>y_1+y_2+y_3$；如果该分量为 2，可得 $x_1+x_2-(y_1+y_2)=y_3-x_3$，即 $x_1+x_2+x_3=y_1+y_2+y_3$；如果该分量为 3，可得 $x_1+x_2-(y_1+y_2)<y_3-x_3$，即 $x_1+x_2+x_3<y_1+y_2+y_3$.

依次类推，想要比较 $x_1+\cdots+x_i$ 和 $y_1+\cdots+y_i$ 之间的大小关系，只需要参与者 $P_j(j\in\{2,\cdots,i-1\})$ 按照要求进行相应的移位添加操作后，将 $\boldsymbol{A}_j$ 发送给 P_{j+1}. 最后，由 P_i 根据 y_i-x_i 的值选择向量 $\boldsymbol{A}_{i-1}$ 的对应分量即可得出 $\sum_{j=1}^{i}x_j$ 和 $\sum_{j=1}^{i}y_j$ 之间的大小关系.

以上所述即为本文判断 $\sum_{i=1}^{n}x_i$ 和 $\sum_{i=1}^{n}y_i$ 大小关系的原理，但还需要使用加密算法实现协议的保密性. 由于此方法不涉及任何同态性，利用具有自盲性的概率加密算法本身所具有的性质即可保证协议的安全性.

为了便于描述，令 $U=\sum_{i=1}^{n}x_i,V=\sum_{i=1}^{n}y_i$. 定义判断数据 U 和 V 大小关系的二元谓词如下：

$$P(U,V)=\begin{cases}1,U>V;\\2,U=V;\\3,U<V.\end{cases}$$

例 3. 选取 $n=4$，设 $x_1=1,y_1=1,x_2=1,y_2=0,x_3=0,y_3=1,x_4=0,y_4=0$. P_1 按照编码方法 3 构造向量 $\boldsymbol{A}_1$ 如下:

$$\boldsymbol{A}_1=(\underbrace{1,1,1,1}_{4\text{个}},2,\underbrace{3,3,3,3}_{4\text{个}}).$$

$x_2-y_2=1>0$，P_2 先将向量 $\boldsymbol{A}_1$ 右移 1 位去掉 $\boldsymbol{A}_1$ 的最后一个分量. 然后，在第一个分量前添加 1 个为 1 的分量，得到 $x_1+x_1-(y_1+y_2)$ 的和向量 $\boldsymbol{A}_2$:

$$\boldsymbol{A}_2=(\underbrace{1,1,1,1,1}_{5\text{个}},2,\underbrace{3,3,3}_{3\text{个}}).$$

$x_3-y_3=-1<0$，P_3 先将向量 $\boldsymbol{A}_2$ 左移 1 位去掉 $\boldsymbol{A}_2$ 的第一个分量. 然后，在最后一个分量后添加 1 个为 3 的分量，得到 $x_1+x_2+x_3-(y_1+y_2+y_3)$ 的和向量 $\boldsymbol{A}_3$:

$$\boldsymbol{A}_3=(\underbrace{1,1,1,1}_{4\text{个}},2,\underbrace{3,3,3,3}_{4\text{个}}).$$

$x_4-y_4=0$，则 P_4 选择向量 $\boldsymbol{A}_3$ 的第 5 个分量，该分量为 2，可得 $\sum_{i=1}^{4}x_i=\sum_{i=1}^{4}y_i$. 事实上，$\sum_{i=1}^{4}x_i=\sum_{i=1}^{4}y_i=2$.

5.2 协议设计

协议 3. N 方盲百万富翁问题的解决方案.

输入：n 个参与者 P_i 分别输入各自的保密数据 x_i,y_i.

输出：$P(U,V)$.

准备：$P_1,\cdots,P_n$ 首先选取 ElGamal 公钥系统的公开参数 g，p，每个参与者 P_i 选择各自的私钥 k_i，联合生成公钥:

$$h=\prod_{i=1}^{n}h_i\ mod\ p=g^{\sum_{i=1}^{n}k_i}\ mod\ p.$$

1. P_1 使用编码方法 3 将数据 x_1-y_1 转化为向量 $\boldsymbol{A}_1=(a_{11},\cdots,a_{1(2n+1)})$，加密 $\boldsymbol{A}_1$ 发送给 P_2，即将

$$E(\boldsymbol{A}_1)=(E(a_{11}),\cdots,E(a_{1(2n+1)})).$$

发送给 P_2.

2. 对于每个 $j\in[2,n-1]$，参与者 P_j 操作如下：

设 $x_j-y_j=k(k>0)$，则 P_j 将 $E(\boldsymbol{A}_{j-1})$ 右移 k 位去掉后 k 个密文，重随机化后在密文 $E'(a_{(j-1)1})$ 前添加 k 个 1 的密文，得到表示 $\sum_{i=1}^{j}(x_i-y_i)$ 的密文向量 A_j，P_j 将 $E(\boldsymbol{A}_j)$ 发送给 P_{j+1}. $E(\boldsymbol{A}_j)$ 每个分量的计算过程如下所示:

FOR i=1 TO $2n$+1

IF $i\leqslant k$

$E(a_{ji})\leftarrow E(1)$

EISE

$$E(a_{ji}) \leftarrow E'(a_{(j-1)(i-k)})$$

END

3. P_n 选择 $E(\boldsymbol{A}_n)$ 的第 $n+1+y_n-x_n$ 个分量，记为 $E(q)=(u,v)$.

4. n 个参与者 $P_1,\cdots,P_n$ 分别计算 $w_i=v^{k_i} \bmod p$ 并公布，然后进一步计算得到得到

$$q=u\left[\prod_{i=1}^{n} w_i\right]^{-1} \bmod p.$$

如果 $q=1$，则表示 $U>V$，即 $\sum_{i=1}^{n}x_i>\sum_{i=1}^{n}y_i$；如果 $q=2$，则表示 $U=V$，即 $\sum_{i=1}^{n}x_i=\sum_{i=1}^{n}y_i$；如果 $q=3$，则表示 $U<V$，即 $\sum_{i=1}^{n}x_i<\sum_{i=1}^{n}y_i$.

5.3　方案分析

正确性分析 本文协议 3 解决的是判断 $\sum_{i=1}^{n}x_i$ 和 $\sum_{i=1}^{n}y_i$ 大小关系的问题. 由原理描述 3 可知，本文将该问题转化为判断 $\sum_{i=1}^{n-1}(x_i-y_i)$ 与 y_n-x_n 大小关系的问题进行解决. 使用移位添加方法由 x_1-y_1 的编码 $\boldsymbol{A}_1$ 求解 $\sum_{i=1}^{n-1}(x_i-y_i)$ 编码 $\boldsymbol{A}_{n-1}$ 的正确性证明与 3.3 节正确性分析中所给出的证明类似，这里不再详细描述. 根据编码方法 3 可知，求得的 $\sum_{i=1}^{n-1}(x_i-y_i)$ 的编码 $\boldsymbol{A}_{n-1}$ 一共有 $2n+1$ 个分量，$a_{(n-1)1}$ 到 $a_{(n-1)(2n+1)}$ 依次代表 $-n$ 到 n 之间的所有整数，小于 $\sum_{i=1}^{n-1}(x_i-y_i)$ 的数所对应的分量为 1，等于 $\sum_{i=1}^{n-1}(x_i-y_i)$ 的数所对应的分量为 2，大于 $\sum_{i=1}^{n-1}(x_i-y_i)$ 的数所对应的分量为 3. $y_n-x_n\in\{-1,0,1\}$，$\boldsymbol{A}_{n-1}$ 中第 $n+1+y_n-x_n$ 个分量代表 y_n-x_n. 若该分量为 1，表示 $\sum_{i=1}^{n}x_i>\sum_{i=1}^{n}y_i$；若该分量为 2，表示 $\sum_{i=1}^{n}x_i=\sum_{i=1}^{n}y_i$；若该分量为 3，表示 $\sum_{i=1}^{n}x_i<\sum_{i=1}^{n}y_i$.

安全性分析 协议 3 的安全性是基于门限解密的 ElGamal 公钥系统的安全性的. 在计算过程中，$P_1,\cdots,P_n$ 收或发的消息都处在密文状态下. P_1 仅发送编码的密文消息，$P_2,\cdots,P_n$ 无法通过所收到的密文获知任何的额外信息，原因与协议 1 的原因相同. 协议 3 是使用 (n,n) 门限密码系统实现的，可以抵抗任意 $n-1$ 个参与者的合谋攻击. 因为证明过程与协议 1 类似，所以这里不再详细加以证明，只给出定理的描述.

定理 3. 协议 3 在半诚实模型下是安全的，且可以抵抗任意数量的合谋攻击.

6　效率分析与比较

文献[24]中的子协议 SLT 协议解决的是密文比较大小问题，又由于其使用的是 Paillier 公钥系统，可以使用加法同态性解决求和问题，是我们已知最接近本文所研究的盲百万富翁问题的文献，故本文将其作为重要的参考与所设计的协议进行比较分析.

本节中我们首先对协议 1、协议 2 和协议 3 的效率进行详细分析，然后将本文的协议 3 与使用文献[24]的 SLT 协议所实现的解决方案进行全面比较.

6.1　协议效率分析

在对一个方案进行效率分析时，一般从计算复杂性和通信复杂性两个角度出发.

在衡量计算复杂性时，因为模指数运算的复杂性比其他运算的复杂性高很多（例如：用比特复杂性来衡量，模指数运算的计算复杂性为 $O(\lg^3 n)$，运用欧几里得扩展算法求逆的计算复杂性为 $O(\lg^2 n)$），所以我们通常忽略协议执行中所需的其他计算开销，只考虑计算代价最高的模指数运算次数.

计算复杂性 协议 1 所涉及的数据范围在 1 到 $2m$ 之间. 三个参与者合作产生公钥共需要 3 次模指数运算. 加密过程中三个参与者最多需要 $8m$ 次模指数运算，解密过程需要 3 次模指数运算. 所以，协议 1 最多需要 $8m+6$ 次模指数运算.

协议 2 所涉及的数据范围在 0 到 $2m$ 之间. 四个参与者合作产生公钥共需要 4 次模指数运算. 加密过程中四个参与者最多需要 $12m+6$ 次模指数运算，解密过程需要 4 次模指数运算. 所以，协议 2 最多需要 $12m+14$ 次模指数运算.

协议 3 所涉及的数据范围在 $-n$ 到 n 之间. n 个参与者合作产生公钥共需要 n 次模指数运算. 加密过程中 n 个参与者最多需要 $4n^2-2n-2$ 次模指数运算，解密过程需要 $2n$ 次模指数运算. 所以，协议 3 最多需要 $4n^2+n-2$ 次模指数运算.

研究人员通常使用通信次数或交换信息的比特数衡量通信复杂性，但随着计算机技术的不断发展，一次交换信息的比特数不再是限制通信的重要指标. 因此，现在通常使用通信次数来衡量通信复杂性.

通信复杂性 在协议 1 中，三个参与者共同构造公钥、加密过程和解密过程各需要 3 次通信，所以共需要 9 次通信；在协议 2 中，四个参与者共同构造公钥、加密过程和解密过程各需要 4 次通信，所以共需要 12 次通信；在协议 3 中，n 个参与者共同构造公钥、加密过程和解密过程各需要 n 次通信，所以共需要 $3n$ 次通信.

与文献[24]的比较 文献[24]中的 SLT 协议可以解决两个密文比较大小的问题，但难于构造抵抗合谋攻击的协议，而本文的协议 3 能够抵抗合谋攻击. 由于不同安全级别的协议不具备可比性，所以本文

的协议 3 也不考虑合谋攻击. 当不考虑合谋攻击时，协议 3 只需要加密系统具有概率加密和密文的自盲性这两个性质，使用 Goldwasser-Micali(GM)公钥系统即可实现协议 3. 为了便于描述，我们将使用文献[24]的 SLT 协议所实现的盲百万富翁问题的解决方案命名为 ESLT 协议(Extended Secure Less than Protocol).

设定两个协议中参与者人数为 n. 使用 GM 公钥系统实现协议 3 时，需要对编码方法 3 进行微小的调整. 具体地，以 x_1-y_1 为例，将其转化为向量 $\boldsymbol{A}=(a_1,\cdots,a_{2n+1})$，其中

$$a_i=\begin{cases}0, & \text{若}\ i\leqslant n+x_1-y_1+1;\\ 1, & \text{若}\ i>n+x_1-y_1+1.\end{cases}$$

在 ESLT 协议中，参与者首先利用 Paillier 公钥系统的加法同态性求得 $E(\sum_{i=1}^{n}x_i)$ 和 $E(\sum_{i=1}^{n}y_i)$，然后调用 SLT 协议比较 $E(\sum_{i=1}^{n}x_i)$ 和 $E(\sum_{i=1}^{n}y_i)$ 的大小得出 $\sum_{i=1}^{n}x_i$ 和 $\sum_{i=1}^{n}y_i$ 的大小关系.

因为 GM 公钥系统加解密进行模乘运算，Paillier 公钥系统加解密进行模指数运算. 模乘运算的复杂性远远低于模指数运算的复杂性，当有模指数运算时，模乘运算的复杂性可以忽略不计. 所以，本文所设计的协议 3 比 ESLT 协议的计算复杂性低. 通信复杂性方面，本文的协议 3 与 ESLT 协议所需的通信次数都为 n 次.

综上所述，与 ESLT 协议相比本文所设计的协议 3 效率更高. 具体的计算复杂性和通信复杂性的比较如表 1 所示.

表 1 计算复杂性和通信复杂性的比较

	模指数运算	模乘运算	通信次数
协议 3	–	$4n^2-2n-2+\log p$	n
ESLT 协议	$2n+1$	$n-1$	n

6.2 实验数据分析

为了更直观、清晰地展现本文所设计方案的效率以及与文献[24]的比较情况，本文使用 Java 语言编程进行了两个模拟实验.

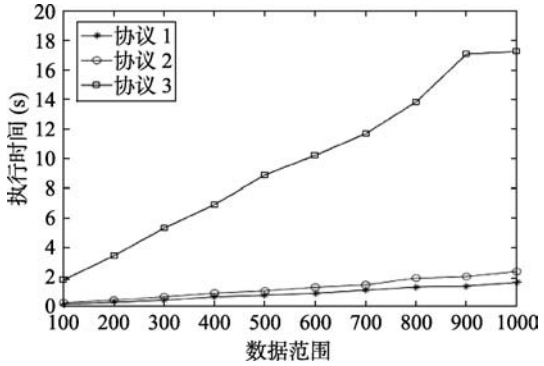
实验测试环境 Windows 10 家庭版，64 位操作系统，Intel(R)Core(TM)i5-6600 处理器 CPU @ 3.31 GHz，8.00GB 内存，用 Java 语言在 MyEclipse 上运行实现. 本文所做模拟实验均在此环境下进行.

实验 1 测试本文所设计协议的实际可行性，实验中每个参与者所持有的数据为 100 到 1000 以内的整数，设定协议 3 中的参与者人数 $n=25$. 忽略预处理时间，使用门限解密的 ElGamal 公钥系统进行模拟.

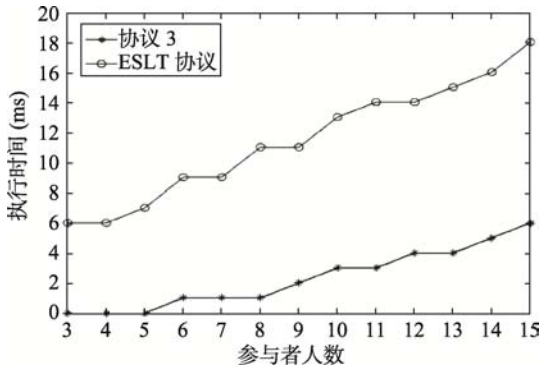
实验 2 比较在参与者不合谋情况下协议 3 与 ESLT 协议的效率，设定参与者人数为 $n\in\{3,4,\cdots,15\}$. 为使实验数据更准确，对 n 的每个参数进行 1000 次模拟测试，计算协议执行时间的算术平均值. 忽略预处理时间，协议 3 使用 GM 公钥系统进行模拟，ESLT 协议使用 Paillier 公钥系统进行模拟.

实验结果 实验 1 结果如图 1 所示. 由图 1 可知，协议的执行时间随数据范围增长基本上呈线性增加. 值得注意的是，在此次实验中，三个协议使用的都是门限解密的 ElGamal 公钥系统，如果选用效率更高的门限解密系统，协议的效率会更高.

实验 2 结果如图 2 所示. 由图 2 可得，协议 3 比 ESLT 协议的效率高.



坚 1 厥谊 1、2、3 拣祆晒限雩旌掘荟坐壶闼盏吴卲剖忧



坚 2 厥谊 3 哨 ESLT 厥谊拣祆晒限雩吞虺聪佞旌壶闼盏吴卲剖忧

7 结 论

本文首先对百万富翁问题进行了拓展，提出了新的安全多方计算问题：盲百万富翁问题. 为了解决该问题，我们利用概率加密方案的性质和移位寄存器的思想设计了新的保密移位添加方法. 然后，结合适当的编码方法构造了三个不同的盲百万富翁问题的解决方案. 三个协议在半诚实模型下都是安

全的，可以抵抗任意数量的合谋攻击. 今后我们将在本文研究的基础上考虑更高效、更普遍的解决方案，并尝试设计恶意模型下盲百万富翁问题的解决方案.

参 考 文 献

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

[2] Orlandi C. Is multiparty computation any good in practice? //Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing. Prague, Czech Republic, 2011: 5848-5851

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

[4] Goldreich O. The fundamental of cryptography: basic applications. London, UK: Cambridge University Press, 2004

[5] Fagin R, Naor M, Winklery P. Comparing information without leaking it. Communications of the ACM, 1996, 39(5): 77-85

[6] Freedman M J, Nissim K, Pinkas B. Efficient private matching and set intersection//Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Interlaken, Switzerland, 2004: 1-19

[7] Kissner L, Song D. Privacy-preserving set operations// Proceedings of the 25th Annual International Cryptology Conference. California, USA, 2005: 241-257

[8] Beimel A, Gabizon A, Ishai Y, et al. Non-interactive secure multiparty computation//Proceedings of the 34th Annual Cryptology Conference. California, USA, 2014: 387-404

[9] Dou J W, Gong L M, Li S D, et al. Efficient private subset computation. Security and Communication Networks, 2016, 9(18): 5965-5976

[10] Samanthula B K, Jiang W. Secure multiset intersection cardinality and its application to Jaccard coefficient. IEEE Transactions on Dependable and Secure Computing, 2016, 13(5): 591-604

[11] Yang X Y, Li S D, Kang J. Private substitution and its applications in private scientific computation. Chinese Journal of Computers, 2018, 425(5): 166-176 (in Chinese)
(杨晓艺, 李顺东, 亢佳. 保密替换及其在保密科学计算中的应用. 计算机学报, 2018, 425(5): 166-176)

[12] Qin J, Zhang Z F, Feng D G, et al. A protocol of comparing information without leaking. Journal of Software, 2004, 15(3): 421-427(in Chinese)
(秦静, 张振峰, 冯登国, 等. 无信息泄漏的比较协议. 软件学报, 2004, 15(3): 421-427)

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

[14] Zhong H, Tian L, Shi R．An efficient and fair private comparison protocol based on range encoding．Journal of Computational Information Systems, 2013, 9(1): 231-240

[15] Lin H Y, Tzeng W G. An efficient solution to the millionaires' problem based on homomorphic encryption//Proceedings of the third International Conference. New York, USA, 2005: 456–466

[16] Li S D, Wang D S. Efficient secure multiparty computation based on homomorphic encryption. Chinese Journal of Electronics, 2013, 41 (4): 798-803(in Chinese)
(李顺东, 王道顺. 基于同态加密的高效多方保密计算. 电子学报, 2013, 41(4): 798-803)

[17] Liu M, Nanda P, Zhang X, et al. Asymmetric commutative encryption scheme based efficient solution to the millionaires' problem//Proceedings of the 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications. New York, USA, 2018: 990-995

[18] Li S D, Guo Y M, Zhou S F, et al. Efficient protocols for the general millionaires' problem. Chinese Journal of Electronics, 2017, 26(4): 696-702

[19] Bessonov M, Grigoriev D, Shpilrain V. Probabilistic solution of Yao's millionaires' problem. IACR Cryptology ePrint Archive, 2017, 2017: 1129

[20] Hibiki O, Yoshifumi M. Efficient card-based cryptographic protocols for the millionaires' problem using private input operations//Proceedings of the 13th Asia Joint Conference on Information Security. Guilin, China, 2018: 23-28

[21] Atallah M J, Du W. Secure multi-party computational geometry//Proceedings of the 7th International Workshop. Providence, USA, 2001: 165-179

[22] Liu W, Luo S S, Wang Y B, et al. A protocol of secure multi-party multi-data ranking and its application in privacy preserving sequential pattern mining//Proceedings of the Fourth International Joint Conference on Computational Sciences and Optimization. Yunnan, China, 2011: 272-275

[23] Li S D, Kang J, Yang X Y, et al. Secure multiparty characters sorting. Chinese Journal of Computers, 2018(5): 1173-1188(in Chinese)
(李顺东, 亢佳, 杨晓艺, 等. 多个字符排序的安全多方计算. 计算机学报, 2018(5): 1173-1188)

[24] Liu X, Choo R, Deng R, et al. Efficient and privacy-preserving outsourced calculation of rational numbers. IEEE Transactions on Dependable and Secure Computing, 2018, 15(1): 27-39

[25] Goldwasser S, Micali S. Probabilistic encryption. Journal of Computer and System Sciences, 1984, 28(2): 270-299

[26] Desmedt Y, Frankel Y. Threshold cryptosystems//Proceedings of the 9th Annual International Cryptology Conference. California, USA, 1989: 307-315

[27] Long Y, Chen K, Mao X. New constructions of dynamic threshold cryptosystem. Journal of Shanghai Jiaotong University (Science), 2014, 19(4): 431-435

[28] Gamal T E. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 1985, 31(4): 469-472

[29] Paillier P. Public-key cryptosystems based on composite degree residuosity classes//Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Prague, Czech Republic, 1999: 223-238

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

ZHANG Meng-Yu, M.S. candidate. Her main research interests include modern cryptography and information security.

Background

Diffie and Hellman's paper, *New Directions in Cryptography*, opens up the study of public key cryptography. Since then, researchers have proposed many research directions based on public key cryptography. Among them, SMC is a key area of public key cryptography, and its goal is to enable participants to perform joint computing while ensuring that participants input privately.

The millionaires' problem is the first problem in secure multiparty computation and a fundamental problem in secure scientific computing. It studies how two parties, Alice and Bob with private numbers x and y, respectively to determine which one is bigger without disclosing any other information. The researchers propose many effective solutions and generalize a series of new secure multiparty computing problems, such as: secure vector dominance problem, maximum (minimum) value problem, sorting problem, and so on. This paper presents a new extended millionaires' problem: Alice, Bob, Carol, and Dave have private numbers x, y, u and v respectively and they want to determine the relation between $x+y$ and $u+v$ without disclo- sing x, y, u, v. No party knows the value of $x+y$, $u+v$ in this scenario. We call this problem the blind millionaires' problem, which has wide application in business cooperation, evaluation system and so on. It is of important theoretical and practical significance.

At present, there is no research based on this problem. To solve this problem, we first propose a method named secret shifts adding method. This method can be used to privately add, subtract and multiply in small domain. There is no limit to the number of participants, and further computation can be made. Based on the secret shift adding method, combining with threshold decryption probabilistic cryptosystem and appropriate encoding scheme, we design secure comparison protocols for three comparing problems in small domain. The first protocol applies to three participants for joint computation, each of which has positive integers. Addition and comparison are impl- emented in the protocol. The second protocol applies to the joint computation of four participants, each of which owns a positive integer. Addition, subtraction and comparison are implemented in the protocol. The third protocol applies to the joint computation of multiple participants, each of which has two data points of 0 or 1. Addition, subtraction, and comparison are implemented in the protocol. All three protocols can correctly output the computing results without disclosing the participant's private data.

The blind millionaires' problem is a new problem first proposed and solved in this paper. We have been conducting research in SMC for more than ten years and continue to study. Our work is supported by the National Natural Science Foundation of China (No. 61272435).