

doi: 10.3969/j.issn.1007-7162.2014.03.004

大数据环境下跨组织间协同优化决策的隐私保护算法

刘洪伟, 刘智慧, 朱 慧, 陆 涛
(广东工业大学 管理学院, 广东 广州 510520)

摘要: 组织协同决策分析的数据具有大数据的分布性、异构性和隐私性等典型特征。安全多方计算是一种基于协同机制或协议的隐私保护算法,但它一些常用的单调张成等方法却无法挣脱计算复杂性的困扰。本文主要研究组织间两种结构的协同优化决策问题,提出针对决策变量与约束参数隐私保护的安全多方计算协议,并给出相对应的安全证明。研究表明对于本文构造的 SMC 协议,可以降低优化协同决策的计算复杂度,部分隐私信息无须加工传送也可以完成计算任务。

关键词: 大数据; 协同优化; 隐私保护; 安全多方计算

中图分类号: TP309.2; F224.31; F490.5

文献标志码: A

文章编号: 1007-7162(2014)03-0021-06

Privacy-preserving Algorithm for Cross-organizational Collaborative Optimization Decisions Based on Big Data

Liu Hong-wei, Liu Zhi-hui, Zhu Hui, Lu Tao

(School of Management, Guangdong University of Technology, Guangzhou 510520, China)

Abstract: The cross-organizational data has the typical characteristics of big data in collaborative optimization decision-making, such as distributedness, heterogeneity, and privacy etc. Secure multi-party computation (SMC) is a privacy-preserving algorithm, based on collaborative mechanisms or protocols. However, the methods typically used, such as monotone span program, cannot get rid of the computational complexity. It discussed two kinds of problems in collaborative optimization decision, and proposed secure multi-party computation protocols for the privacy-preserving of constraint parameters and decision variables. Then, it gave security proof. The results show that the SMC protocols can reduce the computational complexity of collaborative optimization decisions, and computation of some private information can be completed without transferred processing.

Key words: big data; collaborative optimization; privacy-preserving; secure multi-party computation

组织之间的协同管理决策就是利用各组织甚至个人的信息,协同制订全局优化决策问题的解决方案。然而组织间的管理或运营数据,不仅仅存在分布性、异构性等大数据的特点,关键还涉及到众多组织不愿意公开的信息,通常称这类信息为“隐私信息”^[1]。如何保护好各自的隐私信息,又能完成协同决策问题,是大数据时代典型的组织协同优化决策问题的重要难题。

在供应链管理中,有联合库存管理(JMI)问题,

产能约束下多个零部件的协同决策问题等等^[2-4]。但在联合优化决策时,无论是目标函数还是约束条件,可能需要使用到不同组织间的数据,如上下游企业或合同企业的资金、人员、生产能力与库存情况等。在供应链的上下游企业中并不愿意提供本组织内的真实数据给对方,也不愿意将数据交给所谓的“可信”第三方进行计算,因此,如何设计一个“好的”的协同分析机制,在不泄露原始数据的前提下,去完成协同优化决策问题。这就是保护组织隐私数

收稿日期: 2014-06-30

基金项目: 国家自然科学基金资助项目(70971027); 广东省哲学社会科学规划项目(GD10YGL09); 广东省普通高校人文社会科学重点研究项目(12ZS0112)

作者简介: 刘洪伟(1962-),男,教授,博士生导师,主要研究方向为管理信息系统、系统工程。

据的协同决策问题^[1].

安全多方计算(Secure Multi-party Computation, 以下简称 SMC)是目前解决大数据环境下这一类隐私保护计算问题的方法之一^[2]. 安全多方计算这个概念最早是由图灵奖获得者 Yao A C^[3]于1982年提出的,即广为人知的百万富翁问题. Goldreich、Micali 和 Wigderson 将其理论扩展,给出了一般的描述^[4]. 由于安全多方计算具有广泛的应用前景,目前许多国内外专家都致力于安全多方计算的研究. 人们都知道在 SMC 理论上,最有名的构造方法就是单调张成方法^[5],它是通过存取结构(Access Structure)来给出安全多方协议的通用构造矩阵,然而在实际应用时,该方法有着明显的缺点,就是计算复杂度太高,以至于实际应用时难以按这一思路来设计合作机制. 因此近年来学者针对不同的应用提出各种具体构造安全多方协议的方法,如 Du 对科学计算问题就提出了一些高效的安全多方协议,但是科学计算问题的结构是无穷的, Du 的方法目前对简单的线性方程是有效的,对于其他系统,如动态系统、优化问题等就未必有效了^[6]. 在国内,比较多的研究是针对供应链上的协同计算问题来研究,如供应链的订货管理^[7],但该文只是针对一个成本函数来分析,没有考虑约束,因此,在得到成本函数的解析解后,再使用同态加密算法,这样处理方法还相对容易,加上同态算法的复杂度较高,使得实际效率不高.

在本文中,主要对组织间的决策机制分为异构与同构两种情况,并分别研究两种情况下的安全多方计算协议,及对它们的安全性给出证明.

1 基本概念与问题的提出

1.1 半诚实模型下的安全性定义

本节给出了半诚实模型下的两方计算的安全性定义^[8],多方计算的安全性定义可以类推.

在半诚实模型中,一个半诚实参与方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 $f: \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^* \times \{0,1\}^*$ 是一个函数, $f_1(x, y)$ 和 $f_2(x, y)$ 分别代表函数 $f(x, y)$ 的第一个和第二个元素. Π 是计算函数 f 的两方协议. 协议的输入 (x, y) , 执行协议 Π 时,参与方 p_1 (p_2) 得到的信息记作

$$\text{VIEW}_1^\Pi(x, y) = (x, r^1, m_1^1, \dots, m_l^1) \quad (\text{VIEW}_2^\Pi(x, y) = (x, r^2, m_1^2, \dots,$$

$$m_l^2)),$$

其中 r^i ($i = 1, 2$) 是参与方 p_i 产生的随机数, m_i^1 (m_i^2) 是参与方 p_1 (p_2) 接收到的第 i 个消息. $\text{OUTPUT}_i^\Pi(x, y)$ ($i = 1, 2$) 表示 p_i 方的输出结果,显然它是 $\text{VIEW}_i^\Pi(x, y)$ 的一部分.

定义1 若存在多项式时间算法 S_1 与 S_2 使得下面两个公式成立,则 π 能保密地计算 f .

$$\{(S_1(x, f_1(x, y)), f_2(x, y))\}_{x, y \in \{0,1\}^*} \stackrel{c}{=} \{(\text{VIEW}_1^\Pi(x, y), \text{OUTPUT}_2^\Pi(x, y))\}_{x, y \in \{0,1\}^*}, \quad (1)$$

$$\{(f_1(x, y), S_2(y, f_2(x, y)))\}_{x, y \in \{0,1\}^*} \stackrel{c}{=} \{(\text{OUTPUT}_1^\Pi(x, y), \text{VIEW}_2^\Pi(x, y))\}_{x, y \in \{0,1\}^*}, \quad (2)$$

其中, $\stackrel{c}{=}$ 表示计算不可区分,而且 $\text{VIEW}_1^\Pi(x, y)$ 和 $\text{VIEW}_2^\Pi(x, y)$, $\text{OUTPUT}_1^\Pi(x, y)$ 和 $\text{OUTPUT}_2^\Pi(x, y)$ 是相关的随机变量.

1.2 同态加密

同态加密的概念是由 Rivest、Adleman 和 Demoullins 于 1978 年提出的. 同态加密的特殊性质使我们可以直接对密文进行某些运算来代替对明文的运算取得同样的效果,这样不影响明文数据的机密性. Paillier 算法就是一种同态加密算法^[9],它有两个重要的性质:

$$(1) \quad E(m_1) \oplus E(m_2) = g^{m_1+m_2} (r_1 r_2)^N \bmod N^2 = E(m_1 + m_2);$$

$$(2) \quad E(m_1)^{m_2} = g^{m_1 m_2} (r^{m_2})^N \bmod N^2 = E(m_1 m_2).$$

1.3 协同优化决策的模型

本文主要针对大数据环境下的优化问题来研究各合作方的安全多方计算问题:

$$\begin{cases} \text{opt } \xi = g(z), \\ \text{s. t. } f(z) = 0. \end{cases} \quad (3)$$

下面给出协同优化决策时两类优化问题的安全多方计算问题.

1.3.1 决策变量同构时的优化决策问题

设参与协同决策的决策方分别是 $P_1, P_2, \dots, P_n$, 共同求解以下问题:

$$\begin{cases} \text{opt } \xi = g(z, c), \\ \text{s. t. } f(z, \alpha_1, \alpha_2, \dots, \alpha_n) = 0. \end{cases} \quad (4)$$

隐私假设:

- (1) 决策变量是各方共享的;
- (2) α_i 是 P_i 的隐私参数;
- (3) 目标函数的参数 c 是共享的.

1.3.2 决策变量异构时的优化决策问题

设参与方仍是 P_i ($i = 1, 2, \dots, n$), 优化问题的结构如下:

$$\left. \begin{aligned} \text{opt } \xi &= g(z_1, z_2, \dots, z_n, c), \\ \text{s. t. } f(z_i, \alpha_i) &= 0 \quad i = 1, 2, \dots, n. \end{aligned} \right\} \quad (5)$$

隐私假设:

- (1) z_i 是 P_i 的隐私决策变量;
- (2) α_i 是 P_i 的隐私参数;
- (3) 目标函数的参数 c 是共享的.

本文的后半部分将对以上两类问题的安全多方计算问题进行分析,并结合安全性证明.

2 约束同构时安全多方计算

2.1 模型与假设

本节研究在半诚实模型下的约束同构的线性优化问题(本文只考虑存在最优解的安全多方计算,后面的计算亦是如此),其数学模型如下:

$$\left. \begin{aligned} \max \xi &= C^T X, \\ \text{s. t. } \begin{cases} (A_1^T, A_2^T, \dots, A_n^T)^T X = (b_1^T, b_2^T, \dots, b_n^T)^T, \\ X \geq 0. \end{cases} \end{aligned} \right\} \quad (6)$$

假设:

- (1) $C, X \in R^n$ 为共享信息;
- (2) P_i 的隐私信息 A_i, b_i , 其中 $A_i \in R^{m_i \times n}, b_i \in R^{m_i}$, (一般 $m_1 + m_2 + \dots + m_n \leq n$).

2.2 模型(6)的安全多方协议

模型(6)用单纯形法求解的计算步骤如下:

Step1: 找出初始可行基,确定初始基可行解,建立初始单纯形表.

Step2: 在不泄露隐私信息的情况下, $P_1, P_2, \dots, P_n$ 协同检查各非基变量的检验数,若 $\sigma \leq 0$, 则已得到最优解,计算结束. 否则转入下一步.

Step3: 根据 $\max(\sigma) > 0$, 确定了换入变量后,按照 $\theta = \min \left(\frac{(B^{-1}b)_i}{(B^{-1}P_j)_i} \mid (B^{-1}P_j)_i > 0 \right)$, 每个参与方 P_i 独自计算 θ_i , 并选出各自的 $\min(\theta_i)$, 在不泄露各自信息的情况下,安全比较其大小,确定换出变量,替换后得到新基变量,再入下一步.

Step4: 求出新基变量以及新基变量对应的基可行解,得到新的单纯形表.

Step5: 重复 Step2 ~ Step4, 直到终止.

2.2.1 关于 Step2 的安全多方协议

参与方 P_i 隐私数据 x_i , 它们要共同计算 $y = \sum_{i=1}^n x_i$, 但任何一个参与方都不愿意向其他参与方泄漏自己的私有输入 x_i . 在此情况下,本文设计了一个基于 Paillier 算法的安全多方计算协议来完成这个计算任务.

协议1 安全多方求和问题的解决方案

输入: 参与方 P_i 拥有隐私数据为 x_i

输出: $y = \sum_{i=1}^n x_i$

- (1) 若 n 为偶数,将 n 个参与者随机分成 A 和 B 组,对其重新编号,即 $A = \{A_1, A_2, \dots, A_k\}, B = \{B_1, B_2, \dots, B_k\} (k = \frac{n}{2})$, 其中 A_i 和 B_i 的隐私

数据分别标记为 a_i, b_i , 即 $y = \sum_{i=1}^n x_i = \sum_{i=1}^k a_i + \sum_{i=1}^k b_i$.

- ①假设 (G, E, D) 是 Paillier 同态加密方案, τ 是设定的安全参数. 参与方 A_i 运行 $G(\tau)$ 生成同态加密方案的公钥和密钥,用公钥加密 a_i 得到密文 $E(a_i)$;

- ②将 $E(x_i)$ 与公钥一起发送给 B_i ;

- ③ B_i 选择一个随机数 r_i , 计算

$$E(a_i + b_i) = (r_i^N E(a_i)^{b_i}) \bmod N^2;$$

- ④将计算结果 $E(a_i + b_i)$ 发送给 A_i

- ⑤ A_i 用私钥解密 $E(a_i + b_i)$ 得到 $a_i + b_i$, 参与者集合 A

共同计算 $y = \sum_{i=1}^n x_i = \sum_{i=1}^k a_i + \sum_{i=1}^k b_i$, 并把 $\sum_{i=1}^n x_i$ 公开.

- (2) 若 n 为奇数,则再增加一个虚拟参与者 P_{n+1} , 他拥有的隐私数据为 0, 这样可以参照上面的协议来完成这个计算任务.

2.2.2 关于 Step3 的安全多方计算

参与方 P_i 拥有隐私数据 $x_i = \min(\theta_i)$, 它们希望知道哪个 x_i 最小, 但又不愿意泄漏各自的 x_i . 在此情况下,探讨如何安全地进行比较. 为了提高计算效率,本文将安全多方比较问题转换成多个安全两方比较问题,进而得到最终的计算结果. 因此,这个计算问题可以归约为参与方 A 与 B 的隐私数据 x 与 y 的大小比较问题.

首先对保密的数据进行编码,不失一般性,假设 $x, y \in \{w_1, w_2, \dots, w_m\} = U$, 其中 $w_1 < w_2 < \dots < w_m$. 进一步假设 $x = w_k, y = w_l, (1 \leq k, l \leq m)$, 那么 $x \leq y$ 当且仅当 $k \leq l$. 解决方案基于下面的观察:

根据 x, y 和 U , 构造两个新的向量 $A = (a_1, a_2, \dots, a_m), B = (b_1, b_2, \dots, b_m)$, 其中 $a_i = \begin{cases} 0, & i < k \\ 1, & i \geq k \end{cases}$, 即 $a_1 = a_2 = \dots = a_{k-1} = 0, a_k = a_{k+1} = \dots = a_m = 1$; 类似地, $b_j = \begin{cases} 0, & j < l \\ 1, & j \geq l \end{cases}$. 如果 $x \leq y$, 那么 $k \leq l, b_1 = b_2 =$

$\dots = b_{l-1} = 0, a_l = b_l = 1$, 则 $v = \sum_{i=1}^l a_i b_i = \sum_{i=1}^{k-1} a_i b_i + \sum_{i=k}^{l-1} a_i b_i + a_l b_l = 1$;

反之,如果 $x > y$, 那么 $k > l, a_1 = a_2 = \dots = a_l =$

0, 则 $v = \sum_{i=1}^l a_i b_i = 0$.

因此保密地比较 x, y 的大小可以归约到保密计算 $\sum_{i=1}^l a_i b_i$. 为了便于论述, 定义 $P(x, y)$ 如下: 如果 $x \leq y$, $P(x, y) = 1$; 否则 $P(x, y) = 0$. 用 Paillier 算法可以完成这个计算任务.

协议2 安全两方比较问题的解决方案

输入: 参与方 A 的隐私数据为 x , 参与方 B 的隐私数据为 y , 设 $x, y \in \{w_1, w_2, \dots, w_m\} = U$.

输出: $P(x, y)$.

(1) 设 $x = r_k, y = r_l$, 参与方 A 和 B 分别构造两个向量 $A = (a_1, a_2, \dots, a_m), B = (b_1, b_2, \dots, b_m)$, 其中

$$a_i = \begin{cases} 0, & i < k \\ 1, & i \geq k \end{cases}, b_j = \begin{cases} 0, & j < l \\ 1, & j \geq l \end{cases}.$$

(2) 假设 (G, E, D) 是 Paillier 同态加密方案, τ 是设定的安全参数. 参与方 A 运行 $G(\tau)$ 生成同态加密方案的私钥和公钥, 用公钥加密向量 A 得到 $E(A) = (E(a_1), E(a_2), \dots, E(a_m))$.

(3) 将 $E(A)$ 与公钥一起发送给 Bob.

(4) 参与方 B 选择一个随机数 r , 计算

$$E(v) = (r^N \prod_{i=1}^l (E(a_i))^{b_i}) \bmod N^2 = E(\sum_{i=1}^l a_i b_i).$$

(5) 将计算结果 $E(v)$ 告诉参与方 A .

(6) 参与方 A 用私钥解密 $E(v)$ 得到 v 并告诉 B .

2.3 安全性证明

证明1 通过构造满足式(1)和(2)的模拟器 S_1, S_2 来证明协议1的安全性. S_1 工作过程如下:

(1) 给定输入 $(a_i, a_i + b_i)$, S_1 随机选择一个 b'_i 使得 $a_i + b'_i = a_i + b_i$, 用 a_i, b'_i 来模拟;

(2) 加密 a_i 得到 $E(a_i)$;

(3) 选择一个随机数 r'_i , 计算

$$E(a_i + b'_i) = (r_i^N E(a_i) b'_i) \bmod N^2;$$

(4) 解密 $E(a_i + b'_i)$ 得到 $a_i + b'_i$.

在本协议中, $\text{VIEW}_1^\Pi(a_i, b_i) = \{a_i, E(a_i), E(a_i + b_i), a_i + b_i\}$. 令 $S_1(a_i, a_i + b_i) = \{a_i, E(a_i), E(a_i + b'_i), a_i + b'_i\}$. 因为 $a_i + b'_i = a_i + b_i$, 根据 $a_i + b_i$ 的计算方法可知 $E(a_i + b_i) \stackrel{c}{=} E(a_i + b'_i)$. 所以 $\{(S_1(a_i, a_i + b_i), a_i + b_i)\}_{a_i, b_i} \stackrel{c}{=} \{(\text{VIEW}_1^\Pi(a_i, b_i), \text{OUTPUT}_2^\Pi(a_i, b_i))\}_{a_i, b_i}$, 可以用类似的方法构造模拟器 S_2 , 满足 $\{(a_i + b_i, S_2(b_i, a_i + b_i))\}_{a_i, b_i} \stackrel{c}{=} \{(\text{OUTPUT}_1^\Pi(a_i, b_i), \text{VIEW}_2^\Pi(a_i, b_i))\}_{a_i, b_i}$. 证毕.

证明2 通过构造满足式(1)和(2)的模拟器 S_1, S_2 来证明协议2的安全性. S_1 工作过程如下:

(1) 给定输入 $(x, P(x, y))$, S_1 随机选择一个 $y' \in \{w_1, w_2, \dots, w_m\}$ 使得 $P(x, y') = P(x, y)$, 用 x, y' 来模拟. 首先按照协议构造向量 $A = (a_1, a_2, \dots, a_m), B' = (b'_1, b'_2, \dots, b'_m)$.

(2) 加密 A 得到

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

(3) 选择一个随机数 r' , 计算

$$E(v') = ((r')^N \prod_{i=1}^l (E(a_i))^{b'_i}) \bmod N^2 = E(\sum_{i=1}^l a_i b'_i).$$

(4) 解密 $E(v')$ 得到 v' .

在本协议中, $\text{VIEW}_1^\Pi(x, y) = \{A, E(A), E(v)\}$. 令 $S_1(x, P(x, y)) = \{A, E(A), E(v'), v'\}$. 因为 $P(x, y') = P(x, y)$, 根据 v 的计算方法可知 $v = v'$, $E(v)_{x, y} \stackrel{c}{=} E(v')_{x, y'}$. 所以 $\{(S_1(x, P(x, y)), P(x, y))\}_{x, y} \stackrel{c}{=} \{(\text{VIEW}_1^\Pi(x, y), \text{OUTPUT}_2^\Pi(x, y))\}_{x, y}$, 可以用类似的方法构造使 $\{(P(x, y), S_2(y, P(x, y)))\}_{x, y} \stackrel{c}{=} \{(\text{OUTPUT}_1^\Pi(x, y), \text{VIEW}_2^\Pi(x, y))\}_{x, y}$ 成立的模拟器 S_2 . 证毕.

2.4 例子分析

例子1 Alice 掌握: A_1, b_1 , Bob 掌握: A_2, b_2 , 其中 $A_i \in R^{m_i \times n}, b_i \in R^{m_i} (i = 1, 2)$ (一般的 $m_1 + m_2 \leq n$). 在不完全泄漏各自隐私的情况下, 共同解决线性规划问题:

$$\begin{aligned} \max \xi &= C^T X, \\ \text{s. t. } &\begin{cases} (A_1^T, A_2^T)^T X = (b_1^T, b_2^T)^T, \\ X \geq 0. \end{cases} \end{aligned} \quad (7)$$

为了阐述方便起见, 设

$$\begin{pmatrix} A_1 \\ A_2 \end{pmatrix} = \begin{pmatrix} B_1 & D_1 & N_1 \\ D_2 & B_2 & N_2 \end{pmatrix}; X = (X_{B_1}^T, X_{B_2}^T, X_N^T)^T;$$

$$b = (b_1^T, b_2^T)^T; C = (C_{B_1}^T, C_{B_2}^T, C_N^T)^T.$$

X_{B_1}, X_N 分别表示基变量和非基变量, 这时的线性规划问题可变换成如下的等价形式:

$$\begin{aligned} \max \xi &= C_{B_1}^T X_{B_1} + C_{B_2}^T X_{B_2} + C_N^T X_N, \\ \text{s. t. } &\begin{cases} \begin{pmatrix} E & B_1^{-1} D_1 & B_1^{-1} N_1 \\ B_2^{-1} D_2 & E & B_2^{-1} N_2 \end{pmatrix} \begin{pmatrix} X_{B_1} \\ X_{B_2} \\ X_N \end{pmatrix} = \begin{pmatrix} B_1^{-1} b_1 \\ B_2^{-1} b_2 \end{pmatrix}, \\ X_{B_1}, X_{B_2}, X_N \geq 0. \end{cases} \end{aligned}$$

该表达形式称为线性规划问题对应与基变量的典式.

用单纯形法求解, 见表1.

表1 同构单纯形初始表

Tab.1 The isomorphic initial simplex tableau

	基变量		非基变量	等式右边RHS	θ
系数	E	$B_1^{-1}D_1$	$B_1^{-1}N_1$	$B_1^{-1}b_1$	θ_1
矩阵	$B_2^{-1}D_2$	E	$B_2^{-1}N_2$	$B_2^{-1}b_2$	θ_2
检验数 σ^T	0	0	$C_N^T - C_1^T N_1 - C_{B_2}^T B_2^{-1} N_2$		

其计算步骤如下:

Step1: 找出初始可行基, 确定初始基可行解, 建立初始单纯形表.

Step2: 在不泄露隐私信息的情况下, Alice 和 Bob 协同检查各非基变量的检验数, 若 $\sigma \leq 0$, 则已得到最优解, 计算结束. 否则转入下一步.

Step3: 根据 $\max(\sigma) = \sigma_k > 0$, 确定 x_k 为换入变量后, 按照 $\theta = \min_i \left(\frac{(B^{-1}b)_i}{(B^{-1}P_j)_i} \mid (B^{-1}P_j)_i > 0 \right)$, Alice 和 Bob 分别单独计算 θ_1 和 θ_2 , 并选出各自的 $\min(\theta_1)$, $\min(\theta_2)$, 在不泄露各自信息的情况下, 安全比较其大小, 确定换出变量, 替换后得到新基变量, 再入下一步.

Step4: 求出新基变量对应的典式以及新基变量对应的基可行解.

Step5: 重复 Step2 ~ Step4, 直到终止.

关于 Step2 和 Step3 的安全多方计算问题, 可用前面的协议 1 和协议 2 来解决, 因此本节不再详述.

3 约束异构时安全多方计算

3.1 模型与假设

本节研究在半诚实模型下的约束异构的线性优化问题, 其数学模型如下:

$$\begin{aligned} \max \xi &= (C_1^T, C_2^T, \dots, C_n^T) (X_1^T, X_2^T, \dots, X_n^T)^T, \\ \text{s. t. } \begin{cases} \text{diag}(A_1, A_2, \dots, A_n) (X_1^T, X_2^T, \dots, X_n^T)^T = \\ (b_1^T, b_2^T, \dots, b_n^T)^T, \\ X_i \geq 0, i = 1, \dots, n. \end{cases} \end{aligned} \quad (8)$$

假设:

(1) $C_i \in R^n$ 为共享信息;

(2) P_i 的隐私信息 A_i, b_i, X_i , 其中 $A_i \in R^{m_i \times n}$, $b_i \in R^{m_i}$, $X_i \in R^n$ (一般 $m_1 + m_2 + \dots + m_n \leq n$).

3.2 模型(8)的安全多方协议

模型(8)用单纯形法求解的计算步骤如下:

Step1: 找出初始可行基, 确定初始基可行解, 建立初始单纯形表.

Step2: 在不泄露隐私信息的情况下, $P_1, P_2, \dots, P_n$ 各自检查各非基变量的检验数, 若 $\sigma_i \leq 0$, 则已得

到最优解, 计算结束. 否则转入下一步.

Step3: 若 $\max(\sigma_i) > 0$, $P_1, P_2, \dots, P_n$ 选出各自的 $\max(\sigma_i)$, 在不泄露各自信息的情况下, 比较其大小, 确定换入变量, 进入下一步.

Step4: 按 θ 规则, $P_1, P_2, \dots, P_n$ 各自计算 θ_i , 并选出各自的 $\min(\theta_i)$, 在不泄露各自隐私的情况下, 比较其大小, 确定换出变量, 再入下一步.

Step5: 求出新基变量与其对应的基可行解.

Step6: 重复 Step2 ~ Step5, 直到终止.

Step7: $P_1, P_2, \dots, P_n$ 共同计算 $\max \xi$.

模型(8)涉及到的隐私计算问题是安全多方比较问题和安全多方求和问题, 可以用协议 1 和协议 2 来完成这两个计算任务, 因此本节不再详述.

3.3 例子分析

例子 2: Alice 掌握: A_1, b_1 , Bob 掌握: A_2, b_2 , 其中 $A_i \in R^{m_i \times n}$, $b_i \in R^{m_i}$ ($i = 1, 2$) (一般的 $m_1 + m_2 \leq n$), 且 $C_1, X_2 \in R^n$ 是公开的. 在不完全泄露各自隐私的情况下, 共同解决线性规划问题:

$$\begin{aligned} \max \xi &= (C_1^T, C_2^T) (X_1^T, X_2^T)^T, \\ \text{s. t. } \begin{cases} \text{diag}(A_1, A_2) (X_1^T, X_2^T)^T = (b_1^T, b_2^T)^T, \\ X_i \geq 0, i = 1, 2. \end{cases} \end{aligned} \quad (9)$$

根据文献 [5], Alice 和 Bob 各自对系数增广矩阵 $(A_1 : b_1)$ 和 $(A_2 : b_2)$ 作保持可行性 (即 b 列非负) 的初等行变换, 得到 $(A_1' : b_1')$ 和 $(A_2' : b_2')$; 其中 $\text{diag}(A_1', A_2')$ 已含初始可行基. 建立初始单纯形表, 如表 2 所示.

表2 异构初始单纯形表

Tab.2 The isomorous initial simplex tableau

	变量		等式右边 RHS	θ
系数矩阵	A_1'	0	b_1'	θ_1
	0	A_2'	b_2'	θ_2
检验数 σ^T	σ_1^T	σ_2^T		

其计算步骤如下:

Step1: 找出初始可行基, 确定初始基可行解, 建立初始单纯形表.

Step2: 在不泄露隐私信息的情况下, Alice 和 Bob 各自检查各非基变量的检验数, 若 $\sigma \leq 0$, 则已得到最优解, 计算结束. 否则转入下一步.

Step3: 若 $\max(\sigma) > 0$, Alice 和 Bob 选出各自的 $\max(\sigma_1)$, $\max(\sigma_2)$, 在不泄露各自信息的情况下, 比较其大小, 确定换入变量, 进入下一步.

Step4: 按 θ 规则, Alice 和 Bob 分别单独计算 θ_1 和 θ_2 , 并选出各自的 $\min(\theta_1)$, $\min(\theta_2)$, 在不泄露各自信息的情况下, 比较其大小, 确定换出变量, 再入下一步.

Step5: 求出新基变量与其对应的基可行解.

Step6: 重复 Step2 ~ Step5, 直到终止.

Step7: $P_1, P_2, \dots, P_n$ 共同计算 $\max \xi$.

例子2的安全多方计算问题, 可以用协议1和协议2来解决, 因此本节不再详述.

4 结语

无论是生产运作管理还是在供应链管理中, 有大量的优化决策问题, 本文仅仅是提出一种针对线性优化问题的安全多方计算协议, 并对文中提出的协议的安全性给出了证明, 研究表明该协议比一般的单调张成方法生成的安全多方计算协议具有较高的计算效率. 在实际应用系统中, 大部分的系统(如SCM, ERP)中的模型求解, 多数使用Karmarkar方法, 本文没有采用这个方法设计SMC, 也没有考虑非线性约束下的各类优化问题的SMC问题, 当然这是非常庞大的研究内容, 从目前的研究来看, 也不太可能存在一种通用的设计方法, 因此对于不同的优化系统, 可能还是要先设计不同的SMC.

实际应用时, 还要讲究计算的效率问题, 目前多数SMC方法的计算复杂度比较高, 如何提高实际协同决策时的SMC方法的计算效率, 还是一个非常广阔的研究方向.

参考文献:

- [1] 朱慧, 刘洪伟, 陈丽, 等. 网络用户的信息隐私边界及其敏感度等级研究 [J]. 广东工业大学学报, 2013, 30(4): 1-7.
- [2] Zhu H, Liu H W, Chen L, et al. Research on information privacy boundaries and sensitivity of net users [J]. Journal of Guangdong University of Technology, 2013, 30(4): 1-7.
- [3] 郭大宁, 张健. 供应链管理中的联合库存控制 [J]. 东华大学学报: 自然科学版, 2003, 29(5): 63-66.
- [4] Guo D N, Zhang J. United inventory control on supply chain management [J]. Journal of Donghua University: Natural Science, 2003, 29(5): 63-66.
- [5] 张广霞. 联合库存管理法在供应链库存控制中的应用 [J]. 中国市场, 2008, 4(15): 14-15.
- [6] Zhang G X. Joint inventory management appliance in the supply chain inventory control [J]. China Market, 2008, 4(15): 14-15.
- [7] 李果, 张祥, 马士华. 基于不同交货期策略的两供应-单制造商协同供货模型 [J]. 中国管理科学, 2010, 18(5): 66-75.
- [8] Li G, Zhang X, Ma S H. Supply coordination model of two suppliers and one manufacturer system based on different delivery policies [J]. Chinese Journal of Management Science, 2010, 18(5): 66-75.
- [9] 马士华, 龚凤美. 基于 Supply Hub 的供应商配送批量协同决策 [J]. 工业工程与管理, 2009, 14(2): 1-9.
- [10] Ma S H, Gong F M. Collaborative decision of distribution lot-sizing among suppliers based on supply hub [J]. Industrial Engineering and Management, 2009, 14(2): 1-9.
- [11] 李毅鹏, 马士华. 基于安全多方计算的产能约束供应商协调供货 [J]. 控制与决策, 2013, 28(11): 1623-1629.
- [12] Li Y P, Ma S H. Research on suppliers synchronization replenishment under performance constraint based on secure multi-party computation [J]. Control and Decision, 2013, 28(11): 1623-1629.
- [13] 刘洪伟, 石雅强, 梁周扬, 等. 面向聚类挖掘的局部旋转扰动隐私保护算法 [J]. 广东工业大学学报, 2012, 29(3): 28-34.
- [14] Liu H W, Shi Y Q, Liang Z Y, et al. Partial rotation perturbation for privacy-preserving clustering mining [J]. Journal of Guangdong University of Technology, 2012, 29(3): 28-34.
- [15] Goldreich O. Foundations of Cryptography: Volume 2, Basic Applications [M]. Cambridge: England Cambridge university press, 2009: 332-410.
- [16] Yao A C. Protocols for secure computations [C] // M Thorup: 2013 IEEE 54th Annual Symposium on Foundations of Computer Science. Berkeley: IEEE Computer Society, 1982: 160-164.
- [17] Goldreich O, Micali S, Wigderson A. How to play any mental game [C] // Alfred V A: Proceedings of the nineteenth annual ACM symposium on Theory of computing. New York: ACM, 1987: 218-229.
- [18] 刘木兰, 张志芳. 密钥共享体制和安全多方计算 [M]. 北京: 电子工业出版社, 2008: 182-198.
- [19] Du W, Atallah M J. Privacy-preserving cooperative scientific computations [C] // Smith G: Proceedings of the 14th IEEE Computer Security Foundations Workshop. Nova Scotia: IEEE Computer Society, 2001: 0273-0273.
- [20] 鲁芳, 仲伟俊, 张玉林. 成本信息保护下的安全供应链联合订货决策 [J]. 管理工程学报, 2009, 23(04): 163-165.
- [21] Lu F, Zhong W J, Zhang Y L. Secure supply-chain cooperative ordering decision under cost-information protection [J]. Journal of Industrial Engineering and Engineering Management, 2009, 23(04): 163-165.
- [22] Paillier P. Public-key cryptosystems based on composite degree residuosity classes [C] // Jacques Stern: Advances in cryptology—EUROCRYPT'99. Berlin: Springer Berlin Heidelberg, 1999: 223-238.
- [23] 申卯兴, 许进. 求解线性规划的单纯形法的直接方法 [J]. 计算机工程与应用, 2007, 43(30): 94-96.
- [24] Shen M X, Xu J. Direct way of simplex method for solving linear programming model [J]. Computer Engineering and Applications, 2007, 43(30): 94-96.