

doi:10.3969/j.issn.1007-7162.2015.02.008

跨组织间隐私数据水平分布线性规划协同优化算法研究

陆涛,刘洪伟,刘智慧,朱慧,陈丽
(广东工业大学管理学院,广东广州510520)

摘要: 供应链协同优化决策中,在保护上下游成员私有信息的同时,得到全局的协同优化决策方案.利用安全多方计算的理论和基础协议,讨论在半诚实模型下具有线性结构的供应链协同优化算法,针对线性规划模型约束矩阵的信息水平分布与不同组织且目标函数也为隐私信息的情形,提出了基于随机矩阵变换的防推断的安全解决方法.该方法相对于传统的安全多方计算方法具有较高的计算效率.

关键词: 供应链管理;协同优化;SMC;水平分布

中图分类号: TP309.2; F224.31 文献标志码: A 文章编号: 1007-7162(2015)02-0043-05

Collaborative Optimization Algorithm Research on Cross-organization's Privacy Data Horizontally Partitioned Linear Programing

Lu Tao, Liu Hong-wei, Liu Zhi-hui, Zhu Hui, Chen Li
(School of Management, Guangdong University of Technology, Guangzhou 510520, China)

Abstract: This paper mainly studied how to obtain global optimal solutions to collaborative optimization decision-making in supply chain management under the premise of protecting the upstream and downstream members' s private information. By using secure multiparty computation theory and some basic protocols, this paper discussed the supply chain collaborative optimization algorithm for models with linear structure under the semi-honest model and proposed an anti-infered approach to the linear programming model of which constraint matrix data is distributed in different parties by row and objective function is also another party' s privacy information. Compared with the traditional methods of secure multiparty computation, this algorithm has higher efficiency.

Key words: supply chain management; collaborative optimization; SMC; horizontally partitioned

随着经济全球化的深化和信息技术的发展,企业间的合作变得尤为重要,特别是在供应链管理中,为了提高顾客满意度和整个供应链的竞争力,供应链协同是供应链中各企业或组织的必然选择.供应链协同优化决策就是各企业或组织在信息共享的基础上,以整体供应链最优为目标进行协同决策,例如协同物流、协同生产以及协同调度等.然而在实践中,供应链中各成员很少愿意与其他成员共享信息,担心共享信息会给自己带来负面影响,称这些信息为“隐私信息”^[1].如何在不泄漏各自的私有信息情

况下完成供应链的协同优化决策,是供应链管理中的重要难题.

线性规划模型是一类最基本且应用广泛的优化模型,然而在实际应用中模型的约束矩阵和目标函数都是基于不同实体的隐私信息或数据构建的,并且各实体都不愿意公开自己的隐私信息.目前解决基于隐私保护的协同优化问题的主要方法是建立可信第三方,如 IBM® Sterling Transportation Management System (TMS),但是可信第三方并非绝对可信,而且可信第三方可能需要高额的服务费用.在没

有可信第三方的情况下,安全多方计算(Secure Multiparty Computation, SMC)是解决此类问题行之有效的方法.安全多方计算最早由 A. C. Yao^[2]于1982年提出,即百万富翁问题,后来 Goldreich, Micali 和 Wigderson 将其理论扩展,并给出了一般的描述^[3].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.

对于基于隐私保护的线性规划模型,Yuan Hong 等^[4]根据实际应用把数据的分布分为水平分布/同构、垂直分布/异构和任意分布;Mangasarian^[5]和 Li^[6]分别针对等式和不等式约束条件的水平数据分布的隐私保护线性规划模型提出了基于随机矩阵变换的解决方案,但是该解决方案存在可推断攻击;Yuan Hong 等^[7]对 Mangasarian 和 Li 所提出的方法进行了改进,提出了防推断型的解决方案.但是以上的基于隐私保护的线性规划模型的研究都是假设目标函数为公开信息,而在实际应用中目标函数也可能为隐私信息,例如供应链中的制造商、原材料供应商以及其他分布在不同地点的供应链结点进行协同物流,需要选择一家物流运输商.然而不同的物流运输商有不同的价格(但运输商不想泄露自己的价格信息让竞争对手知道),也就导致了不同的目标函数.本文拟对线性规划模型的约束矩阵数据水平分布且目标函数也为实体隐私信息提出基于随机矩阵变换的仿推断解决方法.

1 问题的提出

基于水平数据分布的线性规划是指线性规划的约束矩阵和相应的资源向量按行分布在不同的实体中.即对于标准线性规划

$$\min z = C^T X$$

$$\text{s. t. } \begin{cases} AX \leq b \\ X \geq 0 \end{cases}$$

$$\text{中 } [A \quad b] = \begin{bmatrix} A_1 & b_1 \\ A_2 & b_2 \\ \vdots & \vdots \\ A_p & b_p \end{bmatrix}, \text{ 其中 } A_i X \leq b_i. \text{ (包含等}$$

式约束和不等式约束)为实体 $i (i = 1, \dots, p)$ 的隐私信息, $A \in R^{m \times n}$, $C \in R^n$, $b \in R^n$, $b_i \in R^{m_i}$, $A_i \in R^{m_i \times n}$ ($\sum_{i=1}^p m_i = m$), $X = (x_1, x_2, \dots, x_n)^T$. 另外假设线性规划目标函数系数 C 为实体 $p+1$ (如物流运输商)的隐私信息,本文主要解决了在不泄露实体 $i (i = 1, \dots, p, p+1)$ 的隐私信息情形下求解线性规划.

2 基本理论

本文是在半诚实模型下讨论基于隐私保护的协同优化问题.在半诚实模型中,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^[8].本文主要通过基于随机矩阵变换的方式隐藏各实体的隐私信息,其中主要用到了同态加密体制和安全双方点积协议.

(1) 同态加密体制

同态加密的概念是由 Rivest, Adleman 和 Dertouzos 于1978年提出.同态加密的特殊性质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. Goldwasser-Micali 加密算法^[9]、Benaloh 加密算法^[10]、Naccache-Stern 加密算法^[11]、ElGamal 加密算法^[12]、Paillier 加密算法^[13]等都是同态加密算法.同态加密体制按其性质可以分为加同态和乘同态两种.加同态是指满足 $E(m_1) \cdot E(m_2) = E(m_1 + m_2)$ 的加密方案,例如 Paillier 加密算法;乘同态是指满足 $E(m_1) \cdot E(m_2) = E(m_1 \times m_2)$ 的加密方案,例如 ElGamal 加密算法.

(2) 安全点积协议

安全点积问题可以描述为:Alice 和 Bob 的输入分别为一个 n 维私有向量 $X = (x_1, x_2, \dots, x_n)$ 和 $Y = (y_1, y_2, \dots, y_n)$, Bob 随机选取一个随机数 r_b , Alice 需要得到值 $w = X \cdot Y + r_b$,要求 Alice 不能从 w 中得到任意一个 y_i 的消息,而且 Bob 也不能获得 w 和任意一个 x_i 的消息.协议1描述了一种基于同态加密体制的安全两方点积协议.

协议1 基于同态加密体制的安全两方点积协议:

Step1: Alice 产生一对私钥和公钥 (sk, pk) .

Step2: Alice 将 pk 发送给 Bob.

Step3: Bob 选择 n 个随机数 r_i 并重新构造自己的隐私向量,令 $Y' = (y_1 - r_1, \dots, y_n - r_n)$,并将 Y' 发送给 Alice.

Step4: Alice 利用同态加密算法计算 $c = E_{pk}(x_i)$ 和 $\omega = E_{pk}(x_i(y_i - r_i))$,并将 (c, ω) 发送给 Bob.

Step5: Bob 收到 (c, ω) 后计算 $m_i = c^{r_i} \omega (i = 1, \dots, n)$,

并选择一个随机数 r_b , 计算 $s = E_{pk}(r_b) \prod_{i=1}^n m_i$, 将 s 发送给 Alice.

Step6: Alice 利用私钥 sk 对 s 进行解密: $w = \text{Dec}_{sk}(s) =$

$$\sum_{i=1}^n x_i y_i + r_b$$

目前点积协议得到了广泛的理论研究,且广泛

应用于保护隐私信息的各类协作计算,如数据挖掘、统计分析、信息检索等,并成为SMC一个基本的协议。

3 构建安全的新线性规划模型

3.1 隐藏实体 $i(i = 1, \dots, p)$ 的隐私信息

首先,对于线性规划(1)需要添加松弛变量使不等约束转换成等式约束,但是为了增加变换的随机性和防止攻击者的推断,令实体 $i = 1, \dots, p$ 根据自己私有的原始约束条件在本地产生人造约束条件组成实体 i 新的私有约束条件. 注意人造约束条件不能改变原始约束条件的可行域,例如,实体 i 有不等式约束条件 $2x_1 - 3x_2 \leq 10$, 其中 $x \geq 0$, 则实体 i 可以产生的人造约束条件为 $x_1 - 2x_2 \leq 5$, $x_1 - 3x_2 \leq 10$, $x_1 - 1.7x_2 \leq 5$ 等;如果实体 i 拥有等式约束条件 $x_1 + 2x_2 = 8$, 其中 $x \geq 0$, 则实体 i 可以产生人造约束条件为 $x_1 + x_2 \leq 8$, $0.5x_1 + 0.9x_2 \leq 4$ 等(不建议产生人造等式约束,因为不改变矩阵 A 的秩). 通过增加人造约束条件,原始模型中的 A 和 b 扩展为 $A' \in \mathbf{R}^{m' \times n}$ 和 $b' \in \mathbf{R}^{m'}$ (m' 为所有实体的原始约束条件和人造约束条件的个数总和),即模型转化为

$$\begin{aligned} \min z &= C^T X; \\ \text{s. t. } \begin{cases} A'X \leq b', \\ X \geq 0. \end{cases} \end{aligned} \quad (2)$$

其次,添加松弛变量. 令加入人造约束条件后的线性规划模型(2)中不等式约束条件个数为 l ($l \leq m'$). 同样,为了防止攻击者的推断,实体 $i(i = 1, \dots, p)$ 在本地对其不等式约束条件可以添加多于1个的松弛变量把不等式约束转换成等式约束. 对于模型(2)中第 $j(j = 1, \dots, l)$ 个不等式约束,设其拥有的实体为其增加 t_j 个松弛变量变为等式约束,则最后的模型(2)中拥有 $t = \sum_{j=1}^l t_j \geq l$ 个松弛变量. 令实体 $i(i = 1, \dots, p)$ 转换其不等式约束的所用的松弛变量的个数为 T_i . 一般情况下, T_i 可以取得相当大(如令 $T_i \geq m'_i$, m'_i 为模型(1)中实体 i 私有的约束条件的个数),则有 $t = \sum_{i=1}^p T_i > m' \geq l > \ell$ (ℓ 为模型(2)中的不等式约束条件个数)和 $m' > m \geq \ell$ ($m = \ell$ 时,模型(2)最容易受到攻击者的攻击). 通过添加松弛变量,线性规划(2)变换为

$$\begin{aligned} \min z &= C^T X, \\ \text{s. t. } [A' \quad M'] \begin{bmatrix} X \\ X_s \end{bmatrix} &= b', X \geq 0, X_s \geq 0. \end{aligned} \quad (3)$$

其中 $A' \in \mathbf{R}^{m' \times n}$, 松弛变量集合 $X_s = [s_1, s_2, \dots, s_l]^T$, $M' \in \mathbf{R}^{m' \times l}$ 为所有约束条件中松弛变量的系数矩阵; M' 中对应(2)中每个等式约束的行的元素全为0; M' 中对应(2)中第 $j(j = 1, \dots, l)$ 个不等式约束所在行中 t_j 个松弛变量系数为随机产生的正实数; M' 中其余元素为0. 在水平数据分布的线性规划模型(3)中实体 $i = 1, \dots, p$ 的隐私信息为 $[A'_{i.} \quad M'_{i.}] \begin{bmatrix} X \\ X_s \end{bmatrix} = b'_i$, 其中 $A'_{i.} \in \mathbf{R}^{m'_i \times n}$, $b'_i \in \mathbf{R}^{m'_i}$, $M'_{i.} \in \mathbf{R}^{m'_i \times l}$ 为 M' 中实体 i 拥有的等式和不等式约束条件所对应的行组成,即 $M' = \begin{bmatrix} M'_1. \\ \vdots \\ M'_p. \end{bmatrix} \in \mathbf{R}^{m' \times l}$.

最后,通过产生随机矩阵隐藏线性规划(3)中实体 $i(i = 1, \dots, p)$ 的隐私信息. 由上面可知 $V_{i.} = [A'_{i.} \quad M'_{i.}] \in \mathbf{R}^{m'_i \times (n+l)}$ 为实体 $i(i = 1, \dots, p)$ 的隐私信息,由拥有 $V_{i.}$ 的实体产生一个 $m' \times m'_i$ 随机矩阵 $B_{.i}$, $B_{.i}$ 中的每个元素均匀分布在 $(0, 1)$ 区间上且 $B_{.i}$ 不公开. 设

$$B = [B_{.1} + \lambda E_1 \quad B_{.2} + \lambda E_2, \dots, B_{.p} + \lambda E_p], \quad (4)$$

其中 λ 为实体 $i(1, \dots, p)$ 共同商定的一个确定的较大的实数且 $\lambda \geq n + t$, $E = [E_1 \quad E_2, \dots, E_p]$ 为 $m' \times m'$ 阶单位矩阵,则 B 为可逆矩阵^[14]. 线性规划(3)中将 $B_{.i} + \lambda E_i$ 分别乘以每个实体的私有信息 $V_{i.}$ 和 b'_i , 可得 $(B_{.i} + \lambda E_i)V_{i.}$ 和 $(B_{.i} + \lambda E_i)b'_i$. 线性规划(3)即转化成为线性规划

$$\begin{aligned} \min z &= C^T X, \\ \text{s. t. } BA'X + BM'X_s &= Bb', X \geq 0, X_s \geq 0. \end{aligned} \quad (5)$$

线性规划(5)对于隐藏实体 $i(i = 1, \dots, p)$ 的隐私信息是安全的,这是因为只有实体 i 知道 $B_{.i}$, 其余实体在不知道 $B_{.i}$ 时无法从 $(B_{.i} + \lambda E_i)V_{i.}$ 和 $(B_{.i} + \lambda E_i)b'_i$ 中计算出 $V_{i.}$ 和 b'_i , 所以线性规划(5)不泄露任何实体 $i(i = 1, \dots, p)$ 的隐私信息. 由于 B 可逆,线性规划(5)和线性规划(3)是等价的. 另外,各实体在增加人造约束条件和添加松弛变量时不改变原始线性规划模型(1)的可行域,可以证明,如果 $(X^*, (X_s^*))$ 是线性规划(3)的最优解,那么 X^* 是线性规划的最优解. 隐藏实体 $i(i = 1, \dots, p)$ 的隐私信息的具体算法见算法1.

算法1 基于水平数据分布的约束矩阵隐藏算法

Step1: 实体 $i(i = 1, \dots, p)$ 根据原始的隐私约束条件在本地产生人造约束矩阵成为实体 i 新的隐私信息。

Step2: 实体 $i(i = 1, \dots, p)$ 在本地添加松弛变量使隐私约束条件的不等式约束转化成等式约束, 松弛变量系数为随机产生的正实数。

/* 经过 Step1 和 Step2 后实体 $i(i = 1, \dots, p)$ 的隐私信息为 $A'_{i.}X + M'_{i.}X_s = b'_{i.} *$ /

Step3: 实体 $i(i = 1, \dots, p)$ 共同随机确定一个较大的实数 $\lambda(\geq n + t)$ 。

Step4: 由拥有隐私信息 $A'_{i.}X + M'_{i.}X_s = b'_{i.}$ 的实体 i 产生 $m' \times m'_i$ 阶随机矩阵 $B_{.i}$, $B_{.i}$ 中的元素分布在区间 $(0, 1)$, 且 $B_{.i}$ 不公开。

Step5: 实体 1 计算 $(B_{.1} + \lambda E_1)[A'_{1.} \ M'_{1.}]$ 和 $(B_{.1} + \lambda E_1)b'_{1.}$, 并传送给实体 2。

Step6: 实体 2 计算 $(B_{.1} + \lambda E_1)[A'_{1.} \ M'_{1.}] + (B_{.2} + \lambda E_2)[A'_{2.} \ M'_{2.}]$ 和 $(B_{.1} + \lambda E_1)b'_{1.} + (B_{.2} + \lambda E_2)b'_{2.}$, 并传送给实体 3。

{ 以此类推 }

.....

Step $p + 4$: 实体 p 负责计算 $[BA' \ BM'] = (B_{.1} + \lambda E_1)[A'_{1.} \ M'_{1.}] + \dots + (B_{.p} + \lambda E_p)[A'_{p.} \ M'_{p.}]$ 和 $Bb' = (B_{.1} + \lambda E_1)b'_{1.} + \dots + (B_{.p} + \lambda E_p)b'_{p.}$ 。

/* 得到安全隐藏实体 $i(i = 1, \dots, p)$ 隐私信息的线性规划模型: $\min z = C^T X$

$$\text{s. t. } \begin{cases} [BA' \ BM'] [X \ X_s]^T = Bb' \\ X \geq 0, X_s \geq 0 \end{cases} \quad */$$

3.2 隐藏实体 $p + 1$ 的隐私信息

为了不泄露实体 $p + 1$ 的私有信息 (C), 本文利用变换的思想隐藏 C 的具体信息, 此方法最早是由 Du 针对线性方程组系统提出的^[15], 后来 Du 将其扩展到安全两方的线性规划模型^[16]。由算法 1 可以知道, 线性规划 (5) 中的 BA' 和 BM' 为 $i(i = 1, \dots, p)$ 的公开信息 (因为任何实体 i 不能从 BA' 和 BM' 中推导出其他实体 $j(j = 1, \dots, i - 1, i + 1, \dots, p)$ 的隐私信息)。显然

$$\begin{aligned} C^T Q Q^{-1} X &= C^T X, \\ BA' Q Q^{-1} X + BM' X_s &= Bb' \Leftrightarrow BA' X + BM' X_s = Bb'. \end{aligned} \quad (6)$$

其中 $Q^{-1} (Q^{-1} \in R^{n \times n})$ 的元素全为正实数, $X \geq 0$, $X_s \geq 0$ 。令 $U = BA' Q$, $U' = BM'$, $Y = Q^{-1} X$, $C'^T = C^T Q$, 则线性规划 (5) 转换成

$$\min z' = C'^T Y;$$

$$\text{s. t. } \begin{cases} UY + U' X_s = Bb', \\ Y \geq 0, X_s \geq 0. \end{cases} \quad (7)$$

根据 Du 的方法, 很容易证明如果 $(Y^*, (X_s^*))$ 是线性规划 (7) 的最优解, 那么 $(X^*, (X_s^*)) (X^* = QY^*)$ 为线性规划 (5) 的最优解 (采用反证法)。

由 (6) 可知, 通过转化隐藏实体 $p + 1$ 隐私信息方法的核心在于如何在不泄露其他实体隐私信息的条件下得到 $C^T Q$ 和 $BA' Q$ 。根据矩阵理论, 矩阵相乘可以拆分为多个向量的点积, 即一个 $m \times n$ 阶矩阵乘以一个 $n \times n$ 阶矩阵相当于进行 $m \times n$ 次的两个向量的点积。可以很容易地将协议 1 中的安全两方点积协议扩展到矩阵相乘^[17]。

假设由机器产生元素均为正实数的随机可逆矩阵 Q , 并将 Q 随机进行分解: $Q = Q_1 + Q_2$ ($Q_i (i = 1, 2)$ 的元素均为正实数), 并将 Q_1 通过安全可信通道发送给实体 $p + 1$ (令为 P_1), 将 Q_2 发送给实体 $i(i = 1, \dots, p)$ (此时可以把实体 $i(i = 1, \dots, p)$ 看成一个集体参与方, 令为 P_2)。显然, 任何实体都不知道 Q 的值, 只有 P_1 和 P_2 合谋才能够得到 Q 的值。根据矩阵乘法 $BA' (Q_1 + Q_2) = BA' Q_1 + BA' Q_2$, 首先 P_2 计算 $BA' Q_2$, 并对 $BA' Q_2$ 和 BA' 的元素加密, 将 $BA' Q_2$ 和 BA' 的加密形式发送给 P_1 ; 根据同态加密的性质, P_1 计算 $BA' Q_1$ 的加密形式, 然后计算 $BA' Q_1 + BA' Q_2$ 的加密形式, 并发送给 P_2 ; 最后 P_2 通过解密得到 $BA' Q$ 。具体算法见算法 2。同样在计算 $C^T Q$ 时, P_1 的输入为 $n \times n$ 阶矩阵 Q_1 和 $1 \times n$ 阶矩阵 C^T , P_2 的输入为 $n \times n$ 阶矩阵 Q_2 , 此时应由 P_1 产生一对公钥和私钥。通过把矩阵相乘转化成多个向量的点积, 再利用安全点积协议就可以解决在不泄露双方隐私信息的情况下获得 $C^T Q$ 和 $BA' Q$ 。隐藏实体 $p + 1$ 的隐私信息的具体算法见算法 2。

算法 2 隐藏线性规划目标函数系数的隐私保护算法
 P_1 的输入为 $n \times n$ 阶矩阵 Q_1 。

P_2 的输入为 $n \times n$ 阶矩阵 Q_2 和 $m' \times n$ 阶矩阵 BA' (令 $BA' = H$)。

Step1: P_2 产生一对私钥和公钥 (sk, pk) 。

Step2: P_2 将公钥 sk 发送给 P_1 。

Step3: P_2 计算 $m' \times n$ 阶矩阵 $R = HQ_2$ 。

Step4: P_2 进行加密计算 $R' = \text{Enc}_{pk}(R)$ 。

Step5: P_2 计算 $H' = \text{Enc}_{pk}(H)$ 。

Step6: P_2 将 R' 和 H' 发送给 P_1 。

/* 下面为 P_1 计算加密矩阵后 S' 的步骤 */

Step7: 对于 H' 的每一行 i 和 Q_1 的每一列 j 进行下面循环:

Step9: P_1 计算 $S'_{ij} = \prod_{k=1}^n H'_{ik} Q_{kj} \cdot R'_{ij}$. (其中下标表示所

在行和列交叉处的元素)

{结束循环, P_1 得到加密后的矩阵 $S' = (S'_{ij})$ }

Step10: P_1 将 S' 发送给 P_2 .

Step11: P_2 进行解密计算 $S = \text{Dec}_{sk}(S') =$

$H(Q_1 + Q_2) = BA'Q$

4 安全性和有效性分析

在隐藏实体 $i(1 \leq i \leq p)$ 的隐私信息时,特别地让每个实体增加了人造约束条件且对于不等式约束转化成等式约束要求各实体增加多于1个的松弛变量,有效地减小了推断的可能性,尤其是当实体的个数 p 较小时,如若不增加人造约束条件和多个松弛变量,模型中的隐私信息很容易被推断出来.在算法1中各实体间只需进行 $2(p-1)$ 次的信息交换并且各实体只需进行2次矩阵相乘计算,具有较高的效率.

算法2中的安全性取决于安全点积协议的安全性.对于一次安全点积过程需要 $2m'n$ 次加密、 n 次幂运算和 n 次乘积运算,总共需要进行 $m'n$ 次安全点积协议,即算法过程需要同时进行 $m'n^2$ 的幂运算和 $m'n^2 + mn$ 的乘积运算.最后,需要进行 $m'n$ 的解密运算才能够获得变形后的矩阵,相对于传统的安全多方计算方法具有较高的效率.

5 结论

实际应用中,例如生产运作管理和供应链管理中,存在着大量的优化决策问题.而线性规划模型是应用最为广泛的一种优化决策模型,并且模型数据的分布各种各样.本文针对线性规划约束矩阵数据水平分布且目标函数也为隐私信息的LP模型提出解决方案,此种情况在实际应用中也是广泛存在的.但是基于随机矩阵变换的方法隐藏实体的隐私信息的安全性有待进一步探讨,潜在的攻击仍然存在.本文提出的算法运用到实际应用中可能还存在很大的困难,但是为基于隐私保护的协同优化算法的研究提供了理论研究.另外,对于不同数据分布的线性规划很难提出一种通用的解决方案,只能针对特殊优化决策系统设计不同的解决方案.

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.

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.

- [2] Yao A C. Protocols for secure computations[C]//Proceedings of the 1982 IEEE 23rd Annual Symposium on Foundations of Computer Science. Chicago, USA: IEEE, 1982: 160-164.
- [3] Goldreich O, Micali S, Wigderson A. How to play any mental game or a completeness theorem for protocols with honest majority[C]//Proceedings of the Proceedings of the nineteenth annual ACM symposium on Theory of computing. New York, USA: ACM, 1987: 218-229.
- [4] Hong Y, Vaidya J. Secure transformation for multiparty linear programming[R]. Rutgers Technical Report, 2013.
- [5] Mangasarian O L. Privacy-preserving horizontally partitioned linear programs[J]. Optimization Letters, 2012, 6(3): 431-436.
- [6] Li W, Li H, Deng C. Privacy-preserving horizontally partitioned linear programs with inequality constraints[J]. Optimization Letters, 2013, 7(1): 137-144.
- [7] Hong Y, Vaidya J. An inference-proof approach to privacy-preserving horizontally partitioned linear programs[J]. Optimization Letters, 2014, 8(1): 267-277.
- [8] 刘木兰,张志芳.密钥共享体制和安全多方计算: Secret sharing schemes and secure multiparty computation[M].北京:电子工业出版社,2008.
- [9] Blum M, Goldwasser S. An efficient probabilistic public-key encryption scheme which hides all partial information[C]//Proceedings of the Advances in Cryptology. [S.l.]: Springer, 1985: 289-299.
- [10] Benaloh J C. Secret sharing homomorphisms: Keeping shares of a secret secret[C]//Proceedings of the Advances in Cryptology —CRYPTO'86. [S.l.]: Springer, 1987: 251-260.
- [11] Naccache D, Stern J. A new public key cryptosystem based on higher residues[C]//Proceedings of the Proceedings of the 5th ACM conference on Computer and communications security. Now York: ACM, 1998: 59-66.
- [12] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms[C]//Proceedings of the Advances in Cryptology. [S.l.]: Springer, 1985: 10-18.
- [13] Paillier P. Public-key cryptosystems based on composite degree residuosity classes[C]//Proceedings of the Advances in cryptology—EUROCRYPT'99. [S.l.]: Springer, 1999: 223-238.
- [14] 李庆扬,王能超.数值分析[M].北京:清华大学出版社,2001.
- [15] Du W, Atallah M J. Privacy-preserving cooperative scientific computations[C]//Proceedings of the Computer Security Foundations Workshop. [S.l.]: IEEE, 2001: 273-282.

(下转第103页)