基于全同态加密的理性委托计算协议

李秋贤[1],田有亮[1,2],王 缵[1]
(1. 贵州大学计算机科学与技术学院,贵州贵阳 550025; 2. 公共大数据国家重点实验室,贵州贵阳 550025)

摘 要: 传统委托计算因需验证方验证其计算结果,从而导致协议效率低下. 针对此问题,本文结合博弈委托代理理论和全同态加密技术,提出理性委托计算协议. 该协议通过参与者之间的效用函数保证计算结果的正确性,无需验证方进行验证. 首先,利用博弈委托代理理论,构造委托计算博弈模型;其次,结合全同态加密技术,构造理性委托计算协议;最后,对协议进行实验与分析,结果表明,该协议不但保证了安全性和正确性,并且全局可达帕累托最优.

关键词: 理性委托计算; 博弈论; 效用函数; 帕累托最优; 全同态加密
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112(2019)02-0470-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.02.030

Rational Delegation Computation Protocol Based on Fully Homomorphic Encryption

LI Qiu-xian[1], TIAN You-liang[1,2], WANG Zuan[1]
(1. *College of Computer Science and Technology, Guizhou University, Guiyang, Guizhou* 550025, *China*;
2. *National Key Laboratory of Public Big Data, Guiyang, Guizhou* 550025, *China*)

Abstract: The traditional delegation computation require the verification party to verify the results, which leads to low efficiency of computation protocol. To solve this problem, this paper combines the game principal-agent theory and the fully homomorphic encryption technology to propose a rational delegation computation protocol. This protocol guarantees the correctness of the results through the utility function between the participants, without the validation of the prover. Firstly, we use the game principal-agent theory to construct a game model. Secondly, we combine the fully homomorphic encryption technology to construct the rational delegation computation protocol. Finally, we test and analyze the protocol, the results show that this protocol not only guarantees the safety and validity, and can achieve global Pareto optimality.

Key words: rational delegation computation; game theory; utility function; Pareto optimality; fully homomorphic encryption

1 引言

委托计算[1]是大数据与云计算环境下,解决任务授权过程中产生结果可靠性问题的重要手段. 传统委托计算方案大致可分两类:基于复杂性理论的构造方案[2,3]和基于密码学技术构造的方案[4~6]. Chung 等[7]使用全同态加密技术设计的委托计算方案,使委托方不可能接受除 $F(x_i)$ 之外的结果,提高了委托计算的计算效率. 而在现实生活中,各参与者行为和偏好不同,结合博弈论提出理性委托计算模型对当前大数据环境下的庞大计算任务将具有更加重要的理论意义和实际应用价值.

近年来理性证明已经成为越来越多学者研究的热点,理性证明系统是博弈论与交互式证明相互交叉融合的产物. Tian 等[8,9]基于博弈论框架,研究了秘密共享体制的分发机制和重构机制,引入理性参与者,并对理性密码协议的发展进行了研究;Xiao 等[10,11]也利用博弈论设计了社会规范与声誉系统,并利用博弈论提供了一种研究智能干扰机和二级用户之间的相互作用的强大方法.

收稿日期:2017-12-13;修回日期:2018-11-05;责任编辑:李勇锋
基金项目:国家自然科学基金(No. 61772008);贵州省教育厅科拔尖人才支持项目(黔教合 KY 字[2016]060);贵州省科技重大专项计划(No. 20183001);贵州省科技计划项目(黔科合平台人才[2017]5788 号);教育部—中国移动科研基金研发(No. MCM20170401);贵州大学培育项目(黔科合平台人才[2017]5788)

在委托计算中,由于验证方需要对计算结果进行验证且可能存在一些恶意参与者为了自身的利益而偏离协议.本文结合博弈论与全同态加密技术提出了一个理性委托计算博弈协议,不但提高了委托计算的效率还保证全局可达帕累托最优.

2　基础知识

定义 1(博弈)　博弈表达的基本式由局中人集合 P、策略空间 S 和效用函数 u 三个要素组成,即 $G=\{P,S,u\}$,其中 $P=\{P_1,\cdots,P_n\}$,$S=\{S_1,\cdots,S_n\}$,$u=\{u_1,\cdots,u_n\}$.效用函数 u_i: $S\rightarrow R$(R 代表实数空间),它表示第 i 位局中人在不同策略组合下所得的收益.

定义 2(全同态加密)　一个全同态加密方案一般由以下四个算法组成:预处理阶段、加密阶段、解密阶段和运算函数.

3　委托计算博弈模型

理性委托计算是结合博弈论和委托计算的思想,从参与者自利角度出发,通过效用函数来保障计算结果的可靠性.参与者根据激励合约采取策略,追求各方自身利益的最大化的同时保证全局利益的最优化,从而达到全局帕累托最优.

本节设计的委托计算博弈模型是一个七元组(P,φ,S,$P(\cdot)$,ρ,U,E).

(1)参与者集合 P:参与执行委托计算协议的所有参与方.

(2)外生随机变量 φ:指不受参与方控制的外生随机变量(称为"自然状态").

(3)策略集合 S:委托计算中各参与者可能采取的所有行动集合.

(4)支付函数 $P(\cdot)$:委托方给予计算方委托计算的支付报酬.

(5)参与者风险规避 ρ:指参与者在理性委托计算中所能承担的风险规避程度.

(6)参与者期望效用函数 U:U_n:$S\rightarrow R$(R 代表实数空间),它表示第 n 位局中人在不同策略组合下所得的期望收益.

(7)总期望效用 E:理性委托计算中双方达到最大化期望效用函数.

3.1　参与者

我们首先来建模理性委托计算协议的各参与方.该模型中主要有两个参与方:委托方 P_1 和计算方 P_2,且参与者都是理性的.因此,该委托计算博弈的参与者集合定义为 $P=\{P_1,P_2\}$.

3.2　外生随机变量

在理性委托计算中,存在不受参与方控制的外生随机变量(称为"自然状态").我们令 φ 表示外生随机变量,由委托过程中一系列不确定因素决定,且 φ 服从均值为 0、方差为 σ^2 的正态分布.一般的,存在不确定外生随机影响因素的委托方与计算方之间的博弈如图 1 所示.字母 s 和 d 分别代表委托方和计算方的收益.

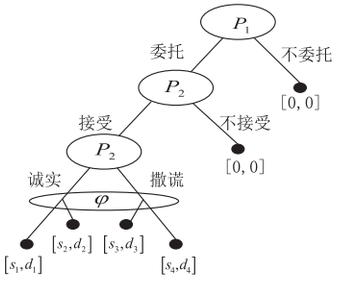


图1　委托方与计算方之间博弈

3.3　策略集合

假设此模型中委托方的策略集为 $s_1=\{s_{11},s_{12}\}$,其中 s_{11} 和 s_{12} 分别表示委托方选择"奖励"和"惩罚"策略.计算方的策略集为 $s_2=\{s_{21},s_{22}\}$,其中 s_{21} 和 s_{22} 分别表示计算方选择"诚实"和"撒谎"策略.双方达到最大化效用函数采用货币形式表示为 $\pi=ks_2+\varphi$,其中 k 为计算方采取不同策略对双方总效用的影响系数,且 $k>0$;由于环境变量 φ 服从正态分布,因此双方总期望效用为 $E(\pi)=E(ks_2+\varphi)=ks_2$,$Var(\pi)=\sigma^2$,即计算方采取的策略决定双方效用的均值,但不会对双方效用的方差有影响.

3.4　支付函数

在该模型中,为了更好的刻画在激励合同的存在下,委托方激励计算方通过效用函数保证计算结果的正确性.所以将委托方给予计算方的支付金额设为线性函数 $P_2(\pi)=\alpha+\beta\pi$,其中 α 为计算方完成任务的固定收入,β 为委托方对计算方的激励系数.

在委托计算过程中,双方将对采取策略付出的努力来最大化自己的利益.其中委托方 P_1 采取不同策略的努力成本可表示为 $C(s_1)=x_1(\pi-\eta\pi)^2/2$,计算方 P_2 的努力成本为:$C(s_2)=x_2s_2{}^2/2$.x_1 和 x_2 分别表示委托方和计算方选择不同策略成本系数,且 $x_1>0$,$x_2>0$,$\eta(0<\eta<1)$ 表示计算方选择不同策略后的成效系数,即计算方在协议中越努力,委托方实际效益与预期效益之间的差距就越小.

3.5　风险规避

在理性委托计算中,各参与者对风险规避的程度存在较大的差异.基于帕累托最优的委托计算博弈模型中考虑参与者风险规避就是因个体间的差异而引入的.参与者的风险规避效用函数为 $u=-e^{\rho\omega}$,其中 ρ 为绝对风险规避度量,ω 是实际货币收入.由于委托方和计算方都是风险规避特性的,都将存在风险成本,其风

险成本分别为：

$$P_{1风险}=\frac{1}{2}\rho_1\mathrm{var}(\pi-P_2(\pi))=\frac{1}{2}\rho_1(1-\beta)^2\sigma^2 \quad (1)$$

$$P_{2风险}=\frac{1}{2}\rho_2\mathrm{var}(P_2(\pi))=\frac{1}{2}\rho_2\beta^2\sigma^2 \quad (2)$$

其中，$P_{1风险}$和$P_{2风险}$分别表示委托方和计算方在协议中的风险成本，即参与方选择不同策略承担的风险，ρ_1和ρ_2分别代表委托方和计算方的风险规避程度，且$\rho_1>0,\rho_2>0$.

3.6 期望效用函数

在理性委托计算方案中，由于委托方与计算方都是风险规避特性的，因此通过在委托计算中参与者得到的实际收入来衡量参与方的效用. 因为存在风险成本，委托方和计算方的实际收入分别为$w_1=\pi-P_2(\pi)-C(s_1)$和$w_2=P_2(\pi)-C(s_2)$. 所以根据参与者的实际收入，可以分别得到委托方和计算方的期望效用函数：

$$U_1=E(\pi-P_2(\pi)-C(s_1)-P_{1风险}) \quad (3)$$

$$U_2=E(P_2(\pi)-P_2(s_2)-P_{2风险}) \quad (4)$$

3.7 总期望效用

由于计算方接受与委托方之间的激励合同所得效用大于计算方不接受此激励合同，即计算方的期望效用不得小于不接受得到的最低保留效用$\bar{u}$，所以计算方必须考虑与自己相关的参与约束 IR.

$$\mathrm{IR}:\alpha+\beta k s_2-\frac{1}{2}x_2 s_2^2-\frac{1}{2}\rho_2\beta^2\sigma^2\geq\bar{u} \quad (5)$$

又因双方的信息不对称，即委托方不能知道计算方会选择哪种策略. 而理性计算方总会选择使得自己期望效用最大的策略，因此委托方希望得到的最大效用只能通过计算方的期望效用最大来实现. 如果策略s_2是委托方期望计算方选择的策略，根据激励合同，只有当计算方选的策略为s_2的效用才比选择策略s'_2更大，因此计算方会因其理性选择策略s_2.

所以，计算方为了保证效用达到最大，将会选择策略s_2，即：$\mathrm{Max}_{s_2}(W)$，令$\partial W/\partial s_2=0$，则$s_2=\beta k/x_2$，则存在一个激励相容约束 IC.

$$\mathrm{IC}:s_2=\beta k/x_2 \quad (6)$$

将 IR 和 IC 带入委托方期望效用的目标函数中，构建拉格朗日函数可得：

$$L(\alpha,\beta)=(1-\beta)k\frac{\beta k}{x_2}-\alpha-\frac{1}{2}x_1(1-\eta)^2k^2\left(\frac{\beta k}{x_2}\right)^2-\frac{1}{2}\rho_1(1-\beta)^2\sigma^2+\phi\left(\alpha+\beta k s_2-\frac{1}{2}x_2 s_2{}^2-\frac{1}{2}\rho_2\beta^2\sigma^2-\bar{u}\right) \quad (7)$$

将构造的拉格朗日函数$L(\alpha,\beta)$求关于α和β的一阶导数，即令$\partial L/\partial\alpha=0$，$\partial L/\partial\beta=0$，此时，$\lambda=1$.

从函数的变化趋势也可得出，委托方的风险规避程度ρ_1和其对计算方的激励系数β是正相关的. 进一步可求得当利益达到最大化的时候，计算方应该选择的策略及努力程度：

$$s_2=\frac{\beta k}{x_2}=\frac{k^3+x_2\rho_1\sigma^2 k}{k^2x_2+x_2(1-\eta)^2k^4+x_2^2(\rho_1+\rho_2)\sigma^2} \quad (8)$$

此时，委托方和计算方总的期望效用达到最大，为：

$$E(\pi)=\frac{k^4+x_2\rho_1\sigma^2k^2}{k^2x_2+x_2(1-\eta)^2k^4+x_2^2(\rho_1+\rho_2)\sigma^2} \quad (9)$$

根据委托计算博弈模型可知，委托方和计算方根据激励合约进行执行，只有委托方激励计算方选择最优的策略，双方利益才能达到最优，整个过程的收益$E(\pi)$也达到最优，及达到全局帕累托最优.

4 理性委托计算协议

4.1 初始化阶段

首先输入安全参数1^λ和委托函数f，输出公钥PK和私钥SK，将公钥传送至云端，私钥保存在本地，其中$f:\{0,1\}^n\rightarrow\{0,1\}^m$. 假设协议中委托方$P_1$具有计算数据$m$，在该阶段委托方对数据进行加密，防止计算方篡改. 并将数据m按照需求分块加密$c_i\leftarrow Encrypt_{FHE}(PK,m_i)$，$i=1,\cdots,n$，得到密文组$c_i=(c_1,c_2,\cdots,c_n)$，把$(c_i,f)$发送给计算方.

4.2 委托计算和承诺阶段

计算方P_2根据自己的能力选择接受此计算任务(c_i,f). 此时，委托方与计算方约定在时间t内完成计算任务. 计算方输入公钥，密文组和求值函数，得到函数值$c_f\leftarrow Eval_{FHE}(PK,c_i,f)$. 完成计算后，采用 Pedersen 承诺对计算结果c_f进行承诺，承诺值为$E_{c_f1}=E_{c_f1}(c_f,r)=g^{c_f}h^r\mathrm{mod}p$和$E_{c_f2}=E_{c_f2}(c_f,r)=hash(c_f\|r)$，并且在$t'$内将承诺值$(E_{c_f1},E_{c_f2})$返回给委托方. 在这个阶段，要求任意概率多项式时间的接收方都不能得到关于承诺值的任何信息.

4.3 验证和支付阶段

当委托方收到计算方返回的承诺值和计算结果后，委托方根据计算方提供的随机数r验证承诺函数是否成立. 如果等式成立，则委托方接收此计算结果；否则拒绝接收. 此时还需要考虑委托方与计算方交互时间t'的范围，若$t'\leqslant t$，根据双方的激励合约，委托方需在t时间内将金额$P_2(\pi)$发送给计算方，反之计算方将支付惩罚金$P_2(\pi)'$给委托方.

委托方和计算方交互式证明以后，委托方只需对承诺进行验证，根据各方的期望效用函数U_1和U_2对自己在委托计算中的成效进行判断. 若任一方偏离协议，对方有权要求得到远大于U_1或U_2的赔偿金作为补偿. 由于此方案中参与者都是理性的，双方通过制定的激

励合约以及双方的效用函数来激励参与者积极遵守协议,从而提高委托计算的效率. 其协议如图 2.

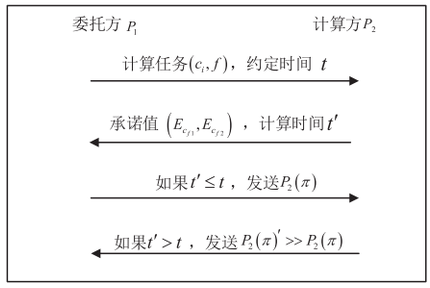


图2　理性委托计算协议

5　协议分析

5.1　安全性分析

定理 1　本文所提协议中,如果全同态加密满足安全性,则所提基于全同态加密的理性委托计算协议是安全的.

证明　首先在委托计算和承诺阶段,假如该协议中存在恶意的计算方将数据 c_i 篡改为 c'_i,使得 $c'_f \leftarrow Eval_{FHE}(PK,c'_i,f)$ 成立. 此时计算方对计算结果 c'_f 进行承诺并选择一个随机数 m,计算 $E'_{c_f1}=g^{c'_f}h^{r+m}\bmod p$ 和 $E'_{c_f2}=hash(c'_f\|r+m)$. 当恶意计算方出示$(c'_f,r+m)$揭开承诺时,根据单项函数的散列性质,恶意方无法从 E_{c_f2}得到(c_f,r).

又因为 g,h 是 Z_p^* 的生成元,存在 l 使得 $h=g^l\bmod p$ 成立 ,即$E_{c_f1}=g^{c_f+lr}\bmod p$. 给定一个$y=g^x\bmod p$,计算离散对数 $x=\log_p y$. 作为对 x 的承诺,把(E_{c_f1},E_{c_f2})给恶意计算方. 但根据离散对数的假设,恶意计算方无法得到 x 的值. 所以攻击者在任意概率多项式时间的找到 c'_f 和 r'使得 $E_{c_f}(c_f,r)=E'_{c_f}(c'_f,r')$的概率是可以忽略的. 因此本文提出的基于全同态加密的理性委托计算协议是安全的.

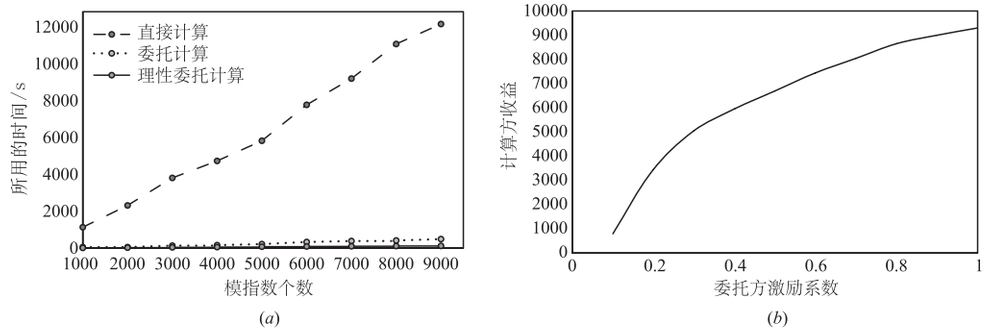
5.2　正确性分析

定理 2　该基于全同态加密的理性委托计算协议具有正确性,并且协议满足全局帕累托最优.

证明　在本协议中,如果参与者方都遵守协议规则,那么将选择对全局最有利的策略. 计算方将在能力范围内接受计算任务. 在计算过程中,计算方在时间 t 内将计算结果进行承诺并返回给委托方. 若计算方采取策略 s_{22},计算方的效用为 $U'_2=E(P_2(\pi)-C(s_{22})-P_{2风险})$,委托方的效用为 $U'_1=E(\pi-P_2(\pi)-C(s_1)-P_{1风险})$,由于环境变量 φ 服从正态分布,因此双方总期望效用为 $E(\pi)=E(ks_{22}+\varphi)=ks_{22}=0$,计算方将会受到严重惩罚. 因此计算方会选择策略 s_{21}最大化自己的效益,委托方的效益也将最大,即该协议具有正确性,并且协议满足全局帕累托最优.

5.3　实验结果与性能分析

针对给出的基于博弈论机制的理性委托计算方案,我们借鉴文献[12]中用户将不同数量的模指数运算委托出去时,所需时间的开销. 以及计算方采用不同策略时,委托方的激励系数对计算方效益的影响,如图 3 所示.



(a)　(b)

图3　协议时间开销对比及效益走势

下面将本文提出的理性委托计算协议与现有的委托计算协议进行比较. 表 1 从委托计算的计算复杂度与通信复杂度与其他协议进行对比.

表 1　本协议与其他协议性能对比

	计算复杂度	通信复杂度
Gennaro 等[6]协议	$O(\|C\|\cdot poly(\lambda))$	≥2
Chen 等[13]协议	$O(1)$	1
本文协议	$O(1)$	1

Gennaro 等[6]提出了基于 Yao 的混淆电路与全同态加密技术构造可验证的委托计算协议,Chen 等[13]提出了在分布式环境中将计算任务委托给不受信任的计算方,本协议是基于委托代理理论和全同态加密技术构造了理性委托计算协议. 协议的计算复杂度与通信复杂度较低,且由实验可知,当计算任务委托给不受信任的计算方时,计算量越大,理性委托计算协议的效率就越高.

6 结论

本文基于博弈委托代理理论和全同态加密技术提出了理性委托计算协议,将计算任务委托给不受信任的计算方.详细分析了在博弈理论框架下委托计算中各参与方的效用及策略,保证了协议的安全性与正确性,且协议中全局能达帕累托最优.

参考文献

[1] Goldwasser S, Kalai Y T, Rothblum G N. Delegating computation: Interactive proofs for Muggles[A]. ACM Symposium on Theory of Computing[C]. Victoria, British Columbia, Canada, DBLP, 2008. 113 – 122.

[2] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof systems[J]. SIAM Journal on Computing, 1989, 18(1): 186 – 208.

[3] Kalai Y T, Raz R. Probabilistically Checkable Arguments [M]. Advances in Cryptology-CRYPTO 2009. Berlin Heidelberg: Springer, 2009. 143 – 159.

[4] Gentry, Craig. Fully homomorphic encryption using ideal lattices[J]. Stoc, 2009, 9(4): 169 – 178.

[5] Gennaro R, Wichs D. Fully Homomorphic Message Authenticators [M]. Advances in Cryptology-ASIACRYPT 2013. Berlin Heidelberg: Springer, 2013. 301 – 320.

[6] Gennaro R, Gentry C, Parno B. Non-interactive Verifiable Computing: Outsourcing Computation to Untrusted Workers[M]. Advances in Cryptology – CRYPTO 2010. Berlin Heidelberg: Springer, 2010. 465 – 482.

[7] Chung K M, Kalai Y, Vadhan S. Improved Delegation of Computation Using Fully Homomorphic Encryption[M]. Advances in Cryptology – CRYPTO 2010. Berlin Heidelberg: Springer, 2010. 483 – 501.

[8] 田有亮,马建峰,彭长根,等. 秘密共享体制的博弈论分析[J]. 电子学报,2011,39(12):2790 – 2795.
TIAN Y L, MA J F, PENG C G, et al. Game-theoretic analysis for the secret sharing scheme[J]. Acta Electronica Sinica, 2011, 39(12): 2790 – 2795.

[9] 田有亮,李秋贤. 理性密码协议研究进展[J]. 贵州大学学报:自然科学版,2018,(3):14 – 23.
TIAN Y L, LI Q X. Research progress on rational cryptography protocol[J]. Journal of Guizhou University: Natural Science Edition, 2018, (3): 14 – 23.

[10] Xiao L, Chen Y, Lin W S, et al. Indirectreciprocity security game for large-scale wireless networks [J]. IEEE Transactions on Information Forensics & Security, 2012, 7(4): 1368 – 1380.

[11] Xiao L, Chen T, Liu J, et al. Anti-jamming transmission stackelberg game with observation errors[J]. IEEE Communications Letters, 2015, 19(6): 949 – 952.

[12] Wang Y, Wu Q, Wong D S, et al. Securely Outsourcing Exponentiations with Single Untrusted Program for Cloud Storage[M]. Computer Security-ESORICS 2014. Springer International Publishing, 2014. 326 – 343.

[13] Chen X, Li J, Susilo W. Efficient fair conditional payments for outsourcing computations[J]. IEEE Transactions on Information Forensics & Security, 2012, 7(6): 1687 – 1694.

作者简介

李秋贤 女,1992 年生,河南温县人,硕士研究生,主要研究方向为密码学与安全协议.
E-mail:547230161@qq.com

田有亮(通信作者) 男,1982 年生,贵州盘县人,博士、教授,主要研究方向为博弈论、密码学与安全协议.
E-mail:youliangtian@163.com