

# 分散环境下的组合资源拍卖

## 利用区块链和差分隐私的边缘事物系统

郭, 丁兴健和佳, IEEE 研究员

**摘要**——随着物联网设备的不断扩展, 近年来出现了边缘计算模式, 以克服传统云计算模式延迟高、网络拥塞、资源消耗大的缺点。因此, 边缘物系统将取代经典的云物/云边缘物系统, 逐渐成为主流, 物联网设备可以将任务卸载到相邻的边缘节点。一个常见的问题是如何利用边缘计算资源。为了公平起见, 可以在边缘物系统中使用双重拍卖来实现有效的资源分配和定价机制。由于缺乏第三方管理机构 and 节点之间的互不信任, 在我们的边缘物系统中, 我们引入区块链来防止恶意节点篡改交易记录 and 智能合约, 充当拍卖人来实现资源拍卖。由于存储在这个基于区块链的系统中的拍卖结果是透明的, 因此它们受到推理攻击的威胁。因此, 本文通过探索指数机制, 设计了一种差异化的私有组合双拍卖机制, 使得边缘计算平台的收益最大化, 其中每个物联网设备请求一个资源包, 边缘节点相互竞争提供资源。既能保证近似真实和高收益, 又能保证隐私安全。通过必要的理论分析和数值模拟, 我们提出的机制的有效性可以得到验证。

**索引术语**—物联网、区块链、智能合约、边缘物系统、组合拍卖、真实性、收益、差别隐私。

### 1. 介绍

WITH 随着电子设备和通信基础设施的迅速完善, 物联网已经成为连接物理环境和系统空间的热门研究课题。物联网设备无处不在, 在我们的生活中扮演着重要的角色, 例如手机、cameras、汽车和交通传感器。近年来, 物联网设备数量激增。根据思科[1] [2]进行的一项调查, 他们预测 2025 年前将有超过 750 亿台物联网设备投入使用。这些物联网设备产生大量数据。怎么

J. 郭和 w. 贾来自人工智能与未来网络研究所, 北京师范大学珠海分校, 中国广东 519087, 以及联合国际学院人工智能与多模态数据处理广东重点实验室, 中国广东珠海 519087。(电子邮件: jianxiongguo@bnu.edu.cn; jiawj@uic.edu.cn)

X. 丁, 北京理工大学软件工程学院, 北京 100124。(电子邮件: dxj@bjut.edu.cn)

(对应作者: 郭)

手稿于 2005 年 4 月 19 日收到; 2015 年 8 月 26 日修订。

利用这些数据更好地服务社会, 已经引起学术界和工业界越来越多的关注, 并带动了智能家居、智能供应链、医疗保健、产品溯源等一系列下游产业的发展。

处理这些数据以产生有价值的信息并不容易, 这通常涉及一些人工智能算法或数据挖掘技术。它要求物联网设备具有一定的计算能力和存储空间。然而, 大多数物联网设备都是轻量级的, 只能临时存储少量数据并执行简单操作。在传统的云物系统中, 物联网设备依靠云中心的计算能力、网络带宽和存储空间来实现自己的功能。通常情况下, 云中心距离物联网设备较远, 导致能耗和网络损耗较高。此外, 它还面临单点故障的威胁[3] [4], 使该系统更加不可靠。于是, cloud edge-things 系统应运而生。有很多边缘服务器均匀分布在空间的各个角落。这些边缘节点为附近的物联网设备提供所需的资源。因此, 物联网设备可以将其任务卸载到相邻的边缘节点, 而不是云中心。尽管云-

边-物系统克服了云-物系统的一些缺陷, 特别是长距离传输, 但它并没有完全摆脱云中心的控制。

因此, 我们关注本文中的边缘事物系统, 它是完全分散的, 没有第三方机构的管理。但是在物联网设备和边缘节点之间的资源分配中, 由于利益冲突, 两者互不信任, 两个实体都希望自己的收益最大化。此外, 存储在边缘节点的交易记录可能被恶意篡改。考虑到这一点, 区块链[5]提供了一个提供安全对等(P2P)网络的机会。区块链是一个分布式分类账, 用于存储系统中所有活动参与者生成的实时数据。它不仅可以实现完全的去中心化, 还具有防篡改和透明的特点。区块链证明的安全 P2P 网络可以作为一种辅助技术来设计我们的边缘系统。

为了反映真实的市场波动和供需关系, 拍卖被证明是有效的, 这样物联网设备就可以以可接受的价格获得所需的资源, 边缘节点也可以从提供资源中受益。在本文中, 我们设计了一个基于区块链的边缘物系统, 其中资源的分配和定价是通过一个组合的双拍卖机制来实现的。这里, 物联网设备是请求资源的买方, 边缘节点是提供资源的卖方。因为我们采用了完全分散的架构, 所以没有合适的实体来充当负责执行拍卖机制和决定拍卖结果的拍卖人。在我们的系统中, 拍卖机制存储在区块链构建的智能合约中, 当收到来自物联网设备和边缘节点的所有请求时, 该合约可以自动运行。不同的物联网设备对每种资源类型有不同的要求。例如, 智能家居中的设备需要更多的计算能力来实现智能算法, 但交通监视器需要更多的存储空间来存储路况数据。每个物联网设备通常根据其任务请求一组资源, 并给出总出价, 这就是组合双拍卖的形成原因。设计拍卖机制的核心是衡量真实性, 从而鼓励买家/卖家出价/询问他们的真实估值。

由于分配和定价结果在区块链是透明的, 因此存在暴露买方/卖方出价/要求的可能风险。招标/询价信息是他们的隐私, 其中可能包含一些商业秘密。对手可以通过改变出价/要价来比较多轮公开拍卖的结果, 从而推断出其他人的出价/要价。这被称为“推理攻击”[6] [7]。为了防止玩家受到推理攻击的困扰, 差分隐私[8]是一种很有前途的技术, 具有很强的理论保证, 可以在设计拍卖机制时引入。尽管在以前的文献[9] [6] [10] [11] [12] [13]中已经提出了几种不同的基于隐私的拍卖机制, 但它们与我们边缘事物系统中的拍卖非常不同。首先, 我们的拍卖是组合式的, 因为每个买家都会对一堆资源给出总出价。其次, 每个边缘节点只能为每种资源类型提供有限的资源。第三, 物联网设备的资源请求只能由一个边缘节点来满足, 它们之间的距离是受约束的。考虑到边缘物系统的实际情况, 我们通过探索指数机制设计了一个有差别的私有组合双拍卖机制, 该机制以与其相应收益成比例的概率选择最终定价。在保证

隐私不被暴露的前提下，同时达到个人理性、预算平衡、计算效率和预期真实。我们的主要贡献可以总结如下。

- 1) 我们提出了一种基于区块链技术的新型边缘物体系结构，以实现完全的去中心化和防回火，其中内置的智能合约充当中心协调器。
- 2) 为了建模一个真实的边缘物系统，我们建立了一个组合双拍卖模型来实现物联网设备和边缘节点之间的资源分配。
- 3) 我们将差分隐私中的指数机制引入到我们的拍卖模型中，以确保隐私保护，并实现预期的真实性和近似高的收益。
- 4) 我们进行了广泛的模拟来评估我们提出的机制的性能。仿真结果验证了我们的理论分析。

组织:秒。第二，我们调查最先进的工作。以秒为单位。第三，引入边缘事物系统模型，正式定义我们的问题。以秒为单位。第四，介绍了差异化隐私描述机制设计。以秒为单位。我们给出了相关性质的证明。最后，我们通过 Sec 中的数值模拟来评估我们的机制。第六章，在第二节展示结论。七。

## II. 相关著作

近年来，资源配置的相关研究引起了学术界的广泛关注。拍卖理论已被应用于一系列相关领域，如移动众筹[14] [15]和能源交易[16] [17]。在移动边缘计算环境中。[18]提出了在物联网设备和边缘节点之间分配计算能力的双拍卖机制，其中物联网设备可以从边缘节点购买计算能力。Habiba 等人。[19]提出了基于位置的移动边缘计算反向拍卖框架，旨在最大化边缘服务器的效用。彭等。[20]在车辆边缘计算中设计了一种基于多属性的双拍卖机制，其中匹配由价格和非价格因素共同决定。然而，一个可信的拍卖师对于通过拍卖机制实现资源分配是必不可少的，尤其是对于双重拍卖。在 P2P 分布式边缘网络中，没有一个合适的实体可以充当拍卖商，保证安全性和可靠性。

区块链技术的出现有可能解决这一困境。它维护一个分散的分类账，并可以通过组合智能合同作为拍卖人。孙等。[21]在[18]中修订了他们以前的工作，引入区块链来实现一个值得信赖的平台。焦等。[22]提出了一个基于拍卖的市场模型，用于在矿工和边缘服务器之间分配计算资源。丁等。[23] [24]试图通过吸引更多的物联网设备从边缘服务器购买计算能力并参与共识过程来构建一个安全的基于区块链的物联网系统，在这一过程中，他们采用了多领导者多玩家 Stackelberg 游戏。郭等。[25]提出了一种基于 DAGblockchain 和双拍卖机制的安全高效的计费调度系统。然而，这些作品中的所有交易模型都是基于对一种资源的分配。他们没有考虑多种资源的分配。此外，他们没有考虑隐私泄露的潜在风险。

由于公开拍卖结果，参与者的敏感信息有被曝光的风险。为了防止对手推断玩家的敏感信息，德沃克等人。[8]创立了差别隐私理论。McSherry 等人。[9]首次将差别隐私应用于拍卖机制并做了完整的理论分析。陈等。[26]将差别隐

私与双频谱拍卖设计相结合，以近似最大化社会福利。郭等。[12]修订了他们在[25]中的工作，引入了差别隐私以避免投标/询价信息的泄露。此外，差分隐私已被用于频谱拍卖[6] [7]、智能电网[27] [28]和移动众筹[29]的机制设计。然而，将差分隐私应用于我们的组合双拍卖模型与现有的工作有很大不同。

## III. 边缘事物系统模型

在这一部分，我们详细介绍了 edgething 架构的系统模型，以及如何将区块链集成为一种有效的技术来克服潜在的安全威胁。这里，我们考虑时间可以离散成时隙，用  $T = \{t_1, t_2, t_3, \dots\}$  表示，其中每个时隙长度相等。下面的讨论是在一个时间段内进行的，包括组合拍卖机制和共识过程。最后，可以制定目标函数和问题定义。

### A. 系统描述

在现有的智能环境中，有大量的物联网设备部署在我们生活的各个角落，它们承担着自己不同的任务，如交通监控、健康记录、导航、机器学习培训等。由于其轻量级特性(资源有限)和延迟敏感性，这些物联网设备可以尝试将其任务卸载到相邻的边缘节点。为了量化对不同资源的需求，我们假设我们的系统中有  $k$  种资源，用  $R = \{r_1, r_2, \dots, r_k\}$  表示，其中每个  $r_i \in R$  代表某种资源，如计算、内存、存储或网络带宽。

一定数量的边缘节点可以在更强大的云中心和移动物联网设备之间形成中间层。在我们的系统中，有  $m$  个物联网设备，用  $TD = \{TD_1, \dots, TD_i, \dots, TD_m\}$  表示。这些物联网设备的计算能力和存储空间有限，因此不足以实现其目标。为了提升服务质量，物联网设备  $TD_i$  所需要的资源可以表示为  $D_i = \{d_{1i}, d_{2i}, \dots, d_{ki}\}$ ，其中  $d_{zi} \in [n, d_{max}]$ 。每个  $d_{zi} \in D_i$  表示物联网设备  $TD_i$  至少需要资源  $r_z$  的  $d_{zi}$  个单位。同样，有  $n$  个边缘节点，用  $EN = \{EN_1, \dots, EN_j, \dots, EN_n\}$  表示。这些边缘节点负责为物联网设备提供不同的资源。由边缘节点  $EN_j$  提供的资源可以表示为  $H_j = \{h_{1j}, h_{2j}, \dots, h_{kj}\}$ ，其中  $h_{ij} \in [h_{min}, h_{max}]$ 。每个  $h_{zj} \in H_j$  表示边缘节点  $EN_j$  最多提供资源  $r_z$  的  $h_{zj}$  个单元。因此，每个资源有限的物联网设备都必须向边缘服务提供商广播其资源请求，希望获得其想要的资源。

如前所述，在每个时隙，边缘节点通过出售资源获利，物联网设备通过购买资源完成任务，这就产生了双重拍卖问题。在双拍卖模式中，所有玩家都必须向拍卖人提交他们的请求。有一个重要的问题是谁将担任拍卖师。一个很自然的想法是让云中心做拍卖师。然而，这有所偏离

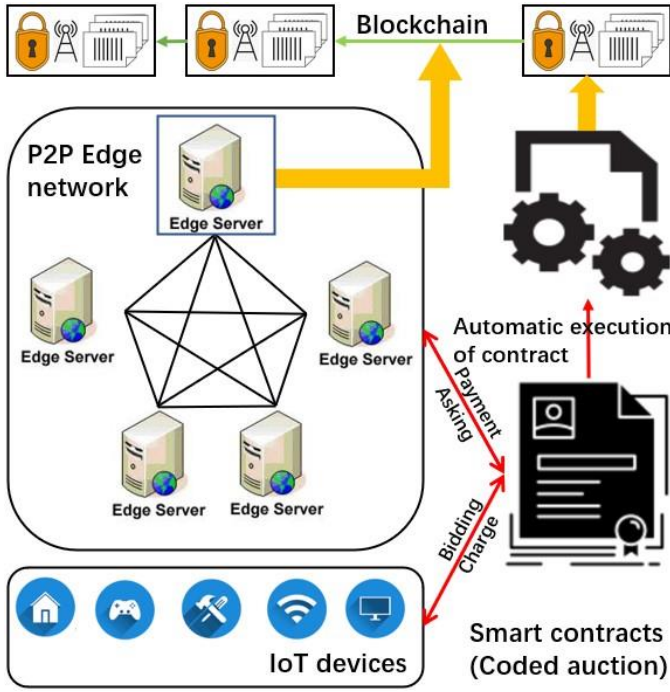


图 1. 基于区块链和智能合约的边缘系统架构。

脱离了我们摆脱云中心的初衷。在尝试集中式云中心时，有几个潜在的安全威胁，可以总结如下。

- 1) 漏洞:云中心受到恶意攻击者或意外灾难的攻击或破坏。它会导致单点故障。
- 2) 不安全:玩家提交的出价/要价信息可能被泄露或篡改。会造成数据丢失和隐私泄露。
- 3) 不可靠性:云中心偏向，为了自身利益与部分节点串通。会导致拍卖结果不公平。
- 4) 通信安全和网络延迟:云中心物理上远离物联网设备和边缘节点，在传输过程中会造成潜在的安全隐患和网络延迟。

为了克服上述缺点并实现去中心化，使用区块链和智能合约作为辅助技术来防止篡改并在没有第三方授权的非相似节点之间建立可信系统。物联网设备和边缘节点之间的事务存储在区块链。图 1 展示了我们支持区块链的边缘系统的架构。如图 1 所示，物联网设备是光节点，不存储区块链，但参与交易。边缘节点是完整的节点，用于存储完整的区块链，并执行一致的过程向区块链添加新块。此外，在区块链部署了智能合约，通过实现物联网设备和边缘节点之间的信息交互，自动执行预定义的拍卖机制，扮演拍卖人的角色。这样的系统不依赖第三方权威机构来充当拍卖人，也继承了区块链权力下放、温和抵制和透明的优势。

### B. 组合拍卖机制

为了模拟真实情况，我们假设每个物联网设备以捆绑的方式提交其资源请求，这制定了一个组合拍卖。例如，物联网设备需要完成训练深度学习模型的任务，从而想要从边缘节点购买计算和内存。更合理的做法是根据其对该任

务的估价给出总报价，而不是单独对每个资源进行报价。此外，我们发现这个任务只能在一个边缘节点上完成。换句话说，计算和内存资源必须来自同一个边缘节点，这增加了我们模型的局限性。

在典型的拍卖中，有三个关键角色，即买方、卖方和拍卖人。在我们的系统中，物联网设备是买家，因此买家集是  $TD$ ；边缘节点是卖家，因此卖家集是  $EN$ ；而聪明的合同就是拍卖师。在每个时隙中，买方请求一组资源，并给出它准备支付给边缘节点的购买这些资源的最大价格。对于每个购买者  $TD_i \in TD$ ，其竞价信息可以用  $B_i = (D_i, B_i, dmi)$  表示，其中  $B_i \in [vmin, vmax]$  是购买资源束  $D_i$  的总竞价(最大买入价格)， $dmi$  是从提供资源的边缘节点到它的最大容忍距离。对于每个卖家  $EN_j \in EN$ ，其询价信息可以用  $A_j = (H_j, A_j)$  表示，其中  $a_j = (a1j, a2j, , akj)$  是询价向量，其中每个  $azj \in a_j$  是每个资源  $rz$  的单位询价(最低售价)。买方的竞价信息和卖方的询价信息都提交给拍卖人，因此本次拍卖可以定义为

$$\Omega = \left( \{B_i\}_{TD_i \in TD}, \{A_j\}_{EN_j \in EN} \right). \quad (1)$$

此外，对于每个买方  $TD_i \in TD$ ，其获得资源束  $D_i$  的估值为  $VI \in [vmin, vmax]$ 。对于每个卖方  $EN_j \in EN$ ，它有一个成本向量  $c_j = (c_j^1, c_j^2, \dots, c_j^k)$ ，其中每个  $c_j^z \in [c_{min}, c_{max}]$  是单位资源成本  $rz$ 。

在每个时间段，一旦收集到竞拍和向玩家询问的信息，拍卖人将确定谁是获胜的买家和卖家，以及如何在他们之间分配资源。资源分配由二进制矩阵  $X_{m \times n}$  表示，称为“分配矩阵”。对于每个  $x_{ij} \in X$ ，如果根据结果， $TD_i$  请求的资源由  $EN_j$  提供，则  $x_{ij} = 1$ ；否则  $x_{ij} = 0$ 。此外，拍卖师需要确定每个资源的清算价格，可以用价格向量  $p = (p1, p2, , pk)$  来表示。对于每个  $p_z \in p$ ，它是购买者为了获得单位资源  $rz$  而必须支付的单价。

备注 1. 这里，我们有每个资源  $rz \in R$  的  $c_{zj} \in [c_{min}, c_{max}]$  和价格向量  $p \in [c_{min}, c_{max}]^k$ 。为简单起见，我们在下面的描述中用  $\vartheta = [c_{min}, c_{max}]$  表示。

### C. 问题定式化

根据上述定义，我们假设每个买方  $TD_i$  的效用由  $u_{TD_i}$  表示，每个卖方  $EN_j$  的效用由  $u_{EN_j}$  表示。拍卖师确定一个清算价格向量  $p$  及其对应的分配矩阵  $X$  后，所有输球玩家的效用都等于零。也就是说，我们对每个失败的买家  $TD_i \in TD$  if  $\sum_{j=1}^n x_{ij} = 0$  的  $u_{TD_i} = 0$ ，对每个失败的卖家  $EN_j \in EN$  if  $\sum_{i=1}^m x_{ij} = 0$  的  $u_{EN_j} = 0$ 。每个中标买家的效用是其估价和对其请求资源的付款之间的差额。总之，对于每个买方  $TD_i \in TD$ ，我们有

$$u_{TD_i} = \sum_{j=1}^n \sum_{z=1}^k VI X_{ij} X_{pz} c_{zj} \quad (2) \quad j=1 \quad z=1$$

如果买方的总付款和总成本之间存在差异, 则每个中标卖方的效用。总之, 对于每个卖家  $ENj \in EN$ , 我们有

$$\begin{aligned} & \sum_{z=1}^k \sum_{i=1}^m (p_z - c_{zj}) x_{ij} d_{zi} \\ & u_{ENj} = X(p_z - c_{zj}) X x_{ij} d_{zi}. \quad (3) \end{aligned}$$

因为买方请求的资源必须来自同一个卖方, 所以存在一个约束, 即  $\sum_{j=1}^n x_{ij} \leq 1$  对每个买方的  $TDi \in TD$ 。

拍卖的结果取决于它的目标。在这个系统中, 我们的目标是最大化边缘计算平台的收入。相应的优化问题可以概括为最大化所有边缘节点的累积效用, 表现为以下问题:

$$\max \sum_{j=1}^n \left[ \sum_{z=1}^k (p_z - a_j^z) \cdot \sum_{i=1}^m x_{ij} \cdot d_i^z \right] \quad (4)$$

其中  $\delta_{ij}$  是买方  $TDi$  和卖方  $ENj$  之间的传输距离。约束(4a)表示从物联网设备到边缘节点的多对一关系。约束(4b)声明每种资源  $r_z$  的总消耗不能大于边缘节点  $ENj$  能够提供的最大  $h_j^z$  量。约束(4c)意味着物联网设备  $TDi$  和为其提供资源的边缘节点之间的距离不能大于该物联网设备允许的最大距离。这个优化问题可以归为整数线性规划问题, 因此是 NP 难的。

#### IV. 机械设计

在这一部分, 我们首先介绍设计有效的组合拍卖机制的基本原理。由于使用了区块链技术, 该系统中的交易变得透明。也就是说, 所有的拍卖结果, 包括中奖者和清算价格, 都将被公开, 这使得系统面临推理攻击的威胁。因此, 我们在机制设计中引入了差别隐私, 以避免用户竞价/询价信息的意外泄露。

##### A. 设计原理

一个有效的拍卖机制必须满足以下四个属性: 个人理性、预算平衡、计算效率和真实性。

**定义 1(个体理性).** 当且仅当所有参与者的效用非负时, 拍卖才是个人理性的。  $TDi \in TD$  and  $u_j^{EN} \geq 0$  在我们的拍卖  $\omega$  中, 每个买家有  $u_i^{TD} \geq 0$ , 每个卖家有  $TNj \in TN$ , 其中  $u_{TDi}$  和  $u_{ENj}$  在(2)和(3)中定义。

**定义 2(预算平衡).** 当且仅当拍卖人有利可图时, 拍卖才是预算平衡的。在我们的拍卖  $\omega$  中, 也就是

$$\sum_{j=1}^n \left[ \sum_{z=1}^k (p_z - a_j^z) \cdot \sum_{i=1}^m x_{ij} \cdot d_i^z \right] \geq 0 \quad (5)$$

**定义 3(计算效率).** 拍卖结果可以在多项式时间内得到。

在拍卖中, 玩家可以在策略意义上操纵他们的出价/要求, 以赢得拍卖。真实性是一个鼓励拍卖中的参与者严格按照他们的估价/成本来出价/要价的概念。然而, 在某些情况下, 很难达到准确的真实性。因此, 我们可以考虑一个近似的真实性, 称为  $\gamma$  真实性[30], 它保证了当真实出价/要价时, 没有人获得超过  $\gamma$  的效用。

**定义 4( $\gamma$ -真实性).** 当且仅当每个玩家的出价/要价接近其主导策略之一时, 拍卖才是近似真实的。在我们的拍卖  $\omega$  中, 对于每个买家  $TDi \in TD$ , 我们有

$$\mathbb{E} [u_i^{TD}(v_i, \Omega_{-i})] \geq \mathbb{E} [u_i^{TD}(b_i, \Omega_{-i})] - \gamma \quad (6)$$

其中  $\omega_{-i}$  是除  $TDi$  之外的其他玩家的策略。对于每个卖家  $ENj \in EN$ , 我们有

$$\mathbb{E} [u_j^{EN}(c_j, \Omega_{-j})] \geq \mathbb{E} [u_j^{EN}(a_j, \Omega_{-j})] - \gamma \quad (7)$$

(4c)

其中  $\omega_{-j}$  是除  $ENj$  之外的其他玩家的策略。

(4d)

当我们在拍卖中讨论真实性时, 我们假设买方提交的重新请求包  $Di$  和卖方提交的总资源  $Hj$  都是可信的, 因为它们可以被监控。由于真实性, 没有玩家有动机操纵其策略来获得更多的效用, 这使得玩家的战略决策更加容易, 并保证了公平的竞争环境。

##### B. 差别隐私

在我们的系统中应用的区块链只能保证物理层面的安全, 但不能防止推理攻击。好奇的玩家可以通过在连续的拍卖回合中改变自己的出价/要价并分析相关的拍卖结果来推断其他玩家的策略。在其他玩家策略的帮助下, 攻击者能够做出对自己有利的决策并增加其收益, 从而破坏公平性。为了防止这种威胁, 我们选择设计一种差别化的私人拍卖机制。差分隐私是一种使攻击者无法高概率区分两个相邻输入的技术[8]。两个数据集  $s = (s_1, s_2, \dots, s_i)$  和  $s_0 = (s_1, s_2, \dots, s_{0i}, \dots)$  是相邻的, 当且仅当它们恰好有一个不同的元素。为了方便起见, 我们用所有买方的出价  $b = (b_1, b_2, \dots, b_m)$  和所有卖方的要价  $A = (a_1, a_2, \dots, a_n)$  来表示。差别隐私的定义如下所示。

**定义 5(差别隐私).** 我们将我们的拍卖机制简化为一个函数  $M()$ , 它将输入出价  $b$  和输入请求  $A$  映射到一个清算价格  $p$ 。机制  $M()$  给出了任意两个相邻的  $\epsilon$ -差分隐私的充要条件

投入  $(b, A)$  和  $(b', A)$  or  $(b, A')$ , 我们有

$$\Pr[M(b, A) = p] \leq \exp(\epsilon) \Pr[M(b_0, A) = p] \quad (8)$$

$$\Pr[M(b, A) = p] \leq \exp(\epsilon) \Pr[(M(b, A_0) = p)] \quad (9)$$

其中常数  $\epsilon$  是隐私预算。

隐私预算是一个参数，用于控制机制提供的隐私保护程度。一般来说，隐私预算越小，隐私保护越强。通过在我们的拍卖机制中引入差别隐私，玩家出价/要价的变化不会显著影响最终的清算价格。因此，它防止我们通过操纵策略和分析拍卖结果进行推理攻击。

指数机制[8]是实现实用差分隐私的主流方法之一。它依赖于将输入/输出对映射到分数的“分数”函数  $Q()$ 。我们拍卖中的得分函数可以定义为  $Q((b, A), p)$ ，其中如果候选输出的得分较高，则更有可能被选中。因此，指数机制可以定义如下。

定义 6(指数机制)。给定一个输出  $p \in \Theta_k$ 、一个评分函数  $Q()$ ，以及一个隐私预算  $\epsilon$ ，指数机制  $M(b, A)$  选择  $p$  作为其输出，概率与其评分  $\epsilon Q$  成正比  $((b, A), p)$ 。因此，我们有

$$M(b, A) = p] \propto \exp \left( \frac{\epsilon Q((b, A), p)}{2\Delta Q} \right) \quad (10)$$

其中  $\Delta Q$  是得分函数  $Q()$  的灵敏度。这是任意两个相邻输入  $(b, A)$  和  $(b', A)$  或  $(b, A_0)$  的最大差值，可以用  $\Delta Q = \max_{(b, A), (b', A)} |Q((b, A), p) - Q((b', A), p)|$  表示。

### C. 算法设计与描述

我们的拍卖机制的设计目标是最大化边缘计算平台的收益，但是算法 1 DPAM

输入:  $\{B_i\} \text{TD}_i \in \text{TD}$ ,  $\{A_j\} \text{EN}_j \in \text{EN}$ ,  $\epsilon$ ,  $\theta$

输出:  $X_p, p$

```

1: 初始化  $\Delta R = \sum_{j=1}^n (c_{max} - c_{min}) \cdot \sum_{z=1}^k h_j^z$ 
2: 对于每个  $p \in \Theta_k$  do
3:   //获胜候选人的确定
4:   为每个  $x_{ij} \in X_p$  初始化  $x_{ij} = 0$ 
5:   初始化  $\text{TDc} \leftarrow \emptyset$ 
6:   对于每个  $\text{TD}_i \in \text{TD}$  do
7:     如果  $\sum_{z=1}^k p_z \cdot d_i^z \leq b_i$  then
8:        $\text{TDc} \leftarrow \text{TDc} \cup \{\text{TD}_i\}$ 
9:     如果...就会结束
10:  结束于
11: 对  $\text{TDc}$  s.t. 进行排序。  $\sum_{z=1}^k d_1^z \geq \sum_{z=1}^k d_2^z \geq \dots$ 
12:  //赋值
13:  初始化  $\{h_j^{1'}, h_j^{2'}, \dots, h_j^{k'}\}$ , 其中  $h_{j0} = h_{jz} \in H_j$ 
```

```

14: 对于每个  $\text{TD}_i \in \text{TDc}$  do
15:   初始化  $\text{ENC}$ ,  $i \leftarrow \emptyset$ 
16:   对于每个  $\text{EN}_j \in \text{EN}$  do
17:     如果每个  $r_z \in R$  的  $h_{zj} \geq d_{zi}$ ,  $\delta_{ij} \leq d_{mi}$ , 并且
        $\sum_{z=1}^k (p_z - a_j^z) \cdot d_i^z \geq 0$ 
        $\text{EN} \cup \{\text{EN}_j\}$  然后
18:        $c, i \uparrow$   $c, i \leftarrow j$ 
19:     如果...就会结束
20:     结束于
21:     如果  $\text{ENC}$ ,  $i \neq \emptyset$ 
22:  $\text{EN}_j \leftarrow \text{ArgMineN}_j \in \text{ENC}$ ,  $i \neq \emptyset$ 
23: 对于每个  $r_z \in R$  do
24:    $h_{zj} \leftarrow h_{zj} \cdot d_{zi}$ 
25:   结束于
26:    $x_{ij} \leftarrow 1$ 
27:   如果...就会结束
28:   结束于
29:    $R((b, A), p) = P_{nj} = 1[P_{kz} = 1(p_z - a_{zj})P_{mi} = 1 \text{ xij } d_{zi}]$ 
30: 结束
31: //定价
32: 根据选择分布选择一个  $p \in \Theta_k$ :

$$\Pr[M(b, A) = p] = \frac{\exp \left( \frac{\epsilon R((b, A), p)}{2\Delta R} \right)}{\sum_{p^0 \in \Theta_k} \exp \left( \frac{\epsilon R((b, A), p^0)}{2\Delta R} \right)}$$

33: return  $X_p, p$ 
```

同时实现  $\epsilon$ -差分隐私、 $\gamma$ -真实性、个体理性、预算平衡和计算效率。该机制可分为三个阶段，中标候选人确定、分配和定价。程序如算法 1 所示。

在确定中标候选人时，我们首先选择  $\text{TD}$  的一个子集作为中标买方候选人，用  $\text{TDc} \subseteq \text{TD}$  表示。给定价格向量  $p \in \Theta_k$ ，我们有  $\text{TD}_i \in$

当且仅当  $\text{TDc}$  满足

$$X_{pz} d_{zi} \leq b_i. \quad (11)$$

然后，我们根据他们请求的资源量，以降序对获胜的买家候选人  $\text{TDc}$  进行排序。对于每个买方  $\text{TD}_i \in \text{TDc}$ ，其请求的资源量定义为  $\sum_{z=1}^k d_i^z$ 。因此，我们对满足  $\sum_{z=1}^k d_1^z \geq \sum_{z=1}^k d_2^z \geq \dots$  的地方进行分类肯定的。接下来，对于每个买方  $\text{TD}_i \in \text{TDc}$ ，我们需要确定其获胜的卖方候选人，用  $\text{ENC}$ ,  $i \in \text{EN}$  表示。我们有  $\text{EN}_j \in \text{ENC}$ ，当且仅当它满足三个条件。

- 1) 其剩余资源  $H_{0j}$  充足。换句话说，我们有每个  $r_z \in R$  的  $h_{zj}' \geq d_{zi}^z$ 。
- 2) 它与  $\text{TD}_i$  的距离接近 enough。因此，我们有  $\delta_{ij} \leq d_{mi}$ 。
- 3) 它通过向买家  $\text{TD}_i$  提供资源而盈利。

这里，我们有  $\sum_{z=1}^k (p_z - a_z) \cdot d_i^z \geq 0$ 。

条件(1)和(2)是明显的。如果条件(3)不能满足， $\text{EN}_j$  ( $x_{ij} = 1$ ) 为  $\text{TD}_i$  提供资源将导致目标值降低。



给定一个买家  $TD_i \in TD_c$ ，我们可以得到它的中奖卖家候选人  $ENC_i$ 。如果  $|ENC_i| \geq 1$ ，如何选择最好的一个提供资源？在作业阶段，我们可以从两个方向去思考。第一种策略是考虑负载均衡，我们尽量安排空闲资源较多的边缘节点提供服务。第二个策略是考虑节省网络带宽，我们尽量安排距离目标买家  $TD_i$  最近的边缘节点。由于边缘节点可以提供多种资源，如何量化“闲置资源”是一个难题。因此，我们在这里使用第二个策略，我们选择一个满足以下条件的  $EN_j \in ENC_i$ ，

$$EN_j = \arg \min_{EN_j \in ENC_i} \{\delta_{ij}\} \quad (12)$$

向买方  $TD_i$  提供资源。

从上面的过程中，我们可以得到中奖的买家和中奖的卖家，以及他们对应的分配矩阵  $X$  给定的价格向量  $p$ 。下一个定价阶段是确定我们选择哪个价格向量  $p \in \Theta_k$ 。这个定价过程来自统一定价[31]和指数机制。给定一个价格向量  $p$ ，它生成一个分配矩阵  $X_p$ ，然后我们可以将平台的相应收入计算为(4)，表示为

$$R((b, A), p) = \sum_{j=1}^n \left[ \sum_{z=1}^k (p_z - a_j^z) \cdot \sum_{i=1}^m x_{ij} \cdot d_i^z \right]. \quad (13)$$

我们把这个平台的收入作为价格  $p$  的分数。得分函数  $R()$  的灵敏度可以表述为

$$\begin{aligned} & \frac{\partial R}{\partial p} = \frac{\partial}{\partial p} \left( \sum_{j=1}^n \sum_{z=1}^k (p_z - a_j^z) \cdot \sum_{i=1}^m x_{ij} \cdot d_i^z \right) \\ & \Leftrightarrow R = X(C_{\max} - c_{\min})Xh_j \quad (14) \end{aligned}$$

因为  $p_z - a_j^z \leq C_{\max} - c_{\min}$  和  $\sum_{i=1}^m x_{ij} \cdot d_i^z \leq h_j^z$ 。然后，我们重复上述过程，计算所有可能价格  $p \in \Theta_k$  下的平台收入。为了确定最终定价，我们定义价格向量的概率分布如下。

$$Pr[M(b, A) = p] = \frac{\exp\left(\frac{R((b, A), p)}{2\Delta R}\right)}{\sum_{p' \in \Theta_k} \exp\left(\frac{R((b, A), p')}{2\Delta R}\right)} \quad (15)$$

$$Pr[M(b, A) = p] = \frac{\exp\left(\frac{R((b, A), p)}{2\Delta R}\right)}{\sum_{p' \in \Theta_k} \exp\left(\frac{R((b, A), p')}{2\Delta R}\right)}$$

其中  $R((b, A), p)$  在(13)中定义， $R$  在中定义(14)。给定所有可能的价格  $p \in \Theta_k$  及其得分，在定价阶段，它随机选择一个价格向量  $p$ ，概率  $Pr[M(b, A) = p]$  如(15)所示。

## V. 理论分析

在这一部分，我们描述了我们提出的机制 DPAM 的理论分析，显示为算法 1 满足期望的属性。

定理 1. DPAM 实现了  $\epsilon$ -差异隐私。

证据。给定两个相邻的输入  $(b, A)$  和  $(b', A)$ ，机制  $M$  从  $\Theta_k$  中随机选择一个清算价格  $p$ 。因此，由  $M$  选择的它们的相应概率的概率比如下所示。

$$\begin{aligned} & \frac{Pr[M(b, A) = p]}{Pr[M(b', A) = p]} \\ &= \frac{\exp\left(\frac{R((b, A), p)}{2\Delta R}\right)}{\sum_{p' \in \Theta_k} \exp\left(\frac{R((b, A), p')}{2\Delta R}\right)} \cdot \frac{\sum_{p' \in \Theta_k} \exp\left(\frac{R((b', A), p')}{2\Delta R}\right)}{\sum_{p' \in \Theta_k} \exp\left(\frac{R((b', A), p')}{2\Delta R}\right)} \\ &= \exp\left(\frac{R((b, A), p) - R((b', A), p)}{2\Delta R}\right) \\ &\leq \exp\left(\frac{\epsilon}{2}\right) \cdot \frac{\sum_{p' \in \Theta_k} \exp\left(\frac{R((b, A), p') + \Delta R}{2\Delta R}\right)}{\sum_{p' \in \Theta_k} \exp\left(\frac{R((b, A), p')}{2\Delta R}\right)} \\ &\leq \exp\left(\frac{\epsilon}{2}\right) \cdot \exp\left(\frac{\epsilon}{2}\right) \cdot \frac{\sum_{p' \in \Theta_k} \exp\left(\frac{R((b, A), p')}{2\Delta R}\right)}{\sum_{p' \in \Theta_k} \exp\left(\frac{R((b, A), p')}{2\Delta R}\right)} \\ &= \exp(\epsilon). \end{aligned}$$

根据对称性，我们有  $Pr[M(b, A) = p] / Pr[M(b', A) = p] \geq \exp(-\epsilon)$ 。根据定义 5，DPAM 对买家来说是有差别的私有。

给定两个相邻的输入  $(b, A)$  和  $(b, A_0)$ ，通过与买方类似的归纳程序，我们有

$$Pr[M(b, A) = p / Pr[M(b, A_0) = p] \leq \exp(\epsilon).$$

因此，DPAM 对卖家来说是  $\epsilon$ -差分私有的，定理 1 已经被证明。□

为了最终实现  $\gamma$  真实性，我们首先引入以下两个引理作为铺垫。

引理 1. 给定清算价格  $p \in \Theta_k$ ，对于每个买方  $TD_i \in TD$ ，DPAM 实现

$$u_i^{TD}((v_i, \Omega_{-i}), p) \geq u_i^{TD}((b_i, \Omega_{-i}), p). \quad (16)$$

证据。  $TD_i \in TD_c$ ，如果它如实出价的话。我们需要关注两个子案例：

- $b_i > v_i$ :  $TD_i$  也将  $TD_c$  中。根据获胜者候选人的确定和分配， $TD_i$  的拍卖结果不会改变。因此，我们有  $u_i^{TD}((v_i, \Omega_{-i}), p) = u_i^{TD}((b_i, \Omega_{-i}), p)$ 。
- $b_i < v_i$ : 如果  $\sum_{z=1}^k p_z \cdot d_i^z \leq b_i$  可以满足，那么  $TD_i$  也将  $TD_c$  中。因此，我们有  $u_i^{TD}((v_i, \omega_i), p) = u_i^{TD}((b_i, \omega_i), p)$ ；否则， $TD_i$  就不在  $TD_c$  了，肯定会输掉拍卖。因此，我们有  $u_i^{TD}((v_i, \omega_i), p) \geq u_i^{TD}((b_i, \omega_i), p) = 0$ 。

TdI  $\Sigma$  /TdC 如果它如实出价。我们需要关注两个子案例:

- $b_i > v_i$ : If  $\sum_{z=1}^k p_z \cdot d_i^z \leq b_i$  可以满意了, TDi

将在 TDC 中。如果可以在分配阶段为其分配一个边缘节点, 则其利用率将为  $uTDi((b_i, \omega_l), p) =$

$$v_i - \sum_{z=1}^k p_z \cdot d_i^z < 0 = u_i((v_i, \Omega_{-i}), p) \text{ k推倒 (网络用词)}$$

- $b_i < v_i$ : TdI 也不会 TDC 中, 这肯定会输掉拍卖。因此, 我们有  $uTDi((v_i, \omega_l), p) = uTDi((b_i, \omega_l), p) = 0$ 。

由上可知, 我们总是有  $uTDi((v_i, \omega_l), p) \geq uTDi((b_i, \omega_l), p)$ , 引理 1 已被证明。□

引理 2. 给定清算价格  $p \in \theta k$ , 对于每个买方  $ENj \in EN$ , DPAM 达到  $uENj((c_j, \omega_j), p) \geq uENj((a_j, \omega_j), p)$ 。(17)

证据。首先, “ $a_j > c_j$ ”意味着这些向量中至少有一个元素满足  $a_j^z > c_j^z$ , 其他元素满足每个  $r_z \in R \in$  的  $a_j^z \geq c_j^z$ 。第二, 我们用  $x_{ij} \in X$  表示卖家如实询问时的分配, 用  $x_{ij} \in X$  表示卖家不如实询问时的分配。

考虑卖家  $ENj \in EN$ , 我们需要关注两个子案例:

- $a_j > c_j$ : 当  $x_{ij} = 1$  时, 拍卖结果为  $x_{ij} = 1$  如果/可以满足; 否则  $x_{ij} = 0$ 。因此, 我们有  $uENj((c_j, \omega_j), p) \geq uENj((a_j, \omega_j), p)$ , 因为  $x_{ij} \geq x_{ij}$ 。
- $a_j < c_j$ : 当  $x_{ij} = 1$  时, 拍卖结果也将是  $x_{ij} = 1$ 。当  $x_{ij} = 0$  且  $\sum_{z=1}^k (p_z - c_z) \cdot d_i^z \geq 0$  时, 拍卖结果到  $x_{ij} = 0$  不会根据分配而改变。然而, 当  $x_{ij} = 0$  且  $\sum_{z=1}^k (p_z - c_z) \cdot d_i^z < 0$ , 有可能发生  $\sum_{z=1}^k (p_z - c_z) \cdot d_i^z \geq 0$ , 如果  $\delta_{ij}$  是该买方的获胜卖方候选人中的最小值, 则导致  $x_{ij} = 1$ 。从 TDi 获得的效用小于零。因此, 我们有  $uENj((c_j, \omega_j), p) \geq uENj((a_j, \omega_j), p)$ 。

由上可知, 我们总有  $uENj((c_j, \omega_j), p) \geq uENj((a_j, \omega_j), p)$ , 引理 2 已被证明。□

定理 2. DPAM 实现了  $\gamma$  真实。

证据。给定两个相邻输入  $(b, A)$  和  $(b', A)$ , 对于任何买方  $TDi \in TD$ , 我们假设  $v_i \in b$  和  $b_i \in b_0$ 。

因此, 我们有

$$\begin{aligned} & \mathbb{E}[u_i^{TD}(v_i, \Omega_{-i})] \\ &= \int_{p \in \theta k} M(b, A) = p \cdot u_i^{TD}((v_i, \Omega_{-i}), p) \end{aligned}$$

$$\geq \exp(\varepsilon) \mathbb{E}[M(b_0, A) = p] u_i^{TD}((b_i, \omega_l), p) \text{ p} \in \theta k$$

$$\begin{aligned} &= \exp(-\varepsilon) \cdot \mathbb{E}[u_i^{TD}(b_i, \Omega_{-i})] \\ &\geq (1 - \varepsilon) \cdot \mathbb{E}[u_i^{TD}(b_i, \Omega_{-i})] \\ &\geq \mathbb{E}[u_i^{TD}(b_i, \Omega_{-i})] - \varepsilon \cdot v_{max}. \end{aligned}$$

对于任何买家  $TDi \in TD$ , 我们都有  $\mathbb{E}[uTDi((b_i, \omega_l))] \leq \max_{TDi \in TD} \{u_i^{TD}\} \leq v_{max} - c_{min} \cdot \min_{TDi \in TD} \{\sum_{z=1}^k d_i^z\} \leq v_{max}$ 。因此, 我们可以得出结论, DPAM 实现了对买家的真实。

给定两个相邻的输入  $(b, A)$  和  $(b, A_0)$ , 对于任何卖家  $ENj \in EN$ , 我们假设  $c_j \in A$  和  $a_j \in A_0$ 。

与上面类似, 我们有

$$\begin{aligned} & \mathbb{E}[u_j^{EN}(c_j, \Omega_{-j})] \\ & \geq \mathbb{E}[u_j^{EN}(a_j, \Omega_{-j})] - \varepsilon \cdot (c_{max} - c_{min}) \cdot k \cdot h_{max}. \end{aligned}$$

对于任何卖家  $ENj \in EN$ , 我们都有  $\mathbb{E}[uENj((c_j, \omega_j))] \leq \max_{ENj \in EN} \{u_j^{EN}\} \leq (c_{max} - c_{min}) \cdot \sum_{z=1}^k h_j^z \leq (c_{max} - c_{min}) k h_{max}$ 。因此, 我们可以得出结论, DPAM 对卖方实现了  $\varepsilon(C_{max}-c_{min})k h_{max}$ -真实性。

给出  $\gamma = \max\{\varepsilon v_{max}, \varepsilon(C_{max}-c_{min})k h_{max}\}$ , DPAM 达到  $\gamma$  真实。□

定理 3. DPAM 实现了个人理性。

证据。根据定理 2, 没有玩家有不诚实出价/要求的动机。我们可以考虑每个买方的  $b_i = v_i$ , 每个卖方的  $TDi \in TD$  和  $a_j = c_j$ ,  $ENj \in EN$ 。根据中标候选人的确定, 每个中标买家的 TDi 必须有  $\sum_{z=1}^k p_z \cdot d_i^z \leq b_i$ , 从而其效用  $u_i^{TD} \geq 0$ 。根据分配, 每个为买家 TDi 提供资源的获胜卖家 ENj 都必须拥有  $\sum_{z=1}^k (p_z - a_z) \cdot d_i^z \geq 0$ , 这意味着为物联网设备提供资源总是会带来正回报。□因此, 它的效用  $uENj \geq 0$ 。

定理 4. DPAM 实现了预算平衡。

证据。根据定理 3, 所有边缘节点的效用都是正的, 因此它们的总和(预算)  $\sum_{j=1}^n u_j^{EN}$  也大于零。□

定理 5. DPAM 没有达到计算效率。

证据。遍历所有可能价格向量  $p \in \theta k$  的主循环包含  $|\theta k|$  次迭代。对于每次迭代, 确定获胜候选的主要步骤是对最多有  $m$  个元素的 TDC 进行排序。因此, 排序 TDC 以  $O(m \log m)$  为界。然后, 在分配中, 每个买方  $TDi \in TDC$  需要  $O(n)$ 。因此, 它的运行时间以  $O(mn)$  为界。算法 1 的总时间复杂度以  $O((Mn+m \log m)|\theta k|)$  为界。因此, 运行时间随  $k$  而不是多项式时间呈指数增长。□

接下来, 我们需要计算我们提出的机制的预期性能。基于(13), 边缘计算平台的预期收入可以表示为

$$\mathbb{E}[R(b, A)] = \mathbb{E}[\Pr[M(b, A) = p] R((b, A), p)] \text{ p} \in \theta k \quad (18)$$

为了获得 DPAM 的近似比, 我们首先引入以下引理。

引理 3. 通过求解(4)中定义的问题, 让  $OPT$  为最优收益,  $OPT\Sigma = \max_{p \in \Theta^k} \{R((b, A), p)\}$  为算法 1 的中标候选人确定和分配过程获得的最大收益。然后, 我们有

$$f(\theta)OPT \leq OPT \int \leq OPT \quad (19)$$

我们用  $F(\Theta) = \frac{\max_{p \in \Theta^k} \{R((b, A), p)\}}{(c_{max} - c_{min}) \cdot n \cdot k \cdot h_{max}}$  作为被占领土的一个因素。

证据。因为  $OPT$  是全局最优的, 所以我们有  $OPT \geq OPT\Sigma$ 。基于(4), 我们有

$$OPT \leq (C_{max} - c_{min})n k h_{max} \quad (20)$$

因为每个边缘节点最多提供  $k$  个  $h_{max}$  单位的资源, 并且总共有  $n$  个边缘节点。根据  $OPT$  的定义, 我们有

$$\begin{aligned} OPT\Sigma &= \max_{p \in \Theta^k} \{R((b, A), p)\} \\ &\geq \frac{\max_{p \in \Theta^k} \{R((b, A), p)\}}{(c_{max} - c_{min}) \cdot n \cdot k \cdot h_{max}} \cdot OPT \\ &= F(\Theta) \cdot OPT \end{aligned}$$

因为关系(20)存在。□

为了实现真实性, 即使没有差别隐私, 收益也不是最优的。这个差可以用  $F(\Theta)$  来界定。引入差异化隐私后, 收益将进一步受损。

定理 6.  $DPAM$  实现的边缘计算平台  $E[R(b, A)]$  的预期收益和最优收益  $OPT$  满足  $E[R(b, A)] \geq$

$$F(\Theta) \cdot OPT - \frac{6\Delta R}{\varepsilon} \cdot \ln \left( e + \frac{\varepsilon OPT |\Theta^k|}{2\Delta R} \right). \quad (21)$$

证据。设  $OPT\Sigma = \max_{p \in \Theta^k} \{R((b, A), p)\}$  为  $DPAM$  返回的最大收益。对于小常数  $t \geq 0$ , 我们定义了四个集合, 分别是  $St = \{p : R((b, A), p) > OPT \cdot t\}$ ,  $S_{-t} = \{p : R((b, A), p) \leq OPT \cdot t\}$ ,  $S_{2t} = \{p : R((b, A), p) > OPT \cdot 2t\}$ ,  $S_{-2t} = \{p : R((b, A), p) \leq OPT \cdot 2t\}$ 。因此, 我们有

$$\Pr[M(b, A) \in S_{2t}] \leq$$

$$\frac{\text{公关}[M(b, A) \in S_{2t}]}{\text{公关}[M(b, A) \in St]} \leq$$

$$\begin{aligned} &= \frac{\sum_{p \in S_{2t}} \frac{\exp\left(\frac{\varepsilon R((b, A), p)}{2\Delta R}\right)}{\sum_{p' \in \Theta^k} \exp\left(\frac{\varepsilon R((b, A), p')}{2\Delta R}\right)}}{\sum_{p \in St} \frac{\exp\left(\frac{\varepsilon R((b, A), p)}{2\Delta R}\right)}{\sum_{p' \in \Theta^k} \exp\left(\frac{\varepsilon R((b, A), p')}{2\Delta R}\right)}} \\ &= \frac{\sum_{p \in S_{2t}} \exp\left(\frac{\varepsilon R((b, A), p)}{2\Delta R}\right)}{\sum_{p \in St} \exp\left(\frac{\varepsilon R((b, A), p)}{2\Delta R}\right)} \leq \frac{|\bar{S}_{2t}| \cdot \exp\left(\frac{\varepsilon(OPT^* - 2t)}{2\Delta R}\right)}{|S_t| \cdot \exp\left(\frac{\varepsilon(OPT^* - t)}{2\Delta R}\right)} \\ &= \frac{|\bar{S}_{2t}|}{|S_t|} \cdot \exp\left(\frac{-\varepsilon t}{2\Delta R}\right). \end{aligned} \quad (22)$$

基于(22), 我们有

$$\begin{aligned} \text{公关}[M(b, A) \in S_{2t}] &\geq 1 - \frac{|\bar{S}_{2t}|}{|S_t|} \cdot \exp\left(\frac{-\varepsilon t}{2\Delta R}\right) \\ &\geq 1 - |\Theta^k| \cdot \exp\left(\frac{-\varepsilon t}{2\Delta R}\right) \end{aligned} \quad (23)$$

由于  $\Pr[M(b, A) \in S_{2t}] + \Pr[M(b, A) \in S_{-2t}] = 1$ ,  $|S_{-2t}| \leq |\Theta^k|$ , 且  $|S_t| \geq 1$ 。因此, 预期收入  $E[R(b, A)]$  可以表示为

$$\begin{aligned} E[R(b, A)] &\geq \sum_{p \in S_{2t}} \Pr[M(b, A) = p] R((b, A), p) \\ &\geq \Pr[M(b, A) \in S_{2t}] \cdot (OPT^* - 2t) \\ &\geq \left[1 - |\Theta^k| \cdot \exp\left(\frac{-\varepsilon t}{2\Delta R}\right)\right] \cdot (OPT^* - 2t) \end{aligned}$$

对于任何令人满意测试

$$t \geq \frac{2\Delta R}{\varepsilon} \cdot \ln \left( \frac{|\Theta^k| OPT^*}{t} \right) \quad (24)$$

我们有  $\exp\left(\frac{-\varepsilon t}{2\Delta R}\right) \leq \frac{t}{OPT^* |\Theta^k|}$ 。因此,

$$\begin{aligned} E[R(b, A)] &\geq \left(1 - |\Theta^k| \cdot \frac{t}{OPT^* |\Theta^k|}\right) \cdot (OPT^* - 2t) \\ &= OPT^* - 3t + \frac{2t^2}{OPT^*} \\ &\geq OPT^* - 3t. \end{aligned} \quad (25)$$

通过给予  $t = \frac{2\Delta R}{\varepsilon} \ln \left( e + \frac{\varepsilon OPT^* |\Theta^k|}{2\Delta R} \right)$ , 我们已经

$$\begin{aligned} t &= \frac{2\Delta R}{\varepsilon} \cdot \ln \left( e + \frac{\varepsilon OPT^* |\Theta^k|}{2\Delta R} \right) \\ &\geq \frac{2\Delta R}{\varepsilon} \cdot \ln \left( OPT^* |\Theta^k| \frac{\varepsilon}{2\Delta R} \right) \\ &\geq \frac{2\Delta R}{\varepsilon} \cdot \ln \left( \frac{|\Theta^k| OPT^*}{t} \right) \end{aligned}$$

因为  $\ln \left( e + \frac{\varepsilon OPT^* |\Theta^k|}{2\Delta R} \right) \geq 1$  和

$t \geq \frac{2\Delta R}{\varepsilon}$ 。最后, 我们把  $t = \frac{2\Delta R}{\varepsilon} \cdot \ln \left( e + \frac{\varepsilon OPT^* |\Theta^k|}{2\Delta R} \right)$  代入(25), 我们有

$$\begin{aligned} E[R(b, A)] &\geq OPT^* - 3t \\ &\geq OPT^* - \frac{6\Delta R}{\varepsilon} \cdot \ln \left( e + \frac{\varepsilon OPT^* |\Theta^k|}{2\Delta R} \right) \\ &\geq F(\Theta) \cdot OPT - \frac{6\Delta R}{\varepsilon} \cdot \ln \left( e + \frac{\varepsilon OPT |\Theta^k|}{2\Delta R} \right). \end{aligned}$$

因此, 定理 6 得到了证明。□

## VI. 实现和仿真

如定理 5 所示, 算法 1 的运行时间可以以  $|\Theta^k|$  为界, 这在计算上效率不高。因此, 在本节中, 我们首先讨论一种将时间复杂度降低到多项式时间的实现技术。然后, 我们通过大量的仿真来实现和评估我们提出的机制。

### A. 实现技术



为了减少运行时间，我们可以借鉴[13]中最近的研究，逐个选择每个资源的单价，而不是选择价格向量。程序如算法 2 所示。

首先，我们定义每个买家的平均单位出价

$TD_i \in \mathbb{TD}$  as  $\bar{b}_i = b_i / (\sum_{z=1}^k d_i^z)$ . 迭代算法 2 DPAM-S 的主循环

输入:  $\{B_i\} \mid TD_i \in \mathbb{TD}, \{A_j\} \mid EN_j \in \mathbb{EN}, \epsilon, \theta$

输出:  $X, p, p$

```

1: 初始化每个  $TD_i \in \mathbb{TD}$  的  $\bar{b}_i = b_i / (\sum_{z=1}^k d_i^z)$ 
2: 初始化  $\epsilon_0 = \epsilon/k$ 
3: for  $\ell \leftarrow 1$  to  $k$  do
4:   初始化  $\Delta R^\ell = \sum_{j=1}^n (c_{max} - c_{min}) \cdot \sum_{z=1}^k h_j^z$ 
5:   对于每个  $p' \in \Theta$  do
6:     对每个  $x_{ij} \in X$ ,  $p'$  初始化  $x_{ij} = 0$ 
7:     初始化
8:       对于每个  $TD_i \in \mathbb{TD}$  do
9:         如果  $P'z=1 \text{ } p_z d_{zi} \leq b_i P'z=1 \text{ } d_{iz}$ , 则
10:           $\mathbb{TD}_c^\ell \leftarrow \mathbb{TD}_c^\ell \cup \{TD_i\}$ 
11:          如果...就会结束
12:        结束于
13:      给  $\mathbb{TD}_c^\ell$  s.t.  $\sum_{z=1}^k d_1^z \geq \sum_{z=1}^k d_2^z \geq \dots$  分类
14:      初始化  $\{h_j^{1'}, h_j^{2'}, \dots, h_j^{\ell'}\}$ , 其中  $h_j^{z'} = h_j^z \in \mathbb{H}_j$  15: 对于
16:        初始化  $\mathbb{EN}_c$ ,  $i \leftarrow \emptyset$  每  $TD_i \in \mathbb{TD}_c^\ell$  个人来说
17:        对于每个  $EN_j \in \mathbb{EN}$  do
18:          如果每个  $r_z \in \{R_1, r\}$ 
19:            的  $h_j^{z'} \geq d_{i,z}^z$ ,  $\delta_{ij} \leq \text{那么}$ 
20:            如果...就会
21:            结束
22:          结束于
23:           $EN_j \leftarrow \text{ArgMin}_{j \in \mathbb{EN}} \{c, i\} \mid \delta_{ij} \mid \mathbb{EN}_{c,i}^\ell \neq \emptyset$ 
24:          对于每个  $r_z \in \{R_1, r\}$  do
25:             $h_j^{z*} \leftarrow h_j^{z*} - d_{i,z}^z$  00
26:          结束于
27:           $x_{ij} \leftarrow 1$ 
28:          如果...就会结
29:          束
30:        结束于
31:      根据选择分布选择  $p' \in \Theta$ :

```

$$M(b, A) = p = \frac{\exp \left( \frac{\epsilon^0 R^\ell((b, A), p)}{2\Delta R^\ell} \right)}{\sum_{p' \in \Theta} \exp \left( \frac{\epsilon^0 R^\ell((b, A), p')}{2\Delta R^\ell} \right)} \Pr[$$

$p_0 \in \Theta$

33: 结束于

34: 返回  $X_k, p_k, p = \{p_1, p_2, \dots, p_k\}$

2[1]r 经历

$k$  次查看各种资源。检查时

——单价  $p' \in \Theta(1 \leq \ell \leq k)$ , 我们已经知道了前面的第一个  $\ell-1$  单价。已经确定了部分价格向量  $(p_1, p_2, \dots, p_{\ell-1})$ 。给定单价  $p' \in \Theta$ , 我们选择部分获胜的买方候选人  $\mathbb{TD}_c^\ell \subseteq \mathbb{TD}$ , 这样对于每个买方  $TD_i \in \mathbb{TD}_c^\ell$ , 我们有

对辊破碎机  $z \leq b_i X_{dzi}$ . (26)

目的地想象

$z=1$

$z=1$

然后，它生成一个分配矩阵  $x$ ,  $p$ , 类似于 DPAM。部分收入可以通过下式计算

$$R^\ell((b, A), p_\ell) = \sum_{j=1}^n \left[ \sum_{z=1}^\ell (p_z - a^z) \cdot \sum_{i=1}^m x_{ij} \cdot d_i^z \right]. \quad (27)$$

$j=1$

$z=1 \quad i=1$

这里，部分得分函数  $r$  的灵敏度可以写成  $\Delta R^\ell = \sum_{j=1}^n (c_{max} - c_{min}) \cdot \sum_{z=1}^k h_j^z$ . 根据指数机制，选择单价  $p' \in \Theta$  的概率分布可以定义如下。

$$\Pr[M(b, A) = p] = \frac{\exp \left( \frac{\epsilon' R^\ell((b, A), p_\ell)}{2\Delta R^\ell} \right)}{\sum_{p' \in \Theta} \exp \left( \frac{\epsilon' R^\ell((b, A), p'_\ell)}{2\Delta R^\ell} \right)} \quad (28)$$

其中  $\epsilon_0 = \epsilon/k$ 。因此，根据算法 2，时间复杂度从  $O((Mn+m \log m) |\Theta| k)$  降低到  $O((Mn+m \log m) k |\Theta|)$ 。

定理 7. DPAM-S 实现了  $\epsilon$ -差分隐私、 $\gamma$  真实性、个体理性、预算平衡、计算效率。此外，DPAM-S 实现的预期收益满足  $E[Rk(b, A)] \geq$

$$F(\Theta) \cdot OPT - \frac{6k\Delta R}{\epsilon} \cdot \ln \left( e + \frac{\epsilon OPT |\Theta|}{2\Delta R} \right). \quad (29)$$

证据。基于本文的定理 1 至定理 6 和[13]中的定理 7，可以证明这个定理。□

有两种机制，DPAM 和 DPAM-S，以最大化边缘计算平台的收入和满足理想的属性。给定固定的隐私预算  $\epsilon$ ，DPAM 实现的收益更好，但 DPAM-S 的运行时间更好。哪种机制更好取决于性能和运行时间之间的要求。

## B. 模拟设置

为了模拟这种场景，我们构建了一个  $1000 \times 1000$  的虚拟矩形区域，其中有  $m$  个物联网设备和  $n$  个边缘节点均匀分布在这个区域。对于每个  $TD_i \in \mathbb{TD}$ ，我们将其坐标定义为

$(x_i, y_i)$ 。同样，我们对每个  $EN_j \in EN$  都有  $(x_j, y_j)$ 。物联网设备  $TD_i$  和边缘节点  $EN_j$  之间的距离  $\delta_{ij}$  可以写成  $\delta_{ij} =$

$\sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$ 。对于每个买方  $TD_i \in TD$ ，其投标信息包含最大允许距离  $\sqrt{d_{mi}}$ 。

$d_{mi}$ ，均匀分布在  $[200^2, 1000^2]$  中，因为物联网设备和边缘节点之间的最大距离  $\sqrt{}$

这个地区是 1000 平方英里。

假设单位资源的价格可以归一化为  $[0, 1]$ ，那么  $\theta = [cmin, cmax] = [0, 1]$ 。为了实现我们的机制，第一步是离散化这个区间  $[0, 1]$ ，以便遍历空间  $\theta^k$  中所有可能的价格向量。这里，我们定义了一个称为“粒度”的概念，用  $\sigma$  表示。 $\sigma = 0.02$  意味着我们将区间  $[0, 1]$  平均分成 50 份，即  $\theta = \{0, 0.02, 0.04, \dots, 0.98, 1\}$ 。粒度可以作为平衡性能和时间复杂度的有效方法。由于  $\theta = [0, 1]$ ，我们在  $[0, 1]$  中对每个卖方  $EN_j \in EN$  和  $r_z \in R$  统一进行  $az_j$  抽样。接下来，我们假设资源类型  $k \in \{1, 2, \dots, 5\}$  的数量，以及每个资源的可用范围  $[hmin, hmax] = [0, 20]$ 。因此，在模拟中，我们使每个卖方的  $hz_j \in H_j$   $EN_j \in EN$  和  $r_z \in R$  均匀分布在  $[10, 20]$  中。同样，我们假设

$[dmin, dmax] = [1, 5]$ ，这样我们使每个买方的  $dzi \in Di$   $TD_i \in TD$  和  $r_z \in R$  均匀分布在  $[1, 5]$  中。

下一步，我们需要讨论买家如何决定他们的总出价。也就是说，我们如何对每个买家的总出价  $b_i$  进行采样  $TD_i \in TD$ 。根据我们前面的描述，单位资源的平均价格是  $(1 + 0)/2 = 0.5$ 。这里，我们指出一个合理的假设，即总出价与买方对资源的总需求有关。因此，我们可以对每个买方的商业智能进行采样，如下所示：

$$b_i = (0.5) \cdot \sum_{z=1}^k d_i^z \cdot U(0.7, 1.3) \quad (30)$$

其中  $U(0.7, 1.3)$  是从区间  $[0.7, 1.3]$  均匀采样的值。

由于差分隐私的引入，拍卖结果具有一定的随机性。因此，给定一个机制，其结果是 500 次试验的平均值。为了分析我们基于差别隐私的机制的性能，我们需要一个参考。例如，在算法 1 的第 32 行，我们选择一个  $p \in \theta^k$ ，使得最大化  $R((b, A), p)$  作为最终结果。通过去除 DPAM 和 DPAM-S 的随机性(差分隐私)，我们可以定义两个确定性拍卖机制，标记为“DTAM”和“DTAM-S”，作为参考。在这里，“DT”意味着“确定性的”。最后，我们选择了三个典型的度量来评估我们提出的机制的性能，如下所示。

- 1) 边缘计算平台的预期收入:可由(18)计算。
- 2) 预期满意度:满意的物联网设备数量与物联网设备总数的比率。
- 3) 运行时间:执行一次试验所花费的时间。

### C. 仿真结果与分析

在任意时隙  $t \in T$ ，有  $m$  个物联网设备(买家)和  $n$  个边缘节点。通常，物联网设备的数量远大于边缘节点的数量，

因此我们在下面的模拟中假设  $m \geq n$ 。我们在这部分的任务

可以分为四个部分，分别讨论粒度的影响、资源类型的数量

物联网设备和隐私预算分别对我们提出的机制的性能产生影响。

粒度:图 2 绘制了四种不同机制的收入、满意度和运行时间随着粒度的增加而变化，其中我们假设  $m = 100$ ， $n = 10$ ， $k = 3$ ， $\epsilon = 200$ 。如图 2 (a)所示，我们可以看到收入会随着粒度的增加而略有下降。这是因为更小的粒度意味着更高的精度，因此我们可以计算更多的价格向量并选择更好的。类似的结果也体现在用户的满意度上。如图 2 (c)所示，运行时间会随着粒度的减小而显著增加。在这里，让我们做一个粗略的分析。假设  $\sigma_1 = 0.1$   $\sigma_2$ ，我们有  $|\theta_1| = 10$   $|\theta_2|$ 。在 DPAM (DTAM)，粒度  $\sigma_1$  下的运行时间是粒度  $\sigma_2$  下的  $10k$  倍。而在 DPAM-S (DPTM-S)中，粒度  $\sigma_1$  下的运行时间是粒度  $\sigma_2$  下的  $10k$  倍。图 3 (c)中的模拟结果总体上符合我们的预期。我们已经提到粒度是一种平衡性能的方法

(一)(预期)收入 (预期)满意度 运行时间

图 2。所提出的机制在不同粒度上的性能, 其中  $m=100$ ,  $n=50$ ,  $k=3$ ,  $\epsilon=200$ 。

(一)(预期)收入 (预期)满意度 运行时间

图 3。在  $m=100$ ,  $n=50$ ,  $\sigma=0.1$ ,  $\epsilon=200$  的不同资源类型上, 所提出机制的性能。

(一)(预期)收入 (预期)满意度 运行时间

图 4。在  $n=50$ ,  $k=3$ ,  $\sigma=0.1$ ,  $\epsilon=200$  的不同边节点数下, 所提出机制的性能。

(一)(预期)收入 (预期)满意度 运行时间

图 5。提出的机制在不同隐私预算下的性能, 其中  $m=100$ ,  $n=50$ ,  $k=3$ ,  $\sigma=0.1$ 。

时间复杂性。基于图 2 的结果, 我们在下面的模拟中设置粒度  $\sigma=0.1$ 。

资源类型的数量:图 3 描绘了性能随着资源类型数量的增加而变化, 其中我们假设  $m=100$ ,  $n=10$ ,  $\sigma=0.1$ ,  $\epsilon=200$ 。如图 3 (a)所示, 我们观察到收入会随着资源类型的增加而呈现上升趋势。这是因为资源类型的增加使得每个边缘节点能够销售更多的资源单元。然而, 当  $k=4$  时有一个例外。从图 3 (b)可以看出, 当  $k=4$  时, 用户的满意度明显下降。这可能是由于数据的随机性, 使得物联网设备的资源请求难以实现, 导致其满意度下降。此外, 另一个重要发现是, DPAM (DPAM-S)和 DTAM (DTAMS)之间的差距随着资源类型的增加而增加。在较大的  $k$  下, 样本空间  $\theta^k$  会变大, 导致较高的随机性。换句话说, 选择最优解的概率会变小。如图 3 (c)所示, 运行时间将随着资源类型数量的增加而显著增加。同样, 我们假设  $k_1 = k_2 + 1$ 。在 DPAM (DTAM),  $k_1$  下的运行时间是  $k_2$  下的  $|\theta|$  倍, 因为我们有  $|\theta|^{k_1} = |\theta|^{k_2} |\theta|$ 。而在 DPAM-S (DPTM-S)中,  $k_1$  下的运行时间是  $k_2$  下的  $(k_2 + 1)/k_2$  倍。如果有大量的资源类型, DPAM (DTAM)是不可复制的, 因为它的运行时间呈指数级

增长。相比之下, DPAM-S (DTAM-S)的运行时间呈线性增长。

物联网设备的数量:图 4 绘制了四种不同机制的收入、满意度和运行时间随着物联网设备数量的增加而变化, 其中我们假设  $n=10$ ,  $k=3$ ,  $\sigma=0.1$ ,  $\epsilon=200$ 。如图 4 (a)和(b)所示, 我们可以看到, 随着物联网设备数量的增加, 收入会增加, 满意度会降低。这是因为有更多可行的买家候选请求资源, 使得边缘节点的资源能够得到更充分的利用。虽然可以满足的物联网设备越来越多, 但物联网设备总数变得多了, 导致满意度下降。如图 4 (c)所示, 运行时间将随着物联网设备数量的增加而线性增长, 总体上符合我们的预期。

隐私预算:图 5 绘制了性能随着隐私预算的增加而变化, 其中我们假设  $m=100$ ,  $n=10$ ,  $k=3$ ,  $\sigma=0.1$ 。如图 5 所示

(a)和(b), 我们观察到 DTAM 和 DTAM-S 的收入和满意度保持不变, 因为它们是确定性机制, 与隐私预算的价值无关。在 DPAM 和 DPAM, 随着隐私预算的增加, 收入和满意度呈上升趋势。实际上, 隐私预算控制着不同隐私所提供的

保护程度。隐私预算越高, 收益和满意度越高, 但隐私保护程度会减弱。如图 5 (c)所示, 随着隐私预算的增加, 运行时间保持不变, 这表明运行时间与隐私预算的选择无关。

基于以上四项任务, 主要结论可归纳如下。粒度对运行时间影响很大, 通常不需要选择很小的粒度来保证精度。在大量资源类型的情况下, 由于时间复杂性的限制, DPAM (DTAM)不适用。在网络带宽充足的情况下, 参与的物联网设备越多, 收益越好。我们需要通过选择隐私预算来平衡隐私保护和收入之间的矛盾。

## VII. 结论

本文提出了一种基于区块链技术和智能合约的边缘物系统, 实现了完全去中心化和防篡改。为了对物联网设备和边缘节点之间的资源分配和定价进行建模, 我们提出了一个新的组合双拍卖问题。然后, 我们在拍卖中引入差别隐私, 以进一步防止隐私泄露。首先, 我们设计了 DPAM 机制, 并证明它满足  $\epsilon$ -差分隐私性、 $\gamma$ -真实性、个体理性、预算平衡, 但不满足计算效率。不适合在资源类型太多的情况下使用。然后, 我们提出了 DPAM-S 机制, 将时间复杂度降低到多项式时间, 并满足上述期望的性质。最后, 我们建立了一个虚拟区域, 通过大量的模拟来测试我们提出的机制, 这证实了我们的理论分析。

## 承认

本工作得到了国家自然科学基金项目“人工智能与多模态数据处理广东重点实验室”的资助。61872239;北京师范大学珠海分校(BNU 珠海)和中国广东珠海 BNU-HKBU 联合国际学院(UIC)AI-DS 研究中心资助的 BNUUIC 人工智能与未来网络研究所。

## 参考

- [1] J. 倪, k. 张, x. 林, 和 x. 沈, “为物联网应用保护雾计算:挑战和解决方案”, IEEE 通信调查和教程, 第一卷。20, 不。1 页。601–628, 2017.
- [2] A. A. 艾丽和 m. 米 (meter 的缩写)。Alam, “Secoff-fciot:基于机器学习的智能城市应用物雾云安全卸载”, 物联网, 第 1 卷。第 7 页。100070, 2019.
- [3] 名词 (noun 的缩写)。Z. 艾特詹和 d. Svetinovic, “通过多签名、区块链和匿名消息流的分散能源交易中的安全性和隐私性”, IEEE 可靠和安全计算事务, 第 1 卷。15, 不。第 5 页。840–852, 2016.
- [4] J. 郭, x. 丁, 和 w. 吴, “支持智能城市分布式电力交易生态系统”, IEEE 物联网杂志, 第一卷。8, 没有。第 3 页。2040–2050, 2020.
- [5] 南。中本聪, “比特币:一个点对点的电子现金系统”, 《去中心化商业评论》, p. 21260, 2008.
- [6] R. 朱, z. 李, 女。吴, k. Shin, 和 g. 陈, “近似收益最大化的差分私有频谱拍卖”, 载《第 15 届移动自组网与计算国际学术研讨会论文集》, 2014 年, 页。185–194.
- [7] R. 朱和 k. G. Shin, “具有近似收益最大化的差异化私有和策略证明频谱拍卖”, 2015 年 IEEE 计算机通信会议(INFOCOM)。电气和电子工程师协会, 2015 年, pp. 918–926.
- [8] C. Dwork, “差异隐私:结果调查”, 在计算模型理论和应用国际会议上。斯普林格, 2008 年, 页。1–19.
- [9] F. 麦克雪莉和 k. 塔尔瓦尔, “通过差别隐私的机制设计”, 在第 48 届 IEEE 计算机科学基础年会(FOCS'07)上。电气和电子工程师协会, 2007 年, 页。94–103.

- [10] H. 金, l. 苏, b. 丁, k. Nahrstedt 和 n. 博里索夫, “为移动人群感应系统提供隐私保护激励”, 2016 年 IEEE 第 36 届分布式计算系统国际会议。电气和电子工程师协会, 2016 年, pp. 344–353.
- [11] J. 林, d. 杨, m. 李, j. 徐, 和 g. 薛, “Bidguard:保护隐私的众包激励机制框架”, 2016 年 IEEE 通信与网络安全会议(CNS)。电气和电子工程师协会, 2016 年, pp. 145–153.
- [12] J. 郭和 w. 吴, “基于差别隐私的在线分配, 整合和边缘计算”, arXiv 预印本 arXiv:2101.02834, 2021.
- [13] T. 倪, z. 陈, l. 陈。张, y. 徐, 还有 h. 钟, “差异化的私有组合云拍卖”, IEEE 云计算交易, 页。1–1, 2021.
- [14] D. 杨, g. 薛, x. 方, 和 j. 唐, “众包的激励机制:智能手机众包”, IEEE/ACM 网络交易, 第一卷。24 不。第 3 页。1732–1744, 2015.
- [15] J. 郭, x. 丁, 和 w. 吴, “车辆网络中基于的可靠交通监控机制”, IEEE 可靠性学报, 第 100–100 页。1–1, 2021.
- [16] W. 王, b. 梁, 和乙。李, “设计具有本地市场的真实频谱双重拍卖”, IEEE 移动计算交易, 第一卷。13 号没有。1 页。75–88, 2012.
- [17] A. Yassine。南。侯赛因。穆罕默德和 m. 吉扎尼, “动态自主电动汽车能源交易的双重拍卖机制”, IEEE 车辆技术交易, 第一卷。68, 不。第 8 页。7466–7476, 2019.
- [18] W. 孙, j. 刘, y. 岳, 和 h. 张, “基于双拍卖的工业物联网移动边缘计算资源分配”, IEEE 工业信息学交易, 第 2 卷。14 号没有。10 页。4692–4701, 2018.
- [19] 单位。哈比巴, s. Maghsudi 和 e. Hossain, “移动边缘计算卸载中高效资源分配的反向拍卖模型”, 2019 年 IEEE 全球通信会议(GLOBECOM)。电气和电子工程师协会, 2019 年, pp. 1–6.
- [20] X. 彭。Ota, 和 m. 董, “车辆雾计算中资源分配的多属性双拍卖”, IEEE 物联网杂志, 第一卷。7, 没有。第 4 页。3094–3103, 2020.
- [21] W. 孙, j. 刘, y. 岳, 和 p. 王, 移动边缘计算的联合资源分配和激励设计, IEEE 无线通信事务, 第一卷。19, 不。第 9 页。6050–6064, 2020.
- [22] Y. 焦, p. 王, d. 尼雅托和 k. 公共区块链网络的云/雾计算资源分配中的拍卖机制。30, 不。第 9 页。1975–1989, 2019.
- [23] X. 丁, j. 郭, 马超。李和 w. 吴, “建立基于的安全物联网的激励机制”, 《IEEE 网络科学与工程学报》, 第 1 卷。8, 没有。1 页。477–487, 2020.
- [24] ——“采用边缘计算的物联网区块链的定价和预算分配”, arXiv 预印本 arXiv:2008.09724, 2020.
- [25] J. 郭, x. 丁, 和 w. 吴, “使用 Dag-区块链的车辆间充电调度的双重拍卖”, arXiv 预印本 arXiv:2010.01436, 2020.
- [26] Z. 陈, t. 倪, h. 钟, s. 张和 j. 崔, “近似社会福利最大化的差分私人双频谱拍卖”, 《信息取证与安全的 IEEE 交易》, 第 1 卷。14 号没有。第 11 页。2805–2818, 2019.
- [27] 问。项, l. 孔, x. 刘, j. 许, 和 w. 王, “Auc2reserve:电动汽车快速充电预约的差异化私人拍卖”, 2016 IEEE 第 22 届嵌入式与实时计算系统与应用国际会议(RTCSA)。电气和电子工程师协会, 2016 年, pp. 85–94.
- [28] D. 李问。杨, w. 余婷。安, y. 张和 w. 赵, “基于差分隐私的智能电网在线双重拍卖”, IEEE 信息取证与安全交易, 第一卷。15 页。971–986, 2019.
- [29] G. 高, 男。肖, j. 吴, s. 张, l. 黄, 和 g. 肖, “Dpdt:一种差异化的私人群体感知数据交易机制”, IEEE 物联网杂志, 第一卷。7, 没有。1 页。751–762, 2019.
- [30] A. k. 古普塔。利格特, f. 麦克雪莉, a. 罗斯和 k. Talwar, “差分私有组合优化”, 载于第 21 届年度 ACM-SIAM 离散算法研讨会论文集。SIAM, 2010 年, 第 10 页。1106–1125.
- [31] Y. 南。儿子, r. k. 巴尔迪克。-H. 李和 s. 短期电力市场拍卖博弈分析:统一的和按投标价支付的定价。19, 不。第 4 页。1990–1998, 2004.



郭获得博士学位。2021 年获得美国德克萨斯州理查森市达拉斯德克萨斯大学计算机科学系学位，2015 年获得中国广东广州华南理工大学化学化工学院学士学位。现任 BNU UIC 人工智能与未来网络研究所助理教授、广东省人工智能与未来网络重点实验室助理教授。多模态数据处理，BNU-HKBU 联合国际学院，珠海，广东，中国。他的研究兴趣包括社交网络、算法设计、数据挖掘、物联网应用、区块链和组合优化。

丁行健于 2012 年获得四川大学电子信息工程学士学位，2017 年获得北京林业大学软件工程硕士学位。他获得了博士学位。2021 年获得中国人民大学信息学院学位。现任北京工业大学软件工程学院助理教授。他的研究兴趣包括无线充电传感器网络，近似算法设计和分析，以及区块链。



贾伟·贾，现任北京师范大学 BNU-UIC 人工智能与未来网络研究所所长、讲座教授；BNU-HKBU 联合公司研究副总裁

国际学院。他的贡献被公认为最优网络路由和部署、选播和服务质量路由、传感器网络、人工智能(知识关系抽取；NLP 等。和边缘计算。他在著名的国际期刊/会议、研究书籍和书籍章节中发表了 600 多篇文章。他就是那个家伙  
美国电气和电子工程师学会会员，中国计算机学会杰出会员。