基于差分隐私的联盟链上双向能源拍卖隐私保护

姜顺荣[1,2],时 坤[1],周 勇[1,2]
(1. 中国矿业大学计算机科学与技术学院,江苏徐州 221116;2. 矿山字化教育部工程研究中心,江苏徐州 221116)

摘 要: 微电网是一个分布式小型发配电系统,根据产消者不同的需求,通过邻近能源交易的方式实现电力的循环流动. 为了在微电网的能源交易中制定最优的定价和交易策略,本文结合联盟链的特点提出了双向密封竞价(Double Sealed Bid,DSB)拍卖方案,该方案在满足关键的经济性质(个人理性、预算平衡等)的基础上通过用户的报价、出价、电量和价格期望等因素共同决定获胜者. 同时为了保护拍卖过程中参与用户的隐私,本文根据DSB拍卖方案的特点,基于差分隐私理论提出了BDP(Blockchain-based Differential Privacy)算法,并通过隐私分析和数据有效性分析表明该算法既满足了差分隐私要求又满足了均值有效性. 最后,本文将BDP算法应用于DSB拍卖方案中,实现了安全高效的双向能源拍卖隐私保护方案-DPDAB(Differential Privacy-based Double Auction on Blockchain),该方案在实现最优的定价和交易策略的同时保护了拍卖过程中参与用户的隐私. 此外,本文通过实验分析了BDP算法对拍卖数据的影响以及处理数据的时间开销对拍卖方案的影响,并通过对比实验证明了DPDAB方案在平均效益、用户满意度和社会福利方面的有效性.

关键词: 双向密封竞价拍卖;差分隐私;联盟链;微电网;能源交易
基金项目: 徐州市科技计划项目(No.kc21044);中央高校基本科研业务费专项项目(No.2020ZDPY0306);国家重点研发计划(No.2020YFB1005500)
中图分类号: TP399 **文献标识码:** A **文章编号:** 0372-2112(2024)09-3023-15
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20221299

Differential Privacy-Based Double Energy Auction Privacy-Preserving on Consortium Blockchain

JIANG Shun-rong[1,2], SHI Kun[1], ZHOU Yong[1,2]
(1. *School of Computer Science and Technology*, *China University of Mining and Technology*, *Xuzhou*, *Jiangsu* 221116, *China*;
2. *Mine Digitization Engineering Research Center of the Ministry of Education*, *Xuzhou*, *Jiangsu*, 221116, *China*)

Abstract: Micro-grid is a distributed small-scale power generation and distribution system, which has realized the circular flow of electricity through adjacent energy trading according to the different needs of prosumers. In order to develop optimal price and transaction strategies in energy trading of micro-grid, we proposed a double sealed bid (DSB) auction scheme according to the characteristics of consortium blockchain. Except met key economic properties (individual rationality, budget balance, and so on), this scheme would determine the final winner based on the users' offers, bids, volumes, average price and other factors. In the meanwhile, in order to protect the personal privacy of users in the auction process, we proposed the blockchain-based differential privacy (BDP) algorithm based on the differential privacy theory and the characteristics of the DSB auction scheme, which was satisfied with differential privacy demands and mean validity through privacy analysis and data validity analysis. Finally, we applied the BDP algorithm to the DSB auction scheme and realized a safe and efficient double energy auction privacy-preserving scheme—differential privacy-based double auction on blockchain (DPDAB), which not only developed the optimal price and transaction strategy but also protected the users' privacy in the process of auction. In addition, we analyzed the influence of the BDP algorithm on auction data and the data computation time overhead on the auction scheme through experiments, and proved the validity of the DPDAB scheme in terms of average benefit, user satisfaction and social welfare through comparative experiments.

Key words: double sealed bid auction; differential privacy; consortium blockchain; micro-grid; energy trading
Foundation Item(s): Xuzhou Science and Technology Program (No.kc21044); Central Universities Basic Research

收稿日期:2022-11-11;修回日期:2023-07-18;责任编辑:梅志强

Business Fund Special Project (No.2020ZDPY0306); National Key R&D Program of China (No.2020YFB1005500)

1 引言

随着光伏、风力发电技术的不断发展,此类新能源技术的发电成本不断降低且产能急剧增加[1],使得微电网技术受到了广泛的关注. 微电网是一个分布式小型发配电系统[2],系统中的用户使用光伏或风力发电技术自主发电并存储在微电网中,同时该网络中电力短缺用户也可以通过微电网以较低的价格邻近购买电力,实现电力循环流动. 此外,可以通过国家电网向微电网输电的方式解决其电力缺失和负载不均的问题. 与传统电网中心化交易模式不同,微电网采用分布式邻近能源交易的方式降低交易成本,减少电力传输损耗. 但是,该交易模式具有参与主体多、交易机制复杂和交易管理困难等特点[3],会产生信任缺失、恶意篡改和虚假交易等问题,而区块链技术可以有效解决上述问题. 因此许多基于区块链的微电网能源交易方案被提出[4~7].

然而在实施微电网能源交易方案时需要进行一系列关键决策(确定交易双方;确定交易的能源单价;确定交易电量;保证交易双方的利益等)来保证交易顺利进行. 通过深入分析能源交易流程,我们发现能源拍卖的方式可以有效地完成微电网能源交易过程中需要的一系列关键决策[8]. 因此,本文的研究目的之一是为基于区块链的微电网能源交易系统,制订一个满足关键经济性质、符合基本拍卖规则、用户友好型的能源拍卖方案. 图1展示了基于区块链的微电网能源拍卖和交易的系统框架图:参与能源拍卖的发电用户向管理中心提交报价,管理中心根据用户报价调用智能合约确定拍卖底价;参与能源拍卖的普通用户根据拍卖底价出价,然后管理中心调用智能合约确定获胜的拍卖双方,并将拍卖结果公开上链;最后智能电站根据拍卖结果进行电力交易.

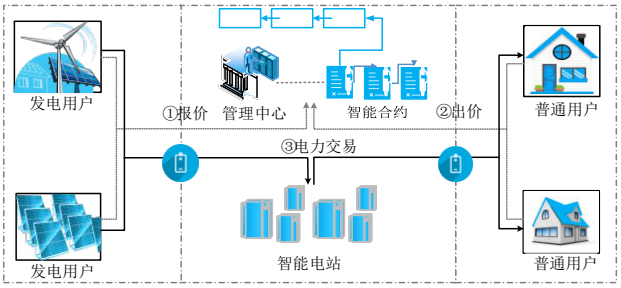


图1 基于区块链的微电网能源拍卖和交易的系统框架图

由于在基于区块链的能源拍卖与交易背景下,拍卖双方都有多个参与者,是多对多的关系,所以传统的一对多的拍卖方案不适合该拍卖背景,需要采取双向拍卖方案[9]. 然而双向拍卖方案需要交易双方频繁出价,最终达成交易. 这会占用大量的计算资源,不适合基于区块链的能源拍卖背景,为此需要重新制订能源拍卖方案. 此外,虽然基于区块链的能源拍卖和交易系统为产消者提供了去中心化的、公开透明的、可追溯的、不可篡改的[10]自由交易环境,但也使得链上能源拍卖数据极易受到攻击,从而泄露用户隐私. 例如,通过尝试不同的报价/出价组合推断可能的拍卖结果[11];结合背景知识,通过链接攻击或差分攻击得到用户的隐私信息[12,13]. 为了预防上述攻击,我们可以使用数据加密的方式保护能源拍卖数据的安全与隐私[14]. 但是链上公开密文拍卖数据会影响系统公开透明的特性,同时加解密操作会耗费大量的计算资源和时间,影响用户查询与验证效率. 而使用差分隐私技术保护拍卖数据中的隐私信息,既能保证系统的公开透明特性,又有较高的查询和验证效率[15],所以可以使用差分隐私技术保护链上能源拍卖数据. 然而由于能源拍卖数据是离散的,所以无法直接使用基于噪声添加的差分隐私算法保护能源拍卖数据的隐私,且基于随机响应的差分隐私算法又不能保证数据的均值有效性,因此现有的差分隐私算法都不能很好的满足链上能源拍卖方案的隐私保护需求,为此需要重新设计差分隐私算法. 综上所述,本文重新设计了链上双向能源拍卖方案以及差分隐私算法,并结合联盟链的特点,提出了一种安全高效的能源拍卖数据隐私保护方案. 本文工作的主要贡献如下.

(1)根据基于联盟链的微电网能源交易系统的特点,设计了双向密封竞价(DSB)拍卖方案,并详细介绍了DSB拍卖方案的具体拍卖流程,同时使用理论分析证明了DSB拍卖方案满足几个关键的经济性质.

(2)本文基于差分隐私理论提出了BDP算法,并结合联盟链和DSB拍卖方案的特点设计了安全高效的双向能源拍卖隐私保护方案-DPDAB.

(3)通过隐私分析证明了BDP算法满足差分隐私要求,并通过数据有效分析证明了使用BDP算法处理后的能源拍卖数据满足均值有效性.

(4)通过实验分析了BDP算法对能源拍卖数据的影响,并通过与其它方案的对比实验验证了DPDAB方案具有较高的有效性.

2 相关工作

在2006年,Dwork[16]首次提出了一种在数据中添加噪声在保护数据隐私的同时尽可能地保证数据统计有效性的思想,这就是差分隐私,其中数据扰动机制是差分隐私算法的核心. 如何设计一个既满足差分隐私要求又可以保证数据有效性的扰动机制是差分隐私算法的重点与难点. 经过多年发展,目前主流的数据扰动机制

有拉普拉斯机制[16]、高斯机制[17]、指数机制[18]和随机响应机制[19]等. 同时近年来出现了许多改进的数据扰动机制,Duchi等[20]基于互信息界理论,权衡隐私保护和统计估计风险,设计了理论上最优的本地差分隐私模型,并基于该模型提出了解决均值估计、中值估计等经典问题的有效方法. Wang等[21]针对分类数据,从互信息角度提出一个最佳的本地差分隐私机制—k子集机制,并证明其在离散分布估计的背景下比现有的方法更优.

由于差分隐私技术的隐私保护效果不依赖于攻击者拥有多少背景知识[22],仅和自身的隐私预算有关,作为一种新的隐私保护模型被应用于各个领域. 近年来,在智能电网领域,出现了许多使用差分隐私技术保护电力聚合数据、用户数据或能源交易数据的研究成果. Ou等[23]提出了适用于用户行为隐私保护的本地化差分隐私算法,并在对智能电网用户行为进行频谱分析的基础上,提出了基于傅立叶变换的数据扰动机制SSA-LDP,该机制在用户端实现了差分隐私保护. Gai等[24]提出了一种基于随机响应的满足本地差分隐私的智能电网聚合数据隐私保护方案. 该方案在保护参与者隐私的同时,实现了对电力供需统计数据的有效性估计. 与此同时,随着区块链技术不断成熟,基于区块链的分布式能源交易模式被广泛研究,结合差分隐私理论产生了诸多隐私保护成果. Gai等[25]在联盟链的基础上,通过账户映射技术生成虚拟账户来代替噪声,并通过加入的账户噪声掩盖用户的交易趋势和交易特征. Zhang等[26]提出了一个基于联盟链的用于邻接能源交易的隐私保护方案,该方案通过账户映射和添加噪声的方法来隐藏用户的交易数据分布信息,达到抵御链接攻击保护用户隐私的目的.

在能源交易时进行一系列关键决策以匹配合适的交易双方是必要的,但上述方案都没有涉及该方面的研究. 因此,为了匹配合适的交易双方,降低能源交易成本,Luo等[27]设计了一种基于区块链的点对点电力交易架构,并提出了一个基于贝叶斯博弈方法的双向拍卖机制. Li等[28]提出了一种基于差分隐私的在线双重拍卖方案,使用差分隐私技术保护电动汽车的敏感出价信息. Hassan等[29]提出使用能源拍卖方案解决能源交易用户匹配问题,他们设计了一种基于区块链的微电网能源拍卖方案,并使用差分隐私技术保护参与者的隐私信息. 如表1展示了各方案之间的差别,其中√表示该方案使用了该项技术,×表示该方案没有使用该项技术.

然而现有的能源拍卖方案在实际应用中存在一些问题,Luo等[27]没有考虑用户数据隐私保护问题,仅依靠区块链自身加密技术无法完全预防攻击者的链接攻击、差分攻击等. Li等[28]使用差分隐私保护了支付阶段和分配阶段的隐私信息,但是该方案无法保护出价阶段的隐私信息且不能保证拍卖师(第三方)是可信的. Hassan等[29]使用差分隐私算法保护拍卖数据的隐私,然而该方案无法验证链上公开拍卖数据的有效性,导致拍卖结果存疑,并且该方案需要多次扰动数据,这会消耗大量的计算资源,加重区块链的计算负担. 综上所述,本文提出了基于差分隐私的联盟链上双向能源拍卖数据隐私保护方案来保护能源拍卖数据中的用户隐私信息,并且通过数据有效性分析证明了链上公开拍卖数据满足均值有效性.

表1　各方案的比较情况

方案	差分隐私	智能电网领域	区块链	拍卖方案
Duchi[20]	√	×	×	×
Wang[21]	√	×	×	×
Ou[23]	√	√	×	×
Gai[24]	√	√	×	×
Gai[25]	√	√	√	×
Zhang[26]	√	√	√	×
Luo[27]	×	√	√	√
Li[28]	√	√	×	√
Hassan[29]	√	√	√	√

3　预备知识

3.1　差分隐私

差分隐私技术就是使用概率学相关知识处理数据,使得攻击者无法通过公开数据获得真实数据相关信息,同时尽可能的保证统计结果准确. 本文涉及到的差分隐私算法相关定义与公式如下.

定义1　ε-本地差分隐私:当且仅当扰动函数f:$x\to R^k$的定义域中任意两个输入x和x',以及任意一个输出$y\in \mathrm{Range}(f)$满足式(1)时,函数f满足ε-本地化差分隐私.

$$\Pr\left[f(x)=y\right]\leqslant \mathrm{e}^{\varepsilon}\times\Pr\left[f(x')=y\right] \tag{1}$$

其中Pr[]表示概率,如果函数f的输出是连续的,概率将替换为概率密度函数. ε表示隐私预算.

定义2　邻近数据集:如果存在两个数据集D和D^*,两个集合相差的元素数目可以由式(2)计算.

$$\Delta=\left|D\oplus D^*\right| \tag{2}$$

当且仅当$\Delta=1$时,D与D^*为邻近数据集.

定义3　l-全局敏感度:对于函数f: $D\to R^k$的l-全局敏感度定义如式(3)所示.

$$\Delta f=\max_{D\sim D'}\left\| f(D)-f(D^*)\right\|_1 \tag{3}$$

其中$\|\cdot\|$为L_1范式.

定义4　拉普拉斯机制:对于函数G: $D\to R^n$,拉普拉斯机制通过式(4)实现$(\varepsilon,0)$-差分隐私.

$$F(D)=G(D)+\boldsymbol{\eta} \tag{4}$$

其中 $\boldsymbol{\eta}$ 为随机向量且各元素服从拉普拉斯分布，即 $\eta_i \sim \mathrm{Lap}(\frac{\Delta f}{\varepsilon})$.

定义 5 多元随机响应：假设扰动函数 P 的定义域为 $x \in \{1,2\cdots,d\}$，用户向数据收集方响应正确数据的概率为 p，响应不同错误数据的概率相同为 q. 即

$$P(y|x)=\begin{cases} p=\dfrac{\mathrm{e}^{\varepsilon}}{\mathrm{e}^{\varepsilon}+d-1}, y=x \\ q=\dfrac{1}{\mathrm{e}^{\varepsilon}+d-1}, y\neq x \end{cases} \tag{5}$$

其中 ε 表示隐私预算.

3.2 Fabric联盟链

Fabric联盟链是多个机构共同参与管理的区块链，适用于具有多个交易实体的联盟，且只有特定成员有访问权限. Fabric具有诸多优点：(1)Fabric是许可链，参与者彼此了解，并不是完全匿名的或完全不信任的，这在一定程度上缓解了信任缺失的情况.(2)Fabric使用通道技术实现不同组织共享不同的分布式账本，交易方必须通过通道的验证才能与账本进行交互，在一定程度上保证了账本的隐私性.(3)Fabric可以设置私有数据，只有被授权的组织可以调用智能合约访问存储在私有数据库中的私有数据. 本文的双向能源拍卖方案便基于Fabric联盟链实现.

3.3 拍卖方案

目前市场上存在许多拍卖方案，其中最基本的四种拍卖方案[30]是英式拍卖、荷兰式拍卖、第一价格密封拍卖和第二价格密封拍卖. 拍卖方案在设计的过程中需要满足一些关键的经济性质，包括个人理性、预算平衡、诚实性[31]. 这些性质既能够保证拍卖方案的公平性又可以有效防止用户扰乱拍卖市场秩序.

(1)个人理性：每个参与拍卖的用户的效益都是非负的. 对于任意理性的买方，其支付价格不能高于其出价；对于任意理性的卖方，收入不能低于其报价.

(2)预算平衡：拍卖师的效益不小于零，即所有买方支付的总报价大于等于所有卖方最终的总出价.

(3)诚实性：任何参与拍卖的用户都无法通过提交虚假的竞标价格来提高自身的利益，即诚实性能够保证每个参与拍卖的用户都按照自己的真实估价进行竞价.

4 能源拍卖系统模型与攻击模型

本文使用的符号描述如表2所示.

4.1 能源拍卖系统模型

首先按照用电区域将用户划分到不同的组织，每个组织包含管理中心和智能电站两个部分，如图2展示了某用电区域基于联盟链的能源拍卖系统. 不同区域的组织共同组成联盟链，并通过Fabric联盟链技术保证不同组织之间协同，如图3展示了基于联盟链的能源拍卖网络结构. 本文设计的能源拍卖系统模型主要包括监管中心、管理中心、智能电站、卖方和买方五个部分.

表2 本文方案使用的符号

符号	含义
$S/B/C$	所有能源卖方/所有能源买方/监管中心
S_k/B_k	编号为 k 的能源卖方/买方
M/E	管理中心/智能电站
$\mathrm{EP}_S/\mathrm{EP}_{S*}$	卖方真实期望报价/BDP处理后的卖方期望报价
$\mathrm{EP}_B/\mathrm{EP}_{B*}$	买方真实期望出价/BDP处理后的买方期望出价
MP	市场能源单价
$\mathrm{Set}_S/\mathrm{Set}_B$	具有拍卖资格的卖方/买方集合
$\mathrm{SP}_k/\mathrm{BP}_k$	编号为 k 的卖方报价/买方出价
$\mathrm{SV}_k/\mathrm{BV}_k$	编号为 k 的卖方/买方请求交易电量
$\mathrm{CertS}_k/\mathrm{CertB}_k$	编号为 k 的卖方/买方拍卖权限证书
W_S/W_B	匹配成功的卖方/买方集合
$\mathrm{TotalV}_S/\mathrm{TotalV}_B$	卖方/买方交易的总电量

(1)监管中心 C 具有颁发证书、设置权限、监管交易等功能，并监管着各用户的拍卖行为. 若 C 发现某用户在拍卖进程中实行了违规操作，将通过终止授权的方式将违规用户剔除交易网络，或通过废除拍卖证书的方式将违规用户剔除本次能源拍卖进程.

(2)管理中心 M 由联盟链中的组织节点构成，其具有审核用户拍卖资格以及提供智能合约运行环境的作用. 各用户是否具有参与本轮拍卖的资格，需要通过 M 审核，只有通过 M 的审核，才能获得 C 授权的拍卖证书. 同时 M 简化了支付流程，各买方 B 只需要考虑向 M 支付，而各卖方 S 只需要考虑从 M 获取收益，具体的交易细节由 M 自动完成.

(3)智能电站 E 是各卖方 S 与各买方 B 交易能源的智能中转站，是组织节点的载体. E 和 M 共享数据，并通过智能系统协调各交易方的电力流动. E 简化了电力流转过程，各卖方 S 只需要考虑向 E 输电，而各买方 B 只需要考虑从 E 取电，具体的交易细节由 E 自动完成.

(4)S_k 在能源拍卖系统模型中是能源出售方，在获得拍卖权限证书后，需要向 M 提交报价 SP_k(每度电的价格)和出售电量 SV_k. 该报价会决定最终的拍卖底价 EP_S.

(5)B_k 在能源拍卖系统模型中是能源购买方，在获得拍卖证书后，会根据公布的拍卖底价 EP_S 和市场价 MP 出价，包括出价 BP_k 和购买电量 BV_k. 该出价会决定最终的交易价格 EP_B. 最终竞拍获胜者由交易双方的出价 SP_k、报价 BP_k、出售电量 SV_k、购买电量 BV_k、拍卖底价 EP_S 以及交易价格 EP_B 共同决定.

4.2 攻击模型

在基于联盟链的能源拍卖系统中，影响到最终拍卖结果的数据都将上链公开，例如各卖方 S 的期望报价

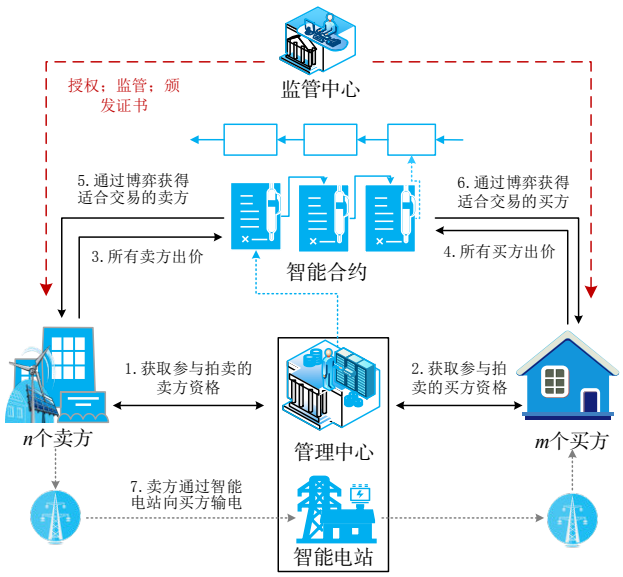


图2　某用电区域的基于联盟链的能源拍卖系统

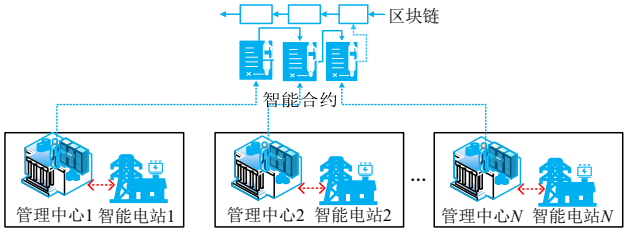


图3　基于联盟链的能源拍卖网络结构

SP_k和出售能源总量$TotalV_S$以及各买方B的期望出价BP_k和购买能源总量$TotalV_B$. 但公开透明的数据极易受到攻击,一旦受到攻击,极易泄露用户的隐私信息,所以需要对能源拍卖数据进行隐私保护处理.

(1)假设攻击者具有多个数据源,例如具有链下能源分配数据和多轮能源拍卖数据. 由于用户对能源的期望出价短时间内不会发生变化,拍卖的能源总量也不会突然增多. 即使用户匿名参加拍卖,攻击者也可以通过分析多轮拍卖数据之间的特征并与链下能源分配数据比较,通过链接攻击获得用户的隐私信息[12].

(2)假设攻击者知道能源拍卖系统中某个区域所有用户的基本信息,以及部分用户的历史能源拍卖数据. 即使该区域的用户是匿名参与能源拍卖的,但由于所有的拍卖数据是公开透明的,所以攻击者仍然可以通过比较匿名的能源拍卖数据与已知的部分用户的历史能源拍卖数据,分析其中的差异性,最终根据先验知识分析出各用户的真实报价/出价,进而获得用户的隐私信息[13].

5　DSB拍卖方案

能源拍卖具有以下几个重要特点[27]:拍卖底价由卖方的报价决定;最终成交价由买方的出价决定;拍卖的能源总量决定竞拍获胜者数量. 本文基于Fabric联盟链的特点提出的DSB拍卖方案除了具有上述能源拍卖特点还具有:卖方和买方都需要针对能源单价进行报价或出价,即是双向的;每轮拍卖周期内,卖方和买方都只能报价或出价一次;在报价周期结束前,报价是密封的;在出价周期结束前,出价是密封的. DSP拍卖方案的具体描述如下.

5.1　初始化

由于DSB能源拍卖方案基于Fabric联盟链实现,因此本文使用Fabric证书体系管理参与拍卖的权限证书. 当用户同时具有组织成员证书和拍卖权限证书时才能参与能源拍卖. 具体步骤如下.

5.1.1　组织成员证书

假设所有参与能源拍卖的用户都是能源拍卖网络成员,且监管中心C已经为各组织成员生成了符合X.509标准的证书文件. 组织成员证书形式为$\text{cert}_o(\text{pk}_o,\text{sk}_o)$. 其中$\text{cert}_o$代表实体$o$证书文件,$\text{pk}_o$代表实体$o$公钥,$\text{sk}_o$代表实体$o$私钥.

5.1.2　拍卖权限证书

假设第i轮能源拍卖起止时间为$[T_{i-1},T_i]$,我们需要在T_{i-1}时间之前完成初始化操作.

(1)分配各参与用户的拍卖权限证书. 如图2的步骤1、步骤2所示,具体的步骤如下.

① 用户使用cert_o证书文件向M提交参与拍卖请求$\text{req}(\text{flag},\text{msg})$,其中flag表示用户申请的拍卖资格类型,msg表示用户资产的基本信息.

② M收到请求后解析拍卖请求,flag=0表示用户申请出售能源;flag=1表示用户申请购买能源. 然后M根据msg中的能源资产信息以及总资产信息判断该用户是否具有参与拍卖的资格.

③ 在用户通过了审核后,M会向C提供该用户的相关信息并为其申请参与第i轮能源拍卖的权限证书. 然后C会将相应的权限证书CertS_k和CertB_k分别发送给S_k/B_k作为第i轮能源拍卖的权限证明.

(2)核实参与用户的拍卖权限证书. M将S/B的拍卖权限证书分别存储在$\hat{\text{Set}}_S=\{\text{CertS}_1,\cdots,\text{CertS}_k,\cdots\}$和$\hat{\text{Set}}_B=\{\text{CertB}_1,\cdots,\text{CertB}_k,\cdots\}$中,其中集合$\hat{\text{Set}}_S$处理卖方报价,集合$\hat{\text{Set}}_B$处理买方出价. 在$M$收到报价/出价信息后,依据集合$\hat{\text{Set}}_S$和$\hat{\text{Set}}_B$核实用户的拍卖权限证书信息.

5.2　拍卖流程

(1)当时间到达T_{i-1}时,开始第i轮能源拍卖. 首先各卖方S使用拍卖权限证书CertS_k报价,开启S_k报价周期,即

$$S_k \rightarrow M:\text{En}(\text{pk}_M,(\text{CertS}_k;(\text{SP}_k,\text{SV}_k))). \tag{6}$$

M将S_k的报价数据以及请求电量数据存储在集合$\hat{\text{Set}}_S$中,在各卖方S报价周期结束后得到集合$\text{Set}_S=$

$\{\text{CertS}_1:(\text{SP}_1,\text{SV}_1),\cdots,\text{CertS}_k:(\text{SP}_k,\text{SV}_k),\cdots\}$，$M$ 调用智能合约处理 Set_S 中各卖方 S 的报价 SP_k，最终得到卖方期望报价 EP_S. 同时将 EP_S 作为 B_k 出价的底价，即 B_k 出价必须满足 $\text{BP}_k \geqslant \text{EP}_s$.

(2)在 S 拍卖数据上链公开后，开启买方 B 出价周期，各买方 B 使用拍卖权限证书 CertB_k 出价，即

$$B_k \rightarrow M\text{: En}(\text{pk}_M,(\text{CertB}_k:(\text{BP}_k,\text{BV}_k))). \tag{7}$$

M 将 B_k 的报价数据以及请求电量数据存储在集合 $\hat{\text{Set}}_B$ 中，在各买方 B 报价周期结束后得到集合 $\text{Set}_B=\{\text{CertB}_1:(\text{BP}_1,\text{BV}_1),\cdots,\text{CertB}_k:(\text{BP}_k,\text{BV}_k),\cdots\}$，$M$ 调用智能合约处理 Set_B 中各买方 B 的报价 BP_k，最终得到卖方期望报价 EP_B，作为拍卖最终成交价.

(3)在 B 拍卖数据上链公开后，为了保证 DSB 能源拍卖方案满足个人理性、预算平衡和弱诚实性[31]，M 调用智能合约通过以下步骤选出获胜的 S_k 和 B_k，并分别构成获胜用户集合 W_S 和 W_B. 具体的判断流程如图 4 所示. 拍卖结果如图 5 所示.

① 设 TV_S 和 TV_B 分别表示各用户 S 和 B 博弈过程中交易双方总电量的变化.

② 令 $\text{TV}_S=0$，根据 SP_k 对集合 Set_S 进行升序排序得到 Set'_S，并从前向后遍历 Set'_S. 如果 $\text{SP}_k \leqslant \text{EP}_S$ 且 $\text{SP}_k \neq 0$（当用户不报价时 $\text{SP}_k=0$），则 $\text{TV}_S=\text{TV}_S+\text{SV}_k$.

③ 令 $\text{TV}_B=0$，根据 BP_k 对集合 Set_B 进行降序排序得到 Set'_B，并从前向后遍历 Set'_B. 如果 $\text{BP}_k \geqslant \text{EP}_B$ 且 $\text{BP}_k \neq 0$，（当用户不出价时 $\text{BP}_k=0$），则 $\text{TV}_B=\text{TV}_B+\text{BV}_k$.

④ 如果 $\text{TV}_S<\text{TV}_B$，则继续遍历 Set'_S. 如果 $\text{SP}_k \leqslant \text{EP}_B \& \text{TV}_S<\text{TV}_B$，则 $\text{TV}_S=\text{TV}_S+\text{SV}_k$.

如果 $\text{TV}_S \geqslant \text{TV}_B$，则停止遍历 Set'_S. 此时 $\text{TotalV}_S=\text{TV}_S$，$\text{TotalV}_B=\text{TV}_B$. 将包含的卖家和买家分别加入集合 W_S 和 W_B.

如果 $\text{SP}_k>\text{EP}_B$，则停止遍历 Set'_B. 令 $\text{TV}_B=0$，重新遍历 Set'_B. 如果 $\text{TV}_S \geqslant \text{TV}_B$，则 $\text{TV}_B=\text{TV}_B+\text{BV}_k$. 直到 $\text{TV}_S<\text{TV}_B$，则 $\text{TV}_B=\text{TV}_B-\text{BV}_k$，并停止遍历 Set'_B. 此时 $\text{TotalV}_S=\text{TV}_S$，$\text{TotalV}_B=\text{TV}_B$. 将包含的卖家和买家分别加入集合 W_S 和 W_B.

⑤ 如果 $\text{TV}_S>\text{TV}_B$，令 $\text{TV}_S=0$，重新遍历 Set'_S. 如果 $\text{TV}_S<\text{TV}_B$，$\text{TV}_S=\text{TV}_S+\text{SV}_k$. 直到 $\text{TV}_S \geqslant \text{TV}_B$，则停止遍历 Set'_S. 此时 $\text{TotalV}_S=\text{TV}_S$，$\text{TotalV}_B=\text{TV}_B$. 将包含的卖家和买家分别加入集合 W_S 和 W_B.

(4)由于竞拍结果与交易双方的总电量有关，所以在获得竞拍获胜用户集合 W_S 和 W_B 后，将出售/购买总电量 TotalV_S 和 TotalV_B 上链公开.

(5)在第 i 论拍卖结束开始第 i+1 轮拍卖之前，需要进行如下操作.

① 竞拍获胜集合 W_B 中的 B_k 通过 M 向 W_S 中的 S_k 转账，S_k 则通过 E 向 B_k 输电. 具体的链上支付和链下能源分配过程可以参考文献[32~34].

② 将竞拍失败的 S_k/B_k 的拍卖权限证书加入到第 i+1 轮拍卖用户集合 $\hat{\text{Set}}_S$ 和 $\hat{\text{Set}}_B$ 中，同时根据 5.1.2 节初始化步骤，分配并核实新的参与用户的拍卖权限证书.

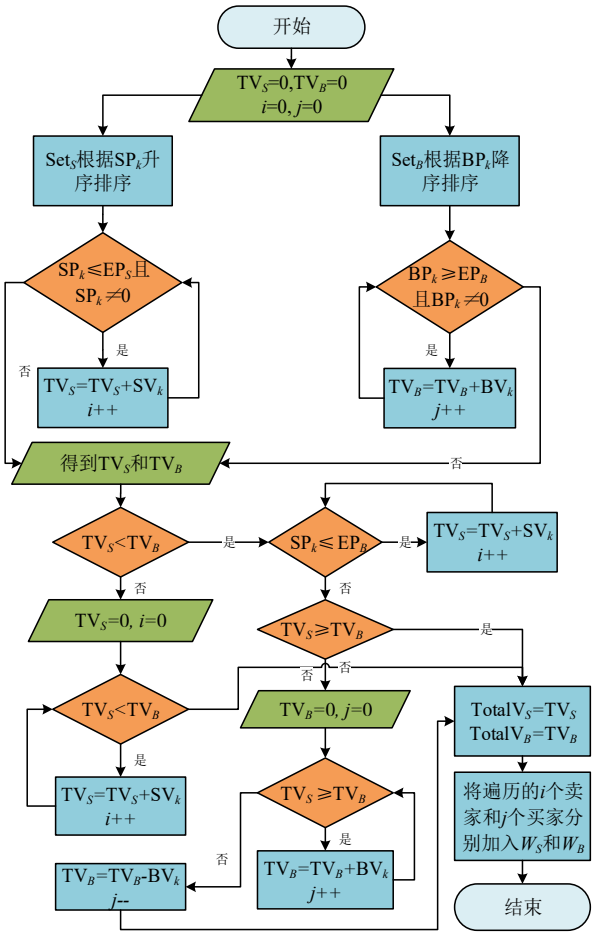


图 4 根据价格和电量判断流程图

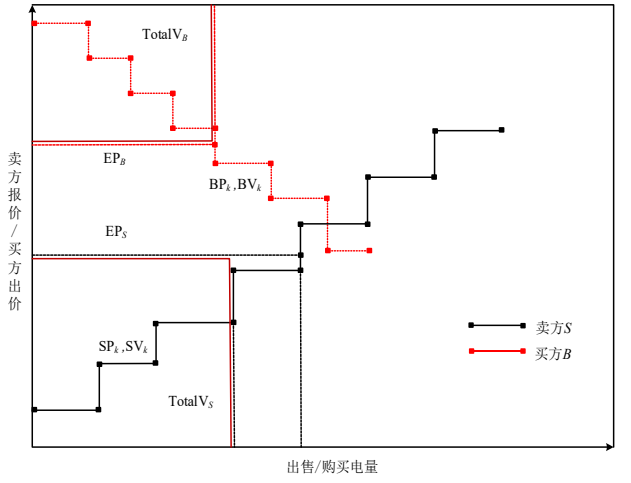


图 5 根据价格和电量选择获胜的 S_k 和 B_k

6 BDP算法

由3.2节可知,Fabric联盟链具有创建私有数据集合的功能,这使得Fabric联盟链成为了半可信的第三方.Fabric联盟链在收集数据过程是可信的,在将数据上链公开后将变得不可信.所以本文将Fabric联盟链抽象成两个第三方,即可信T和不可信NT.具有拍卖证书的S报价/B出价等价于T收集数据,然后T使用数据扰动机制保护拍卖数据中的隐私信息,并将扰动后的数据给NT(上链公开).为了满足双向密封竞价拍卖方案的隐私保护需求,本文基于Fabric联盟链设计了差分隐私算法-BDP算法.具体如算法1所示.

算法1　BDP算法

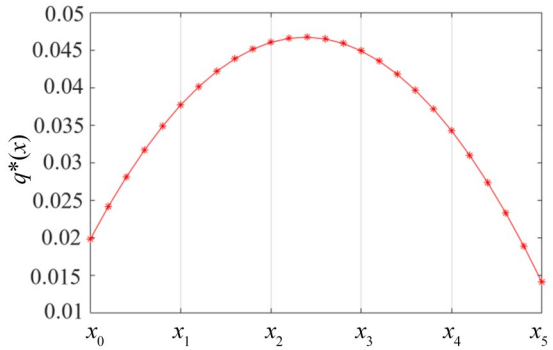
输入:$(x, p(x^*=y \mid x))$
输出:(y)
创建长度为n+1的数组arr
arr[0]=p
/*计算落在不同区间内的概率*/
/*arr[i]中所有元素之和为1*/
FOR i=1 to n
　$pp_i=p_i\times m_i$
　arr[i]=pp_i
END FOR
/*根据不同区间的概率划分区间[0,1]*/
FOR i=1 to n
　arr[i]=arr[i]+ arr[i−1]
　i++
END FOR
a=Rand(0,1)
IF$a\leqslant$arr[0]
　$y=x$
　RETURN y
ELSE
　遍历arr找到a所在位置(arr[i−1],arr[i]]
　根据a在arr中所在位置确定y所在区间[x_{i-1}, x_i]
　在区间[x_{i-1},x_i]随机生成整数,即y=x_{i-1}+RanInt(0,m_i) /*m_i为区间[x_{i-1}, x_i]长度*/
　RETURN y
END IF

6.1 数据扰动机制

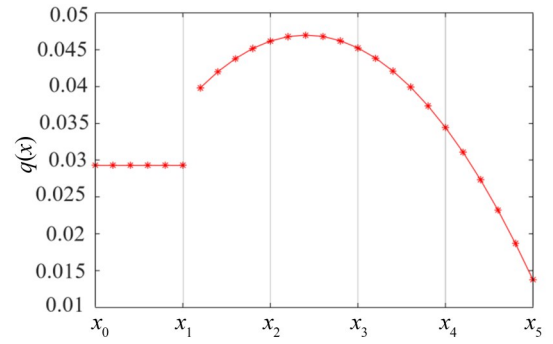
能源拍卖数据是离散型数据,可信T可以通过处理离散的报价或出价数据获得拍卖数据的概率分布函数.然而由于拍卖数据的概率分布过于复杂,直接根据其概率分布函数设计数据扰动机制是困难的,所以在保证拍卖数据期望值不变的情况下,本文将拍卖数据的概率分布函数转换成概率分布分段函数处理,以此来简化扰动机制.具体描述如下.

假设离散拍卖数据的概率分布函数如图6(a)所示,则概率分布分段函数$q^*(x)$在区间$[x_0,x_1]$内的期望值为

$$E_1(x)=\sum_{x=x_0}^{x_1}\left(x\times q_1^*(x)\right) \tag{8}$$



(a) 拍卖数据概率分布函数



(b) 拍卖数据概率分布的分段函数

图6　在区间$[x_0,x_1]$内拍卖数据概率分布转换情况

其中$q_1^*(x)$表示区间$[x_0,x_1]$内概率分布函数.转换成概率分布分段函数时要保证期望$E_1(x)$不变,所以在区间$[x_0,x_1]$内的概率计算如下

$$E_1(x)=\frac{(x_0+x_1)\times m_1\times q_1(x)}{2}$$

$$\Rightarrow q_1(x)=\frac{2\times\sum_{x=x_0}^{x_1}\left(x\times q_1^*(x)\right)}{(x_0+x_1)\times m_1} \tag{9}$$

其中m_1为区间$[x_0,x_1]$内离散数据个数,$q_1(x)$表示区间$[x_0,x_1]$内概率分布的分段函数.

根据式(9)求得概率分布分段函数$q(x)$在区间$[x_0,x_1]$内的概率分布情况,如图6(b)所示.拍卖数据的概率分布分段函数$q(x)$的公式如下.令$R=\sum_{j=1}^{n}\left(t_j\times m_j\right)$,则

$$q(x)=\begin{cases}\dfrac{t_1}{R}, x\in[x_0,x_1]\\ \dfrac{t_2}{R}, x\in[x_1,x_2]\\ \cdots\\ \dfrac{t_n}{R}, x\in[x_{n-1},x_n]\end{cases} \tag{10}$$

其中$\min\{t_i\}=1$,详细的转换过程如算法2所示.因此,根据$q(x)$设计的数据扰动机制如下

算法2 概率分布分段函数转换算法

输入:$(q^*(x), n, \text{List}(x_0, x_1, \cdots, x_n))$
输出:$(q(x))$
根据n确定List长度
/*根据 计算不同区间内的期望*/
FOR i=1 to n
$E_i(x)=\sum_{x=x_{i-1}}^{x_i}\left(x\times q_i^*(x)\right)$
i++
END FOR
/*根据$q^*(x)$的期望计算不同区间内的概率分布分段函数$q(x)$*/
FOR i=1 to n
$E_i(x)=\dfrac{(x_{i-1}+x_i)\times m_i\times q_i(x)}{2}$
$q_i(x)=\dfrac{2\times\sum_{x=x_{i-1}}^{x_i}\left(x\times q_i^*(x)\right)}{(x_{i-1}+x_i)\times m_i}$ /*m_i为区间$[x_{i-1},x_i]$内离散数据个数*/
i++
END FOR
根据多元方程组$\begin{cases}q_1(x)\times\sum_{j=1}^{n}\left(t_j\times m_j\right)=t_1\\ q_2(x)\times\sum_{j=1}^{n}\left(t_j\times m_j\right)=t_2\\ \cdots\\ q_n(x)\times\sum_{j=1}^{n}\left(t_j\times m_j\right)=t_n\end{cases}$计算$(t_1,t_2,\cdots,t_n)$的值
令$(t_1,t_2,\cdots,t_n)=(t_1,t_2,\cdots,t_n)\times\dfrac{1}{\min\{t_i\}}$
/*既不会改变$q(x)$又可以保证$\min\{t_i\}$=1*/
将$(t_1,t_2,\cdots,t_n)$代入得到$q(x)$
RETURN $q(x)$

$$p(x^*=y\mid x)=\begin{cases}\dfrac{e^{\varepsilon}}{e^{\varepsilon}+R}, y=x\\ \dfrac{t_1}{e^{\varepsilon}+R}, y\neq x\text{且}y\in[x_0,x_1]\\ \dfrac{t_2}{e^{\varepsilon}+R}, y\neq x\text{且}y\in[x_1,x_2]\\ \cdots\\ \dfrac{t_n}{e^{\varepsilon}+R}, y\neq x\text{且}y\in[x_{n-1},x_n]\end{cases}\tag{11}$$

其中,y为扰动后拍卖数据,$p(x^*=y|x)$为扰动后拍卖数据的概率分布函数,ε是隐私预算. 本文根据上述扰动机制扰动拍卖数据,达到保护拍卖数据中隐藏的用户隐私信息的目的.

6.2 隐私分析

为了保证上述数据扰动机制满足差分隐私定义要求. 本文限制了隐私预算ε的取值范围,其需要满足以下条件.

$$e^{\varepsilon}\geqslant\max\{t_i\}\Rightarrow\varepsilon\geqslant\ln(\max\{t_i\})\tag{12}$$

在ε满足式(12)条件时,上述差分隐私算法的隐私分析过程如下.

$$\frac{\Pr\left[f(x)=y\right]}{\Pr\left[f(x')=y\right]}=\frac{p\left(x^*=y\mid x\right)}{p\left(x^*=y\mid x'\right)}\leqslant\frac{\dfrac{e^{\varepsilon}}{e^{\varepsilon}+R}}{\dfrac{t_i}{e^{\varepsilon}+R}}=\frac{e^{\varepsilon}}{t_i}\leqslant\frac{e^{\varepsilon}}{\min\left(t_i\right)}=e^{\varepsilon}\tag{13}$$

根据定义1可知,$p(x^*=y|x)$扰动机制满足式(1),所以BDP算法满足ε-差分隐私.

6.3 数据有效性分析

本文设计的基于联盟链的能源拍卖系统的拍卖底价EP_S为各卖方S的报价期望,最终交易价格EP_B为各买方B的出价期望. 所以为了保证拍卖双方的利益,需要尽可能地保证扰动前后数据x与y的期望值相近甚至相同. 根据扰动前拍卖数据x的概率分布函数$q(x)$和拍卖数据扰动机制$p(x^*=y|x)$可以分别得到x与y的期望值$E(x)$和$E(y)$,具体计算过程如下.

$$R=\sum_{j=1}^{n}\left(t_j\times m_j\right),p=\frac{e^{\varepsilon}}{e^{\varepsilon}+R},p_i=\frac{t_i}{e^{\varepsilon}+R},q_i=\frac{t_i}{R}\tag{14}$$

$$N=\sum_{j=1}^{n}\sum_{x=x_{j-1}}^{x_j}\left(x\times q_j\right),O=\sum_{j=1}^{n}\sum_{x=x_{j-1}}^{x_j}\left(x\times t_i\right)\tag{15}$$

$$M=\sum_{j=1}^{n}\sum_{i=x_{j-1}}^{x_j}\left(i\times p_i\right)=\sum_{j=1}^{n}\sum_{i=x_{j-1}}^{x_j}\left(\frac{i\times t_i}{e^{\varepsilon}+R}\right)=\frac{\sum_{j=1}^{n}\sum_{i=x_{j-1}}^{x_j}\left(i\times t_i\right)}{e^{\varepsilon}+R}=\frac{O}{e^{\varepsilon}+R}\tag{16}$$

$$E(x)=\sum_{x=x_0}^{x_n}(x\times q(x))=\frac{\sum_{j=1}^{n}\sum_{x=x_{j-1}}^{x_j}x\times t_i}{\sum_{j=1}^{n}\left(t_j\times m_j\right)}=\frac{O}{R}$$
$$=\sum_{j=1}^{n}\sum_{x=x_{j-1}}^{x_j}x\times\left(\frac{t_i}{\sum_{j=1}^{n}\left(t_j\times m_j\right)}\right)=\sum_{j=1}^{n}\sum_{x=x_{j-1}}^{x_j}\left(x\times q_j\right)=N\tag{17}$$

$$E(y)=\sum_{j=1}^{n}\left(q_j\times\sum_{x=x_{j-1}}^{x_j}\left(i\times p+\sum_{j=1}^{n}\sum_{x=x_{j-1}}^{x_j}\left(i\times p_i\right)\right)\right)$$
$$=p\times\sum_{j=1}^{n}\sum_{x=x_{j-1}}^{x_j}\left(i\times q_j\right)+M\times\left(\sum_{j=1}^{n}\sum_{x=x_{j-1}}^{x_j}\left(q_j\right)\right)$$
$$=p\times N+M\times 1$$
$$=N\times\left(p+\frac{M}{N}\right)\tag{18}$$

由式(14)、式(16)和式(17)可知$p=\dfrac{e^{\varepsilon}}{e^{\varepsilon}+R},M=$

$\frac{O}{e^{\varepsilon}+R}$, $N=\frac{O}{R}$,所以

$$E(y)=N\times\left(p+\frac{M}{N}\right)$$
$$=N\times\left(\frac{e^{z}}{e^{z}+R}+\frac{\frac{O}{e^{z}+R}}{\frac{O}{R}}\right)$$
$$=N\times\left(\frac{e^{z}}{e^{z}+R}+\frac{R}{e^{z}+R}\right)=N \tag{19}$$

综上所述,$E(x)=E(y)$,所以使用BDP算法扰动的拍卖数据满足均值有效性.

7　DPDAB隐私保护方案

本节主要介绍DPDAB隐私保护方案,包括以下三个部分:(1)使用BDP算法保护DSB能源拍卖方案的报价/出价阶段和支付阶段拍卖数据的隐私;(2)根据扰动后的能源拍卖数据计算期望报价EP_S和期望出价EP_B;(3)通过理论分析说明隐私保护的DSB能源拍卖方案满足个人理性、预算平衡和弱诚实性三个性质. 如图7展示了基于差分隐私的联盟链上双向能源拍卖流程.

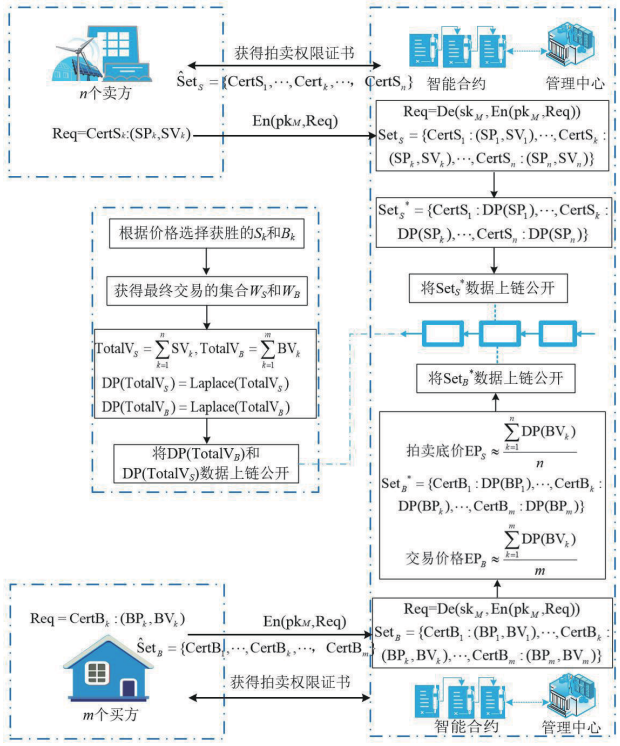


图7　基于差分隐私的联盟链上双向能源拍卖流程

7.1　能源拍卖数据隐私保护

DSB能源拍卖方案需要将各卖方S的报价SP_k和各买方B的出价BP_k以及售/购买总电量$TotalV_S$和$TotalV_B$上链公开. 因此,本文使用BDP算法处理S_k的真实报价SP_k以及B_k的真实出价BP_k来分别保护S_k和B_k的隐私,同时使用基于拉普拉斯机制的差分隐私算法保护出售/购买总电量$TotalV_S$和$TotalV_B$中隐藏的隐私信息. 具体方法描述如下.

7.1.1　保护SP_k和BP_k的隐私

(1)SP_k和BP_k数据特点:在DSP拍卖方案中,各用户S和B每轮拍卖只能提交一次价格. 由拍卖背景可知,S_k的报价范围受到市场能源单价MP和S_k的个人理性的限制,即$SP_k\in[\min\{SP_k\},\max\{SP_k\}]$,其中$\max\{SP_k\}\leqslant MP$. MP由$B_k$的个人理性拍卖性质决定,即理性的各买家$B$不会以高于市场能源单价MP的价格购买拍卖的能源. B_k的出价范围受到拍卖底价EP_S和市场能源单价MP的限制,即$BP_k\in[\min\{SP_k\},\max\{SP_k\}]$,其中$\min\{SP_k\}\geqslant EP_S$,$\max\{SP_k\}\leqslant MP$. EP_S由S_k的个人理性拍卖性质决定;MP由B_k的个人理性拍卖性质决定. 同时各买方S的报价数据以及各买方B的出价数据都是离散的,通常能源单价会精确到小数点后两位.

(2)使用BDP算法保护SP_k和BP_k的隐私:可信T收集各卖方S和买方B的报价和出价数据后,便会获得SP_k和BP_k的概率分布函数. 接着使用6.1节的数据扰动机制保护SP_k和BP_k的隐私,并将扰动后的出价和报价数据给不可信NT上链公开. 具体操作如下.

记SP_k的域为$Dom(SP_k)$. 首先将SP_k和$Dom(SP_k)$扩大100倍得到SP_k^*和$Dom(SP_k)^*$,其中SP_k^*为整数类型. 然后在$Dom(SP_k)^*$上对整数SP_k^*使用BDP算法,得到的扰动数据$DP(SP_k^*)$. 最后将$DP(SP_k^*)$缩小100倍得到扰动报价数据$DP(SP_k)$. 具体扰动过程在算法2中描述. 同理对BP_k使用BDP算法可以得到扰动出价数据$DP(BP_k)$. 最后将$DP(SP_k)$和$DP(BP_k)$数据链上公开.

7.1.2　保护$TotalV_S$和$TotalV_B$的隐私

本文使用拉普拉斯机制保护$TotalV_S$和$TotalV_B$的隐私. 根据定义2可以得到集合W_S的邻近数据集为W_S^*. 对集合W_S中的SP_k进行求和操作得到$TotalV_S$,所以操作函数f为求和函数. 由定义3可知$\Delta f=\max\{SP_k\}$,其中$SP_k\in W_S^*$. 因此由定义4可知$\mathrm{Lap}(\Delta f/\varepsilon)=-(\Delta f/\varepsilon)\times\mathrm{sign}(\alpha)\times\ln(1-2|\alpha|)$,所以$TotalV_S$的差分隐私扰动结果为$DP(TotalV_S)=TotalV_S+\mathrm{Lap}(\Delta f/\varepsilon)$,其中$\alpha$服从标准均匀分布即$\alpha\sim U(0,1)$. 同理可以得到$DP(TotalV_B)$. $DP(TotalV_S)$和$DP(TotalV_B)$为最终链上公开的用户出售和购买的能源总量数据.

7.2　计算EP_S和EP_B

根据6.3数据有效性分析证明可知,使用BDP算法扰动前后数据的期望值相同. 所以根据扰动前数据集Set_S求得的EP_S与根据扰动后数据集$Set_S^*=\{CertS_1:(DP(SP_1),SV_1),\cdots,CertS_k:(DP(SP_k),SV_k),\cdots\}$求得的$EP_S^*$

近似，即 $EP_S \approx EP_S^*$. 所以拍卖底价 EP_S 根据集合 Set_S^* 求得，即

$$EP_S \approx EP_S^* = \frac{\sum_{k=1}^{m} DP(SP_k)}{m} \tag{20}$$

其中 m 为有效报价用户个数. 同理可以计算 EP_B.

7.3 理论分析

在拍卖中，每个参与的用户都是自私且理性的，他们会采取策略最大化自己的效益. 效益就是获胜用户对于商品的估价和实际成交价格之差. 对于所有未获胜的买方或卖方，其效益均为零. 各卖方 S 的效益是最终收到的费用与自己的报价之差，而各买方 B 的效益是自己的出价和最终支付的价格之差. 买卖双方总效益计算公式如下.

$$\begin{cases} U_S^i = \sum\limits_{k \in W_S} \left(EP_B^* - SP_k\right) \times SV_k \\ U_B^i = \sum\limits_{k \in W_B} \left(BP_k - EP_B^*\right) \times BV_k \end{cases} \tag{21}$$

其中，i 表示拍卖轮次编号，k 表示参与拍卖用户编号. 合理的拍卖方案需要满足个人理性、预算平衡和弱诚实性三个性质.

性质 1 个人理性：DSB 拍卖方案满足个人理性.

证明 对于竞拍获胜的各卖方 S，出售电量价格为 EP_B^*，出售电量为 SV_k，各卖方 S 的报价为 $SP_k \leqslant EP_S^*$，又因为 $SP_k \leqslant EP_B^*$ 且 $SV_k>0$，所以 S_k 的效益 $U_{Sk}=(EP_B^*-SP_k)\times SV_k>0$. 对于竞标获胜的各买方 B，购买电量价格为 EP_B^*，购买电量为 BV_k，各买方 B 的出价为 $BP_k \geqslant EP_S^*$，因为 $BV_k>0$，所以 B_k 的效益 $U_{B_k}=(BP_k-EP_B^*)\times BV_k>0$. 对于没有获胜的 S_k/B_k 的效益为 0. 综上所述，DSB 拍卖方案满足个人理性.

性质 2 预算平衡：DSB 拍卖方案满足预算平衡.

证明 对于竞拍获胜者，双方交易价格为 EP_B^*，卖方出售电量为 $TotalV_S$，买方购买电量为 $TotalV_B$. 由 5.2 节拍卖流程可知 $TotalV_S \geqslant TotalV_B$，DSB 能源拍卖方案将多余的 $TotalV_S - TotalV_B$ 的电量传输给 E，并将 $(TotalV_S - TotalV_B)\times(MP - EP_B^*)$ 作为 E 的收益. 因此卖方收益为 $a=TotalV_S \times EP_B^*$，买方支出为 $b=(TotalV_S - TotalV_B)\times(MP - EP_B^*)+TotalV_S \times EP_B^*$，因为 $TotalV_S \geqslant TotalV_B$ 且 $MP \geqslant EP_B^*$，所以 $b-a \geqslant 0$. 对于没有获胜的 S_k/B_k 的收益为 0，因此 $b-a=0$. 综上所述，DSB 拍卖方案满足预算平衡.

性质 3 弱诚实性：DSB 拍卖方案满足弱诚实性.

证明 严格的诚实性会受到很多限制，几乎无法达成，只能通过拍卖规则达成弱诚实性. 双向密封竞价拍卖方案结合联盟链的性质（完善的证书体系和权限系统）以及特殊的能源的拍卖背景（出价受到市场价格和自身所拥有的资产限制，且竞拍获胜者由拍卖双方互相博弈得到）. 通过报价越低越容易获胜的方式保证各卖方 S 的弱诚实性，通过出价越高越容易获胜的方式保证各买方 B 的弱诚实性. 综上所述，DSB 拍卖方案满足弱诚实性.

8 实验分析

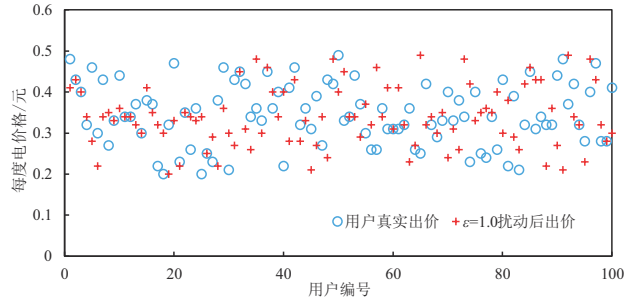
本文在 Hyperledger Fabric 2.4 联盟链平台上实现了基于差分隐私的联盟链上双向能源拍卖数据隐私保护方案，并对其有效性和时间开销进行了评估. 进行实验的基础能源拍卖系统具有 2 个组织和 1 个 order 节点，并且每个组织有 2 个 peer 节点和 1 个 ca 节点. 具体的实验环境是 AMD Ryzen 5 3400G with Radeon Vega Graphics 3.70 GHz, 16.0 GB RAM, Ubuntu18.04 系统.

本文的实验评估在 $[T_i, T_{i+1}]$ 时间段内进行，i 为拍卖轮次编号. 根据市场电价 MP 以及能源交易系统的历史交易记录，本文假设卖家的期望报价在 [0.2, MP] 元之间. 同时本文假设参与拍卖的用户购买/出售电量在 [10, 50] kWh 之间. 大于 10 kWh 是因为要设置参与能源拍卖的门槛；小于 50 kWh 是因为购买/出售大量电力的用户可以直接和智能电网交易以获取更大的效益.

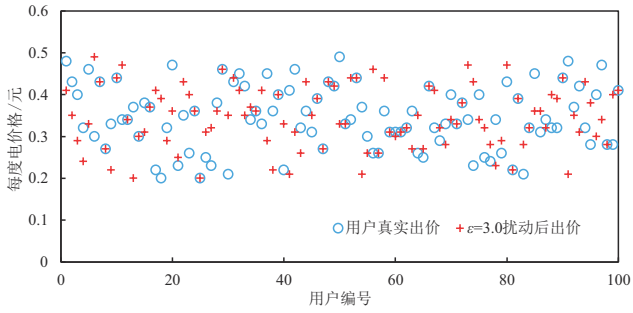
在本文的实验评估中，我们设计了如下指标：(1)BDP 算法对拍卖数据的影响，主要包括不同隐私预算下扰动前后拍卖数据对比以及扰动前后出价概率分布比较. (2)拍卖方案的有效性，主要将本文 DPDAB 方案与 PBOAD[28] 和 DEAL[29] 两个方案对比，对比指标包括卖方平均效益、买方平均效益、满意度比例和社会福利. (3)拍卖系统的时间开销，主要包括参与能源拍卖的用户数量以及能源交易系统的节点数量对拍卖时间开销的影响.

8.1 BDP 算法对拍卖数据的影响

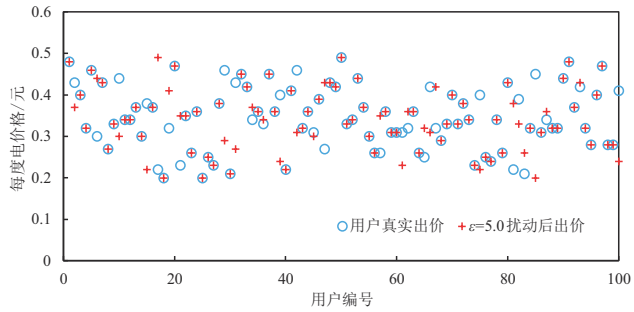
本文设计了 BDP 差分隐私算法来保护拍卖数据的隐私. 但在进行实验前，需要确定不同隐私预算 ε 对拍卖数据的影响并选取合适 ε. 如图 8 所示，横坐标表示参与能源拍卖的用户编号，共有 100 个用户；纵坐标表示每度电的价格（元/kWh）. 图中圆圈是用户的真实出价，十字符号表示不同隐私预算 ε 下扰动后的用户出价. 十字符号和圆圈重合程度越低，表示隐私保护效果越好；重合程度越高，表示隐私保护效果越差. 如图 8 所示，当 ε=1.0，重合度为 11%；当 ε=3.0，重合度为 32%；当 ε=5.0，重合度为 71%. 所以 ε 越大隐私保护效果越差，ε 越小隐私保护效果越好. 由 6.2 可知，BDP 算法的隐私预算 ε 还需要满足 $\varepsilon \geqslant \ln(\max\{t_i\})$. 通过实验可知，用户报价/出价数据使得 $\max\{t_i\}<e$，所以 $\varepsilon \geqslant 1.0$，综上所述，$\varepsilon \geqslant 1.0$ 且 ε 当越接近 1.0 时，BDP 算法的隐私保护效果越好. 本文实验评估的隐私预算 ε=1.0.



(a) 隐私预算 ε=1.0



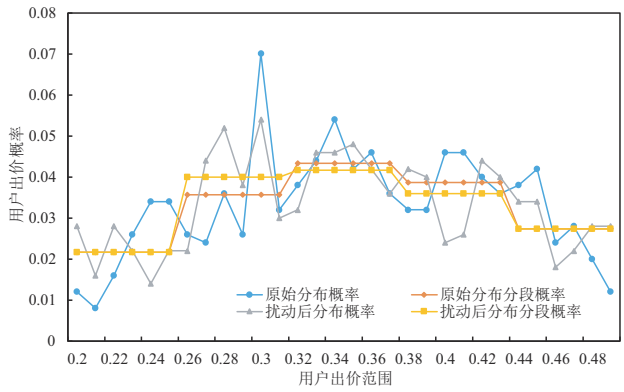
(b) 隐私预算 ε=3.0



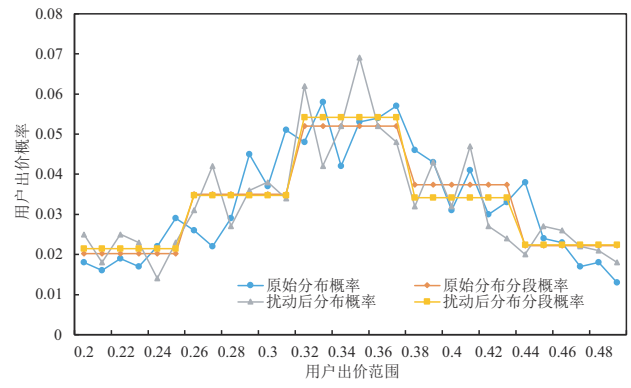
(c) 隐私预算 ε=5.0

图 8　不同隐私预算下扰动前后拍卖价格对比

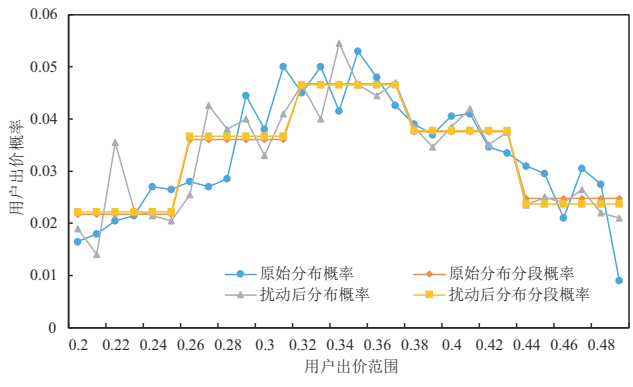
由 6.3 节数据有效性分析可知,扰动前后拍卖出价数据的分布概率相近且出价数据的期望值近似. 如图 9 所示,横坐标表示用户的可能出价(元/kWh);纵坐标表示用户对不同出价的概率. 原始分布概率根据所有用户的真实出价数据计算得到,扰动后分布概率根据通过 BDP 算法扰动后的所有用户出价数据计算得到. 原始分布分段概率和扰动后分段概率分别根据用户的真实出价数据和扰动后出价数据使用算法 1 计算得到. 由图 9 可知,扰动前后拍卖出价数据的分布概率大致相同,且随着参与拍卖的用户数量逐渐增多,扰动前后拍卖出价数据的分布概率越相近. 根据图 9 中的数据计算可知,当有 500 个用户时,扰动前后的出价数据的期望值分别为 0.36 和 0.35;当有 1 000 个用户时,扰动前后的出价数据的期望值分别为 0.34 和 0.34;当有 1 500 个用户时,扰动前后的出价数据的期望值分别为 0.35 和 0.35. 综上所述,扰动前后的出价数据的期望值近似,且当参与拍卖的用户足够多时,扰动前后的出价数据的期望值相等.



(a) 500 用户



(b) 1 000 用户



(c) 2 000 用户

图 9　不同数量用户扰动前后出价概率分布

8.2　拍卖方案的有效性

本文与 PBOAD 和 DEAL 两个方案对比,并从以下标准衡量本文方案 DPDAB 的有效性. (1)卖方平均效益=卖方总效益/竞拍成功卖方数量;(2)买方平均效益=买方总效益/竞拍成功买方数量;(3)满意度=竞拍成功用户数量/总用户数量;(4)社会福利=卖方总效益+买方总效益+拍卖师收益.

如图10~12所示,展示了不同数量交易用户下不同拍卖方案的平均效益和用户满意度情况,其中横坐标是一段时间内拍卖轮次编号,每轮参与拍卖的用户数量都不相同. 图10纵坐标表示卖方平均效益;图11纵坐标表示买方平均效益;图12纵坐标表示用户满意度比例. 由图10~12可知,DPDAB、PBODA和DEAL方案的多轮拍卖平均的平均卖方效益分别为3.80,1.68和1.20,本文DPDAB方案平均卖方效益最高;平均的平均买方效益分别为0.81,1.69和1.18,PBODA方案平均买方效益最高;平均的用户满意度比例分别为0.52,0.51和1.0,DEAL方案的用户满意度比例最高. 综上,三个对比方案各有优劣. 然而在拍卖中,由于拍卖价格低于市场价,为了激励卖家参与拍卖,需要给予卖方更多的效益,由上述数据可知,DPDAB方案的激励效果最好. 此外,DPDAB、PBODA和DEAL方案的买卖双方平均效益之和分别为4.61,3.37和2.38,本文DPDAB方案的平均总效益最高,PBODA方案次之,DEAL方案最差. 综上所述,从拍卖效益角度,本文DPDAB方案最好.

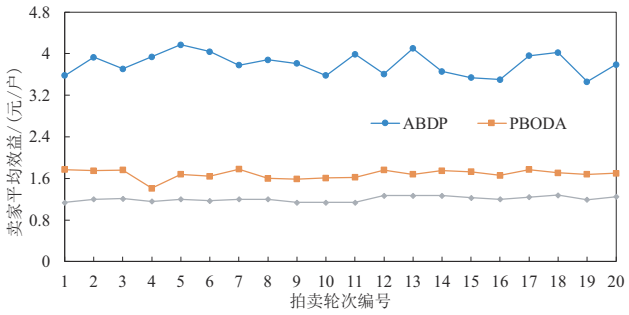


图10 多次交易的卖家平均效益

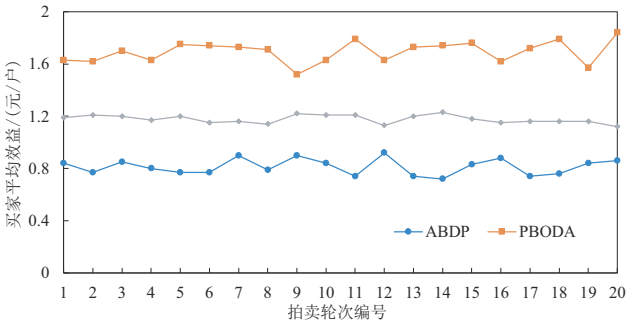


图11 多次交易的买家平均效益

由图12可知,DEAL方案的用户满意度比例为1.0,而另外两个方案的满意度在0.5左右,这与拍卖方案的设计有关. DEAL方案采用单边竞价拍卖机制,即卖方不报价,而是采用同一底价,然后由多个买方出价,再根据DEAL拍卖方案得的最终的获胜买方. 该方案虽然可以使用户满意度提高,但是单边竞价的拍卖机制使得平均效益很差. DPDAB和PBODA方案采用双边竞价拍卖机制,即拍卖双方都报价/出价,然后根据各自的拍卖方案获得最终的获胜卖方/买方. 虽然两个方案单轮拍卖的用户满意度都只有0.5左右,但是未获胜的用户仍然可以参与下轮能源拍卖. 通过多轮拍卖,更多的用户会成功匹配,用户满意度比例也会逐渐提高.

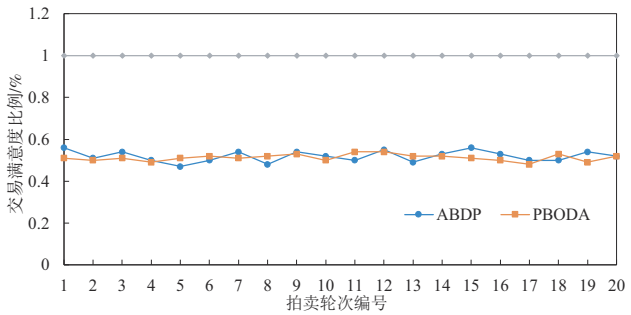


图12 多次交易的用户满意度比例

如图13展示了不同方案中不同数量的参与拍卖用户产生的社会福利的变化情况,由图中数据可知,随着参与拍卖的用户逐渐增多,不同方案所产生的社会福利都在增加. 但在参与拍卖用户数量相同的情况下,不同方案的社会福利不同. 在参与拍卖用户数量相同情况下,本文DPDAB方案的社会福利最高,DEAL方案的社会福利次之,PBODA方案的社会福利最差. 由社会福利计算公式可知,社会福利受到买卖双方效益和用户满意度比例影响,由于DEAL方案的用户满意度比例大约是另外两个方案满意度比例的2倍,所以该方案具有较高的社会福利,但仍然比DPDAB方案的社会福利低. 此外,虽然本文DPDAB方案与PBODA方案的用户满意度比例相近,但DPDAB方案的社会福利远高于PBODA方案的社会福利. 综上所述,从社会福利角度,本文DPDAB方案最好.

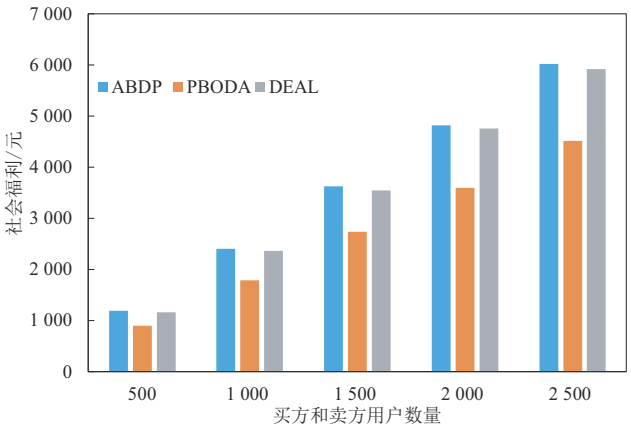


图13 参与拍卖的不同数量用户产生的社会福利

最后本节从公平性,透明性,出价隐私,身份隐私,支付隐私,分配隐私方面对DPDAB、PBOAD和DEAL方案进行比较,如表3所示. 在表中,“√”代表已经实现,“×”代表没有实现. (1)公平性,这是一个拍卖方案必须

要满足的一个性质. 由于三个方案的交易双方的报价/出价以及拍卖师处理拍卖数据过程是公平的,所以三个方案都满足公平性. (2)透明性和不可篡改,这是区块链的性质,本文DPDAB和DEAL方案都是基于联盟区块链实现,所以可以保证相关拍卖数据公开透明且不可篡改. (3)身份隐私,由于DEAL方案仅根据出价获得竞拍获胜者,在匹配成功后需要买卖双方协商交易的电量,该协商过程会泄露身份隐私. (4)出价隐私、支付隐私和分配隐私分别表示能源拍卖流程中的三个主要阶段的隐私保护情况. 根据三个方案的具体描述可知,本文DPDAB方案考虑了出价和支付阶段的隐私,没有考虑分配阶段的隐私;PBOAD方案考虑了支付和分配阶段的隐私,没有考虑出价阶段的隐私;DEAL方案仅考虑了支付阶段的隐私,没有考虑出价和分配阶段的隐私.

表3　不同拍卖方案之间比较结果

方案	DPDAB	PBOAD	DEAL
公平性	√	√	√
透明性	√	×	√
不可篡改	√	×	√
身份隐私	√	√	×
出价隐私	√	×	×
支付隐私	√	√	√
分配隐私	×	√	×

8.3　拍卖系统的时间开销

为了评估不同数量节点以及参与拍卖用户数量对实验时间开销的影响,我们通过改变节点数量和参与拍卖用户数量的方式测量基于联盟链的能源拍卖系统的时间开销,如图14和图15所示. 图14展示了处理卖方报价/买方出价数据的时间开销随用户数量和联盟链节点数量的变化情况,其中X轴表示参与竞拍的用户数量,Y轴表示联盟链节点数量,Z轴表示处理卖方报价/买方出价数据的时间开销. 图15展示了得到拍卖获胜者的时间开销随用户数量和联盟链节点数量的变化情况,其中X轴表示参与竞拍的用户数量,Y轴表示联盟链节点数量,Z轴表示博弈出拍卖获胜者的时间开销. 由图14和图15中的数据可知,随着参与拍卖用户数量逐渐增多,时间开销越大;随着节点数量增多,时间开销也越大. 当有8个组织,16个节点,1 600个买家和卖家参与能源拍卖时,处理卖方报价/买方出价数据总的时间开销达到了7.39 s,平均处理一个用户报价/出价数据的时间约为4.94 ms,该时间开销是极小的.博弈出拍卖获胜者总的时间开销达到了5.55 s,但是每轮能源拍卖周期分为报价阶段,出价阶段和结算阶段,所以整个拍卖周期会持续一段时间[29]. 假设能源拍卖周期为3 600 s,即$T_i - T_{i-1} =$

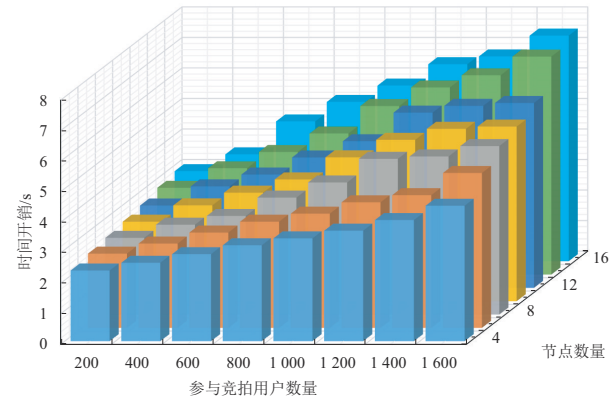


图14　处理卖方报价/买方出价数据时间开销

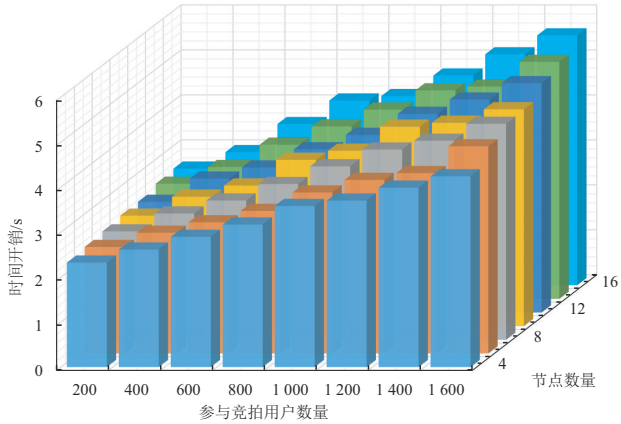


图15　博弈得到拍卖获胜者的时间开销

3 600,将1 600个用户的博弈时间分担到整个拍卖周期,则博弈时间开销相较于整个拍卖周期占比约为0.153%. 此外,8个组织,16个节点和1 600个用户规模已经可以满足大多数的能源拍卖. 综上所述,DSB能源拍卖方案的出价/报价的时间开销以及博弈出获胜者的时间开销,在能源拍卖领域是可行的,即该方案在保证拍卖数据隐私性的同时没有影响到拍卖系统的性能.

9　结束语

在本文,我们研究了联盟链上能源拍卖数据的隐私保护问题,并提出了一种安全高效的隐私保护方案-DPDAB. 该方案主要包括两个部分:满足差分隐私要求的BDP算法以及满足拍卖规则的DSB能源拍卖方案. 我们通过隐私分析证明了BDP差分隐私算法满足差分隐私要求,同时通过理论和实验分析了BDP算法对拍卖数据有效性的影响,并确定了隐私预算ε的合适取值范围. 此外,我们根据理论分析证明了DPDAB方案满足关键的经济性质即个人理性、预算平衡和弱诚实性,并与其它方案比较证明了该方案在用户平均效益、用户满意度和社会福利方面的有效性.

参考文献

[1] WANG N Y, ZHOU X, LU X, et al. When energy trading meets blockchain in electrical power system: The state of the art[J]. Applied Sciences, 2019, 9(8): 15-61.

[2] HASSAN M UL, REHMANI M H, KOTAGIRI R, et al. Differential privacy for renewable energy resources based smart metering[J]. Journal of Parallel and Distributed Computing, 2019, 131: 69-80.

[3] MORSTYN T, FARRELL N, DARBY S J, et al. Using peer-to-peer energy-trading platforms to incentivize prosumers to form federated power plants[J]. Nature Energy, 2018, 3: 94-101.

[4] SIANO P, DE MARCO G, ROLAN A, et al. A survey and evaluation of the potentials of distributed ledger technology for peer-to-peer transactive energy exchanges in local energy markets[J]. IEEE Systems Journal, 2019, 13(3): 3454-3466.

[5] VAN LEEUWEN G, ALSKAIF T, GIBESCU M, et al. An integrated blockchain-based energy management platform with bilateral trading for microgrid communities[J]. Applied Energy, 2020, 263: 114613.

[6] GUAN Z T, LU X, YANG W T, et al. Achieving efficient and Privacy-preserving energy trading based on blockchain and ABE in smart grid[J]. Journal of Parallel and Distributed Computing, 2021, 147: 34-45.

[7] 穆程刚, 丁涛, 董江彬, 等. 基于私有区块链的去中心化点对点多能源交易系统研制[J]. 中国电机工程学报, 2021, 41(3): 878-890.
MU C G, DING T, DONG J B, et al. Development of decentralized peer-to-peer multi-energy trading system based on private blockchain technology[J]. Proceedings of the CSEE, 2021, 41(3): 878-890. (in Chinese)

[8] CUI Z H, ZHANG J J, WANG Y C, et al. A pigeon-inspired optimization algorithm for many-objective optimization problems[J]. Science China Information Sciences, 2019, 62(7): 70212.

[9] HASSAN M U, REHMANI M H, CHEN J J. Optimizing blockchain based smart grid auctions: A green revolution [J]. IEEE Transactions on Green Communications and Networking, 2022, 6(1): 462-471.

[10] 曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述:原理、进展与应用[J]. 通信学报, 2020, 41(1): 134-151.
ZENG S Q, HUO R, HUANG T, et al. Survey of blockchain: Principle, progress and application[J]. Journal on Communications, 2020, 41(1): 134-151. (in Chinese)

[11] CAI X J, NIU Y, GENG S J, et al. An under-sampled software defect prediction method based on hybrid multi-objective cuckoo search[J]. Concurrency and Computation: Practice and Experience, 2020, 32(5): 54-78.

[12] SERJANTOV A, SEWELL P. Passive attack analysis for connection-based anonymity systems[C]//European Symposium on Research in Computer Security. Berlin, Heidelberg: Springer, 2003: 116-131.

[13] NYBERG K, KNUDSEN L R. Provable security against a differential attack[J]. Journal of Cryptology, 1995, 8(1): 27-37.

[14] 刘明达, 陈左宁, 拾以娟, 等. 区块链在数据安全领域的研究进展[J]. 计算机学报, 2021, 44(1): 1-27.
LIU M D, CHEN Z N, SHI Y J, et al. Research progress of blockchain in data security[J]. Chinese Journal of Computers, 2021, 44(1): 1-27. (in Chinese)

[15] HASSAN M UL, REHMANI M H, CHEN J J. Differential privacy in blockchain technology: A futuristic approach[J]. Journal of Parallel and Distributed Computing, 2020, 145: 50-74.

[16] DWORK C, MCSHERRY F, NISSIM K, et al. Calibrating noise to sensitivity in private data analysis[M]//Theory of Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006: 265-284.

[17] DWORK C, ROTH A. The algorithmic foundations of differential privacy[J]. Foundations and Trends in Theoretical Computer Science, 2014, 9(3-4): 211-407.

[18] MCSHERRY F, TALWAR K. Mechanism design via differential privacy[C]//48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07). Piscataway: IEEE, 2007: 94-103.

[19] ERLINGSSON Ú, PIHUR V, KOROLOVA A. RAPPOR: Randomized aggregatable privacy-preserving ordinal response[C]//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2014: 1054-1067.

[20] DUCHI J C, JORDAN M I, WAINWRIGHT M J. Minimax optimal procedures for locally private estimation[J]. Journal of the American Statistical Association, 2018, 113 (521): 182-201.

[21] WANG S W, HUANG L S, NIE Y W, et al. Local differential private data aggregation for discrete distribution estimation[J]. IEEE Transactions on Parallel and Distributed Systems, 2019, 30(9): 2046-2059.

[22] 叶青青, 孟小峰, 朱敏杰, 等. 本地化差分隐私研究综述[J]. 软件学报, 2018, 29(7): 1981-2005.
YE Q Q, MENG X F, ZHU M J, et al. Survey on local dif-

ferential privacy[J]. Journal of Software, 2018, 29(7): 1981-2005. (in Chinese)

[23] OU L, QIN Z, LIAO S L, et al. Singular spectrum analysis for local differential privacy of classifications in the smart grid[J]. IEEE Internet of Things Journal, 2020, 7 (6): 5246-5255.

[24] GAI N, XUE K K, ZHU B, et al. An efficient data aggregation scheme with local differential privacy in smart grid [J]. Digital Communications and Networks, 2022, 8(3): 333-342.

[25] GAI K K, WU Y L, ZHU L H, et al. Privacy-preserving energy trading using consortium blockchain in smart grid [J]. IEEE Transactions on Industrial Informatics, 2019, 15 (6): 3548-3558.

[26] ZHANG X Y, JIANG S R, LIU Y L, et al. Privacy-preserving scheme with account-mapping and noise-adding for energy trading based on consortium blockchain[J]. IEEE Transactions on Network and Service Management, 2022, 19(1): 569-581.

[27] LUO L, FENG J C, YU H F, et al. Blockchain-enabled two-way auction mechanism for electricity trading in Internet of electric vehicles[J]. IEEE Internet of Things Journal, 2022, 9(11): 8105-8118.

[28] LI D H, YANG Q Y, YU W, et al. Towards differential privacy-based online double auction for smart grid[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 971-986.

[29] HASSAN M U, REHMANI M H, CHEN J. DEAL: Differentially private auction for blockchain-based microgrids energy trading[J]. IEEE Transactions on Services Computing, 2019, 13(2): 263-275.

[30] CRAMTON P. Ascending auctions[J]. European Economic Review, 1998, 42(3/4/5): 745-756.

[31] 倪天娇. 差分隐私保护的网络资源拍卖机制研究[D]. 合肥: 安徽大学, 2021.
NI T J. Research on Network Resource Auction Mechanisms with Differential Privacy[D]. Hefei: Anhui University, 2021. (in Chinese)

[32] JIA Y B, WAN C, YU P, et al. Security constrained P2P energy trading in distribution network: An integrated transaction and operation model[J]. IEEE Transactions on Smart Grid, 2022, 13(6): 4773-4786.

[33] WANG L L, ZHOU Q, XIONG Z, et al. Security constrained decentralized peer-to-peer transactive energy trading in distribution systems[J]. CSEE Journal of Power and Energy Systems, 2021, 8(1): 188-197.

[34] GUERRERO J, CHAPMAN A C, VERBIC G. Decentralized P2P energy trading under network constraints in a low-voltage network[J]. IEEE Transactions on Smart Grid, 2019, 10(5): 5163-5173.

作者简介

姜顺荣　男,1986年12月出生于江苏盐城市. 博士毕业于西安电子科技大学通信工程学院,美国佛罗里达大学联合培养博士生,副教授,硕士生导师. 主要研究方向为网络空间安全和隐私保护,具体包括车联网、云计算和区块链等应用场景.
E-mail: jsywow@gmail.com

时　坤　男,1996年11月出生于江苏徐州市. 现于中国矿业大学攻读硕士学位. 主要从事区块链和隐私保护方面的研究工作.
E-mail: shikunss123@163.com

周　勇　男,1974年9月出生. 毕业于中国矿业大学,教授,博士(后),博士生导师. 入选江苏省“333人才工程”和“六大人才高峰”培养对象. 曾在美国明尼苏达大学进修,是南京大学高级访问学者. 从事数据挖掘、机器学习、人工智能、区块链、进化计算和无线传感器网络等方面的理论与应用研究.
E-mail: yzhou@cumt.edu.cn