DOI:10.12158/j.2096-3203.2024.05.001

计及隐私保护的弱中心化多产消者能量共享机制

漆磊[1]，艾芊[1]，嵇文路[2]，李嘉媚[1]，王帝[1]，潘小辉[2]
（1. 上海交通大学（电力传输与功率变换控制教育部重点实验室），上海 200240；
2. 国网江苏省电力有限公司南京供电分公司，江苏 南京 210019）

摘　要：在双碳目标的背景下，虚拟电厂、微电网等形式的产消者大规模涌现。多产消者之间的能量共享能够提升整体的经济效益与新能源消纳水平。在计及各产消者数据隐私的基础上，文中提出弱中心化模式下的多产消者能量共享协同运行机制。首先，构建含多种分布式资源的产消者内部调度模型，并考虑负荷需求以及新能源出力的波动性与随机性，基于条件风险价值（conditional value at risk，CVaR）量化不确定性带来的风险。然后，提出多产消者弱中心化电价迭代机制，利用供需关系引导电价更新。同时考虑到产消者隐私保护，基于 Paillier 同态加密算法和秘密共享原理设计电量数据聚合方法。该方法能够在各方主体隐私得到保护的前提下获取系统的供需信息。最后，通过算例验证了文中所提机制的有效性与合理性，且经过能量共享后多产消者整体成本降低 12.6%。

关键词：弱中心化；能量共享；产消者；隐私保护；条件风险价值（CVaR）；Paillier 同态加密算法
中图分类号：TM72　　**文献标志码：**A　　**文章编号：**2096-3203（2024）05-0002-11

0　引言

随着双碳目标的提出，风电、光伏等分布式资源得到快速发展，电力系统中新能源的渗透比将持续增长[1-3]。同时，海量的需求侧用户转变为可控资源，电力系统也从传统的“源随荷动”向“源荷互动”转变[4-7]。在此背景下，虚拟电厂、微电网等分布式资源聚合管理技术应运而生[8-11]，呈现出产消者的源荷双重特性。若采用传统的“自发自用、余量上网”机制，无法充分激励产消者的积极性。而多产消者之间的能量共享、协同共济，能够提高能源利用效率，进一步促进新能源的消纳与发展。

多产消者的协同运行架构按照中心化机构的存在与否可以分为去中心化交易模式[12-14]、中心化交易模式[15-19]。按照交易的求解形式，又可以分为分布式优化模型[12-17]、集中式优化模型[18-19]。在去中心化交易模式下，由于不存在交易协调中心，交易形式以分布式交易为主。产消者需要通过彼此交互数据信息实现协同优化，故而存在通信效率不高的问题。在中心化交易模式中，协调中心按照职能可以解耦为“计算中心”和“信息中心”，因此系统可以是集中式优化模型[18-19]，也可以是分布式优化模型[15-17]。其中，集中式优化模型的计算效率随着产消者规模增大而降低[20]；而分布式优化模型中，虽然计算职能由产消者自身承担，但仍然需要产消者与协调中心进行信息交互，因此数据的隐私安全取决于协调中心的安全性，一旦协调中心的数据信息泄露，系统的隐私安全将无法得到保障[21]。在上述研究基础上，文中提出弱中心化交易架构，将中心化架构中协调中心作为“信息中心”的职能进一步弱化。协调中心仅作为信息处理的平台，获取不到信息的真实内容。因此，即使协调中心出现数据隐私泄露，真实的数据也不会被攻击者获取。

在隐私保护方面，隐私泄露的风险来源[22-23]包括：外部窃听者窃听产消者与协调中心或产消者间的交互信息；协调中心通过分析产消者接收的信息推断产消者的交易数据；诚实但好奇的半诚实产消者通过收集到的数据分析其他产消者的数据隐私。3 种类型的攻击者通过各种手段窃取产消者在交易过程中的数据，并能够通过交易信息反推产消者在竞价以及控制方面的特性，从而获取在电力市场中的竞争优势[24]。

针对上述问题，在分布式协同计算领域，文献[25]提出了一种基于安全多方计算秘密共享协议的分布式协同优化框架，实现多方代理的完全隐私保护。文献[26-28]建立了基于差分隐私的平均共识算法，在传输状态中注入给定分布的零均值噪声，提高传输状态的安全性，但这种算法不能保证收敛到初始值的精确平均值[29]。为了进一步保证算法的收敛性能，实现精确的平均共识，文献[30-31]提出了基于同态加密算法的平均共识算法，交互信息为经过加密的真实数据，该算法能够在抵御外部窃听者窃取状态信息的基础上，实现安全精确

收稿日期：2024-02-26；修回日期：2024-05-15
基金项目：国家重点研发计划资助项目（2021YFB2401203）；国家电网有限公司总部科技项目（5108-202218038A-1-1-ZN）

的多方共识。

文中在上述研究基础上,进一步弱化协调中心对于数据信息的掌握程度,建立计及隐私保护的多产消者弱中心化协同运行机制。首先,考虑负荷需求以及新能源出力的不确定性,建立基于条件风险价值(conditional value at risk,CVaR)理论的产消者内部调度模型。然后,构建多产消者系统电价迭代机制,同时提出考虑隐私保护的电量数据聚合方法。在保护产消者数据隐私的前提下,基于供需关系还原电能作为商品的基本属性,充分发挥电价的调节作用。最后,通过算例分析验证了文中所提机制的有效性与合理性。

1　弱中心化模式下的多产消者能量共享协同运行框架

文中提出的弱中心化模式下的多产消者能量共享协同运行框架如图 1 所示。

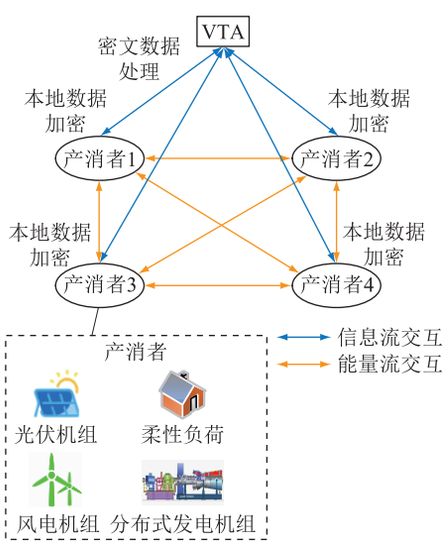

图 1　多产消者协同运行框架

Fig.1　Synergistic operational framework of multiple prosumers

多产消者系统(multi-prosumer system,MPS)具有多个产消者,每个产消者包括多种类型的分布式资源。在系统中设置虚拟交易代理(virtual transaction agent,VTA),使其起到协调交易的作用。VTA 可由任一具备良好通信条件的机构担任。在多产消者协同运行过程中,VTA 仅仅是处理产消者交易数据信息的辅助平台,产消者自身的优化计算工作仍在本地进行。同时,产消者向 VTA 传递的信息均通过算法进行加密,VTA 利用密文数据进行信息处理。

在理想交易框架中,中心机构是一个完全可信的第三方主体,既不会泄露各产消者的交易信息,也不会试图获取产消者任何额外的交易信息。在交易过程中,各产消者可以直接将交易信息传递至中心机构处理。但是,在现实交易框架中,完全可信的第三方主体并不存在。因此,在文中提出的交易模式中,假设 VTA 为半诚实参与者[23]。作为半诚实参与者,VTA 在协助交易时会严格执行交易规则,但在这过程中可能会收集各产消者的交易数据,也可能会与恶意产消者合作,尝试推测其他产消者的隐私信息。

基于上述背景,在文中所提基于加密算法的弱中心化交易框架的基础上,VTA 作为弱化的“信息中心”,仅仅有信息的“处理权”,而没有“知情权”,因此产消者能够在不暴露交易隐私数据的情况下,实现多方协同计算。

2　基于电价迭代机制的多产消者能量共享协同运行模型

2.1　基于 CVaR 的产消者调度模型

产消者由内部多种资源聚合而成,具有源荷双重特性,考虑产消者内部资源包括分布式发电机组(distributed generator,DG)、光伏机组(photovoltaic,PV)、风电机组(wind turbine,WT)以及柔性负荷(flexible load,FL)。

DG 运行成本与约束条件如下:

$$C_{i,s}^{\mathrm{DG}}(t)=a_i P_{i,s}^{\mathrm{DG}}(t)+b_i\left(P_{i,s}^{\mathrm{DG}}(t)\right)^2 \tag{1}$$

$$P_{i,\min}^{\mathrm{DG}} \leqslant P_{i,s}^{\mathrm{DG}}(t) \leqslant P_{i,\max}^{\mathrm{DG}} \tag{2}$$

$$-\Delta P_{i,\max}^{\mathrm{DG}} \leqslant P_{i,s}^{\mathrm{DG}}(t)-P_{i,s}^{\mathrm{DG}}(t-1) \leqslant \Delta P_{i,\max}^{\mathrm{DG}} \tag{3}$$

式中:i 为 MPS 中产消者的编号;s 为负荷需求与新能源出力的典型场景;$C_{i,s}^{\mathrm{DG}}(t)$、$P_{i,s}^{\mathrm{DG}}(t)$ 分别为 DG 的运行成本与实际出力;a_i、b_i 为 DG 的成本系数;$P_{i,\max}^{\mathrm{DG}}$、$P_{i,\min}^{\mathrm{DG}}$ 分别为 DG 出力的上、下界限;$\Delta P_{i,\max}^{\mathrm{DG}}$ 为 DG 的爬坡能力界限。

按照 FL 的响应特性,可将其分为可中断负荷(interruptible load,IL)以及可转移负荷(translational load,TL),其调用成本及约束条件如下:

$$C_{i,s}^{\mathrm{IL}}(t)=P_{i,s}^{\mathrm{IL}}(t)c_{\mathrm{IL},i} \tag{4}$$

$$C_{i,s}^{\mathrm{TL}}(t)=\left(P_{i,s}^{\mathrm{TL,up}}(t)+P_{i,s}^{\mathrm{TL,down}}(t)\right)c_{\mathrm{TL},i} \tag{5}$$

$$0 \leqslant P_{i,s}^{\mathrm{IL}}(t) \leqslant P_{i,\max}^{\mathrm{IL}}(t) \tag{6}$$

$$0 \leqslant P_{i,s}^{\mathrm{TL,down}}(t) \leqslant P_{i,\max}^{\mathrm{TL}}(t) \tag{7}$$

$$0 \leqslant P_{i,s}^{\mathrm{TL,up}}(t) \leqslant P_{i,\max}^{\mathrm{TL}}(t) \tag{8}$$

$$\sum_{t=1}^{T} P_{i,s}^{\mathrm{TL,down}}(t)=\sum_{t=1}^{T} P_{i,s}^{\mathrm{TL,up}}(t) \tag{9}$$

式中:T 为调度周期;$C_{i,s}^{\mathrm{IL}}(t)$、$C_{i,s}^{\mathrm{TL}}(t)$ 分别为 IL 用户和 TL 用户的调用成本;$c_{\mathrm{IL},i}$、$c_{\mathrm{TL},i}$ 分别为 IL 用户负荷中断和 TL 用户负荷转移的单位补偿费用;

$P_{i,s}^{\mathrm{IL}}(t)$ 为 IL 用户的负荷中断量；$P_{i,s}^{\mathrm{TL,up}}(t)$、$P_{i,s}^{\mathrm{TL,down}}(t)$ 分别为 TL 用户的负荷上调量与下调量，应满足在整个调度周期内两者相同；$P_{i,\max}^{\mathrm{IL}}(t)$、$P_{i,\max}^{\mathrm{TL}}(t)$ 分别为负荷最大中断上限与转移上限。

在调度周期内，产消者 i 的交易调度模型可以表示为：

$$\min \sum_{s=1}^{S}\sum_{t=1}^{T}\rho_s\left(C_{i,s}^{\mathrm{DG}}(t)+C_{i,s}^{\mathrm{IL}}(t)+C_{i,s}^{\mathrm{TL}}(t)+C_{i}^{\mathrm{MPS}}(t)\right) \tag{10}$$

$$C_i^{\mathrm{MPS}}(t)=P_i^{\mathrm{MPS}}(t)\lambda^{\mathrm{MPS}}(t)= \left(P_i^{\mathrm{MPS,buy}}(t)-P_i^{\mathrm{MPS,sell}}(t)\right)\lambda^{\mathrm{MPS}}(t) \tag{11}$$

$$-P_{\max}^{\mathrm{MPS}}\leqslant P_i^{\mathrm{MPS}}(t)\leqslant P_{\max}^{\mathrm{MPS}} \tag{12}$$

$$P_{i,s}^{\mathrm{new}}(t)\Delta t+P_{i,s}^{\mathrm{DG}}(t)\Delta t+P_{i,s}^{\mathrm{TL,down}}(t)\Delta t+P_{i,s}^{\mathrm{IL}}(t)\Delta t= P_i^{\mathrm{MPS}}(t)+P_{i,s}^{\mathrm{L}}(t)\Delta t+P_{i,s}^{\mathrm{TL,up}}(t)\Delta t \tag{13}$$

式中：S 为负荷需求与新能源出力的典型场景总数量；ρ_s 为场景概率；$C_i^{\mathrm{MPS}}(t)$、$P_i^{\mathrm{MPS}}(t)$、$\lambda^{\mathrm{MPS}}(t)$ 分别为产消者与 MPS 交易的收益、电量和电价；$P_i^{\mathrm{MPS,buy}}(t)$、$P_i^{\mathrm{MPS,sell}}(t)$ 分别为与 MPS 交易的购、售电量；$P_{\max}^{\mathrm{MPS}}$ 为 MPS 交易电量的最大值；$P_{i,s}^{\mathrm{new}}(t)$ 为新能源出力，即 $P_{i,s}^{\mathrm{PV}}(t)$ 与 $P_{i,s}^{\mathrm{WT}}(t)$ 之和，$P_{i,s}^{\mathrm{PV}}(t)$、$P_{i,s}^{\mathrm{WT}}(t)$ 分别为 PV、WT 出力；$P_{i,s}^{\mathrm{L}}(t)$ 为负荷功率；Δt 为时间尺度，为 1 h。

CVaR 理论常应用于经济金融领域，用于对风险的衡量与管理，其定义为超过风险价值（value at risk，VaR）理论下的资产平均损失值[32]。为降低负荷及新能源不确定性，文中采用 CVaR 度量不确定性带来的风险，对产消者的运行成本进行风险管理。考虑负荷及新能源不确定性的 CVaR[32] 为：

$$\delta_i=\xi_i+\frac{1}{1-\beta}\sum_{s=1}^{S}\rho_s\eta_{i,s} \tag{14}$$

式中：δ_i 为产消者成本的 CVaR；ξ_i 为产消者成本的 VaR；β 为置信水平；$\eta_{i,s}$ 为产消者成本超过 VaR 的值。

为便于求解，式(14)的约束条件如下：

$$\eta_{i,s}\geqslant 0 \tag{15}$$

$$\sum_{t=1}^{T}\left(C_{i,s}^{\mathrm{DG}}(t)+C_{i,s}^{\mathrm{IL}}(t)+C_{i,s}^{\mathrm{TL}}(t)+C_{i}^{\mathrm{MPS}}(t)\right)-\xi_i\leqslant\eta_{i,s} \tag{16}$$

考虑 CVaR 的产消者调度模型的目标函数包括 2 个部分，具体如式(17)所示，第一部分为多场景下产消者的交易调度成本，第二部分为 CVaR。

$$\min C_i=\sum_{s=1}^{S}\sum_{t=1}^{T}\rho_s\left(C_{i,s}^{\mathrm{DG}}(t)+C_{i,s}^{\mathrm{IL}}(t)+C_{i,s}^{\mathrm{TL}}(t)+C_{i}^{\mathrm{MPS}}(t)\right)+\gamma\delta_i \tag{17}$$

式中：C_i 为产消者的调度成本；γ 为风险偏好系数，表示产消者对风险的态度，其值大于等于 0。当 γ 为 0 时，产消者为风险中立者，既不考虑规避风险，也不主动追求风险；当 γ 不断增大时，产消者为风险回避者，将主动规避风险，倾向于增加调度成本以避免较大的成本波动风险。

2.2 基于供需关系的电价迭代机制

按照经济学理论，价格是由市场的供需关系决定。因此，在能量共享过程中，电价的迭代情况应反映多产消者整体的供需变化情况。而 MPS 的供需情况又取决于各产消者的调度决策情况。

在产消者的调度决策过程中，由于 DG 的成本与输出功率 $P_{i,s}^{\mathrm{DG}}$ 之间是二次函数关系，其边际成本为：

$$\frac{\partial C_i}{\partial P_{i,s}^{\mathrm{DG}}}=a_i+2b_iP_{i,s}^{\mathrm{DG}} \tag{18}$$

当电价 λ^{MPS} 小于 DG 最大出力的边际成本 $a_i+2b_iP_{i,\max}^{\mathrm{DG}}$ 时，DG 存在最优出力点，即 $P_{i,s}^{\mathrm{DG}}=(\lambda^{\mathrm{MPS}}-a_i)/(2b_i)$，且随着 λ^{MPS} 增加而增加。当电价 λ^{MPS} 增加而大于 DG 最大出力的边际成本 $a_i+2b_iP_{i,\max}^{\mathrm{DG}}$ 时，DG 发电成本低于电价，因此 DG 倾向于最大程度增加出力。

由于 FL 中 IL 和 TL 的成本与输出功率之间是一次函数关系，其边际成本即为调用成本。故当电价 λ^{MPS} 小于 FL 边际成本时，FL 用户将不进行需求响应；当电价 λ^{MPS} 增加而大于 FL 边际成本时，FL 用户将积极参与需求响应，进行负荷调整。

考虑到功率平衡约束，产消者与 MPS 交易电量 P_i^{MPS} 可以表示为：

$$P_i^{\mathrm{MPS}}=\left(P_{i,s}^{\mathrm{L}}-P_{i,s}^{\mathrm{new}}-P_{i,s}^{\mathrm{IL}}-P_{i,s}^{\mathrm{TL,down}}+P_{i,s}^{\mathrm{TL,up}}-P_{i,s}^{\mathrm{DG}}\right)\Delta t \tag{19}$$

式(19)中，负荷 $P_{i,s}^{\mathrm{L}}$、新能源预测值 $P_{i,s}^{\mathrm{new}}$ 均不可调度。

由此可以看出，随着电价 λ^{MPS} 增加，产消者内部分布式资源都倾向于增加自身出力，因此 $P_i^{\mathrm{MPS,buy}}$ 减少或 $P_i^{\mathrm{MPS,sell}}$ 增加；而当电价 λ^{MPS} 降低时，产消者内部分布式资源都倾向于降低自身出力，因此 $P_i^{\mathrm{MPS,buy}}$ 增加或 $P_i^{\mathrm{MPS,sell}}$ 减少。

按照上述规律，可得电价 λ^{MPS} 的更新迭代过程[33]为：

$$\lambda_{k+1}^{\mathrm{MPS}}=\lambda_k^{\mathrm{MPS}}+\rho\left(\sum_{i=1}^{n}P_{i,k}^{\mathrm{MPS,buy}}-\sum_{i=1}^{n}P_{i,k}^{\mathrm{MPS,sell}}\right) \tag{20}$$

式中：λ_k^{MPS} 为在第 k 轮迭代中的交易电价；$P_{i,k}^{\mathrm{MPS,buy}}$、

$P_{i,k}^{\mathrm{MPS,sell}}$ 分别为产消者 i 在第 k 轮迭代中的购电意愿量与售电意愿量;ρ 为电价调整系数,满足 $\rho \geqslant 0$;n 为产消者数量。

按照上述电价的调整更新原则,当电量关系供不应求,即 $\sum_i P_{i,k}^{\mathrm{MPS,buy}} > \sum_i P_{i,k}^{\mathrm{MPS,sell}}$ 时,电价将增加,$\lambda_{k+1}^{\mathrm{MPS}} > \lambda_k^{\mathrm{MPS}}$,故而下一次迭代时产消者 $P_i^{\mathrm{MPS,buy}}$ 将减少或 $P_i^{\mathrm{MPS,sell}}$ 将增加,系统整体朝着供需平衡状态迭代。反之,当电量关系供过于求时,电价将降低,$\lambda_{k+1}^{\mathrm{MPS}} < \lambda_k^{\mathrm{MPS}}$,产消者 $P_i^{\mathrm{MPS,buy}}$ 将增加或 $P_i^{\mathrm{MPS,sell}}$ 将减少,系统仍朝着供需平衡状态迭代。

同时,随着电价的调整,在 MPS 整体持续呈现缺电或余电的情况下,由系统供需关系驱动的电价会超过电网的购电价格或售电价格,此时交易买卖双方中处于劣势的一方则倾向于与电网展开交易。因此,规定当电价超出电网电价形成的电价区间时,以电网电价作为该时刻的电价。

$$\lambda_k^{\mathrm{MPS}} = \begin{cases} \lambda_{\mathrm{buy}}^{\mathrm{grid}} & \lambda_k^{\mathrm{MPS}} \geqslant \lambda_{\mathrm{buy}}^{\mathrm{grid}} \\ \lambda_k^{\mathrm{MPS}} & \lambda_{\mathrm{sell}}^{\mathrm{grid}} < \lambda_k^{\mathrm{MPS}} < \lambda_{\mathrm{buy}}^{\mathrm{grid}} \\ \lambda_{\mathrm{sell}}^{\mathrm{grid}} & \lambda_k^{\mathrm{MPS}} \leqslant \lambda_{\mathrm{sell}}^{\mathrm{grid}} \end{cases} \tag{21}$$

式中:$\lambda_{\mathrm{sell}}^{\mathrm{grid}}$、$\lambda_{\mathrm{buy}}^{\mathrm{grid}}$ 分别为电网的售电价格与购电价格。

3　考虑隐私保护的供需电量数据聚合方法

在多产消者协同运行机制中,VTA 直接收集每轮迭代中各产消者的交易电量,并依据系统的供需电量来更新交易电价。然而,产消者在迭代过程中的交易电量数据是重要的中间计算结果,暴露中间计算结果可能被其他主体反推出关键的隐私信息,或者被外部窃听者获取从而造成隐私泄露。因此,在无完全可信的第三方中心机构的情况下,产消者的交易信息不能随意地输出到 MPS 中。

针对上述问题,一种隐私保护方案是将输出数据进行隐私化处理,即将中间计算结果转化为密文数据向外输出。但在多产消者协同运行框架下,如何对多产消者的密文数据进行协同计算也是一个值得研究的问题。文中则基于此问题,提出了一种基于同态加密算法和秘密共享原理的供需电量数据聚合方法,有效实现了多方隐私数据的协同计算。

3.1　基于 Paillier 同态加密算法与秘密共享原理的电量数据聚合方法

同态加密算法能够对明文进行加密获得对应密文,再对密文进行特定运算后所得到的结果进行解密,等价于直接对明文进行相同运算操作[34]。同态加密在不暴露数据具体内容的情况下进行计算,有效保障了数据的安全性与隐私性。满足同态性质的函数可表示为:

$$D(E(m_1)) \otimes D(E(m_2)) = m_1 \otimes m_2 \tag{22}$$

式中:$D(\cdot)$、$E(\cdot)$ 分别为解密运算、加密运算;m_1、m_2 为明文数据;⊗表示某一运算符号。

Paillier 同态加密算法是一种具有加法同态的半同态加密算法,其流程包含 3 个部分:密钥生成、加密过程、解密过程[35-36]。其中,加法同态性质指的是密文相乘等价于明文相加。

$$E(m_1) \cdot E(m_2) = E(m_1 + m_2) \tag{23}$$

秘密共享的思想在于将秘密信息进行拆分,并将拆分后的数据分发给具有保密权限的成员,最终只有若干成员协作,结合彼此的数据才能恢复秘密信息[37]。在 MPS 计算迭代过程中,VTA 需要根据系统中的电量供需关系来更新电价,但是为保护交易隐私数据,产消者的交易电量信息无法直接透露给 VTA。因此,文中结合秘密共享原理中秘密拆分的思想以及 Paillier 同态加密算法,提出了一种计及隐私保护的供需电量数据聚合方法,具体方法如图 2 所示。

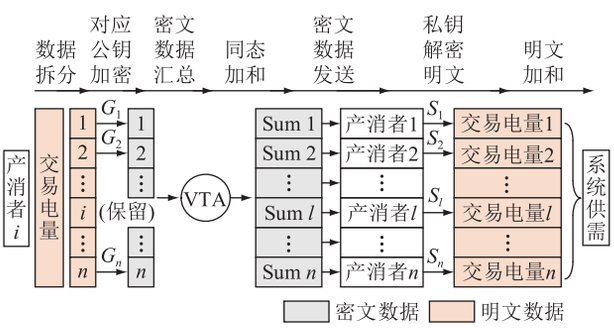

图 2　电量数据聚合方法示意

Fig.2　Schematic diagram of electricity data aggregation method

在数据聚合前,产消者需要根据系统中成员数量对交易电量进行拆分:$P_{i,1}(t)$、$P_{i,2}(t)$、…、$P_{i,i}(t)$、…、$P_{i,n}(t)$,满足 $\sum_{j=1}^{n} P_{i,j}(t) = P_i^{\mathrm{MPS}}(t)$。其中,$P_{i,j}(t)$ 为产消者 i 将交易电量拆分给产消者 j 的电量数据。值得注意的是,拆分而来的电量数据仅用作数据聚合,并不具备实际的物理意义。各成员数据拆分情况如下:

$$\begin{cases} P_1^{\mathrm{MPS}}(t) = P_{1,1}(t) + P_{1,2}(t) + \cdots + P_{1,n}(t) \\ P_2^{\mathrm{MPS}}(t) = P_{2,1}(t) + P_{2,2}(t) + \cdots + P_{2,n}(t) \\ \vdots \\ P_n^{\mathrm{MPS}}(t) = P_{n,1}(t) + P_{n,2}(t) + \cdots + P_{n,n}(t) \end{cases} \tag{24}$$

然后,产消者 i 分别利用其他产消者的公钥 G_1、

G_2、…、G_{i-1}、G_{i+1}、…、G_n 对 $P_{i,l}(t)$ 进行加密，即 $E_{G_l}(P_{i,l}(t))$，后将密文数据发送给 VTA。

VTA 接收同态加密后的数据后，将采用同一公钥加密的密文数据进行同态加和：

$$E_{G_l}\left(\sum_{i=1,i\neq l}^{n}P_{i,l}(t)\right)=\prod_{i,i\neq l}E_{G_l}(P_{i,l}(t)) \quad (25)$$

计算完成后，VTA 再将加和后的密文数据发送至各产消者，并由各产消者通过私钥 S_1、S_2、…、S_l、…、S_n 进行解密，即 $D_{S_l}\left(E_{G_l}\left(\sum_{i=1,i\neq l}^{n}P_{i,l}(t)\right)\right)$。

产消者将解密后的明文结果 $\sum_{i=1,i\neq l}^{n}P_{i,l}(t)$ 与一开始拆分交易数据时保留的部分 $P_{l,l}(t)$ 相加。此时，产消者的解密明文 $\sum_{i=1}^{n}P_{i,l}(t)$ 是一种没有实际物理意义的数据，而各产消者解密后的数据相加可得该时刻系统中的供需关系 $\sum_{i=1}^{n}P_i^{\mathrm{MPS}}(t)$，可用于计算下一轮迭代中的交易电价。

3.2 基于电量数据聚合方法的多产消者协同运行求解流程

在上述研究的基础上，文中提出了计及隐私保护的多产消者协同运行模型，具体求解流程如下。

（1）在进入电价迭代前，VTA 发布 MPS 内部初始交易电价 λ_0^{MPS}，满足初始电价在电网电价区间内，即 $\lambda_{\mathrm{sell}}^{\mathrm{grid}}\leqslant\lambda_0^{\mathrm{MPS}}\leqslant\lambda_{\mathrm{buy}}^{\mathrm{grid}}$，记迭代次数 $k=0$。

（2）产消者根据电价进行内部调度，求解本地最优交易调度策略，决策与 MPS 的交易电量 P_i^{MPS}。

（3）根据系统中成员的数量，产消者将交易电量数据进行拆分：$P_{i,1}(t)$、$P_{i,2}(t)$、…、$P_{i,i}(t)$、…、$P_{i,n}(t)$，满足 $\sum_{j=1}^{n}P_{i,j}(t)=P_i^{\mathrm{MPS}}(t)$。

（4）各产消者依据对应编号采用其他产消者的公钥对电量进行加密，即 $E_{G_l}(P_{i,l}(t))$，得到加密密文后发送至 VTA。

（5）VTA 接收密文后，将相同公钥加密的密文进行同态加和，如式(25)所示，并根据公钥将加和后的密文发送至对应产消者。

（6）各产消者接收 VTA 加密密文后，采用私钥进行解密，并与保留的电量数据进行明文加和，即 $\sum_{i=1}^{n}P_{i,l}(t)$，求解得出结果后发送至 VTA。

（7）VTA 接收来自其他产消者的电量明文数据后，计算整体电量供需情况以及交易电价，并与上一时刻电价相比，判断电价是否稳定。若未稳定，则由产消者按照新一轮电价重新调度决策，迭代次数 $k=k+1$。若达到稳定则结束迭代，MPS 以最后的电价迭代结果进行交易。

3.3 协同运行模型隐私保护分析

根据引言可知，MPS 可能受到的隐私泄露风险来自 3 个方面：外部攻击、VTA 攻击与合谋攻击。

外部攻击指 MPS 外的攻击者通过攻击窃取产消者向外发送的密文。在不知道公钥与私钥的情况下，外部攻击者即使获取密文数据也无法明确知道明文数据，故而基于 Paillier 算法的性质，外部攻击可以被有效抵御。

VTA 攻击指 VTA 试图将各产消者发送的密文数据结合各产消者公钥进行解密。VTA 可能试图通过掌握的公钥信息对明文数据进行加密生成密文数据。根据 Paillier 算法的加密流程[35-36]可知，加密过程中密文的生成依赖于一个随机变量，而随机变量在每次加密时都随机选取，即使拥有公钥也无法推得相同的密文。

合谋攻击指某恶意产消者与 VTA 合作窃取其他产消者密文，并利用掌握的私钥破解 VTA 汇集的密文信息。根据秘密共享原理，每个产消者向 VTA 发送的电量数据都是经过拆分的，不会暴露产消者在任一时刻的交易电量数据。恶意产消者与 VTA 合作后能够解密的数据只是其他产消者交易电量的一部分，无法判断该产消者在某一时刻的交易电量。

4 算例分析

文中算例构建的 MPS 包含 4 个产消者，各产消者包含的设备参数、需求响应参数、电价信息分别如表 1—表 3 所示。

表 1 DG 设备参数

Table 1 Equipment parameters of DG

产消者	最大出力/kW	爬坡能力/kW	a_i	b_i
产消者 1	100	50	15.6	0.20
产消者 2	100	30	12.2	0.15
产消者 3	100	30	15.6	0.20
产消者 4	200	80	12.2	0.20

表 2 需求响应参数

Table 2 Parameters of demand response

产消者	IL 调用容量/%	TL 调用容量/%
产消者 1	10	5
产消者 2	10	5
产消者 3	15	5
产消者 4	10	10

表 3　电价信息

Table 3　Electricity price information

时段	上网电价/[元·(kW·h)$^{-1}$]	销售电价/[元·(kW·h)$^{-1}$]
01:00—07:00、20:00—24:00	0.30	0.50
07:00—10:00、14:00—18:00	0.40	0.75
10:00—14:00、18:00—20:00	0.40	1.00

各产消者的负荷以及新能源预测出力如图 3 所示。其中,产消者 1 中只包含光伏资源,产消者 2 中只包含风电资源,产消者 3 和产消者 4 同时包含风电与光伏资源。各产消者需求响应中 IL 的调用成本为 0.20 元/kW,TL 的调用成本为0.15元/kW。

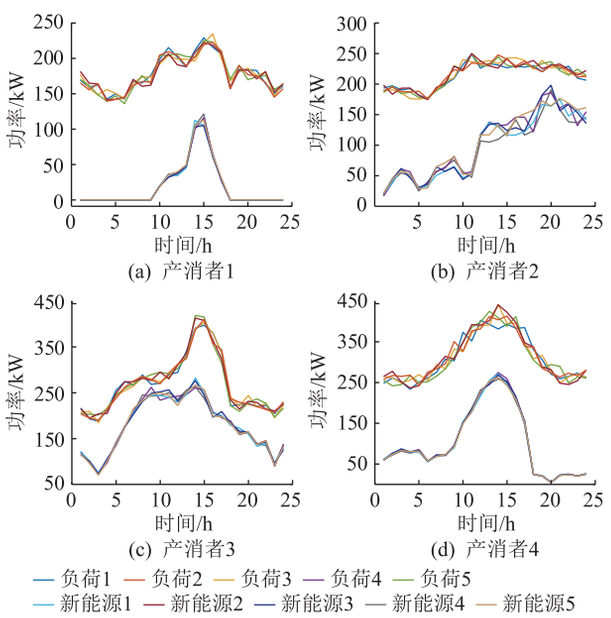

图 3　产消者负荷及新能源典型出力场景

Fig.3　Typical output scenarios of prosumer load and new energy

4.1　多产消者协同运行情况分析

4.1.1　多产消者迭代情况分析

多产消者电价随产消者的供需情况进行更新迭代。迭代过程中,电价的变化情况依赖于电价调整系数ρ。文中设置 4 个和 8 个产消者的算例进行分析,多产消者迭代收敛情况见表 4。设置ρ为 0.000 1、0.000 3、0.000 5 和 0.001 0,在 4 产消者系统和 8 产消者系统中均可收敛,收敛后得到的 MPS 总成本与ρ为 0.000 1 时的最大偏差仅为0.15%和 0.22%,均在误差范围内。由收敛结果可知,MPS 的迭代次数与ρ的大小密切相关,而不是产消者的数量。因此,从产消者迭代效率的角度出发,ρ值选取在 0.000 3~0.001 0 较为合适。同时,收敛迭代结果也验证了电价迭代机制的稳定性与快速性。

表 4　多产消者迭代收敛情况

Table 4　The case of iterative convergence of multiple prosumers

MPS	ρ	迭代次数	总成本/元
4 产消者系统	0.000 1	72	4 824.50
	0.000 3	25	4 823.49
	0.000 5	15	4 822.46
	0.001 0	9	4 817.15
8 产消者系统	0.000 1	40	9 902.69
	0.000 3	13	9 901.26
	0.000 5	12	9 880.50
	0.001 0	6	9 887.70

4.1.2　多产消者能量共享情况分析

以 4 产消者系统为例,分析 MPS 的能量共享情况。设置方案 1 为多产消者之间进行弱中心化能量共享协同运行,方案 2 为多产消者直接与电网进行交易,即传统的“自发自用,余量上网”。表 5 为 2 种方案的对比。从整体来看,经过能量共享后 MPS 的总成本降低 12.6%,且各产消者均可实现自身成本的降低,故而能量共享可充分激励产消者的积极性。

表 5　多产消者交易方案对比

Table 5　Comparison of trading schemes for multiple prosumers　　元

产消者	方案 1 成本	方案 2 成本
产消者 1	1 615.39	1 830.32
产消者 2	221.68	444.70
产消者 3	829.56	949.86
产消者 4	2 153.69	2 203.19
总和	4 820.31	5 428.07

方案 1 中多产消者能量共享中交易电量和交易电价分别如图 4 和图 5 所示。

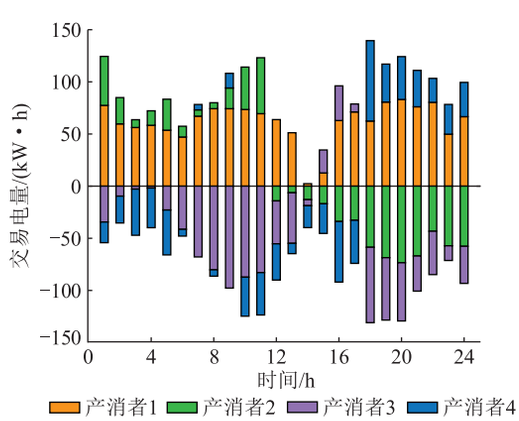

图 4　产消者电量交易示意

Fig.4　Schematic diagram of electricity trading for prosumers

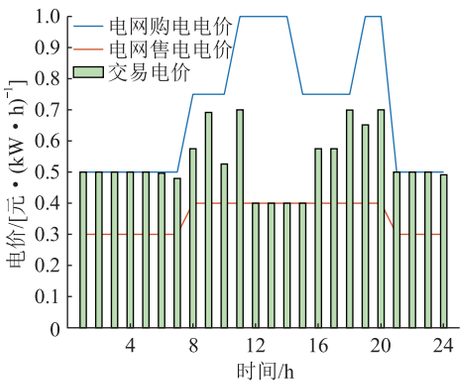

图 5　产消者交易电价示意

Fig.5　Schematic diagram of electricity price for prosumer transactions

图 4 中,交易电量为正表示产消者从 MPS 中购电,为负则表示产消者向 MPS 售电。同时结合电量和电价的情况进行分析:在 1 时—6 时和 21 时—23 时,MPS 处于供不应求状态,售电产消者的电量可以被完全消纳,而购电产消者的需求得不到满足,因此系统的交易电价为电网的购电电价;在 12 时—15 时,MPS 整体处于供过于求状态,购电产消者的购电需求得到满足,但售电产消者的电能无法在能量共享中消纳,故而系统交易电价为电网售电电价;在其他时间,随着电价的迭代,多产消者可以达到供需平衡状态,因此电价位于电网的购电和售电价格之间。上述分析说明,各产消者均可从过程中获益,从而更加积极地参与多产消者能量共享。

4.1.3　CVaR 分析

不同风险偏好系数 γ 下的 MPS 成本变化规律如图 6 所示。由图中数据可知,随着风险偏好系数 γ 的增加,MPS 能够规避更高程度的运行风险,相应的运行成本也增加。当风险偏好系数较小时,系统对于运行中的风险呈激进态度,倾向于增加 CVaR 成本,以降低系统运行成本;当风险偏好系数较大时,系统对于运行中的风险呈保守态度,倾向于降低 CVaR 成本,以提升系统经济性效益。在运行场景中,MPS 可以权衡运行风险以及系统成本,在规避一定程度风险的情况下尽可能地降低系统成本。

4.2　电量数据聚合方法分析

4.2.1　安全性分析

针对 MPS 可能面临的攻击,设计了如下 2 种案例分析文中所提加密方案的安全性。

案例 1:对某一产消者在单次迭代下 24 个时段的交易数据进行加密,分析不同明文数据与密文数据的对应关系。

案例 2:对某一产消者在单次迭代下同一时刻的交易数据进行多次加密,分析同一明文数据与密

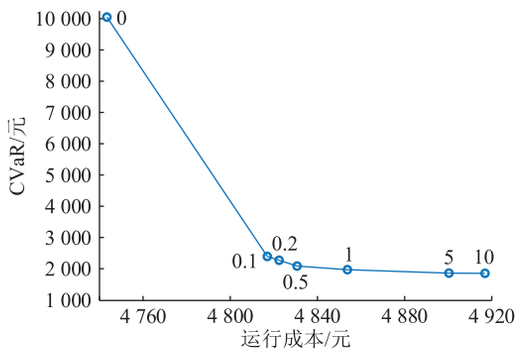

图 6　不同风险偏好系数下的成本变化

Fig.6　Changes in costs with different risk appetite factors

文数据的对应关系。

由于密文数据的实际取值远大于明文数据,文中将密文数据按照响应的比例放缩至与明文数据统一的量级进行比较。并且,2 种案例仅为对比明文数据和密文数据的对应关系,因此省略数据的单位信息。图 7 和图 8 分别为 2 种案例下明文数据与密文数据的对应关系。从图中不难看出,无论是对不同数据进行加密还是对同一数据进行多次加密,明文与密文之间不存在任何相关性。密文数据取决于每次加密产生的随机数,与明文数据之间不是简单的正相关或负相关关系。因此,从明文数据很难推导得到密文数据。

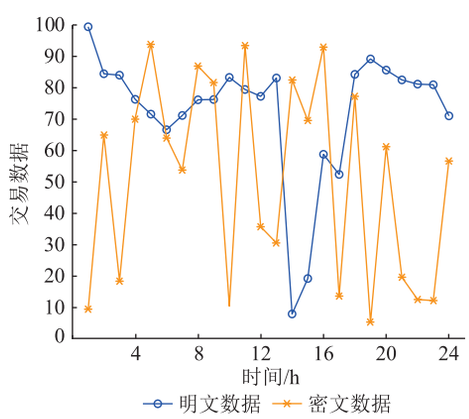

图 7　案例 1 数据情况

Fig.7　Case 1 data situation

综上所述,不论是外部攻击者还是 VTA,在拿到产消者的密文数据后都无法获知产消者的真实明文数据。

4.2.2　即时性分析

表 6 为产消者对明文数据的加密和解密时间以及前后明文对比。由表 6 可知,在经过加密与解密前后,产消者的数据保持不变。同时,由加密时间与解密时间可知,产消者加密和解密某一数据的时间平均为 14.249 ms。以 4 产消者系统为例,按照一

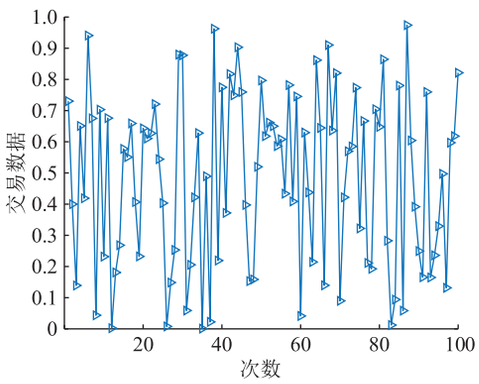

图 8　案例 2 数据情况

Fig.8　Case 2 data situation

天 24 个时段计算,可得产消者在单次迭代中加密和解密时间之和约为 1.026 s。

表 6　加密和解密情况

Table 6　Encryption and decryption situation

参数	产消者 1	产消者 2	产消者 3	产消者 4
加密前明文	16.003	28.250	29.418	−17.894
加密时间/ms	11.000	11.012	10.999	10.990
解密后明文	16.003	28.250	29.418	−17.894
解密时间/ms	3.985	2.999	3.000	3.011

按照加密和解密的平均时间 14.249 ms 计算,假设 MPS 中共有 n 名产消者,产消者在单次迭代中的加密和解密时间为:

$$T_{\text{all}} = 14.249 \times 24(n-1)\ \text{ms} \approx 0.342(n-1)\ \text{s} \tag{26}$$

式中:T_{all} 为总时间。由式(26)可知,在日前以 1 h 为时间尺度的优化调度中,各产消者具有较为宽松的求解迭代时间,基本可实现实时计算。

文中设置弱中心化迭代模式和去中心化迭代模式进行通信次数对比。图 9 为 2 种模式下的通信次数对比。去中心化迭代模式下,各产消者求解系统供需电量需要经过 2 次全体的相互通信,因此通信次数为 $2(n-1)^2$。而在弱中心化迭代模式下,由于 VTA 的存在,各产消者仅须向 VTA 传递信息即可,因此弱中心化的通信次数为 $2n$。由此可知,相较于去中心化模式,弱中心化模式下的通信开销显著降低。

4.2.3　适应性分析

算法的适应性体现在迭代过程中某一产消者因为通信故障退出交易,其他产消者能否重新更新电价。假设在文中提出的 4 产消者系统中,产消者 2 因通信故障未能及时将交易信息反馈至 VTA,VTA 确认产消者 2 掉线后,向其他产消者宣布其退出交易。图 10 为某一时刻电量数据聚合过程。假

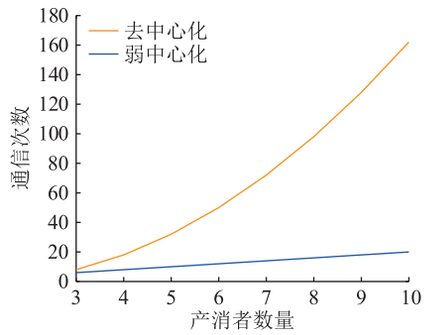

图 9　通信次数对比

Fig.9　Comparison of the number of communications

设上一轮迭代中该时刻电价为 0.450 元/(kW·h),电价迭代系数为 0.001。

		数据接收方			
		产消者1	产消者2	产消者3	产消者4
数据发送方	产消者1	15.469	47.59	−5.472	18.781
	产消者2	~~5.469~~	~~14.564~~	~~6.345~~	~~16.261~~
	产消者3	−14.589	16.79	12.756	−6.22
	产消者4	9.654	−50.694	15.789	−14.194

⇩ 产消者2因通信故障掉线

		数据接收方		
		产消者1	产消者3	产消者4
数据发送方	产消者1	63.059	−5.472	18.781
	产消者3	14.589	29.546	−6.22
	产消者4	9.654	15.789	−64.888

图 10　某一场景下的电量数据聚合过程

Fig.10　The process of aggregating power data in a given scenario

产消者 1、3 和 4 明确产消者 2 退出交易后,将产消者 2 公钥加密的电量数据与本地保存的电量数据加和,并保存在本地。VTA 按照正常流程,对收集到的采用相同公钥加密的密文数据进行加和,再将加和后的密文分发至产消者 1、3 和 4。后续产消者 1、3 和 4 仍可实现电价更新。

若产消者 2 没有退出交易,系统供需关系为供过于求,需求方超过供应方的电量为 55.777 kW·h,电价应更新为 0.501 元/(kW·h)。而当产消者 2 退出交易,供需关系仍然为供过于求,但需求方超过供应方的电量为 45.66 kW·h,电价更新为 0.496 元/(kW·h)。这是由于产消者 2 退出交易后,系统中的需求电量降低,因此电价也相应降低,该变化表明电价更新机制符合市场运行规律,体现了文中方法的适应性与合理性。

5　结论

文中提出了一种弱中心化模式下计及隐私保护的多产消者能量共享协同运行机制,利用供需关系引导多产消者的电量交互,并基于 Paillier 同态加

密算法和秘密共享原理设计了电量数据聚合方法，实现了产消者协同运行过程中数据隐私的保护。

（1）基于 CVaR 的产消者调度模型能够通过调节偏好因子实现风险波动和运行成本的权衡。

（2）弱中心化模式下的多产消者能量共享实现了产消者间的协同运行，相较于传统的“自发自用、余量上网”机制能够使得多产消者整体成本降低 12.6%。同时，通过系统供需关系引导电价更新，符合市场的运行规律，激励产消者参与协同运行的积极性。

（3）基于 Paillier 同态加密算法和秘密共享思想的电量数据聚合方法，在有效保护产消者交易数据隐私的基础上，具有良好的计算和通信效率，并且计算性能不受产消者节点通信故障影响，适应性较强。

参考文献：

[1] 王彩霞，时智勇，梁志峰，等. 新能源为主体电力系统的需求侧资源利用关键技术及展望[J]. 电力系统自动化，2021，45(16)：37-48.
WANG Caixia，SHI Zhiyong，LIANG Zhifeng，et al. Key technologies and prospects of demand-side resource utilization for power systems dominated by renewable energy[J]. Automation of Electric Power Systems，2021，45(16)：37-48.

[2] 陈国平，李明节，董昱，等. 构建新型电力系统仿真体系研究[J]. 中国电机工程学报，2023，43(17)：6535-6551.
CHEN Guoping，LI Mingjie，DONG Yu，et al. Research on the simulation technology architecture for the new-type power system[J]. Proceedings of the CSEE，2023，43(17)：6535-6551.

[3] 郭威，张凯，魏新杰，等. 高渗透率分布式光伏接入的新型电力系统净功率预测[J]. 电测与仪表，2022，59(12)：48-55.
GUO Wei，ZHANG Kai，WEI Xinjie，et al. Net power prediction for a novel power system with high permeability distributed photovoltaic access[J]. Electrical Measurement & Instrumentation，2022，59(12)：48-55.

[4] 文云峰，杨伟峰，汪荣华，等. 构建 100%可再生能源电力系统述评与展望[J]. 中国电机工程学报，2020，40(6)：1843-1856.
WEN Yunfeng，YANG Weifeng，WANG Ronghua，et al. Review and prospect of toward 100% renewable energy power systems[J]. Proceedings of the CSEE，2020，40(6)：1843-1856.

[5] 王玲玲，刘恋，张锞，等. 电力系统灵活调节服务与市场机制研究综述[J]. 电网技术，2022，46(2)：442-452.
WANG Lingling，LIU Lian，ZHANG Ke，et al. A review of power system flexible ramping product and market mechanism[J]. Power System Technology，2022，46(2)：442-452.

[6] 王一，朱涛，张玉欣，等. 适应中国电力现货市场发展的容量补偿机制初探[J]. 电力系统自动化，2021，45(6)：52-61.
WANG Yi，ZHU Tao，ZHANG Yuxin，et al. Preliminary study on capacity compensation mechanism adapted to development of electricity spot market in China[J]. Automation of Electric Power Systems，2021，45(6)：52-61.

[7] 蒙志全，楼贤嗣，时涵，等. 面向电力系统调度需求的负荷资源调控技术研究综述[J]. 浙江电力，2022，41(8)：31-40.
MENG Zhiquan，LOU Xiansi，SHI Han，et al. A review of load resource scheduling and control geared to the needs of power system scheduling[J]. Zhejiang Electric Power，2022，41(8)：31-40.

[8] 王健，郑峻峰，黄际元，等. 虚拟电厂关键技术综述与发展展望[J]. 供用电，2023，40(12)：43-54，86.
WANG Jian，ZHENG Junfeng，HUANG Jiyuan，et al. Key technology and development prospects of virtual power plants[J]. Distribution & Utilization，2023，40(12)：43-54，86.

[9] 刘任，刘洋，许立雄，等. 计及分布式需求响应的多微电网系统协同优化策略[J]. 电力建设，2023，44(5)：72-83.
LIU Ren，LIU Yang，XU Lixiong，et al. Multi-microgrid system collaborative optimization strategy considering distributed demand response[J]. Electric Power Construction，2023，44(5)：72-83.

[10] 吴晓刚，唐家俊，吴新华，等. “双碳”目标下虚拟电厂关键技术与建设现状[J]. 浙江电力，2022，41(10)：64-71.
WU Xiaogang，TANG Jiajun，WU Xinhua，et al. Key technologies and present situation of virtual power plant under "dual-carbon" goals[J]. Zhejiang Electric Power，2022，41(10)：64-71.

[11] 康重庆，陈启鑫，苏剑，等. 新型电力系统规模化灵活资源虚拟电厂科学问题与研究框架[J]. 电力系统自动化，2022，46(18)：3-14.
KANG Chongqing，CHEN Qixin，SU Jian，et al. Scientific problems and research framework of virtual power plant with enormous flexible distributed energy resources in new power system[J]. Automation of Electric Power Systems，2022，46(18)：3-14.

[12] 吴毓峰，杨胜春，潘振宁，等. 无协调主体的多产消者完全端到端交易机制[J]. 电力系统自动化，2023，47(3)：96-103.
WU Yufeng，YANG Shengchun，PAN Zhenning，et al. Complete peer-to-peer transaction mechanism for multiple prosumers without coordination entity[J]. Automation of Electric Power Systems，2023，47(3)：96-103.

[13] 姚星安，刘文昊，龚学良，等. 基于改进对偶动态规划的产销者点对点交易全分散式出清方法[J]. 电网技术，2023，47(11)：4564-4575.
YAO Xing'an，LIU Wenhao，GONG Xueliang，et al. Fully decentralized clearing for peer-to-peer trading of prosumers based on improved dual dynamic programming[J]. Power System Technology，2023，47(11)：4564-4575.

[14] 葛少云，程雪颖，刘洪，等. 园区多微网 P2P 电-碳耦合交易市场设计[J]. 高电压技术，2023，49(4)：1341-1349.
GE Shaoyun，CHENG Xueying，LIU Hong，et al. Market design of P2P electricity carbon coupling transaction among multi-microgrids in a zone[J]. High Voltage Engineering，2023，49(4)：1341-1349.

[15] 周鑫,韩肖清,李廷钧,等. 计及需求响应和电能交互的多主体综合能源系统主从博弈优化调度策略[J]. 电网技术,2022,46(9):3333-3346.
ZHOU Xin, HAN Xiaoqing, LI Tingjun, et al. Master-slave game optimal scheduling strategy for multi-agent integrated energy system based on demand response and power interaction [J]. Power System Technology,2022,46(9):3333-3346.

[16] 李鹏,吴迪凡,李雨薇,等. 基于综合需求响应和主从博弈的多微网综合能源系统优化调度策略[J]. 中国电机工程学报,2021,41(4):1307-1321,1538.
LI Peng,WU Difan,LI Yuwei,et al. Optimal dispatch of multi-microgrids integrated energy system based on integrated demand response and Stackelberg game[J]. Proceedings of the CSEE,2021,41(4):1307-1321,1538.

[17] 刘方,徐耀杰,杨秀,等. 考虑电能交互共享的虚拟电厂集群多时间尺度协调运行策略[J]. 电网技术,2022,46(2):642-656.
LIU Fang,XU Yaojie,YANG Xiu,et al. Multi-time scale coordinated operation strategy of virtual power plant clusters considering power interactive sharing[J]. Power System Technology,2022,46(2):642-656.

[18] 郭宴秀,苏建军,刘洋,等. 考虑电热交互和共享储能的多综合能源系统运行优化[J]. 中国电力,2023,56(4):138-145.
GUO Yanxiu,SU Jianjun,LIU Yang,et al. Optimal operation of multiple integrated energy systems considering power and heat interaction and shared energy storage system[J]. Electric Power,2023,56(4):138-145.

[19] 胡鹏,艾欣,杨昭,等. 考虑电能共享的综合能源楼宇群日前协同优化调度[J]. 电力自动化设备,2019,39(8):239-245.
HU Peng, AI Xin, YANG Zhao, et al. Day-ahead optimal scheduling for cluster building with integrated energy system considering power sharing[J]. Electric Power Automation Equipment,2019,39(8):239-245.

[20] LIAN J M,REN H Y,SUN Y N,et al. Performance evaluation for transactive energy systems using double-auction market[J]. IEEE Transactions on Power Systems, 2019, 34(5): 4128-4137.

[21] 郭庆来,田年丰,孙宏斌. 支撑能源互联网协同优化的隐私计算关键技术[J]. 电力系统自动化,2023,47(8):2-14.
GUO Qinglai,TIAN Nianfeng,SUN Hongbin. Key technologies of privacy computation supporting collaborative optimization of energy Internet[J]. Automation of Electric Power Systems, 2023,47(8):2-14.

[22] HUO X,LIU M X. Privacy-preserving distributed multi-agent cooperative optimization—paradigm design and privacy analysis[J]. IEEE Control Systems Letters,2021,6:824-829.

[23] ROCKAFELLAR R T,URYASEV S. Conditional value-at-risk for general loss distributions[J]. Journal of Banking & Finance,2002,26(7):1443-1471.

[24] 倪明,颜诘,柏瑞,等. 电力系统防恶意信息攻击的思考[J]. 电力系统自动化,2016,40(5):148-151.
NI Ming,YAN Jie,BO Rui,et al. Power system cyber attack and its defense[J]. Automation of Electric Power Systems, 2016,40(5):148-151.

[25] NOZARI E, TALLAPRAGADA P, CORTÉS J. Differentially private average consensus:obstructions,trade-offs,and optimal algorithm design[J]. Automatica,2017,81:221-231.

[26] KATEWA V,PASQUALETTI F,GUPTA V. On privacy vs. cooperation in multi-agent systems[J]. International Journal of Control,2018,91(7):1693-1707.

[27] FIORE D,RUSSO G. Resilient consensus for multi-agent systems subject to differential privacy requirements[J]. Automatica,2019,106:18-26.

[28] WANG H D,XU W Y,LU J Q. Privacy-preserving push-sum average consensus algorithm over directed graph via state decomposition[C]//2021 3rd International Conference on Industrial Artificial Intelligence (IAI). Shenyang, China. IEEE, 2021:1-6.

[29] TIAN N F,GUO Q L,SUN H B,et al. Fully privacy-preserving distributed optimization in power systems based on secret sharing[J]. iEnergy,2022,1(3):351-362.

[30] RUAN M H,GAO H,WANG Y Q. Secure and privacy-preserving consensus[J]. IEEE Transactions on Automatic Control, 2019,64(10):4035-4049.

[31] HADJICOSTIS C N,DOMÍNGUEZ-GARCÍA A D. Privacy-preserving distributed averaging via homomorphically encrypted ratio consensus[J]. IEEE Transactions on Automatic Control, 2020,65(9):3887-3894.

[32] 孙毅,李飞,胡亚杰,等. 计及条件风险价值和综合需求响应的产消者能量共享激励策略[J]. 电工技术学报,2023,38(9):2448-2463.
SUN Yi, LI Fei, HU Yajie, et al. Energy sharing incentive strategy of prosumers considering conditional value at risk and integrated demand response[J]. Transactions of China Electrotechnical Society,2023,38(9):2448-2463.

[33] 白利芳,祝跃飞,李勇军,等. 全同态加密研究进展[J/OL]. 计算机研究与发展,1-19[2024-01-11]. https://kns.cnki.net/kcms/detail/11.1777.tp.20231123.1043.004.html.
BAI Lifang,ZHU Yuefei,LI Yongjun,et al. Research progress of fully homomorphic encryption[J/OL]. Journal of Computer Research and Development,1-19[2024-01-11]. https://kns.cnki.net/kcms/detail/11.1777.tp.20231123.1043.004.html.

[34] 赵鹏杰,吴俊勇,林凯骏,等. 基于一致性算法的多微电网点对点分布式能量交易策略[J]. 电网技术,2023,47(1):205-218.
ZHAO Pengjie,WU Junyong,LIN Kaijun,et al. Peer to peer distributed transactive energy strategy for multi-microgrid based on consistency algorithm[J]. Power System Technology,2023, 47(1):205-218.

[35] 巩林明,李顺东,窦家维,等. 同态加密方案及安全两点直线计算协议[J]. 软件学报,2017,28(12):3274-3292.
GONG Linming,LI Shundong,DOU Jiawei,et al. Homomorphic

encryption scheme and a protocol on secure computing a line by two private points[J]. Journal of Software,2017,28(12):3274-3292.

[36] 周鑫,贺欢,王彬,等. 基于 Paillier 加密和共识机制的分解协调式算法[J]. 全球能源互联网,2023,6(4):362-369.
ZHOU Xin,HE Huan,WANG Bin,et al. Coordination-decomposition algorithm based on paillier encryption and consensus mechanism[J]. Journal of Global Energy Interconnection,2023,6(4):362-369.

[37] 陈信. 基于秘密共享和同态加密的隐私数据融合方案[D]. 上海:华东师范大学,2022.
CHEN Xin. Privacy-preserving data aggregation scheme based on secret sharing and homomorphic encryption[D]. Shanghai:East China Normal University,2022.

作者简介:


漆磊

漆磊(2000),男,硕士在读,研究方向为能源共享、能源点对点交易(E-mail:qilei_hitsz@163.com);

艾芊(1969),男,博士,教授,博士生导师,研究方向为虚拟电厂规划与运行、大数据与数字孪生;

嵇文路(1974),男,博士,研究员级高级工程师,从事智能配电网、调度自动化工作。

A weakly centralized multiple prosumers energy-sharing mechanism that takes into account privacy protection

QI Lei[1], AI Qian[1], JI Wenlu[2], LI Jiamei[1], WANG Di[1], PAN Xiaohui[2]

(1. Shanghai Jiao Tong University (Key Laboratory of Control of Power Transmission and Conversion, Ministry of Education),Shanghai 200240,China;2. State Grid Jiangsu Electric Power Co.,Ltd., Nanjing Power Supply Branch,Nanjing 210019,China)

Abstract:In the context of the dual-carbon goal,virtual power plants,microgrids and other forms of prosumers have emerged on a large scale. Energy sharing among multiple prosumers can improve the overall economic efficiency and new energy consumption. A collaborative operation mechanism for energy sharing among multiple prosumers under the weak centralization model is proposed. The mechanism considers the data privacy of each prosumer. Firstly, an internal scheduling model of prosumers with multiple distributed resources is constructed. The model considers the volatility and randomness of load demand and new energy output, quantifying the risk of uncertainty based on conditional value at risk (CVaR). Then, a weakly centralized tariff iteration mechanism for multiple prosumers is proposed, which uses the supply and demand relationship to guide the tariff update. Meanwhile, considering the privacy protection of prosumers, the power data aggregation method is designed based on Paillier homomorphic encryption algorithm and secret sharing principle. The method is able to obtain the system supply and demand information while ensuring the privacy of all parties. Finally,the effectiveness and rationality of the mechanism proposed in this paper is verified by an arithmetic example,and the overall cost of multiple prosumers is reduced by 12.6% after energy sharing.

Keywords: weak centralization; energy sharing; prosumer; privacy protection; conditional value at risk (CVaR); Paillier homomorphic encryption algorithm

(编辑　陆海霞)