基于去中心化云计算的隐私保护型分布式能源资源控制

Xiang Huo，*IEEE* 研究生会员，Mingxi Liu，*IEEE* 会员

arXiv:2301.02198v1 [math.OC] 5 Jan 2023

摘要——**可再生能源资源的快速普及为电力配电网络带来了前所未有的挑战：管理大量并网可控设备时，面临控制可扩展性危机以及潜在的终端用户隐私泄露。尽管这一问题十分重要，关于以完全可扩展的方式实现分布式能源资源（DER）控制隐私保护的研究仍然不足。为弥补这一空白，本文设计了一种新颖的去中心化隐私保护型分布式能源资源控制框架，该框架：1）可适应分布式能源资源数量及其异质性，实现可扩展控制；2）消除点对点通信，并保护所有参与的分布式能源资源免受各类对手的攻击，确保其隐私安全；3）与当前最先进的隐私保护方法相比，具有更高的计算效率和精度。本文建立了一个强耦合优化问题，对分布式能源资源的功耗和输出进行控制，其中包括太阳能光伏和储能系统，并采用投影梯度法求解。云计算与秘密共享无缝集成到所提出的去中心化计算方案中，以实现隐私保护。仿真结果证明了所提方法在分布式能源资源控制应用中的能力。**

索引词——**分布式优化、分布式能源资源、隐私保护、秘密共享**

I. 引言

A. 相关工作

Large-scale 部署分布式能源资源（DER）已被证明能够有效减少碳足迹，并提供电压控制、负荷跟踪和备用电源等电网边缘服务 [1]。分布式能源资源包括储能系统（ESS）、太阳能光伏（PV）和电动汽车（EV），以及其他监测和可控设备，能够为构建更先进、更可靠且更具成本效益的电网提供重大机遇 [2],[3]。尽管将分布式能源资源整合到电网中可带来诸多益处，例如提高能源效率并促进经济发展，但分布式能源资源的高渗透率也给现有控制策略的可扩展性带来了日益严峻的挑战 [4]。

为应对大规模分布式能源资源控制问题中的上述挑战，分布式和去中心化控制策略凭借出色的可扩展性，正受到越来越多的关注。例如，文献 [5]设计了一种基于局部下垂控制和一致性控制的分布式协调方法，以解决太阳能光伏高渗透率引发的电压升高问题。Zhang等在 [6]提出了一种异步分布式领导者-跟随者控制策略，通过优化调度分布式能源资源来降低电压以实现削峰和长期节能。为减轻通信负担，文献 [7]提出了一种分布式低通信算法，用于控制孤岛型光伏-电池混合系统。尽管分布式方法具有可扩展性，但通常需要大量点对点通信。为解决这一问题，Navidi等在[8] 提出了一种两层去中心化分布式能源资源协调架构，可将解决方案扩展到大型网络，且本地控制器之间无需直接通信。文献 [9], 针对具有可控光伏和储能系统的辐射状配电系统设计了一种去中心化随机控制策略，以最大限度地降低需求平衡成本。Huo等在 [10] 提出了一种采用维度缩减的去中心化收缩原始-多重对偶次梯度算法，从而在智能体群体规模和网络维度方面实现可扩展性关于。

尽管去中心化方法具有更强的可扩展性和通信效率，但其易遭受隐私泄露的问题严重阻碍了实际应用。此外，分布式和去中心化策略都高度依赖必要的通信，而这些通信可能泄露用户的敏感信息，并使系统漏洞暴露给对手。差分隐私（DP）凭借其严谨的数学定义，在解决隐私问题方面受到广泛关注 [11]。基于差分隐私的方法会对数据集、约束条件或目标函数持续添加随机扰动，以保护隐私。在 [12], 中，研究者提出了一种基于差分隐私的聚合算法，用于补偿太阳能发电波动并保护用户个人信息。Han等人在 [13] 中开发了一种基于差分隐私的分布式优化算法，以保护参与主体的隐私。Gough等人在 [14] 中设计了一种创新的符合差分隐私的算法，以确保消费者智能电表的数据得到保护。尽管基于差分隐私的方法在隐私保护方面取得了成功，但由于引入了扰动，这类方法不可避免地会产生精度损失。

相比之下，基于加密的策略通过将原始数据加密为密文来实现高精度的隐私保护，只有持有私钥的人才能解密这些密文。Lu 等人 在 [15] 中提出了一种高效且保护隐私的智能电网通信聚合方案，该方案使用 Paillier密码系统对数据进行加密。在 [16], 中，研究者基于同态密码系统设计了一种隐私保护且具备容错能力的方案，以实现计量数据的安全聚合。同样，Cheng 等人 在 [17]中提出了一种基于同态加密的新型隐私保护协作式分布式能源管理系统，以解决配电系统和微电网中的隐私问题。尽管精度很高，但其缺点

作者就职于美国犹他大学电气与计算机工程系，地址为美国犹他州盐湖城，邮编 84112（电子邮箱：xiang.huo, mingxi.liu@utah.edu）。

在于基于加密的方法普遍存在由加密和解密造成的计算开销。其他与硬件集成的隐私保护方法，例如混淆电路 [18], [19],，则缺乏灵活性，且由于硬件成本高昂而不经济。

秘密共享（SS） [20] 是一种轻量级密码学方法，可在一组参与者之间安全地分发秘密。每位参与者都会获得秘密的一个份额，只有当参与者人数超过阈值时，部分参与者协作才能根据各自的份额重构秘密。Nabil 等人等在 [21]采用 SS 设计了一种检测方案，用于识别窃电的恶意用户。该方案中，系统运营商只收集用户经过掩码处理的电表读数，以避免侵犯隐私。在 [22], ，研究人员开发了一种基于 SS 的电动汽车充电控制协议，以实现用于夜间低谷填充的隐私保护型电动汽车充电控制。与基于加密的策略相比，基于 SS 的方法既能保护隐私，又能避免沉重的计算负担。尽管 SS 具有上述优势，但由于配电网结构高度复杂、分布式能源资源数量庞大，且缺乏隐私保证方面的理论支持，鲜有研究探讨将 SS 应用于分布式能源资源控制。为弥补这些不足，本文设计了一种新颖的基于 SS 的隐私保护算法，可高效、安全、准确地解决大规模分布式能源资源控制问题。

B. 贡献声明

本文的贡献有三点：1）我们提出了一种新颖的去中心化隐私保护算法，能够在大规模分布式能源资源控制中同时实现可扩展性和隐私保护。据我们所知，本文首次提出了一种用于分布式能源资源隐私保护的基于秘密共享的算法，并提供了去中心化解决方案、隐私保证和严格的安全性证明；2）所提出的方法消除了频繁的点对点通信，并保护参与其中的分布式能源资源免受各种类型对手的侵害。所设计的框架可作为安全且可扩展的分布式能源资源控制基准。3）与最先进的方法相比，所提出的方法计算开销更低，且能够像不考虑隐私的算法一样获得精度相同的解。

本文其余部分安排如下：第二节构建配电网、光伏系统和储能系统的模型，并将分布式能源资源控制问题构建为一个约束优化问题。第三节通过投影梯度法推导分布式解，并介绍相应的分布式能源资源聚合与控制策略。第四节给出基于秘密共享的隐私保护分布式能源资源控制算法及隐私分析。第五节给出仿真结果并进行分析。第六节总结全文。

II. 问题构建

A. 支路潮流模型

考虑一个含有 n 个母线的辐射状配电网，其中 $\mathbb{B} = \{0, 1, \ldots, n\}$ 表示母线集合。令 l_{ij} 表示连接母线 i 和 j 的线路段， $\mathbb{L} = \{1, \ldots, h\}$ 表示线路集合， $\mathbb{C}_j$ 表示母线 j 的子母线集合， V_j 表示母线 j 处的电压幅值， $\mathcal{P}_{ij}$ 和 $\mathcal{Q}_{ij}$ 分别表示从母线 i 流向母线 j 的有功功率潮流和无功功率潮流， r_{ij} 和 x_{ij} 分别表示线路 l_{ij} 的电阻和电抗。对于母线 j，令 p_j^c 和 q_j^c 分别表示有功功率消耗和无功功率消耗， p_j^g 和 q_j^g 分别表示其有功功率发电量和无功功率发电。为简化网络模型，可将非线性 DistFlow模型[23] 线性化为 LinDistFlow模型，忽略高阶项且误差可忽略不计 [24]。因此，本文采用 LinDistFlow模型，其表示为

$$\mathcal{P}_{ij} - \sum_{u \in \mathbb{C}_j} \mathcal{P}_{ju} = p_j^c - p_j^g \tag{1a}$$

$$\mathcal{Q}_{ij} - \sum_{u \in \mathbb{C}_j} \mathcal{Q}_{ju} = q_j^c - q_j^g \tag{1b}$$

$$V_i^2 - V_j^2 = 2(r_{ij}\mathcal{P}_{ij} + x_{ij}\mathcal{Q}_{ij}). \tag{1c}$$

图1展示了一个连接屋顶太阳能光伏系统和储能系统的辐射型13节点配电网，本文将以此为例展开讨论。

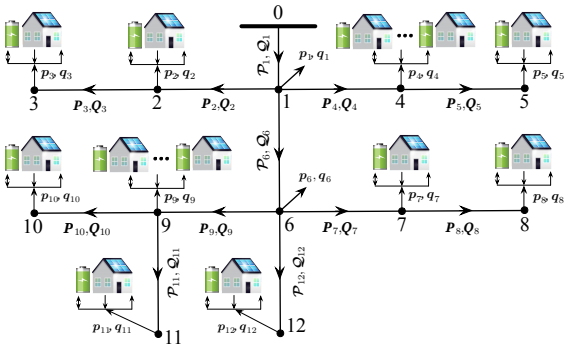


图1. 连接屋顶太阳能光伏系统和储能系统的辐射型13节点配电网。

本文的一个控制目标是通过控制光伏系统和储能系统的动态特性，最大限度地降低配电网的总功率损耗，其近似表示为

$$f_1(\boldsymbol{p}_1^g, \ldots, \boldsymbol{p}_n^g) = \sum_{l_{ij} \in \mathbb{L}} r_{ij} \left(\frac{\|\boldsymbol{\mathcal{P}}_{ij}\|_2^2 + \|\boldsymbol{\mathcal{Q}}_{ij}\|_2^2}{V_0^2} \right) \tag{2}$$

其中， V_0 表示额定电压幅值， $\boldsymbol{p}_j^g$、$\boldsymbol{\mathcal{P}}_{ij}$和$\boldsymbol{\mathcal{Q}}_{ij} \in \mathbb{R}^T$分别表示 p_j^g、 $\mathcal{P}_{ij}$和 $\mathcal{Q}_{ij}$在 T个时间间隔内的增广向量。注意，我们仅考虑有功功率损耗，并假设无功功率潮流$\boldsymbol{\mathcal{Q}}_{ij}$ 为常向量。为简化起见，此处未计入无功功率损耗，但可在不影响算法设计的情况下将其纳入。有功潮流受以下约束

$$\mathbf{0} \leq \boldsymbol{\mathcal{P}}_{ij} \leq \overline{\boldsymbol{\mathcal{P}}}_{ij} \tag{3}$$

其中$\overline{\boldsymbol{\mathcal{P}}_{ij}}$表示有功功率潮流限值的最大值。

B. 太阳能光伏

令 $\mathbb{V}$ 表示总计 $\mathcal{V}$ 个太阳能光伏系统的集合。在一天中的 T 个时间间隔内，第 ν 个光伏逆变器的有功功率注入 $\tilde{\boldsymbol{p}}_\nu \in \mathbb{R}^T$ 应满足

$$\mathbf{0} \leq \tilde{\boldsymbol{p}}_\nu \leq \overline{\boldsymbol{p}}_\nu^v \tag{4}$$

其中，$\overline{\boldsymbol{p}}_{\nu}^{v}$ 表示最大有功功率注入，且假设其可由预测得知。在此，弃电成本可通过 [25] 计算

$$f_2(\tilde{\boldsymbol{p}}_\nu) = \|\tilde{\boldsymbol{p}}_\nu - \overline{\boldsymbol{p}}_\nu^v\|_2^2. \tag{5}$$

C. 储能系统

令 $\mathbb{S}$ 表示 $\mathcal{E}$ 储能系统的集合。第 σ 个储能系统的充放电功率 $\hat{\boldsymbol{p}}_\sigma \in \mathbb{R}^T$ 受以下约束

$$-\underline{\boldsymbol{p}}_\sigma^s \le \hat{\boldsymbol{p}}_\sigma \le \overline{\boldsymbol{p}}_\sigma^s \tag{6}$$

其中，$\underline{\boldsymbol{p}}_\sigma^s$ 和 $\overline{\boldsymbol{p}}_\sigma^s$ 分别表示最大放电功率和最大充电功率。令 s_σ^0 表示第 σ 个储能系统的初始荷电状态（SoC），且 $\boldsymbol{H}_\sigma \triangleq [s_\sigma^0, \ldots, s_\sigma^0]^\intercal \in \mathbb{R}^T$。将 T 个时间区间内的充放电功率进行聚合，则第 σ个储能系统的容量受以下约束

$$\underline{\boldsymbol{p}}_\sigma^a \le \boldsymbol{H}_\sigma + \boldsymbol{A}\hat{\boldsymbol{p}}_\sigma \Delta T \le \overline{\boldsymbol{p}}_\sigma^a \tag{7}$$

其中，$\underline{\boldsymbol{p}}_\sigma^a$ 和 $\overline{\boldsymbol{p}}_\sigma^a$ 分别表示其容量下限和上限，ΔT 表示采样时间，聚合矩阵 $\boldsymbol{A}$ 为由 1 和 0 组成的下三角矩阵，即当 $\hat{\imath} \ge \hat{\jmath}$ 时，元素 $\boldsymbol{A}_{\hat{\imath},\hat{\jmath}} = 1$；当 $\hat{\imath} < \hat{\jmath}$ 时，元素 $\boldsymbol{A}_{\hat{\imath},\hat{\jmath}} = 0$，且 $\forall \hat{\imath}, \hat{\jmath} = 1, \ldots, T$。因此，在 T 个时隙期间，储能系统 σ 的荷电状态可通过使用 $\boldsymbol{A}$ 对充放电功率进行聚合得到。

此外，第 σ 个储能系统的退化成本根据充放电的平滑度，通过 [26] 计算

$$f_3(\hat{\boldsymbol{p}}_\sigma) = \|\boldsymbol{B}\hat{\boldsymbol{p}}_\sigma\|_2^2. \tag{8}$$

其中，$\boldsymbol{B}$ 计算相邻时刻之间的充放电差异，即 $\boldsymbol{B}_{\hat{\imath},\,\hat{\imath}} = 1$, $\forall \hat{\imath} = 1, \ldots, T$, $\boldsymbol{B}_{\hat{\imath},\,\hat{\imath}+1} = -1$, $\forall \hat{\imath} = 1, \ldots, T-1$，其余元素均为零。

D. 问题构建

随后，将该优化问题构建为：最小化配电网内有功功率总损耗、光伏弃电成本和储能系统退化成本之和

$$\begin{aligned} \min_{\tilde{\boldsymbol{p}}, \hat{\boldsymbol{p}}} \quad & \delta_1 f_1(\boldsymbol{p}^g) + \sum_{\nu=1}^{\mathcal{V}} \delta_2 f_2(\tilde{\boldsymbol{p}}_\nu) + \sum_{\sigma=1}^{\mathcal{E}} \delta_3 f_3(\hat{\boldsymbol{p}}_\sigma) \\ \text{s.t.} \quad & (1a), (3), (4), (6), (7) \end{aligned} \tag{P1}$$

其中，$\tilde{\boldsymbol{p}} = [\tilde{\boldsymbol{p}}_1^\intercal, \ldots, \tilde{\boldsymbol{p}}_n^\intercal]^\intercal$ $\boldsymbol{p} = [\boldsymbol{p}_1^\intercal \ \ldots \ \boldsymbol{p}_n^\intercal]^\intercal$ $\boldsymbol{p}^g = [\boldsymbol{p}_1^g \ \ldots \ \boldsymbol{p}_n^{g\intercal}]^\intercal$，$\delta_\alpha$ 为表示与目标函数 $f_\alpha(\cdot)$相关联的成本系数。请注意，成本系数为常数，可灵活调整全局和局部目标函数的权重，并调节不同的单位。

III. 分布式优化

A. 投影梯度法

本文通过投影梯度法（PGM）实现了求解（**P1**）的可扩展性。PGM 将集中式优化问题分解为各智能体的局部优化，从而形成并行计算结构。令 $\mathbb{M} = \{1, \ldots, m\}$ 表示智能体集合，例如母线或分布式能源资源，它们共同协作求解（**P1**）。在此设置下，第 κ 个智能体使用 PGM 更新其决策变量 $\boldsymbol{x}_\kappa$，方法如下：

$$\boldsymbol{x}_\kappa^{(\ell+1)} = \mathbb{P}_{\mathbb{X}_\kappa}[\boldsymbol{x}_\kappa^{(\ell)} - \gamma_\kappa^{(\ell)} \Phi_\kappa(\boldsymbol{x}^{(\ell)})] \tag{9}$$

其中，ℓ 表示迭代次数，$\intercal$,$\intercal$包含所有决策变量，即问题（**P1**）中的$\tilde{\boldsymbol{p}}_\nu$和$\hat{\boldsymbol{p}}_\sigma$，$\gamma_k^{(\ell)}$ 表示步长，$\Phi_\kappa(\cdot)$表示拉格朗日函数关于$w.r.t.\ \boldsymbol{x}_\kappa^{(\ell)}$的梯度，而 $\mathbb{P}_{\mathbb{X}_\kappa}[\cdot]$表示向集合 $\mathbb{X}_\kappa$上的投影运算。$\boldsymbol{x}^{(\ell)} = [\boldsymbol{x}_1^{(\ell)} \ \ldots \ \boldsymbol{x}_m^{(\ell)}]^\intercal$

在（**P1**）中，（4）中第 ν个光伏的局部约束以及（6）和（7）中第 σ个储能系统的局部约束可由两个可行集 $\mathbb{P}_\nu^v$ 和 $\mathbb{P}_\sigma^e$ 表示为

$$\mathbb{P}_\nu^v \triangleq \{\tilde{\boldsymbol{p}}_\nu | \, \boldsymbol{0} \le \tilde{\boldsymbol{p}}_\nu \le \overline{\boldsymbol{p}}_\nu^v\} \tag{10a}$$

$$\mathbb{P}_\sigma^e \triangleq \{\hat{\boldsymbol{p}}_\sigma | \, -\underline{\boldsymbol{p}}_\sigma^s \le \hat{\boldsymbol{p}}_\sigma \le \overline{\boldsymbol{p}}_\sigma^s, \ \underline{\boldsymbol{p}}_\sigma^a \le \boldsymbol{H} + \boldsymbol{A}\hat{\boldsymbol{p}}_\sigma \Delta T \le \overline{\boldsymbol{p}}_\sigma^a\}. \tag{10b}$$

下文旨在减少耦合项的数量，并基于网络拓扑将（1a）和（3）中的网络约束改写为单个不等式约束。为此，我们首先利用各母线的有功功率发电量表示（1a）中的有功潮流，具体如下

$$\boldsymbol{p}_i = \tilde{\boldsymbol{p}}_i - \hat{\boldsymbol{p}}_i - \boldsymbol{p}_i^c \tag{11}$$

其中，$\boldsymbol{p}_i$ 表示母线 i 处的聚合有功发电量，$\tilde{\boldsymbol{p}}_i = \sum_{\nu=1}^{\mathcal{V}_i} \tilde{\boldsymbol{p}}_\nu$ 和 $\hat{\boldsymbol{p}}_i = \sum_{\sigma=1}^{\mathcal{E}_i} \hat{\boldsymbol{p}}_\sigma$ 分别表示连接至母线 i 的所有光伏系统和储能系统的聚合有功功率。$\mathcal{V}_i$ 和 $\mathcal{E}_i$ 分别表示连接至母线 i 的光伏系统和储能系统的总数。

对于配电网中的第 ι 条线路潮流$\boldsymbol{\mathcal{P}}_\iota$，起始母线定义为潮流开始流动的母线，终端母线集合定义为第 ι 条线路潮流直至到达配电网边缘所经过的母线集合。令 $\boldsymbol{Z} \in \mathbb{R}^{n \times n}$ 表示配电网的邻接矩阵，$\boldsymbol{Z}_\iota$ 表示 $\boldsymbol{Z}$ 的第 ι 行，该行表示第 ι 条线路潮流的邻接向量。令 $\boldsymbol{Z}_\iota(i)$ 表示 $\boldsymbol{Z}_\iota$ 的第 i 个元素；若第 ι 个功率流以母线 i 为终端母线，则 $\boldsymbol{Z}_\iota(i) = 1$，例如 $\boldsymbol{Z}_9 = [0,0,0,0,0,0,0,0,0,1,1,1,0]$。于是，配电网中的功率流可表示为 $\boldsymbol{Z}$。将 $\boldsymbol{Z}$ 扩展至 T 个时隙，可得

$$\tilde{\boldsymbol{Z}} = \begin{bmatrix} \boldsymbol{Z}_1(1)\boldsymbol{I} & \boldsymbol{Z}_1(2)\boldsymbol{I} & \cdots & \boldsymbol{Z}_1(n)\boldsymbol{I} \\ \vdots & \vdots & & \vdots \\ \boldsymbol{Z}_n(1)\boldsymbol{I} & \boldsymbol{Z}_n(2)\boldsymbol{I} & \cdots & \boldsymbol{Z}_n(n)\boldsymbol{I} \end{bmatrix} \tag{12}$$

其中，$\boldsymbol{I} \in \mathbb{R}^{T \times T}$表示单位矩阵，且 $\tilde{\boldsymbol{Z}} \in \mathbb{R}^{nT \times nT}$。

下文令$\tilde{\boldsymbol{P}} \in \mathbb{R}^{nT}$ 表示所有母线在式（11）中定义的有功功率发电量之和，则有

$$\tilde{\boldsymbol{P}} = \begin{bmatrix} \boldsymbol{p}_1 \\ \vdots \\ \boldsymbol{p}_n \end{bmatrix} = \begin{bmatrix} \sum_{\nu=1}^{\mathcal{V}_1} \tilde{\boldsymbol{p}}_\nu - \sum_{\sigma=1}^{\mathcal{E}_1} \hat{\boldsymbol{p}}_\sigma - \boldsymbol{p}_1^c \\ \vdots \\ \sum_{\nu=\mathcal{V}_{n-1}+1}^{\mathcal{V}_n} \tilde{\boldsymbol{p}}_\nu - \sum_{\sigma=\mathcal{E}_{n-1}+1}^{\mathcal{E}_n} \hat{\boldsymbol{p}}_\sigma - \boldsymbol{p}_n^c \end{bmatrix}. \tag{13}$$

此外，$\tilde{\boldsymbol{P}}$ 可简洁地改写为

$$\tilde{\boldsymbol{P}} = \sum_{i=1}^{n} \boldsymbol{\Delta}_i \left(\tilde{\boldsymbol{p}}_i - \hat{\boldsymbol{p}}_i - \boldsymbol{p}_i^c\right) \tag{14}$$

其中， $\boldsymbol{\Delta}_i$ 表示聚合矩阵，其第 i个块由单位矩阵 $\boldsymbol{I}$表示，其他所有块均为零，例如 $\boldsymbol{\Delta}_1 = [\boldsymbol{I}, \boldsymbol{0}, \ldots, \boldsymbol{0}]^\mathsf{T} \in \mathbb{R}^{nT\times T}$.。然后，第 ι条线路的有功功率潮流可计算为

$$\boldsymbol{\mathcal{P}}_\iota = \tilde{\boldsymbol{Z}}_\iota \tilde{\boldsymbol{P}}. \tag{15}$$

因此，式（3）中的潮流限值约束变为

$$\boldsymbol{0} \le \tilde{\boldsymbol{Z}}_\iota \tilde{\boldsymbol{P}} \le \overline{\boldsymbol{\mathcal{P}}}_\iota. \tag{16}$$

因此，问题（**P1**）可写为

$$\begin{aligned} \min_{\tilde{\boldsymbol{p}},\hat{\boldsymbol{p}}} \quad & \delta_1 f_1(\boldsymbol{p}^g) + \sum_{\nu=1}^{\mathcal{V}} \delta_2 f_2(\tilde{\boldsymbol{p}}_\nu) + \sum_{\sigma=1}^{\mathcal{E}} \delta_3 f_3(\hat{\boldsymbol{p}}_\sigma) \\ \text{s.t.} \quad & \boldsymbol{p}_\nu \in \mathbb{P}_\nu^v, \ \forall \nu \in \mathbb{V} \\ & \boldsymbol{p}_\sigma \in \mathbb{P}_\sigma^e, \ \forall \sigma \in \mathbb{S} \\ & \boldsymbol{0} \le \tilde{\boldsymbol{Z}}_\iota \tilde{\boldsymbol{P}} \le \overline{\boldsymbol{\mathcal{P}}}_\iota, \forall \iota \in \mathbb{L} \end{aligned} \tag{P2}$$

（**P2**）中的优化问题旨在求解最优决策变量，即储能系统的充放电功率 $\tilde{\boldsymbol{p}}_\sigma$'s 和光伏系统的有功功率注入 $\hat{\boldsymbol{p}}_\nu$'s。接下来，我们将重点介绍如何基于式（9）中定义的投影梯度法，以分布式方式求解（**P2**）。为使用投影梯度法求解（**P2**），我们首先推导其松弛拉格朗日函数:

$$\begin{aligned} \mathcal{L}(\tilde{\boldsymbol{p}}, \hat{\boldsymbol{p}}, \boldsymbol{\mu}_l, \boldsymbol{\mu}_u) = & \delta_1 f_1(\boldsymbol{p}^g) + \sum_{\nu=1}^{\mathcal{V}} \delta_2 f_2(\tilde{\boldsymbol{p}}_\nu) + \sum_{\sigma=1}^{\mathcal{E}} \delta_3 f_3(\hat{\boldsymbol{p}}_\sigma) \\ & + \sum_{\iota=1}^{L} \boldsymbol{\mu}_{u\iota}^\mathsf{T}(\tilde{\boldsymbol{Z}}_\iota \tilde{\boldsymbol{P}} - \overline{\boldsymbol{\mathcal{P}}}_\iota) - \sum_{\iota=1}^{L} \boldsymbol{\mu}_{l\iota}^\mathsf{T} \tilde{\boldsymbol{Z}}_\iota \tilde{\boldsymbol{P}} \end{aligned} \tag{17}$$

其中， $\boldsymbol{\mu}_l = [\boldsymbol{\mu}_{l1}^\mathsf{T}, \ldots, \boldsymbol{\mu}_{lL}^\mathsf{T}]^\mathsf{T}$和 $\boldsymbol{\mu}_u = [\boldsymbol{\mu}_{u1}^\mathsf{T}, \ldots, \boldsymbol{\mu}_{uL}^\mathsf{T}]^\mathsf{T}$、 $\boldsymbol{\mu}_{l\iota}$ 和 $\boldsymbol{\mu}_{u\iota}$ 分别表示与线路 ι的潮流上下限相关联的对偶变量。

假设 $\tilde{\boldsymbol{p}}_\nu$ 和$\hat{\boldsymbol{p}}_\sigma$ 分别为连接至母线 i的第 ν个光伏系统和第σ个储能系统的决策变量。对原变量 $\tilde{\boldsymbol{p}}_\nu$ 和$\hat{\boldsymbol{p}}_\sigma$求式（17）的次梯度*w.r.t.* ，可得:

$$\begin{aligned} \nabla_{\tilde{\boldsymbol{p}}_\nu} \mathcal{L}(\cdot) = & 2\delta_2(\tilde{\boldsymbol{p}}_\nu - \overline{\boldsymbol{p}}_\nu^v) + \frac{2\delta_1}{V_0^2} \sum_{\iota=1}^{L} r_\iota (\tilde{\boldsymbol{Z}}_\iota \boldsymbol{\Delta}_i)^\mathsf{T} (\tilde{\boldsymbol{Z}}_\iota \tilde{\boldsymbol{P}}) \\ & + \sum_{\iota=1}^{L} (\tilde{\boldsymbol{Z}}_\iota \boldsymbol{\Delta}_i)^\mathsf{T} (\boldsymbol{\mu}_{u\iota} - \boldsymbol{\mu}_{l\iota}) \end{aligned} \tag{18a}$$

$$\begin{aligned} \nabla_{\hat{\boldsymbol{p}}_\sigma} \mathcal{L}(\cdot) = & 2\delta_3 \hat{\boldsymbol{p}}_\sigma - \frac{2\delta_1}{V_0^2} \sum_{\iota=1}^{L} r_\iota (\tilde{\boldsymbol{Z}}_\iota \boldsymbol{\Delta}_i)^\mathsf{T} (\tilde{\boldsymbol{Z}}_\iota \tilde{\boldsymbol{P}}) \\ & - \sum_{\iota=1}^{L} (\tilde{\boldsymbol{Z}}_\iota \boldsymbol{\Delta}_i)^\mathsf{T} (\boldsymbol{\mu}_{u\iota} - \boldsymbol{\mu}_{l\iota}). \end{aligned} \tag{18b}$$

在不影响算法设计有效性的前提下，为便于表述，假设所有电力线路具有相同的电阻 $\bar{r}$ ，则式（18）变为

$$\nabla_{\tilde{\boldsymbol{p}}_\nu} \mathcal{L}(\cdot) = 2\delta_2(\tilde{\boldsymbol{p}}_\nu - \overline{\boldsymbol{p}}_\nu^v) + \bar{\delta}_1 \boldsymbol{\pi}_i \tilde{\boldsymbol{P}} + \boldsymbol{\psi}_i(\boldsymbol{\mu}_u - \boldsymbol{\mu}_l) \tag{19a}$$

$$\nabla_{\hat{\boldsymbol{p}}_\sigma} \mathcal{L}(\cdot) = 2\delta_3 \hat{\boldsymbol{p}}_\sigma - \bar{\delta}_1 \boldsymbol{\pi}_i \tilde{\boldsymbol{P}} - \boldsymbol{\psi}_i(\boldsymbol{\mu}_u - \boldsymbol{\mu}_l) \tag{19b}$$

其中，$\bar{\delta}_1 = \frac{2\delta_1}{V_0^2}\bar{r}$、 $\boldsymbol{\pi}_i = \sum_{\iota=1}^{L} (\tilde{\boldsymbol{Z}}_\iota \boldsymbol{\Delta}_i)^\mathsf{T} \tilde{\boldsymbol{Z}}_\iota$，且 $\boldsymbol{\psi}_i$ 表示 $\boldsymbol{Z}$ 的第i列块。

式（19）中拉格朗日函数次梯度的详细推导见附录A。

因此，根据式（18）中计算得到的次梯度，在第 ℓ 次迭代中，第 ν 个光伏和第 σ 个储能系统可通过投影梯度法更新其决策变量:

$$\tilde{\boldsymbol{p}}_\nu^{(\ell+1)} = \Pi_{\mathbb{P}_\nu^v} \left(\tilde{\boldsymbol{p}}_\nu^{(\ell)} - \alpha_{\nu,\ell}^v \nabla_{\tilde{\boldsymbol{p}}_\nu} \mathcal{L}^{(\ell)}(\cdot) \right) \tag{20a}$$

$$\hat{\boldsymbol{p}}_\sigma^{(\ell+1)} = \Pi_{\mathbb{P}_\sigma^e} \left(\hat{\boldsymbol{p}}_\sigma^{(\ell)} - \alpha_{\sigma,\ell}^e \nabla_{\hat{\boldsymbol{p}}_\sigma} \mathcal{L}^{(\ell)}(\cdot) \right) \tag{20b}$$

其中，$\alpha_{\nu,\ell}^v$ 和 $\alpha_{\sigma,\ell}^e$ 分别表示第 ν 个光伏和第 σ 个储能系统的原始步长， $\mathcal{L}^{(\ell)}(\cdot)$ 表示第 ℓ 次迭代时式（17）中计算得到的拉格朗日函数。对偶变量也可以使用投影梯度法以类似方式更新。

B. 分布式能源资源聚合与控制

在投影梯度法的迭代过程中，第 i 个智能体需要计算 $\Phi_i(\boldsymbol{x}^\ell)$ 中需要用到所有其他智能体的决策变量 $\boldsymbol{x}_i$'s。如式 (19) 所示，计算次梯度$\nabla_{\tilde{\boldsymbol{p}}_\nu}\mathcal{L}(\cdot)$ 和 $\nabla_{\hat{\boldsymbol{p}}_\sigma}\mathcal{L}(\cdot)$ 确实需要所有智能体的决策变量 $\boldsymbol{P}$。具体而言，式 (19a) 和 (19b) 中次梯度的计算通过以下内容相互耦合

$$\mathcal{C} = \mathcal{C}_p + \mathcal{C}_d = \bar{\delta}_1 \boldsymbol{\pi}_i \tilde{\boldsymbol{P}} + \boldsymbol{\psi}_i(\boldsymbol{\mu}_u - \boldsymbol{\mu}_l) \tag{21}$$

其中， $\mathcal{C}_p$ 和 $\mathcal{C}_d$ 分别表示与原始变量和对偶变量相关的耦合项。

为清楚说明次梯度计算中的信息交换需求，我们以连接在母线 2 上的第 $\hat{\nu}$ 个光伏为例，展示其原始变量更新过程。第 $\hat{\nu}$ 个光伏可以使用式 (19a) 中的次梯度更新其决策变量 $\tilde{\boldsymbol{p}}_{\hat{\nu}}$ ，具体如下

$$\nabla_{\tilde{\boldsymbol{p}}_{\hat{\nu}}} \mathcal{L}(\cdot) = 2\delta_2(\tilde{\boldsymbol{p}}_{\hat{\nu}} - \overline{\boldsymbol{p}}_{\hat{\nu}}^v) + \sum_{\iota=1}^{2} \left(\bar{\delta}_1 \boldsymbol{\pi}_\iota \tilde{\boldsymbol{P}} + \boldsymbol{\mu}_{u\iota} + \boldsymbol{\mu}_{l\iota} \right) \tag{22}$$

其中，$\boldsymbol{\pi}_1 \tilde{\boldsymbol{P}} = \sum_{i=1}^{n} \boldsymbol{p}_i$ 和 $\boldsymbol{\pi}_2 \tilde{\boldsymbol{P}} = \boldsymbol{p}_2 + \boldsymbol{p}_3$。因此，第 $\hat{\nu}$ 个光伏需要来自所有母线的有功功率发电量 $\boldsymbol{p}_i$， $\forall i = 1, \ldots, n$，以执行式 (20a) 中的更新。

根据上述观察结果，可以采用两种不同的聚合与控制策略，即母线级聚合与控制和*DER* 级聚合与控制，如图 2 所示。在母线级聚合与控制中，第 i 个

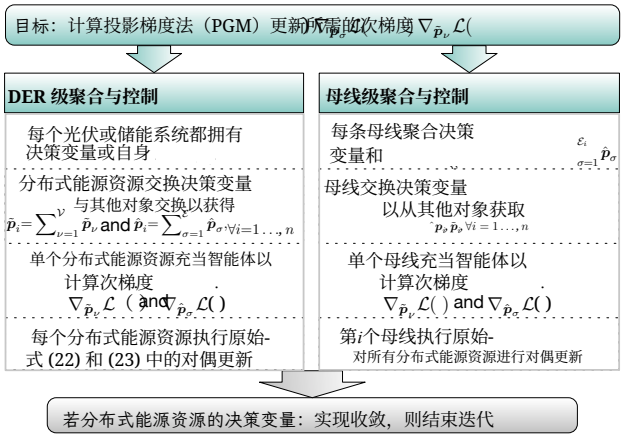


图 2. 通过母线级和 DER 级架构对分布式能源资源进行聚合与控制。

母线（智能体）聚合决策变量 $\tilde{\boldsymbol{p}}_i = \sum_{\nu=1}^{\mathcal{V}_i} \tilde{\boldsymbol{p}}_\nu$

以及 $\hat{\boldsymbol{p}}_i = \sum_{\sigma=1}^{\mathcal{E}_i} \hat{\boldsymbol{p}}_\sigma$，其中仅传输聚合决策变量，并将其用于原始更新。相比之下，分布式能源资源级控制策略要求每个分布式能源资源都充当智能体，并接收其他所有分布式能源资源在式 (20) 更新中所需的全部数据。然而，由于接入配电网的分布式能源资源数量庞大，分布式能源资源级控制可能导致大量数据交换和繁重的本地计算。因此，我们采用计算和通信效率更高的母线级聚合与控制方案。我们将在后文说明，所提出的隐私保护算法可以直接扩展至分布式能源资源级控制（详情请参见**注释 1**）。

除了可扩展性和效率之外，母线级方法和分布式能源资源级方法中不可避免的隐私信息暴露也引发了根本性的隐私问题，例如，电力负荷可能会泄露敏感的商业活动和/或客户的日常作息。为解决隐私问题，我们将开发一种新型的基于秘密共享的算法，以便在执行（20）时实现安全信息交换。

IV. 基于秘密共享的隐私保护分布式能源资源控制

A. 实数到整数的量化

请注意，秘密共享方案需要使用模运算，而不是实数运算。然而，分布式优化通常需要进行实数计算，例如使用实数决策变量和参数。因此，需要进行实数到整数变换，以将秘密共享集成到分布式优化中。我们采用定点数数量化[27]，将实数映射到整数空间，并将定点实数集合定义为

$$\mathbb{Q}_{\theta,\gamma,\zeta} \triangleq \left\{-\theta^{\gamma}, -\theta^{\gamma}+\theta^{-\zeta}, \ldots, \theta^{\gamma}-2\theta^{-\zeta}, \theta^{\gamma}-\theta^{-\zeta}\right\} \quad (23)$$

其中，$\theta \in \mathbb{N}_{1+}$ 表示基，$\gamma \in \mathbb{N}$ 表示幅值，$\zeta \in \mathbb{N}$ 表示分辨率。因此，通过定义满射映射 $m(\cdot): \mathbb{R} \mapsto \mathbb{Q}_{\theta,\gamma,\zeta}$，可以将实数映射到$\mathbb{Q}_{\theta,\gamma,\zeta}$中的最近点。为限制量化误差，映射 $m(\cdot)$ 需要满足

$$|m(\varphi)-\varphi| \leq \theta^{-\zeta}, \forall \varphi \in [-\theta^{\gamma}, \theta^{\gamma}] \quad (24)$$

量化误差受分辨率限制，范围为$\mathbb{Q}_{\theta,\gamma,\zeta}$。为了将实数集合映射到整数集合 $\mathbb{Z}$，我们只需将$\mathbb{Q}_{\theta,\gamma,\zeta}$ 缩放 θ^{ζ} 倍，得到

$$\mathbb{Z}_{\theta,\gamma,\zeta} = \theta^{\zeta}\mathbb{Q}_{\theta,\gamma,\zeta} = \left\{-\theta^{\gamma+\zeta}, -\theta^{\gamma+\zeta}+1, \ldots, \theta^{\gamma+\zeta}-1\right\} \quad (25)$$

其中$\mathbb{Z}_{\theta,\gamma,\zeta} \subseteq \mathbb{Z}$ 表示整数域中的定点集合。此外，秘密共享要求输入位于域 $\mathbb{E}$内。因此，我们进一步通过模运算将$z \in \mathbb{Z}_{\theta,\gamma,\zeta}$中的每个元素映射到 $\mathbb{E}$，得到

$$g(z) = z \bmod e. \quad (26)$$

注意，$z \in \mathbb{Z}_{\theta,\gamma,\zeta}$ 可以是任意负整数，而式（26）中的模运算会改变负输入的符号，即对于 $\hat{z} < 0$，$g(\hat{z}) = \hat{z} + e$。为处理负整数运算，我们引入 $g(\cdot)$ 的部分逆，定义如下：

$$\psi(z) = \begin{cases} z-e & \text{if } z \geq \frac{e}{2}, \\ z & \text{otherwise.} \end{cases} \quad (27)$$

因此，我们可以轻松得到 $z = \psi(g(z))\ \forall z \in \mathbb{E}$。

B. 基于秘密共享的隐私保护算法

*1) Shamir*秘密共享方案：在介绍隐私保护算法设计之前，我们先简要介绍 Shamir秘密共享方案 [20]，该方案具有高效、轻量的私密信息分发结构。假设一位管理者（秘密持有者）希望将秘密 ω 分发给特定代理，并要求至少 d个代理协作才能恢复该秘密。在这种需求下，Shamir秘密共享方案基于以下拉格朗日插值思想来实现秘密分发与恢复。

定理 1 (多项式插值 [28])。设 $\{(\varsigma_1, y_1), \ldots, (\varsigma_d, y_d)\} \subseteq \mathbb{R}^2$ 是一组点，其 ς_i 的取值均不相同。则存在唯一的 $\mathcal{Y}$ 次多项式 $\mathcal{Y}$，满足 $y_i = \mathcal{Y}(\varsigma_i)\ \forall i = 1, \ldots, d$。■

在基于秘密共享的方案中，管理者首先构造一个次数为 $d-1$ 的随机多项式，形式如下：

$$y(z) = \omega + a_1 z + \cdots + a_{d-1} z^{d-1} \quad (28)$$

其中，ω表示一个整数秘密，$a_1, \ldots, a_{d-1}$是均匀分布于域 $\mathbb{E}$ 当$[0, e)$ 中的随机系数，e 表示一个大于 ω的素数。其次，管理者使用非零整数输入计算式 (28) 的输出，例如，令 $\tau = 1, \ldots, n$，以获取 $(\tau, y(\tau))$，其中 $y_\tau^{\Pi} = y(\tau) \bmod e$。然后，将份额 y_τ^{Π} 分发给智能体 τ。最后，根据**定理 1**，至少需要 d 个持有份额的智能体来重构多项式，从而通过以下方式恢复秘密 ω

$$\omega = \sum_{\tau=1}^{d} y_\tau^{\Pi} \prod_{\substack{\upsilon=0 \\ \upsilon \neq \tau}}^{d} \frac{\upsilon}{\upsilon - \tau}. \quad (29)$$

2）提出的隐私保护算法：接下来，我们将在母线级聚合与控制架构中介绍基于秘密共享的双层去中心化隐私保护算法，以同时实现隐私保护和可扩展性。在配电网层，所有分布式能源资源的决策变量并行更新，且每条母线仅向服务器发送掩蔽数据。在云计算层，服务器计算聚合消息，并将其分发至相关母线。所提出的隐私保护算法的计算结构如图 3 所示。

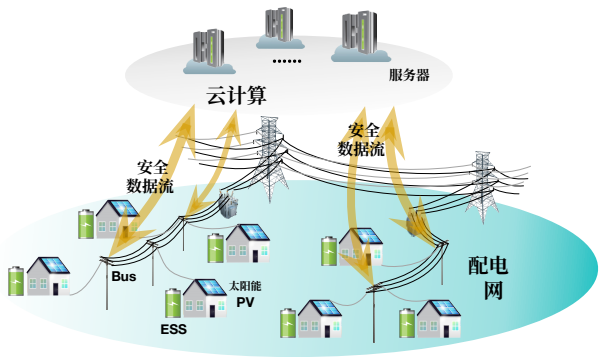


图 3. 配电网中分布式能源资源控制的双层隐私保护计算结构。

令 $\mathbb{C}$ 表示云的集合，$c \geq 2$ 表示云的总数。第 i 条母线使用式（28）生成一个 $d-1$ 阶随机多项式，以获得

$$y_i^{(\ell)}(z) = \omega_i^{(\ell)} + a_{i,1}^{(\ell)} z + \cdots + a_{i,d-1}^{(\ell)} z^{d-1} \tag{30}$$

其中，$2 \leq d \leq c$, $\omega_i^{(\ell)}$ 表示母线 i 在第 ℓ次迭代时的秘密，ℓ 表示迭代次数，而 $a_{i\,1}^{(\ell)}$、、.....、 $a_i^{(\ell)}$、$_{d-1}$表示在域 $\mathbb{E}$中均匀分布的随机系数。请注意，对于 $\boldsymbol{p}_i$这类向量秘密，默认采用式（30）对该向量进行逐元素计算。

在第 ℓ次迭代时，第 u个云首先生成一个随机整数 $\alpha_u^{(\ell)}$，然后将 $\alpha_u^{(\ell)}$广播给所有母线。随后，第 i个母线可基于式（30），使用接收到的输入计算 $y_i^{(\ell)}(\alpha_u^{(\ell)})$、 $\forall u = 1$、.....、 c。最后，第 i个母线将 $y_i^{(\ell)}(\alpha_u^{(\ell)})$发回第 u个云。请注意，式（21）中的耦合项$\tilde{\boldsymbol{\pi}}_i \boldsymbol{P}$ 是所有 $\boldsymbol{p}_i$的线性组合，需要用到来自$\tilde{}$个母线的私有发电/用电详情。因此，需要采用$\boldsymbol{\pi}_i \boldsymbol{P}$ 的安全计算框架，以保护母线和分布式能源资源所有者的隐私。

假设各云知晓网络拓扑矩阵 $\boldsymbol{Z}$，该矩阵不包含母线$\tilde{}$或分布式能源资源的任何隐私信息。为了计算母线 i 的聚合信息 $\boldsymbol{\pi}_i \boldsymbol{P}$，第 u 个云首先利用 $\boldsymbol{\pi}_i$ 的系数，将收到的输出 $y_1(\alpha_u^{(\ell)}) \ldots, y_n(\alpha_u^{(\ell)})$相乘，得到

$$\{\alpha_u^{(\ell)}, \boldsymbol{\pi}_i(1) y_1^{(\ell)}(\alpha_u^{(\ell)}), \ldots, \boldsymbol{\pi}_i(n) y_n^{(\ell)}(\alpha_u^{(\ell)})\} \tag{31}$$

然后，第 u 个云将（31）中的输出相加，得到一组新的输入和输出:

$$\bar{\mathcal{A}}_{u,i} = \{\alpha_u^{(\ell)}, \sum_{\hat{\imath}=1}^{n} \boldsymbol{\pi}_i(\hat{\imath})\, y_{\hat{\imath}}^{(\ell)}(\alpha_u^{(\ell)})\}. \tag{32}$$

$\tilde{}$最后，第 u 个云计算 $\mathcal{A}_{u,i}$, $\forall i = 1, \ldots, n$ 和$\tilde{}$，并将新的输入输出份额$\mathcal{A}_{u,i}$ 广播给第 i 条母线。

因此，在从总共 c 个云服务器接收到新的份额后，第 i 条母线现在可以访问

$$\tilde{\mathcal{A}}_i = \left\{ \alpha_{\hat{\jmath}}^{(\ell)}, \sum_{\hat{\imath}=1}^{n} \boldsymbol{\pi}_i(\hat{\imath})\, y_{\hat{\imath}}^{(\ell)}(\alpha_{\hat{\jmath}}^{(\ell)}), \forall \hat{\jmath} = 1, \ldots, c \right\}. \tag{33}$$

$\tilde{}$注意， $\mathcal{A}_i$ 总共包含 c 个份额，可据此构造如下形式的新多项式:

$$\tilde{y}_i^{(\ell)}(z) = \boldsymbol{\pi}_i \tilde{\boldsymbol{P}} + \tilde{a}_{i,1}^{(\ell)} z + \cdots + \tilde{a}_{i,d-1}^{(\ell)} z^{d-1} \tag{34}$$

$\tilde{}$其常数项恰好为 $\boldsymbol{\pi}_i \boldsymbol{P}$。

在此信息交换过程中，每个母线仅向每台服务器发送一个份额，因此单台云服务器无法根据收到的份额重构秘密，也就无法推断代理的真实决策变量。云服务器只需利用随机化多项式的输出计算聚合消息。所提方法的详细内容见**算法 1**

算法 1 能够在保持与非隐私保护 PGM 方法相同的精确解的同时实现隐私保护。决策变量将持续更新，直到收敛误差 $\epsilon_\nu^{(\ell)} \triangleq \|\tilde{\boldsymbol{p}}_\nu^{(\ell)} - \tilde{\boldsymbol{p}}_\nu^{(\ell-1)}\|_2^2$和 $\epsilon_\sigma^{(\ell)} \triangleq \|\hat{\boldsymbol{p}}_\sigma^{(\ell)} - \hat{\boldsymbol{p}}_\sigma^{(\ell-1)}\|_2^2$ 小于阈值 ϵ_0。**算法 1** 的正确性通过**定理 2**进行了说明。

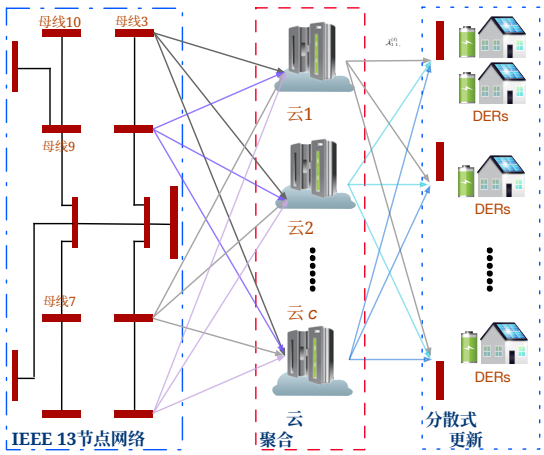


图4. 配电网络与云服务器之间的信息交换结构（仅标注了母线3和云1发送的消息）。

算法 1基于秘密共享的隐私保护分布式能源资源控制策略

1：代理初始化决策变量、容差 ϵ_0、基 θ、幅值 γ、分辨率 ζ、迭代计数器 $\ell = 0$ 和最大迭代次数 ℓ_{max}。2：当 $\epsilon_\nu^{(\ell)}(\sigma) > \epsilon_0$ 且 $\ell < \ell_{max}$ 时，执行 3：每个母线使用式（23）—（26）执行实数到整数的转换，然后获得整数秘密 $\omega_i^{(\ell)}$。4：第 u个云生成随机整数 $\alpha_u^{(\ell)}$，然后将 $\alpha_u^{(\ell)}$广播给所有母线。5：第 i个母线使用式（30）生成随机多项式 $y_i^{(\ell)}(z)$，其中 $\omega_i^{(\ell)}$ 为常数项，使用 $\alpha_1^{(\ell)}$、.....、 $\alpha_c^{(\ell)}$计算输出，以获得 $y_i^{(\ell)}(\alpha_1^{(\ell)})$.....、 $y_i^{(\ell)}$ $\alpha_c^{(\ell)}$ $y_i^{(\ell)}$ $\alpha_u^{(\ell)}$ u ( )，然后将 ( ) 发送至第 个云。_6：第 u个云根据式（32）构造 $\mathcal{A}_u$、$_i$，然后将_$\mathcal{A}_u$、$_i$ 广播给第 i个母线。_7：第 i个母线根据式（33）构造 $\mathcal{A}_i$，使用 c 个份额重构$\tilde{}$聚合秘密以获得 $\boldsymbol{\pi}_i \boldsymbol{P}$，然后计算式（21）中的 $\mathcal{C}_p$。8：第 i 个母线使用式（27）将 $\mathcal{C}_p$ 转换回实数，然后通过 PGM 使用式（9）更新连接至母线 i 的分布式能源资源的决策变量 $\tilde{\boldsymbol{p}}_\nu^{(\ell)}$或 $\hat{}\boldsymbol{p}_\sigma^{(\ell)}$。第 i个母线计算误差 $\epsilon_\nu^{(\ell)}$或 $\epsilon_\sigma^{(\ell)}$。9：$\ell = \ell + 1$。10：结束 while

定理 2 (正确性). 设 $\mathbb{E}$ 表示输入秘密 $\omega_1, \ldots, \omega_n$ 的定义域，$\mathcal{C}_p$ 表示期望输出。那么，**算法 1** 满足:

$$\Pr\left[\forall c \geq d, \mathrm{Rec}\left(\mathbb{A}, \mathbb{E}, \boldsymbol{Z}, \bar{\delta}_1, \theta, \gamma, \zeta\right) = \mathcal{C}_p\right] = 1 \tag{35}$$

$\tilde{}$ $\tilde{}$其中， $\mathbb{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_c\}$ 表示来自代理的份额集合，Pr[·] 表示概率，Rec(·) 表示秘密重构操作。■

定理 2指出，**算法 1** 能够正确获取聚合信息 $\mathcal{C}_p$，进而用于实现精确的原始变量和对偶更新。

定理 2 的详细证明见附录 B。

备注 1： 尽管**算法 1**是基于母线级聚合与控制开发的，但也可以扩展到分布式能源资源级聚合与控制。在分布式能源资源级聚合与控制中，每个分布式能源资源都需要生成式 (30) 中的多项式，并按照式 (33) 作为独立智能体参与秘密重构。此外，根据实际应用情况，也可以按家庭或区域对分布式能源资源进行分组和控制，由新的分组充当智能体，并遵循**算法 1**的类似设计。□

备注 2： 多服务器架构将秘密共享方案无缝集成到分布式能源资源聚合与控制中。服务器组对母线生成的份额进行聚合并广播给母线，以实现秘密恢复。聚合任务分配给多个服务器，以确保单个服务器无法恢复任何秘密。□

C. 隐私分析

所提出的方法旨在保护分布式能源资源的决策变量，因为这些变量一旦泄露，可能导致客户敏感信息泄露。为解决这一问题，**算法 1** 能够针对两类对手实现隐私保护：一类是诚实但好奇的智能体，它们遵循算法，但可能利用所持有和接收的数据推断其他智能体的隐私信息；另一类是外部窃听者，它们会窃听并截取通信信道中交换的消息。

命题 1： (安全云计算)。 在**算法 1**中，少于 $d-1$ 个云无法推断出任何有关聚合决策变量 $\mathcal{C}_p$的信息。■

命题 1 阐述了所提出算法针对被攻陷的云服务器的安全性。根据**定理 1**中的多项式插值，至少需要 d 个云才能通过合谋获取任何秘密。

命题 1 基于正确性分析得以证明。详细证明请参阅附录 C。

假设 1。 单个智能体的通信链路中至少有一条能够防范外部窃听者。■

假设 1 对于基于秘密共享的方案至关重要且普遍适用。给定通过不同通信链路发送的 d 对份额，即 $\{(\varsigma_1, y_1)$.....$(\varsigma_d, y_d)\} \subseteq \mathbb{R}^2$，如果外部窃听者窃听所有通信链路以获取这些份额，那么它便可以直接利用**定理 1**通过拉格朗日插值推导出秘密。

定理 3 (针对对手的隐私保护)。 通过使用 **算法 1**，以下两个陈述成立：

1) **算法 1** 能够在存在诚实但好奇的代理时，安全地计算并更新代理之间的决策变量。2) 外部窃听者无法获知代理的任何隐私信息。■

定理 3 在存在诚实但好奇的代理和外部窃听者的情况下，提供隐私保护保证。从安全多方计算（安全多方计算）的角度可以证明**算法 1** 的隐私保护。在给出详细的隐私分析和证明之前，我们先介绍一些安全多方计算的概念。

定义 1 （计算不可区分性 [29]）。 设$\{D_\varkappa\}_{\varkappa\in\mathbb{N}}$ 和 $\{E_\varkappa\}_{\varkappa\in\mathbb{N}}$ 为安全参数为 $\varkappa$的两个分布族；若对于任意非一致概率多项式时间算法 $\mathcal{G}$， $\delta(\varkappa)$都是可忽略的，其中

$$\delta(\varkappa)=\left|\Pr_{x_1\leftarrow D_\varkappa}[\mathcal{G}(x_1)=1]-\Pr_{x_2\leftarrow E_\varkappa}[\mathcal{G}(x_2)=1]\right| \tag{36}$$

我们称 $\{D_\varkappa\}_{\varkappa\in\mathbb{N}}$ 和 $\{E_\varkappa\}_{\varkappa\in\mathbb{N}}$ 在计算上不可区分，记作 $D_\varkappa \overset{c}{\equiv} E_\varkappa$。■

因此，**定义 1** 指出，任何多项式时间算法都无法区分两个计算上不可区分的分布，因为这些算法的输出不会有显著差异。接下来，**定义 2**给出了安全多方计算中的标准隐私概念。

定义 2 ([30], [31])。 设 Π 是一个用于计算函数 $\mathcal{F}(\bar{x})$输出的 m方协议，其中 $\bar{x}=\{x_1,\ldots,x_m\}$，且 $\mathcal{F}_\rho(\bar{x})$表示 $\mathcal{F}(\bar{x})$的第 ρ个输出。令$\mathbb{M}=\{M_1,\ldots,M_m\}$ 表示参与方集合。执行 Π 期间第 ρ方的视图记为 $\text{VIEW}_\rho^\Pi(\bar{x})$。如果存在一个多项式时间算法 $\mathcal{S}$，使得对于 $\mathbb{M}$中的每个参与方 M_ρ ，都有以下关系成立，则称 Π 能够私下计算 $\mathcal{F}(\bar{x})$。

$$\mathcal{S}(\rho, x_\rho, \mathcal{F}_\rho(\bar{x})) \overset{c}{\equiv} \text{VIEW}_\rho^\Pi(\bar{x}). \tag{37}$$

■

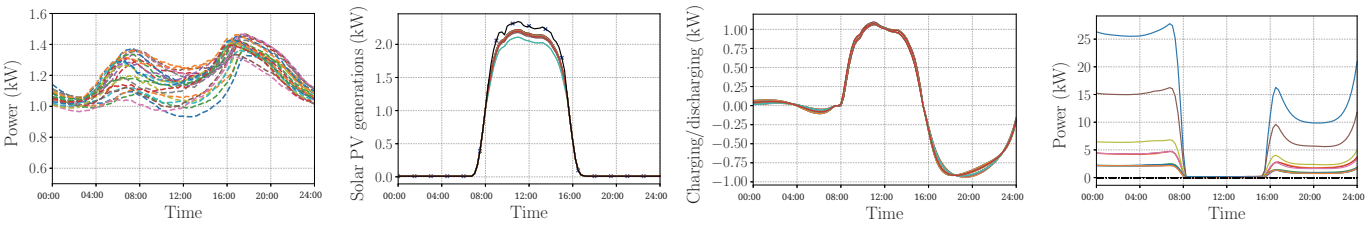
定义 2指出，可以基于计算不可区分性来评估 m 方协议的安全性，即可以仅根据各方的输入和输出，高效地模拟其视图。换言之，安全多方计算允许一组参与者在不泄露任何其他信息的情况下，获知对其私有输入应用某个约定函数后得到的正确输出。**定义 1**和**定义 2** 的理论基础有助于证明**算法 1**˜ ˜能够在各智能体之间安全地计算 $\boldsymbol{\pi}_1\boldsymbol{P},\ldots,\boldsymbol{\pi}_n\boldsymbol{P}$。

定理 3 的详细证明见附录 D。

V. 仿真结果

采用简化的单相 IEEE 13节点测试馈线 [32] 验证所提出的去中心化隐私保护型分布式能源资源控制策略。具体而言，除馈线首端外，假设每条母线均连接 2 栋住宅，且每栋住宅都配备一个储能系统和 5 块太阳能板，最多可产生 2.5 kW 的太阳能输出。所有住宅储能系统的最大容量均为 10 kWh，所有储能系统的初始荷电状态统一设为 4 kWh，最大充电和放电功率分别为 $\pm$3 kW [33]。预测的太阳能光伏发电数据取自加利福尼亚州 CAISO 于 2021 年 1 月 1 日提供的数据，时间间隔为 $\Delta T=15$ 分钟 [34]。

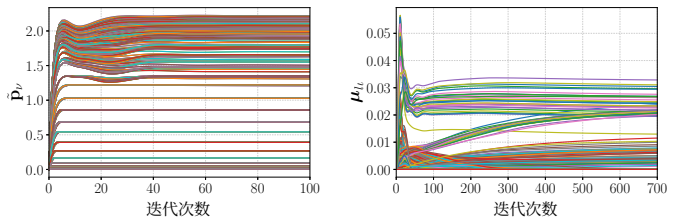
总共由 $c=4$ 个云负责消息聚合与分发。所有多项式的次数设为 $d-1=3$，整数域选为 $\mathbb{E}=[0,2^{31}-1)$ 。对于定点数量化，基、幅值和分辨率统一设为 $\theta=2$、$\gamma=27$ 和 $\zeta=4$。对于图1所示的配电网，假设所有24户住宅都位于同一区域，且太阳辐照度相同。所有住宅的基准负荷曲线



(a) 24 个住宅的异质基线负荷 (b) 24 个住宅的太阳能注入功率 (c) 24 个储能系统的充放电功率 (d) 配电网中 12 条线路的功率流 图 5. 通过控制配电网中的分布式能源资源得到的 **(P2)** 最优解。

如图5(a) [34]所示。根据经验，原始和对偶步长分别设为 $\alpha^{v}_{\nu,\ell}=2.3$、$\alpha^{e}_{\sigma,\ell}=1.8$ 和 $\beta_{\mu_{li},\ell}=5\times10^{-4}$。请注意，潮流限值（16）中只有下界处于激活状态，因此此处仅展示与 $\boldsymbol{\mu}_{li}$ 相关的结果。

图 5(b) 和图 5(c) 分别显示了太阳能光伏和储能系统的有功功率发电量以及充放电功率。大约在 12:00，太阳能光伏发电量达到最大，储能系统以峰值功率充电。16:00 之后，储能系统中储存的能量被释放，用于满足家庭内部用电需求并补偿配电网中的功率损耗。图 5(d) 展示了 12 条线路的功率流，没有发生反向潮流。此外，在不影响预期原始-对偶收敛的情况下，获得了准确的原始解和对偶解。原始变量和对偶变量的迭代解如图 6 所示。图。



(a) 太阳能光伏的决策收敛 (b) 对偶变量 $\boldsymbol{\mu}$变量 $\tilde{\mathbf{p}}_{\nu}$ $_{li}$

Fig. 6. 原始变量和对偶变量的收敛

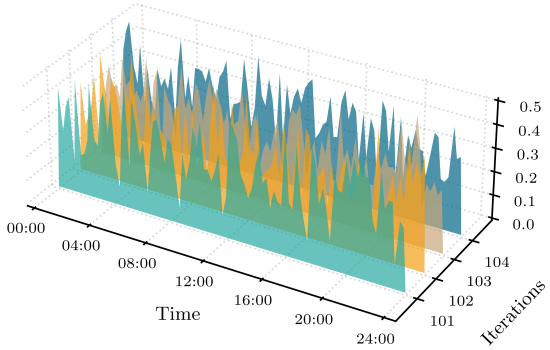


图 7. 母线6在不同迭代次数下生成的随机份额

7 展示了母线6使用随机多项式 $y_6^{(\ell)}(z)=\omega_6^{(\ell)}+a_1^{(\ell)}z+a_2z^2+a_3^{(\ell)}z^3$ 生成的归一化份额，其中系数 $a_i^{(\ell)}$、$i=1$、2、3 在每次迭代和不同的时隙中都会随机化。由于外部窃听者通过窃听传输的份额，无法获得足够的信息来进行多项式重构，因此**算法 1** 的隐私保护得以保证。

份额。在不失一般性的前提下，假设母线6是诚实但好奇的。图8展示了模拟器的存在，该模拟器

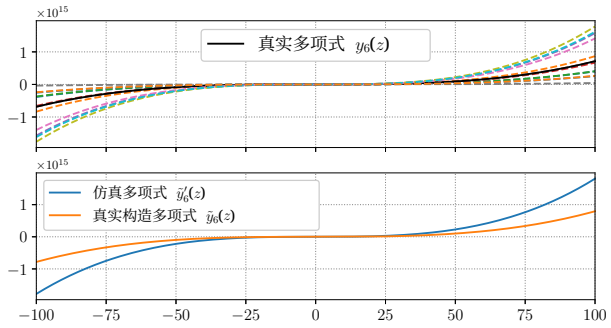


图 8. 模拟器生成的多项式，以实现代理之间的计算不可区分性

可以生成真实多项式 $y_6(z)$ 和模拟多项式 $y_i'(z)$（虚线），$\forall i=1,\ldots,n, i\neq6$，使得 $\tilde{}$ $\tilde{}(\boldsymbol{\pi}_6\boldsymbol{P})'=\boldsymbol{\pi}_6\boldsymbol{P}$。因此，计算不可区分性 $\tilde{y}_6'(\alpha_j)\overset{c}{\equiv}\tilde{y}_6(\alpha_j)\ \forall j=1,\ldots,c$ 在任意 $\tilde{}$ $\tilde{}$迭代和任意时间段均成立，并且此处可在母线之间安全地计算 $\boldsymbol{\pi}_1\boldsymbol{P},\ldots,\boldsymbol{\pi}_n\boldsymbol{P}$，而第 i条母线只能获知其自身视图 VIEW$_i$中包含的信息。

VI. 结论

本文提出了一种结合云计算架构的新型去中心化隐私保护算法，用于配电网中的分布式能源资源控制。该分布式能源资源控制问题被建模为一个约束优化问题，目标是最小化线路损耗、光伏弃电成本和储能系统退化成本。通过将秘密共享融入去中心化投影梯度法，所提出的方法实现了对分布式能源资源所有者私人数据的隐私保护，包括分布式能源资源的发电量、用电量和日用电量。本文通过隐私保证以及针对诚实但好奇的智能体和外部窃听者的分析，严格证明了所提出方法的安全性。仿真结果验证了所提出方法在配备可控储能系统和太阳能光伏系统的改进型 IEEE 13节点测试馈线上的适用性。此外，所设计的方法可直接用于隐私保护场景下的一般大规模去中心化优化问题。

附录A 投影梯度法更新的推导

我们以图1中的 IEEE 13节点测试馈线为例，说明式 (18) 中次梯度的推导。为证明

(18a)，我们首先考虑功率损耗最小化目标函数的次梯度，有功功率损耗为

$$f_1(\boldsymbol{p}_1^g,\ldots,\boldsymbol{p}_n^g)=\delta_1\sum_{l_{ij}\in\mathbb{L}}r_{ij}\left(\frac{\|\boldsymbol{\mathcal{P}}_{ij}\|_2^2}{V_0^2}\right)=\frac{\delta_1\bar{r}}{V_0^2}\sum_{\iota\in\mathbb{L}}\|\boldsymbol{\mathcal{P}}_\iota\|_2^2$$
$$=\frac{\bar{\delta}_1}{2}\sum_{\iota\in\mathbb{L}}\|\boldsymbol{\mathcal{P}}_\iota\|_2^2. \tag{38}$$

将（15）代入（38），得到

$$f_1(\boldsymbol{p}_1^g,\ldots,\boldsymbol{p}_n^g)=\frac{\bar{\delta}_1}{2}\sum_{\iota\in\mathbb{L}}\|\tilde{\boldsymbol{Z}}_\iota\tilde{\boldsymbol{P}}\|_2^2. \tag{39}$$

不失一般性，假设第 ν 个光伏，其决策变量为 $\tilde{\boldsymbol{p}}_\nu$，连接至母线 i，则有

$$\nabla_{\tilde{\boldsymbol{p}}_\nu}\mathcal{L}(\cdot)=\delta_1\nabla_{\tilde{\boldsymbol{p}}_\nu}f_1(\boldsymbol{p}_1^g,\ldots,\boldsymbol{p}_n^g)+\delta_2\nabla_{\tilde{\boldsymbol{p}}_\nu}f_2(\tilde{\boldsymbol{p}}_\nu)$$
$$+\sum_{\iota=1}^{L}\nabla_{\tilde{\boldsymbol{p}}_\nu}\boldsymbol{\mu}_{u\iota}^{\mathsf{T}}(\tilde{\boldsymbol{Z}}_\iota\tilde{\boldsymbol{P}}-\overline{\boldsymbol{\mathcal{P}}}_\iota)-\sum_{\iota=1}^{L}\nabla_{\tilde{\boldsymbol{p}}_\nu}\boldsymbol{\mu}_{l\iota}^{\mathsf{T}}\tilde{\boldsymbol{Z}}_\iota\tilde{\boldsymbol{P}}. \tag{40}$$

将（14）和（38）代入（40）的第一项，得到

$$\delta_1\nabla_{\tilde{\boldsymbol{p}}_\nu}f_1(\cdot)=\frac{\bar{\delta}_1}{2}\nabla_{\tilde{\boldsymbol{p}}_\nu}\sum_{\iota\in\mathbb{L}}\|\tilde{\boldsymbol{Z}}_\iota\tilde{\boldsymbol{P}}\|_2^2$$
$$=\bar{\delta}_1\sum_{\iota\in\mathbb{L}}\left(\nabla_{\tilde{\boldsymbol{p}}_\nu}\tilde{\boldsymbol{Z}}_\iota\sum_{\hat{\imath}=1}^{n}\boldsymbol{\Delta}_{\hat{\imath}}\tilde{\boldsymbol{p}}_{\hat{\imath}}\right)\left(\tilde{\boldsymbol{Z}}_\iota\tilde{\boldsymbol{P}}\right)$$
$$=\bar{\delta}_1\sum_{\iota\in\mathbb{L}}\left(\tilde{\boldsymbol{Z}}_\iota\boldsymbol{\Delta}_i\right)^{\mathsf{T}}\left(\tilde{\boldsymbol{Z}}_\iota\tilde{\boldsymbol{P}}\right). \tag{41}$$

对（5）取次梯度，（40）的第二项变为

$$\delta_2\nabla_{\tilde{\boldsymbol{p}}_\nu}f_2(\tilde{\boldsymbol{p}}_\nu)=\delta_2\nabla_{\tilde{\boldsymbol{p}}_\nu}\|\tilde{\boldsymbol{p}}_\nu-\overline{\boldsymbol{p}}_\nu^v\|_2^2=2\delta_2\left(\tilde{\boldsymbol{p}}_\nu-\overline{\boldsymbol{p}}_\nu^v\right). \tag{42}$$

然后，将（14）代入右侧（40）的第三项，得到

$$\sum_{\iota=1}^{L}\nabla_{\tilde{\boldsymbol{p}}_\nu}\boldsymbol{\mu}_{u\iota}^{\mathsf{T}}(\tilde{\boldsymbol{Z}}_\iota\tilde{\boldsymbol{P}}-\overline{\boldsymbol{\mathcal{P}}}_\iota)=\sum_{\iota=1}^{L}\nabla_{\tilde{\boldsymbol{p}}_\nu}\boldsymbol{\mu}_{u\iota}^{\mathsf{T}}\tilde{\boldsymbol{Z}}_\iota(\sum_{\hat{\imath}=1}^{n}\boldsymbol{\Delta}_{\hat{\imath}}\tilde{\boldsymbol{p}}_{\hat{\imath}})$$
$$=\sum_{\iota=1}^{L}(\tilde{\boldsymbol{Z}}_\iota\boldsymbol{\Delta}_i)^{\mathsf{T}}\boldsymbol{\mu}_{u\iota}. \tag{43}$$

类似地，（40）的最后一项可直接得到

$$-\sum_{\iota=1}^{L}\nabla_{\tilde{\boldsymbol{p}}_\nu}\boldsymbol{\mu}_{l\iota}^{\mathsf{T}}(\tilde{\boldsymbol{Z}}_\iota\tilde{\boldsymbol{P}})=-\sum_{\iota=1}^{L}(\tilde{\boldsymbol{Z}}_\iota\boldsymbol{\Delta}_i)^{\mathsf{T}}\boldsymbol{\mu}_{l\iota}. \tag{44}$$

最后，将 (41)、(42)、(43)、(44) 代入 (40)，即可证明 (18a)。按照类似思路，可轻松证明 (18b) 中原始变量 $\hat{\boldsymbol{p}}_\sigma$ 的次梯度。

附录 B 定理证明2

证明：为证明**算法 1**的正确性，我们展示所提出的方法与非隐私投影梯度法具有相同的原始解和对偶解。回顾一下，第 u 个云按照 (31) 将接收到的 n 输出与 $\boldsymbol{\pi}_i$ 的元素相乘，可得

$$\begin{cases}\boldsymbol{\pi}_i(1)y_1(\alpha_u)=\boldsymbol{\pi}_i(1)\left(\omega_1+a_{1,1}\alpha_u+\cdots+a_{1,d-1}\alpha_u^{d-1}\right)\\ \vdots\\ \boldsymbol{\pi}_i(n)y_n(\alpha_u)=\boldsymbol{\pi}_i(n)\left(\omega_n+a_{n,1}\alpha_u+\cdots+a_{n,d-1}\alpha_u^{d-1}\right)\end{cases} \tag{45}$$

然后，将 (45) 左侧求和，即可得到 (31) 中的聚合输出 $\sum_{\hat{\imath}=1}^{n}\boldsymbol{\pi}_i(\hat{\imath})y_i(\alpha_u)$。因此，如 (32) 所示，所有云提供的总计 c 对份额可视为某个多项式的输入和输出

$$\tilde{y}(z)=\sum_{\hat{\imath}=1}^{n}\boldsymbol{\pi}_i(\hat{\imath})\omega_{\hat{\imath}}+\tilde{a}_1z+\cdots+\tilde{a}_{d-1}z^{d-1} \tag{46}$$

其中 $\tilde{a}_{\hat{\jmath}}=\sum_{\hat{\imath}=1}^{n}\boldsymbol{\pi}_{\hat{\imath}}(\hat{\imath})a_{\hat{\imath}\hat{\jmath}}$，$\hat{\jmath}=1,\ldots,d-1$ 和 $\sum_{\hat{\imath}=1}^{n}\boldsymbol{\pi}_{\hat{\imath}}(\hat{\imath})\omega_{\hat{\imath}}$ 恰好为 $\boldsymbol{\pi}_i\boldsymbol{P}$。然后，如**定理 1**所述，由于 $d\le c$，可使用 (33) 中的 c 对份额轻松恢复聚合秘密 $\boldsymbol{\pi}_i\boldsymbol{P}$。

附录 C 命题证明1

证明：在 $d-1$ 个云串通的情况下，它们可以构造以下方程组

$$\begin{cases}\tilde{y}_i(\alpha_1)=\tilde{\omega}+\tilde{a}_{i,1}\alpha_1+\cdots+\tilde{a}_{i,d-1}\alpha_1^{d-1}\\ \vdots\\ \tilde{y}_i(\alpha_{d-1})=\tilde{\omega}+\tilde{a}_{i,1}\alpha_{d-1}+\cdots+\tilde{a}_{i,d-1}\alpha_{d-1}^{d-1}\end{cases} \tag{47}$$

其中，$\tilde{y}_i(z)$定义于式 (34) 中，且 $\tilde{\omega}=\boldsymbol{\pi}_i\boldsymbol{P}$。在式 (47) 中，$\tilde{a}_{i,\hat{\imath}},\forall\hat{\imath}=1,\ldots,d-1$ 和 $\tilde{\omega}$ 均为未知量，因此，$d-1$ 个云总共可得出 $d-1$ 个方程，但有 d 个未知量，导致解欠定。

附录 D 定理 3 的证明

定理 3

证明：为证明**算法 1** 能够抵御诚实但好奇的代理并实现隐私保护，我们旨在验证诚实但好奇的代理接收到的任何信息都可以被高效模拟。也就是说，诚实但好奇的代理无法利用接收到的数据从其他代理处获取有用信息，因为它无法区分接收到的数据与自身数据。在执行**算法 1**的第 ℓ 次迭代期间，母线 i 的视图可描述为

$$\text{VIEW}_i=\{\alpha_1,\ldots,\alpha_c,\theta,\gamma,\zeta,\boldsymbol{\pi}_i\tilde{\boldsymbol{P}},y_i(z),\omega_i,\bar{\mathcal{A}}_i,$$
$$\tilde{y}_i(\alpha_j),\forall j=1,\ldots,c,\mathcal{C}_p,\mathcal{C}_d\}. \tag{48}$$

根据**定义 2**，我们需要证明存在一个多项式时间算法，记为模拟器 $\mathcal{S}$，能够使用智能体 i 的数据模拟 VIEW_i，即

$$\mathcal{S}(\Xi_i)\overset{c}{\equiv}\text{VIEW}_i \tag{49}$$

其中，$\Xi_i\triangleq\{\alpha_1,\ldots,\alpha_c,\theta,\gamma,\zeta,\boldsymbol{\pi}_i\tilde{\boldsymbol{P}},y_i(z),\omega_i,\bar{\mathcal{A}}_i,\tilde{y}_i(\alpha_j),\forall j=1,\ldots,c,\mathcal{C}_p,\mathcal{C}_d\}$ 表示智能体i 可访问的数据集合。式（49）表明，智能体 i接收到的任何内容都可以根据其自身知识 Ξ_i高效地重构。为此，模拟器需要生成满足以下条件的 $\tilde{y}_i'(\alpha_j),\forall j=1,\ldots,c$

$$\tilde{y}_i'(\alpha_j)\overset{c}{\equiv}\tilde{y}_i(\alpha_j),\forall j=1,\ldots,c. \tag{50}$$

为实现这一目标，模拟器首先生成其他代理的秘密 $w_{j\neq i}'\in\mathbb{E}$，使得

$$\boldsymbol{\pi}_i\tilde{\boldsymbol{P}}=w_i+\sum_{j\neq i}w_j'. \tag{51}$$

然后，它按照式（30）生成一组随机多项式，以获得 $y'_j(z)\ \forall j \neq i$，其中 $w'_j,\ \forall j \neq i$ 为相应的常数项，即

$$\begin{cases} y_i(z) = w_i + a_{i,1}z + \cdots + a_{i,d-1}z^{d-1} & \text{(52a)} \\ y'_j(z) = w'_j + a'_{i,1}z + \cdots + a'_{i,d-1}z^{d-1}, \forall j \neq i. & \text{(52b)} \end{cases}$$

因此，模拟器可以将 $\{\alpha_1, \ldots, \alpha_c\}$ 用作式（52）的输入，并得到

$$\tilde{\mathcal{A}}'_i = \left\{ \alpha_{\hat{\jmath}}, y_i(\alpha_{\hat{\jmath}}) + \sum_{j \neq i} y'_j(\alpha_{\hat{\jmath}}), \forall, \hat{\jmath} = 1, \ldots, c \right\}. \quad (53)$$

根据 **定理 1** 和 **定理 2**，式（53）中的份额可用于构造一个如下形式的新多项式

$$\tilde{y}'_i(x) = (\boldsymbol{\pi}_i \tilde{\boldsymbol{P}})' + \tilde{a}'_{i,1}z + \cdots + \tilde{a}'_{i,d-1}z^{d-1} \quad (54)$$

其中 $(\boldsymbol{\pi}_i \boldsymbol{P})' = \boldsymbol{\pi}_i \boldsymbol{P}$。因此，根据 **定义 2**，式（50）和（49）成立，**算法 1** 可在代理之间安全地计算 $\boldsymbol{\pi}_1 \boldsymbol{P}, \ldots, \boldsymbol{\pi}_n \boldsymbol{P}$。

接下来，我们证明**算法 1** 针对外部窃听者的隐私保护能力。在**假设 1**下，假设智能体 1 不受外部窃听者侵扰。外部窃听者通过窃听其他任意智能体的通信信道，最多只能获取

$$\Xi_e = \left\{ \alpha_1, \ldots, \alpha_c, y_i(\alpha_u), \bar{\mathcal{A}}_{u,i}, \forall i = 2, \ldots, n, u = 1, \ldots, c \right\}. \quad (55)$$

由于（55）不足以构造式（33），外部窃听者无法推断 $y_i(z)$ 的内容，也无法推断 $\tilde{y}'_i(z)$ 的内容，即无法推断代理的隐私信息 $\boldsymbol{p}_i$ 或聚合消息 $\boldsymbol{\pi}_i \boldsymbol{P}$。

参考文献

[1] J. Campbell，《由分布式能源资源提供的辅助服务》，橡树岭国家实验室，美国田纳西州橡树岭，技术报告，2005年。[2] J. R. Aguero、E. Takayesu、D. Novosel 和 R. Masiello，《电网现代化：可持续未来面临的挑战与机遇》，*IEEE*《电力与能源杂志》，第15卷，第3期，第74–83页，2017年。[3] I.-K. Song、W.-W. Jung、J.-Y. Kim、S.-Y. Yun、J.-H. Choi 和 S.-J. Ahn，《采用分布式能源资源的智能配电网运行方案：降低损耗与供电恢复》，*IEEE Trans. Smart Grid*，第4卷，第1期，第367–374页，2012年。[4] D. K. Molzahn、F. D¨orfler、H. Sandberg、S. H. Low、S. Chakrabarti、R. Baldick 和 J. Lavaei，《电力系统分布式优化与控制算法综述》，*IEEE Trans. Smart Grid*，第8卷，第6期，第2941–2962页，2017年。[5] M. Zeraati、M. E. H. Golshan 和 J. M. Guerrero，《高光伏渗透率配电网中电池储能系统电压调节的分布式控制》，*IEEE Trans. Smart Grid*，第9卷，第4期，第3582–3593页，2016年。[6] Q. Zhang、Y. Guo、Z. Wang 和 F. Bu，《主次级一体化配电系统中的分布式最优节能降压》，*IEEE Trans. Smart Grid*，第12卷，第5期，第3889–3900页，2021年。[7] Y. Pan、A. Sangwongwanich、Y. Yang 和 F. Blaabjerg，《低通信开销的孤岛串联光伏-电池混合系统分布式控制》，*IEEE*《电力电子汇刊》，第36卷，第9期，第10 199–10 213页，2021年。[8] T. Navidi、A. El Gamal 和 R. Rajagopal，《用于分布式能源资源协调的两层分散式控制架构》，载于 *IEEE Conf. Decis. Control* 论文集，美国佛罗里达州迈阿密，2018年12月17日至29日，第6019–6024页。[9] W. Lin 和 E. Bitar，《分布式能源资源的分散式随机控制》，*IEEE*《电力系统汇刊》，第33卷，第1期，第888–900页，2017年。[10] X. Huo 和 M. Liu，《网络化环境中多智能体系统的双维可扩展协同优化》，*IEEE Trans. Control Syst. Technol.*，第30卷，第6期，第2317–2332页，2022年。

[11] C. Dwork、F. McSherry、K. Nissim 和 A. Smith，《在隐私数据分析中校准噪声与敏感度》，载于 Theory Cryptogr. Conf. 论文集，美国纽约州纽约，2006年3月4日至7日，第265–284页。[12] J. Dong、T. Kuruganti、S. Djouadi、M. Olama 和 Y. Xue，《对可控负荷进行隐私保护聚合以补偿太阳能发电波动》，载于 IEEE Electron. Power Grid 论文集，美国南卡罗来纳州查尔斯顿，2018年11月12日至14日，第1–5页。[13] S. Han、U. Topcu 和 G. J. Pappas，《差分隐私分布式约束优化》，IEEE Trans. Autom. Control，第62卷，第1期，第50–64页，2016年。[14] M. B. Gough、S. F. Santos、T. AlSkaif、M. S. Javadi、R. Castro 和 J. P. Catal˜ao，《在智能电网环境中保护智能电表数据的隐私》，IEEE Trans. Ind. Inform.，第18卷，第718页，2021 1，707 no. pp. – 。[15] R. Lu、X. Liang、X. Li、X. Lin 和 X. Shen，《EPPA：一种用于智能电网安全通信的高效隐私保护聚合方案》，IEEE Trans. Parallel Distrib. Syst.，第23卷，第9期，第1621–1631页，2012年。[16] A. Mohammadali 和 M. S. Haghighi，《一种用于智能电网计量数据聚合的多维容错隐私保护同态方案》，IEEE Trans. Smart Grid，第12卷，第6期，第5212–5220页，2021年。[17] Z. Cheng、F. Ye、X. Cao 和 M.-Y. Chow，《基于同态加密的隐私保护协作式分布式能源管理系统》，IEEE Trans. Smart Grid，第12卷，第6期，第5233–5243页，2021年。[18] S. Wang、Q. Hu、Y. Sun 和 J. Huang，《基于位置的服务中的隐私保护》，IEEE Commun. Mag.，第56卷，第3期，第134–140页，2018年。[19] R. Gilad-Bachrach、K. Laine、K. Lauter、P. Rindal 和 M. Rosulek，《安全数据交换：云端市场》，载于 ACM SIGSAC Conf. Cloud Comput. Security Workshop 论文集，英国伦敦，2019年11月11日，第117–128页。[20] A. Shamir，《如何共享一个秘密》，Commun. ACM，第22卷，第11期，第612–613页，1979年。[21] M. Nabil、M. Ismail、M. M. Mahmoud、W. Alasmary 和 E. Serpedin，《PPETD：面向高级计量基础设施网络、具备负荷监测和计费功能的隐私保护窃电检测方案》，IEEE Access，第7卷，第96 334–96 348页，2019年。[22] X. Huo 和 M. Liu，《基于秘密共享的电动汽车充电分布式隐私保护控制》，Electr. Power Syst. Res.，第211卷，文章号108357，2022年。[23] M. Baran 和 F. F. Wu，《辐射状配电系统中电容器的最优配置》，IEEE Trans. Power Deliv.，第4卷，第1期，第735–743页，1989年。[24] M. Farivar、L. Chen 和 S. Low，《配电系统局部电压控制的均衡与动态特性》，载于 IEEE Conf. Decis. Control 论文集，意大利佛罗伦萨，2013年12月10日至13日，第4329–4334页。[25] J. Li、Z. Xu、J. Zhao 和 C. Zhang，《考虑光伏限发的有源配电网络分布式在线电压控制》，IEEE Trans. Ind. Inform.，第15卷，第10期，第5519–5530页，2019年。[26] J. Forman、J. Stein 和 H. Fathy，《通过差分进化优化动态电池参数表征实验》，载于 Am. Control Conf. 论文集，美国华盛顿特区，2013年6月17日至19日，第867–874页。[27] M. S. Daru 和 T. Jager，《使用秘密共享与一次一密的加密云端控制》，载于 IEEE Conf. Decis. Control 论文集，法国尼斯，2019年12月11日至13日，第7215–7221页。[28] J. Humpherys 和 T. J. Jarvis，《应用数学基础》第一卷：数学分析。Soc. Ind. Appl. Math，2020年。[29] O. Goldreich，《密码学基础：第二卷，基本应用》。剑桥大学出版社，2009年。[30] D. Evans、V. Kolesnikov 和 M. Rosulek，《安全多方计算实用入门》，Found. Trends Privacy Security，第2卷，第2–3期，第70–246页，2018年。[31] O. Goldreich，《安全多方计算》，手稿，预印本，第78卷，第110页，1998年。[32] M. Liu、P. K. Phanivong、Y. Shi 和 D. S. Callaway，《住宅配电网络中电动汽车的分散式充电控制》，IEEE Trans. Control Syst. Technol.，第27卷，第1期，第266–281页，2019年。[33] 美国国家可再生能源实验室。住宅电池储能。[在线]。网址：https://atb.nrel.gov/electricity/2021/residential battery storage [34] 美国能源信息署。年度电力报告。[在线]。网址：https://www.eia.gov/todayinenergy/detail.php?id=49276