On Privacy Preservation of Distributed Energy Resource Optimization in Power Distribution Networks

Xiang Huo, *Member, IEEE* and Mingxi Liu, *Member, IEEE*

***Abstract*— The exploding deployment of distributed energy resources (DERs) brings unprecedented challenges to the optimization of large-scale power distribution networks – numerous grid-tied devices pose severe control scalability crises. Besides, the exposure of private DER data, such as energy generation and consumption profiles, is leading to prevalent customer privacy breaches. Despite the importance, research on privacy-preserving DER control in a fully scalable manner is still lacking. To fill the gap, in this paper, a hierarchical DER aggregation and control framework is first developed to achieve scalability over the large DER population and ensure capability for privacy preservation integration. Second, a novel privacy-preserving optimization algorithm is proposed for the developed DER aggregation and control framework based on the secret sharing technique. Finally, privacy preservation guarantees of the developed algorithm are designed against honest-but-curious adversaries and external eavesdroppers. Simulations on a 13-bus test feeder demonstrate the efficacy of the proposed approach in preserving the private DER data within power distribution networks.**

***Index Terms*— Decentralized optimization, distributed energy resources, privacy preservation, secret sharing**

I. Introduction

A. Background and Related Works

CONTROL of distributed energy resources (DERs) in power distribution networks has proven efficacy in lowering carbon emissions and offering grid-edge services such as voltage control, load shaping, and backup power supply [1]. DERs, including energy storage systems (ESSs), solar photovoltaics (PVs), and electric vehicles (EVs), along with other monitoring and controllable devices, are revolutionizing the operation of power distribution networks towards a more cost-effective fashion [2]. Though integrating DERs into power distribution networks can offer multifarious benefits, scalability issues and privacy concerns hinder the implementation of existing DER control strategies [3].

To address scalability, distributed and decentralized strategies are drawing surging attention owing to their paralleled computing structure. For example, a distributed coordination method based on local droop and consensus control is designed in [4] to deal with the voltage rise problem caused by the high penetration of solar PVs. To reduce the communication burden, a distributed low-communication algorithm is proposed in [5] to control islanded PV-battery-hybrid systems. Compared to distributed methods, decentralized strategies eliminate the massive peer-to-peer communications. Navidi *et al.* [6] develop a two-layer decentralized DER coordination architecture that can provide scalable solutions with extensive parallelization and eliminate direct communications between local controllers. In [7], a decentralized shrunken primal-multi-dual subgradient algorithm with network dimension reduction is developed to achieve scalability *w.r.t.* both agent population size and network dimension. Lin and Bitar [8] propose a decentralized stochastic control strategy for radial power distribution systems with controllable PVs and ESSs to cut down the demand balancing cost.

Despite the outstanding scalability and efficiency, the implementation of both distributed and decentralized DER control strategies relies heavily on mandatory communications that can disclose customers' sensitive information. Differential privacy (DP) has been a de facto standard in addressing privacy concerns owing to its rigorous privacy definition [9]. DP-based methods achieve privacy preservation by adding well-calibrated noise into the computing process, obscuring the attributes of any single individual's data. This ensures that privacy is preserved regardless of the combination of computations performed on the dataset, providing strong privacy guarantees against arbitrary adversaries, e.g., any re-identification attack [10]. A centralized differentially private optimal power flow mechanism is developed in [11]. However, centralized structures generically suffer from poor scalability compared to distributed or decentralized ones. Dvorkin *et al.* [12] develop an adversarial inference model based on DP that first questions the privacy properties of distributed optimal power flow. Subsequently, the authors develop a differentially private variant of the alternating direction method of multipliers to ensure information privacy during neighbor exchanges. This model is later extended in [13] for the distributed optimization of AC power flow problems. In [14], a DP-based aggregation algorithm is proposed to compensate for solar power fluctuations and protect customers' personal information. Han *et al.* [15] develop a distributed privacy-preserving optimization algorithm based on DP to preserve

Xiang Huo was with the University of Utah, Salt Lake City, UT 84112 USA. He is now with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843 USA (e-mail: xiang.huo@tamu.edu).

Mingxi Liu is with the Department of Electrical and Computer Engineering, University of Utah, Salt Lake City, UT 84112 USA (e-mail: mingxi.liu@utah.edu).

This work was done at the University of Utah and is supported by NSF Award: ECCS-2145408.

the privacy of the participating agents in constrained optimizations. Despite the success in privacy preservation, DP-based methods invariably suffer from accuracy loss due to the added perturbations.

In contrast, encryption-based strategies can achieve high-accuracy privacy preservation by encrypting the sensitive data into ciphertexts, and only those holding private keys can decrypt the ciphertexts. Despite the high accuracy, the spectrum of adversaries in encryption-based strategies is more specific and can be proven from the secure multi-party computing (SMC) perspective against certain internal adversaries, e.g., honest-but-curious agents, the system operator, and particular external adversaries, e.g., eavesdroppers [16]–[18]. Centralized privacy-preserving energy control systems have been established based on homomorphic encryption (HE), e.g., the Paillier cryptosystem [16], [19]. They are easy to implement but lack scalability. In [17], a decentralized privacy-preserving approach is developed by combining partially HE with decentralized optimization. Similarly, Wu *et al.* [18] develop a

guarantees secure computation for aggregators at different scales; 3) The developed DER control algorithm achieves lower computational overhead compared with encryption-oriented approaches and ensures high accuracy as the non-privacy-concerned algorithms.

The rest of this paper is organized as follows: In Section II, we introduce the models of power distribution networks, PVs, and ESSs, then formulate the DER control problem into a constrained optimization problem. Section III develops two decentralized DER aggregation and control strategies based on the projected gradient method. The SS-based privacy-preserving DER control algorithm and privacy analyses are given in Section IV. We give simulation results and analyses in Section V. Section VI concludes the paper.

II. Problem Formulation

A. Branch Flow Model

For an n-bus radial distribution network, let $\mathcal{B} =$

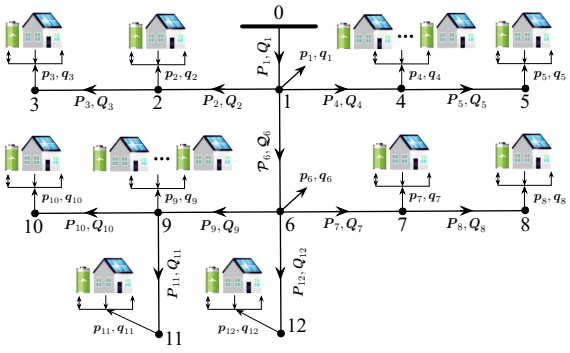


Fig. 1: A radial 13-bus distribution network connected with rooftop solar PVs and ESSs.

work connected with residential houses, rooftop solar PVs, and ESSs. This paper aims to ensure customer privacy in the optimization and control of DERs while providing grid services for power distribution networks.

One grid service objective is to minimize the power loss of the distribution network, which can be calculated by:

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

where V_0 denotes the nominal voltage magnitude, $\boldsymbol{p}_j^g$, $\boldsymbol{P}_{ij}$, and $\boldsymbol{Q}_{ij}\in\mathbb{R}^T$ are augmented vectors of p_j^g, P_{ij}, and Q_{ij} across T time intervals, respectively. Note that only active power loss is primarily considered as it can directly lead to energy cost savings for utilities and consumers.

The active power flows are constrained by:

$$\mathbf{0}\le\boldsymbol{P}_{ij}\le\overline{\boldsymbol{P}}_{ij}, \quad (3)$$

where $\overline{\boldsymbol{P}}_{ij}$ denotes the maximum active power flow limit.

B. Solar Photovoltaic

Let $\mathcal{V}$ denote the set of solar PVs. During T time intervals of a day, the active power injection $\tilde{\boldsymbol{p}}_\nu\in\mathbb{R}^T$ from the νth PV inverter should satisfy:

$$\mathbf{0}\le\tilde{\boldsymbol{p}}_\nu\le\overline{\boldsymbol{p}}_\nu^v, \quad (4)$$

where $\overline{\boldsymbol{p}}_\nu^v$ denotes the maximum active power injection that is obtained by the solar forecast. We assume the solar power generation can be forecasted when designing the algorithm. The curtailment cost occurs when solar PVs generate more electricity than the electricity demand, which can lead to financial losses. To minimize the curtailment cost, the solar PV's objective is formulated as follows [26]:

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

C. Energy Storage System

Let $\mathcal{S}$ denote the set of ESSs. The charging/discharging power $\hat{\boldsymbol{p}}_\sigma\in\mathbb{R}^T$ of the σth ESS is constrained by:

$$-\underline{\boldsymbol{p}}_\sigma^s\le\hat{\boldsymbol{p}}_\sigma\le\overline{\boldsymbol{p}}_\sigma^s, \quad (6)$$

where $\underline{\boldsymbol{p}}_\sigma^s$ and $\overline{\boldsymbol{p}}_\sigma^s$ denote the maximum discharging and charging power, respectively. Let s_σ^0 denote the initial state of charge (SoC) of the σth ESS and $\boldsymbol{H}_\sigma=[s_\sigma^0,\dots,s_\sigma^0]^\mathsf{T}\in\mathbb{R}^T$. By aggregating $\hat{\boldsymbol{p}}_\sigma$ across each time slot, the SoC of the σth ESS is constrained by:

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

where $\underline{\boldsymbol{p}}_\sigma^a$ and $\overline{\boldsymbol{p}}_\sigma^a$ denote its lower and upper capacity bounds, respectively, ΔT denotes the sampling time, and the aggregation matrix $\boldsymbol{A}$ is lower triangular consisting of only ones and zeros, i.e., element $A_{\hat{\imath},\hat{\jmath}}=1$ if $\hat{\imath}\ge\hat{\jmath}$, element $A_{\hat{\imath},\hat{\jmath}}=0$ if $\hat{\imath}<\hat{\jmath}$, $\hat{\imath},\hat{\jmath}=1,\dots,T$.

Furthermore, the ESS's degradation cost is minimized by reducing the fluctuations during charging and discharging, and decreasing the charging mode switch frequency through [27]:

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

where the matrix $\boldsymbol{B}$ calculates discharging and charging differences between adjacent times, i.e., element $B_{\hat{\imath},\hat{\imath}}=1$, $\hat{\imath}=1,\dots,T$, element $B_{\hat{\imath},\hat{\imath}+1}=-1,\hat{\imath}=1,\dots,T-1$, and all other elements of $\boldsymbol{B}$ are zeros.

III. Decentralized Optimization

A. Projected Gradient Method

The DER control in power distribution networks is formulated into a constrained optimization problem. Specifically, the objective function minimizes the active power loss, solar curtailment cost, and ESS degradation cost, while the constraints include the power flow limit and DERs' local constraints. The optimization problem is written into:

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

where $\boldsymbol{p}^g=[\boldsymbol{p}_1^{g\mathsf{T}},\dots,\boldsymbol{p}_n^{g\mathsf{T}}]^\mathsf{T}$, and δ_α denotes the constant cost coefficients that can adjust the weights on objective functions and regulate different units. Problem (**P1**) aims to exemplify a general coupled convex problem formulation that includes both objectives and constraints associated with power distribution networks and DERs. The integration of nonlinear and nonconvex components, such as discrete loads and nonlinear ESS dynamics, would require more theoretical tools. Gradient-based methods are widely used to solve (**P1**) by decomposing the centralized optimization problem into local optimizations at agents. We adopt the projected gradient method (PGM) to solve (**P1**) in a decentralized fashion where each agent owns a local feasible set for projection.

Let $\mathcal{M}=\{1,\dots,m\}$ denote the set of agents, e.g., aggregators or DERs, who work cooperatively to solve (**P1**). In this setting, the κth agent updates its decision variable $\boldsymbol{x}_\kappa$ using PGM by [28]:

$$\boldsymbol{x}_\kappa^{(\ell+1)}=\Pi_{\mathcal{X}_\kappa}\left(\boldsymbol{x}_\kappa^{(\ell)}-\gamma_\kappa^{(\ell)}\Phi_\kappa(\boldsymbol{x}^{(\ell)})\right), \quad (9)$$

where ℓ denotes the iteration number, $\boldsymbol{x}^{(\ell)}=[\boldsymbol{x}_1^{(\ell)\mathsf{T}},\dots,\boldsymbol{x}_m^{(\ell)\mathsf{T}}]^\mathsf{T}$ denotes the vector of all decision variables, i.e., $\tilde{\boldsymbol{p}}_\nu$ and $\hat{\boldsymbol{p}}_\sigma$ in (**P1**), $\gamma_\kappa^{(\ell)}$ denotes the primal step size, $\Phi_\kappa(\cdot)$ denotes the gradient of the Lagrangian *w.r.t.* $\boldsymbol{x}_\kappa^{(\ell)}$, and $\Pi_{\mathcal{X}_\kappa}(\cdot)$ denotes the projection operation onto set $\mathcal{X}_\kappa$.

The local constraints of the νth PV and the σth ESS can be represented by two feasible sets $\mathcal{P}_\nu^v$ and $\mathcal{P}_\sigma^e$, respectively:

$$\mathcal{P}_\nu^v\triangleq\{\tilde{\boldsymbol{p}}_\nu|\,(4)\}, \quad (10a)$$

$$\mathcal{P}_\sigma^e\triangleq\{\hat{\boldsymbol{p}}_\sigma|\,(6),(7)\}. \quad (10b)$$

B. DER Aggregation and Control Framework

In PGM, DER aggregation is mandatory because the ith agent needs to calculate $\Phi_i(\boldsymbol{x}^\ell)$ in (9) where the decision variables contain $\boldsymbol{x}_i$'s from all other agents. When DER acts as an independent agent, regarded as *self-governed control* (SGC), it receives all decision variables of other DERs to execute the PGM updates in a distributed way. SGC is more suitable for small-scale networks and can suffer from massive data exchange due to the numerous DERs in large-scale distribution networks.

In contrast, DERs' decision variables can be updated via *bus-delegated aggregation and control* (BDAC) by aggregators in a decentralized way based on the distribution network

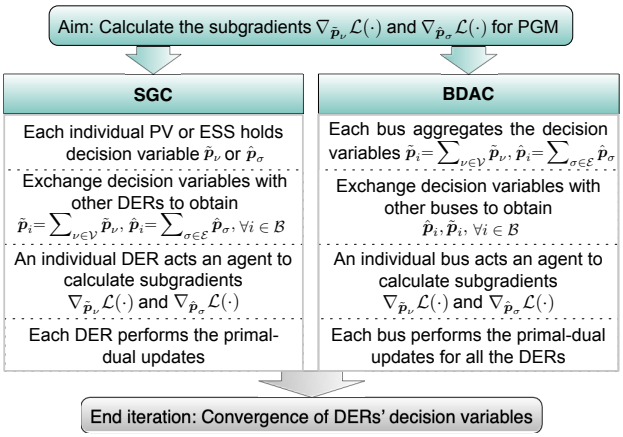


Fig. 2: Aggregation and control of DERs via DER-governed and bus-delegated architectures.

Despite the realization of scalability, both SGC and BDAC methods suffer from privacy breaches in information exchange, i.e., the exposure of DERs' decision variables that can reveal sensitive business information and customers' daily routines [29], [30]. To eliminate the privacy concern, we first design a decentralized DER optimization scheme within the BDAC framework. Then, a novel SS-based algorithm will be synthesized with cloud computing to achieve privacy-preserving information exchange. Apart from PGM, the proposed privacy preservation technique can also handle asynchronous multiple-step approaches [7], [31], and can be extended to other gradient-based methods such as the regularized primal-dual subgradient [32] and multi-objective learning [33].

The aggregated active power injection $\boldsymbol{p}_i$ at the ith bus can be obtained by an aggregator as:

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

where $\mathcal{V}_i$ and $\mathcal{E}_i$ denote the sets of PVs and ESSs connected at bus i, respectively, $\tilde{\boldsymbol{p}}_i = \sum_{\nu\in\mathcal{V}_i}\tilde{\boldsymbol{p}}_\nu$ and $\hat{\boldsymbol{p}}_i = \sum_{\sigma\in\mathcal{E}_i}\hat{\boldsymbol{p}}_\sigma$ denote the aggregated active power of all PVs and ESSs at bus i, respectively.

By aggregating the active power generation and consumption of each bus according to BDAC, problem (**P1**) can be written into a compact form of:

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

where $\tilde{\boldsymbol{p}} = [\tilde{\boldsymbol{p}}_1^\mathsf{T},\dots,\tilde{\boldsymbol{p}}_n^\mathsf{T}]^\mathsf{T}$, $\hat{\boldsymbol{p}} = [\hat{\boldsymbol{p}}_1^\mathsf{T},\dots,\hat{\boldsymbol{p}}_n^\mathsf{T}]^\mathsf{T}$, $\tilde{\boldsymbol{P}}\in\mathbb{R}^{nT}$ denotes the augmented active power generation and $\tilde{\boldsymbol{Z}}\in\mathbb{R}^{nT\times nT}$ denotes the augmented adjacency matrix. While only power flow limits are included as global constraints to avoid over-complicating the problem formulation, integrating additional global constraints, e.g., voltage bounds, can be readily achieved without affecting the algorithm design.

The detailed formulation of (**P2**) based on the network topology can be found in APPENDIX I.

The optimization problem in (**P2**) seeks to find the optimal decision variables, i.e., charging and discharging power $\tilde{\boldsymbol{p}}_\sigma$'s of the ESSs and the active power injection $\hat{\boldsymbol{p}}_\nu$'s of the PVs. In what follows, we focus on solving (**P2**) in a decentralized fashion. The relaxed Lagrangian of (**P2**) is:

$$\begin{aligned}&\mathcal{I}(\tilde{\boldsymbol{p}},\hat{\boldsymbol{p}},\boldsymbol{\mu}_l,\boldsymbol{\mu}_u)\\ &\quad=\delta_1 f_1(\boldsymbol{p}^g)+\sum_{i\in\mathcal{B}}\Big(\sum_{\nu\in\mathcal{V}_i}\delta_2 f_2(\tilde{\boldsymbol{p}}_\nu)+\sum_{\sigma\in\mathcal{E}_i}\delta_3 f_3(\hat{\boldsymbol{p}}_\sigma)\Big)\\ &\qquad+\sum_{\iota\in\mathcal{I}}\Big(\boldsymbol{\mu}_{u\iota}^\mathsf{T}(\tilde{\boldsymbol{Z}}_\iota\tilde{\boldsymbol{P}}-\overline{\boldsymbol{P}}_\iota)-\boldsymbol{\mu}_{l\iota}^\mathsf{T}\tilde{\boldsymbol{Z}}_\iota\tilde{\boldsymbol{P}}\Big),\end{aligned}\tag{12}$$

where $\boldsymbol{\mu}_l = [\boldsymbol{\mu}_{l1}^\mathsf{T},\dots,\boldsymbol{\mu}_{lL}^\mathsf{T}]^\mathsf{T}$ and $\boldsymbol{\mu}_u = [\boldsymbol{\mu}_{u1}^\mathsf{T},\dots,\boldsymbol{\mu}_{uL}^\mathsf{T}]^\mathsf{T}$, $\boldsymbol{\mu}_{l\iota}$ and $\boldsymbol{\mu}_{u\iota}$ denote the dual variables associated with lower and upper power flow limits of the ιth line, respectively.

Without loss of generality, suppose the νth PV and σth ESS are connected at bus i. Take the subgradients of (12) *w.r.t.* the primal variables $\tilde{\boldsymbol{p}}_\nu$ and $\hat{\boldsymbol{p}}_\sigma$, respectively, we have:

$$\begin{aligned}\nabla_{\tilde{\boldsymbol{p}}_\nu}\mathcal{L}(\cdot)=&\,2\delta_2(\tilde{\boldsymbol{p}}_\nu-\overline{\boldsymbol{p}}_\nu^v)+\frac{2\delta_1}{V_0^2}\sum_{\iota\in\mathcal{I}}r_\iota(\tilde{\boldsymbol{Z}}_\iota\boldsymbol{\Delta}_i)^\mathsf{T}(\tilde{\boldsymbol{Z}}_\iota\tilde{\boldsymbol{P}})\\ &+\sum_{\iota\in\mathcal{I}}(\tilde{\boldsymbol{Z}}_\iota\boldsymbol{\Delta}_i)^\mathsf{T}(\boldsymbol{\mu}_{u\iota}-\boldsymbol{\mu}_{l\iota}),\end{aligned}\tag{13a}$$

$$\begin{aligned}\nabla_{\hat{\boldsymbol{p}}_\sigma}\mathcal{L}(\cdot)=&\,2\delta_3\hat{\boldsymbol{p}}_\sigma-\frac{2\delta_1}{V_0^2}\sum_{\iota\in\mathcal{I}}r_\iota(\tilde{\boldsymbol{Z}}_\iota\boldsymbol{\Delta}_i)^\mathsf{T}(\tilde{\boldsymbol{Z}}_\iota\tilde{\boldsymbol{P}})\\ &-\sum_{\iota\in\mathcal{I}}(\tilde{\boldsymbol{Z}}_\iota\boldsymbol{\Delta}_i)^\mathsf{T}(\boldsymbol{\mu}_{u\iota}-\boldsymbol{\mu}_{l\iota}).\end{aligned}\tag{13b}$$

For the simplicity of presentation, we further assume all power lines have the same resistance $\bar{r}$, herein (13) becomes:

$$\nabla_{\tilde{\boldsymbol{p}}_\nu}\mathcal{L}(\cdot)=2\delta_2(\tilde{\boldsymbol{p}}_\nu-\overline{\boldsymbol{p}}_\nu^v)+\bar{\delta}_1\boldsymbol{\pi}_i\tilde{\boldsymbol{P}}+\boldsymbol{\psi}_i(\boldsymbol{\mu}_u-\boldsymbol{\mu}_l),\tag{14a}$$

$$\nabla_{\hat{\boldsymbol{p}}_\sigma}\mathcal{L}(\cdot)=2\delta_3\hat{\boldsymbol{p}}_\sigma-\bar{\delta}_1\boldsymbol{\pi}_i\tilde{\boldsymbol{P}}-\boldsymbol{\psi}_i(\boldsymbol{\mu}_u-\boldsymbol{\mu}_l),\tag{14b}$$

where $\bar{\delta}_1=\frac{2\delta_1}{V_0^2}\bar{r}$, $\boldsymbol{\pi}_i=\sum_{\iota\in\mathcal{I}}(\tilde{\boldsymbol{Z}}_\iota\boldsymbol{\Delta}_i)^\mathsf{T}\tilde{\boldsymbol{Z}}_\iota$, and $\boldsymbol{\psi}_i$ denotes the ith column block of $\tilde{\boldsymbol{Z}}$.

Therefore, with the subgradients in (13), the νth PV and the σth ESS update their decision variables by:

$$\tilde{\boldsymbol{p}}_\nu^{(\ell+1)}=\Pi_{\mathcal{P}_\nu^v}\left(\tilde{\boldsymbol{p}}_\nu^{(\ell)}-\gamma_{\nu,\ell}^v\nabla_{\tilde{\boldsymbol{p}}_\nu}\mathcal{L}^{(\ell)}(\cdot)\right),\tag{15a}$$

$$\hat{\boldsymbol{p}}_\sigma^{(\ell+1)}=\Pi_{\mathcal{P}_\sigma^e}\left(\hat{\boldsymbol{p}}_\sigma^{(\ell)}-\gamma_{\sigma,\ell}^e\nabla_{\hat{\boldsymbol{p}}_\sigma}\mathcal{L}^{(\ell)}(\cdot)\right),\tag{15b}$$

where $\gamma_{\nu,\ell}^v$ and $\gamma_{\sigma,\ell}^e$ denote the primal step sizes of the νth PV and the σth ESS, respectively, $\mathcal{L}^{(\ell)}(\cdot)$ denotes the Lagrangian function at the ℓth iteration.

As indicated in (14), calculating subgradients $\nabla_{\tilde{\boldsymbol{p}}_\nu}\mathcal{L}(\cdot)$ and $\nabla_{\hat{\boldsymbol{p}}_\sigma}\mathcal{L}(\cdot)$ indeed requires the decision variables $\tilde{\boldsymbol{P}}$ from all the buses. Specifically, the calculation of subgradients in (14a) and (14b) are coupled through:

$$\mathcal{D}_i=\underbrace{\bar{\delta}_1\boldsymbol{\pi}_i\tilde{\boldsymbol{P}}}_{\text{primal variables}}+\underbrace{\boldsymbol{\psi}_i(\boldsymbol{\mu}_u-\boldsymbol{\mu}_l)}_{\text{dual variables}}.\tag{16}$$

For example, suppose PV $\hat{\nu}$ is connected at bus 2, then its primal update is coupled through $\bar{\delta}_1 \boldsymbol{\pi}_2 \tilde{\boldsymbol{P}} = \sum_{i=1}^{n} \boldsymbol{p}_i + \boldsymbol{p}_2 + \boldsymbol{p}_3$ that contains the active power generations $\boldsymbol{p}_i, i \in \mathcal{B}$ from all buses. The dual variables simply represent penalties for the violation of constraints. Therefore, the update of PV $\hat{\nu}$ requires the decision variables of all other DERs in the distribution network. By adopting the developed BDAC structure, only bus-to-bus communications are required, leading to reduced computing and communicating costs for local controllers. Finally, the $\hat{\nu}$th PV can update $\tilde{\boldsymbol{p}}_{\hat{\nu}}$ using (15a). This paper spearheads the transition of plaintext optimization to the secret space, focusing on basic subgradient calculations, i.e., only addition and multiplication. It sets the groundwork for exploring more complex gradient computations, such as projection, set operators, and other intricate operators that do not rely on addition and multiplication.

The detailed derivation of the PGM updates for BDAC can be found in the APPENDIX II.

IV. SS-BASED PRIVACY-PRESERVING DER CONTROL

A. Real Number to Integer Quantization

Note that the SS scheme requires integer arithmetic instead of real arithmetic. However, decentralized optimization genetically involves real number calculations, including decision variables and regulation parameters. Therefore, a real number to integer transformation is needed to integrate SS into decentralized optimization. We adopt the fixed-point number quantization [34] to map the real numbers onto the integer space. The fixed-point real-number set is defined as:

$$\mathcal{Q}_{\theta,\gamma,\zeta} = \left\{ -\theta^{\gamma}, -\theta^{\gamma} + \theta^{-\zeta}, \ldots, \theta^{\gamma} - 2\theta^{-\zeta}, \theta^{\gamma} - \theta^{-\zeta} \right\}, \tag{17}$$

where $\theta \in \mathbb{N}_{1+}$ denotes the basis, $\gamma \in \mathbb{N}$ denotes the magnitude, and $\zeta \in \mathbb{N}$ denotes the resolution. Therefore, by defining a surjective mapping $m(\cdot) : \mathbb{R} \mapsto \mathcal{Q}_{\theta,\gamma,\zeta}$, a real number can be mapped to the closest point in $\mathcal{Q}_{\theta,\gamma,\zeta}$. To limit the quantization error, the mapping $m(\cdot)$ needs to satisfy:

$$|\check{\varphi} - \varphi| \leq \theta^{-\zeta}, \forall \varphi \in [-\theta^{\gamma}, \theta^{\gamma}], \tag{18}$$

where $\check{\varphi} = m(\varphi)$ and the quantization error is restricted by the resolution within the range of $\mathcal{Q}_{\theta,\gamma,\zeta}$.

To map the real-number set onto the integer set $\mathcal{Z}$, $\mathcal{Q}_{\theta,\gamma,\zeta}$ is scaled by θ^{ζ} as:

$$\mathcal{Z}_{\theta,\gamma,\zeta} = \left\{ -\theta^{\gamma+\zeta}, -\theta^{\gamma+\zeta}+1, \ldots, \theta^{\gamma+\zeta}-1 \right\}, \tag{19}$$

where $\mathcal{Z}_{\theta,\gamma,\zeta} \subseteq \mathcal{Z}$ denotes the fixed-point set in the integer field. Moreover, SS requires the inputs to be within the field $\mathbb{E} \triangleq [0, e)$ where e denotes a prime number. We further map the elements in $\mathcal{Z}_{\theta,\gamma,\zeta}$ onto $\mathbb{E}$ by the modular operation:

$$\hat{z} = z \bmod e. \tag{20}$$

Note that $z \in \mathcal{Z}_{\theta,\gamma,\zeta}$ can be any negative integer, and the modular operation in (20) will change the sign of a negative input, i.e., $g(z^-) = z^- + e, \forall z^- < 0$. To address the negative integer operation, we introduce the partial inverse of $g(\cdot)$ as

$$\psi(\hat{z}) = \begin{cases} \hat{z} - e & \text{if } z \geq \frac{e}{2}, \\ \hat{z} & \text{otherwise.} \end{cases} \tag{21}$$

Therefore, we have $z = \psi(\hat{z}), \forall \hat{z} \in \mathbb{E}$.

Since the quantization error can be made arbitrarily small, the algorithm convergence can always be guaranteed by reducing the quantization error at the cost of computational load. Therefore, the optimality of the proposed privacy-preserving algorithm is preserved under the additional SS-based privacy preservation measures. This property is given by Theorem 2 and Proposition 1.

B. SS-based Privacy-Preserving Algorithm

1) Shamir's secret sharing scheme: Before introducing the privacy-preserving algorithm design, we first briefly introduce Shamir's SS scheme [22]. Shamir's SS has an efficient and lightweight private information distribution structure. Suppose a secret holder (manager) seeks to distribute a secret ω to certain agents and requires the cooperation of at least d agents to retrieve the secret. In such needs, Shamir's SS is grounded on the following Lagrange interpolation theory:

Theorem 1 (*Polynomial interpolation* [35]). Let $\{(\varsigma_1, y_1), \ldots, (\varsigma_d, y_d)\} \subseteq \mathbb{R}^2$ be a set of points whose values of $\varsigma_{\hat{\imath}}$, $\hat{\imath} = 1, \ldots, d$ are all distinct. Then there exists a unique polynomial F of degree $d-1$ that satisfies $y_{\hat{\imath}} = F(\varsigma_{\hat{\imath}})$. ■

In SS-based schemes, the manager first constructs a random polynomial of degree $d-1$ as:

$$y(z) = \omega + a_1 z + \cdots + a_{d-1} z^{d-1}, \tag{22}$$

where ω denotes an integer secret, $a_1, \ldots, a_{d-1}$ denote random coefficients that are uniformly distributed in the field $\mathbb{E} \triangleq [0, e)$, and e denotes a prime number that is larger than both ω and z. Secondly, the manager calculates the outputs of (22) using non-zero integer inputs, e.g., setting $\tau = 1, \ldots, n$ to retrieve $(\tau, y(\tau))$. Then the manager distributes the share $y(\tau)$ to the τth agent. According to Theorem 1, at least d agents with d shares can reconstruct (22). Therefore, the secret can be retrieved by:

$$\omega = \sum_{\tau=1}^{d} y(\tau) \prod_{\substack{\upsilon=0 \\ \upsilon \neq \tau}}^{d} \frac{\upsilon}{\upsilon - \tau}. \tag{23}$$

2) Proposed privacy-preserving DER control algorithm: We next propose a hierarchical privacy-preserving DER control framework as shown in Fig. 3. In this framework, 1) the power grid operation center monitors the overall grid statuses, service provision, and grid operational constraints; 2) The aggregators aggregate and control one or more DER clusters or directly controlling customer-side DERs; and 3) the DER control platform coordinates the private DER data transmission between the aggregators in a privacy-preserving fashion.

The developed hierarchical DER control framework achieves scalability by enabling decentralized optimization of DER clusters and ensures the integratability of privacy preservation techniques for computing DER data. In the aforementioned framework, both SGC and BDAC schemes can be utilized to aggregate and control the DERs' decision variables. We next present the detailed procedures for integrating SS into the proposed privacy-preserving DER control framework via BDAC.

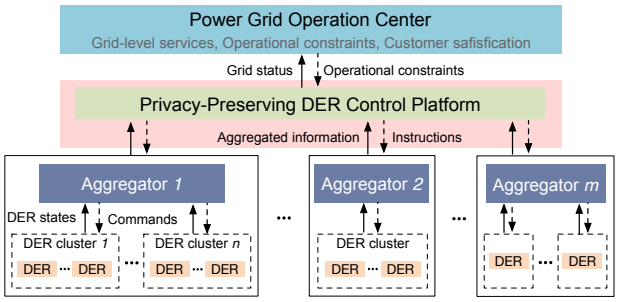


Fig. 3: Privacy-preserving DER control in a hierarchical framework.

Assumption 1. The cloud computing platform has access to the network topology. □

The network topology can be described by an adjacency matrix $\boldsymbol{Z}$ that contains no private information about the DERs. Details of $\boldsymbol{Z}$ can be found in the APPENDIX I.

Let $\mathcal{C}$ denote the set of clouds and $c \geq 2$ denote the cloud number. Each bus is delegated by an aggregator to control the DERs connected to it. Note that it is equally applicable for a single aggregator to oversee a group of buses. The computing and communication between aggregators are powered by cloud servers. For the ith bus, an aggregator is responsible for obfuscating its private input by generating a random polynomial of order $d-1$ as:

$$y_i^{(\ell)}(z) = \check{p}_i^{(\ell)}(t) + a_{i,1}^{(\ell)} z + \cdots + a_{i,d-1}^{(\ell)} z^{d-1}, \tag{24}$$

where $2 \leq d \leq c$, $\check{p}_i^{(\ell)}(t)$ denotes the active power injection at bus i after the real-to-integer transformation and $a_{i,1}^{(\ell)}, \ldots, a_{i,d-1}^{(\ell)}$ denote random coefficients. Note that for any real vector secret, such as $\boldsymbol{p}_i$, the real-to-integer transformation can be performed elementwisely.

At the ℓth iteration, the uth cloud firstly generates a random integer $\alpha_u^{(\ell)}$ that contains no private information of the DERs, then it broadcasts $\alpha_u^{(\ell)}$ to all the buses. Subsequently, the buses adopt $\alpha_u^{(\ell)}$, $u = 1, \ldots, c$ as random inputs of its polynomial. Therefore, the ith bus can generate shares of $y_i^{(\ell)}(\alpha_u^{(\ell)})$, $u = 1, \ldots, c$. Note that the coupling term $\boldsymbol{\pi}_i \tilde{\boldsymbol{P}}$ in (16) is a linear combination of $\boldsymbol{p}_i$'s that requires the private power generation and consumption data from DERs at all buses. Therefore, a secure computing framework for $\boldsymbol{\pi}_i \tilde{\boldsymbol{P}}$'s is required to preserve the privacy of buses and DER owners.

To achieve privacy preservation, each bus first sends $y_i^{(\ell)}(\alpha_u^{(\ell)})$ to the uth cloud. Consequently, the uth cloud receives $y_i^{(\ell)}(\alpha_u^{(\ell)})$, $i \in \mathcal{B}$. Then the uth cloud multiplies the received outputs $y_i^{(\ell)}(\alpha_u^{(\ell)})$, $i \in \mathcal{B}$, utilizing the coefficients of $\boldsymbol{\pi}_i$ to obtain a new set of outputs:

$$\left\{ \pi_i(1) y_1^{(\ell)}(\alpha_u^{(\ell)}), \ldots, \pi_i(n) y_n^{(\ell)}(\alpha_u^{(\ell)}) \right\}. \tag{25}$$

Accordingly, the uth cloud can obtain a new input-output pair for the ith bus as:

$$\bar{\mathcal{A}}_{u,i} = \left\{ \alpha_u^{(\ell)}, \sum_{\hat{\imath}=1}^{n} \pi_i(\hat{\imath})\, y_{\hat{\imath}}^{(\ell)}(\alpha_u^{(\ell)}) \right\}. \tag{26}$$

Finally, the uth cloud sends the new input-output share $\bar{\mathcal{A}}_{u,i}$ back to the ith bus. As a result, after receiving $\bar{\mathcal{A}}_{u,i}$'s from in total c clouds servers, the ith bus now has access to:

$$\tilde{\mathcal{A}}_i = \left\{ \alpha_{\hat{\jmath}}^{(\ell)}, \sum_{\hat{\imath}=1}^{n} \pi_i(\hat{\imath})\, y_{\hat{\imath}}^{(\ell)}(\alpha_{\hat{\jmath}}^{(\ell)}), \hat{\jmath} \in \mathcal{C} \right\}, \tag{27}$$

indicating that all clouds' output data has been aggregated for the ith bus.

Lastly, a total of c shares are contained in $\tilde{\mathcal{A}}_i$, which can be used to construct a new polynomial of the form:

$$\tilde{y}_i^{(\ell)}(z) = \pi_i \tilde{P}(t) + \tilde{a}_{i,1}^{(\ell)} z + \cdots + \tilde{a}_{i,d-1}^{(\ell)} z^{d-1}, \tag{28}$$

whose constant term is exactly the aggregated decision variables. The ith bus is thus ready to perform primal updates.

The information exchange structure of the proposed privacy-preserving DER control framework via BDAC is shown in Fig. 4. In the proposed structure, the ith bus can only access

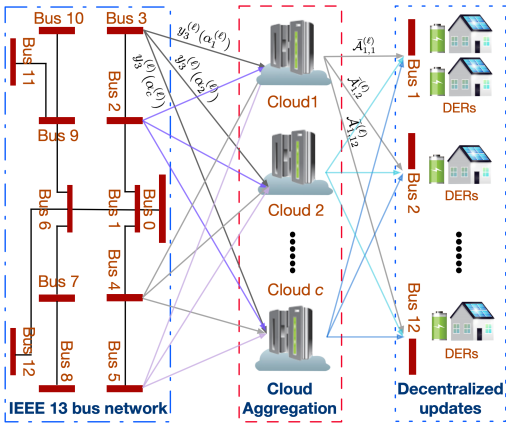


Fig. 4: Information exchange structure for BDAC using cloud servers (messages sent from bus 3 and cloud 1 are labeled).

DERs that are within its jurisdiction, e.g., decision variables of connected DERs. The uth cloud only receives a single share of each bus so it is incapable of reconstructing the secret solely based on the received shares. Therefore, the multi-server information exchange structure allows the privacy-preserving generation, aggregation, and broadcasting of shares for all buses. The secret retrieval process distributes the aggregation task to multiple clouds to ensure that a single cloud cannot retrieve any secrets. The detailed procedures of the proposed method are presented via Algorithm 1.

Algorithm 1 can achieve privacy preservation while maintaining exact solutions as non-privacy PGM-based methods. The decision variables will be continuously updated till the convergence errors $\epsilon_\nu^{(\ell)} \triangleq \|\tilde{\boldsymbol{p}}_\nu^{(\ell)} - \tilde{\boldsymbol{p}}_\nu^{(\ell-1)}\|_2^2$ and $\epsilon_\sigma^{(\ell)} \triangleq \|\hat{\boldsymbol{p}}_\sigma^{(\ell)} - \hat{\boldsymbol{p}}_\sigma^{(\ell-1)}\|_2^2$ are smaller than the threshold ϵ_0. The correctness of Algorithm 1 is presented by the following theorem.

Theorem 2 (*Correctness*). Let $\mathbb{E}$ denote the domain of the input secrets $\hat{\omega}_1, \ldots, \hat{\omega}_n$, and $\mathcal{O}_i$ denote the desired outputs. Then, Algorithm 1 satisfies:

$$\Pr\left[\forall c \geq d, \mathrm{Rec}\left(\mathcal{A}, \mathbb{E}, \boldsymbol{Z}, \bar{\delta}_1, \theta, \gamma, \zeta\right) = \mathcal{O}_i\right] = 1, \tag{29}$$

where $\mathcal{A} = \{\tilde{\mathcal{A}}_1, \ldots, \tilde{\mathcal{A}}_c\}$ denotes the set of shares from agents, $\Pr[\cdot]$ denotes probability, and $\mathrm{Rec}(\cdot)$ denotes the secret reconstruction operation. ■

Proof: To prove the correctness, we show that the proposed method has the exact primal solutions as the non-privacy PGM.

Algorithm 1 Decentralized privacy-preserving DER control via BDAC.

1: Agents initialize decision variables, basis θ, magnitude γ, resolution ζ, tolerance ϵ_0, iteration counter $\ell = 0$, and maximum iteration ℓ_{max}.
2: **while** $\epsilon_{\nu(\sigma)}^{(\ell)} > \epsilon_0$ and $\ell < \ell_{max}$ **do**
3: Each bus performs real-to-integer transformation using (17)-(20), then obtains the integer secret $\hat{\omega}_i^{(\ell)}$.
4: The uth cloud generates a random integer $\alpha_u^{(\ell)}$, then it broadcasts $\alpha_u^{(\ell)}$ to all the buses.
5: The ith bus generates a random polynomials $y_i^{(\ell)}(z)$, with $\hat{\omega}_i^{(\ell)}$ as the constant term.
6: Each bus calculates the polynomial outputs using $\alpha_1^{(\ell)}$, $\ldots$, $\alpha_c^{(\ell)}$ to obtain $\hat{y}_i^{(\ell)}(\alpha_1^{(\ell)})$, $\ldots$, $\hat{y}_i^{(\ell)}(\alpha_c^{(\ell)})$, then sends $\hat{y}_i^{(\ell)}(\alpha_u^{(\ell)})$ to the uth cloud.
7: The uth cloud forms $\bar{\mathcal{A}}_{u,i}^{(\ell)}$ and sends it to the ith bus.
8: The ith bus formulates $\tilde{\mathcal{A}}_i^{(\ell)}$, then reconstructs the aggregated secret using c shares to obtain $\boldsymbol{\pi}_i \tilde{\boldsymbol{P}}^{(\ell)}$, finally obtains $\mathcal{O}_i^{(\ell)}$ in (16).
9: The ith bus transforms $\mathcal{O}_i^{(\ell)}$ back to real numbers using (21), then updates decision variables $\tilde{\boldsymbol{p}}_\nu^{(\ell)}$ and $\hat{\boldsymbol{p}}_\sigma^{(\ell)}$ by PGM.
10: Calculate the convergence errors $\epsilon_\nu^{(\ell)}$ and $\epsilon_\sigma^{(\ell)}$.
11: $\ell = \ell + 1$.
12: **end while**

Recall that the uth cloud multiplies the received n outputs by the elements of $\boldsymbol{\pi}_i$ according to (25), it yields:

$$\begin{cases} \pi_i(1) y_1^{(\ell)}(\alpha_u^{(\ell)}) = \pi_i(1)\left(\breve{p}_1^{(\ell)}(t) + \sum_{\hat{\jmath}=1}^{d-1} a_{1,\hat{\jmath}}^{(\ell)} {\alpha_u^{(\ell)}}^{\hat{\jmath}}\right), \\ \qquad\qquad \vdots \\ \pi_i(n) y_n^{(\ell)}(\alpha_u^{(\ell)}) = \pi_i(n)\left(\breve{p}_n^{(\ell)}(t) + \sum_{\hat{\jmath}=1}^{d-1} a_{n,\hat{\jmath}}^{(\ell)} {\alpha_u^{(\ell)}}^{\hat{\jmath}}\right). \end{cases} \tag{30}$$

By summing the left hand side of (30), the aggregated outputs $\sum_{\hat{\imath}=1}^{n} \pi_i(\hat{\imath}) y_{\hat{\imath}}^{(\ell)}(\alpha_u^{(\ell)})$ in (25) can be readily obtained. Therefore, in total c pairs of shares from all clouds as in (26) can be seen as the input-output pairs of a polynomial:

$$\tilde{y}^{(\ell)}(z) = \sum_{\hat{\imath}=1}^{n} \pi_i(\hat{\imath}) \hat{\omega}_{\hat{\imath}}^{(\ell)} + \tilde{a}_1^{(\ell)} z + \cdots + \tilde{a}_{d-1}^{(\ell)} z^{d-1}, \tag{31}$$

where $\tilde{a}_{\hat{\jmath}}^{(\ell)} = \sum_{\hat{\imath}=1}^{n} \pi_i(\hat{\imath}) a_{\hat{\imath},\hat{\jmath}}^{(\ell)}$, $\hat{\jmath} = 1, \ldots, d-1$ and $\sum_{\hat{\imath}=1}^{n} \pi_i(\hat{\imath}) \hat{\omega}_{\hat{\imath}}^{(\ell)}$ is exactly $\boldsymbol{\pi}_i \tilde{\boldsymbol{P}}^{(\ell)}$. Therefore, the aggregated secret $\boldsymbol{\pi}_i \tilde{\boldsymbol{P}}^{(\ell)}$ can be retrieved by using c pairs of shares since $d \le c$, as stated by Theorem 1. □

Proposition 1 (*Quantization error*): Let $\theta \in \mathbb{N}_{1+}$, $\gamma \in \mathbb{N}$, and $\zeta \in \mathbb{N}$. The quantization error for the aggregation of $\bar{\delta}_1 \pi_i \tilde{P}^{(\ell)}(t)$ is bounded by $\bar{\delta}_1 \sum_{\hat{\imath}=1}^{n} \pi_i(\hat{\imath}) \theta^{-\zeta}$. ■

Proof: For the $\hat{\imath}$th secret $w_{\hat{\imath}}^{(\ell)}$, its quantization error is bounded by $|\breve{w}_{\hat{\imath}}^{(\ell)} - w_{\hat{\imath}}^{(\ell)}| \le \theta^{-\zeta}$. Following the proof of Theorem 2, the quantization error during the DER aggregation is $\bar{\delta}_1 \sum_{\hat{\imath}=1}^{n} \pi_i(\hat{\imath})(\breve{w}_{\hat{\imath}}^{(\ell)} - w_{\hat{\imath}}^{(\ell)})$, where $\bar{\delta}_1 > 0$ and $\pi_i(\hat{\imath}) \ge 0$. Therefore, the quantization error for aggregation of $\bar{\delta}_1 \pi_i \tilde{P}^{(\ell)}(t)$ is bounded by $\bar{\delta}_1 \sum_{\hat{\imath}=1}^{n} \pi_i(\hat{\imath}) \theta^{-\zeta}$. □

Remark 1. The scalability of Algorithm 1 is achieved in three key aspects. First, the scalability of PGM enables paralleled computing between agents. The developed privacy preservation technique is a fundamental tool that can be easily extended to other scalable algorithms [31]–[33]. Second, the scalability is largely enhanced by the lightweight SS architecture, which leads to major improvements in algorithm computing and communication efficiency. Third, the overall structure-wise scalability. Depending on the application scale, DERs can also be clustered by household or district units in the framework of SGC. In such scenarios, Algorithm 1 can adapt to assign each local cluster with one or more DERs as an autonomous aggregator, i.e., generating, distributing, and computing on shares independently. □

C. Privacy Analysis

Algorithm 1 preserves the private decision variables of DERs against both internal and external stealthy adversaries who aim to infer private data using only the messages transmitted during the algorithm's iterations. Specifically, Algorithm 1 achieves privacy preservation against two types of adversaries, including *honest-but-curious agent* who follows the algorithm but may utilize the possessed and received data to infer the private information of other agents, and *external eavesdroppers* who wiretap and intercept exchanged messages from communication channels. The developed SS-based privacy-preserving algorithm can achieve the same security level against both internal and external adversaries considered in the state-of-the-art SMC schemes [16]–[18], [23]. Admittedly, other attack vectors, e.g., direct invasion into the smart meters, can also obtain customers' sensitive information. However, we'd like to note that our paper aims to handle stealthy attack vectors with minimal intrusions from a secure computing perspective. The direct invasion is not considered stealthy as their footprint is more obvious.

Proposition 2. (*Secure cloud computing*). Any group of clouds with a number less than d cannot infer any information of the aggregated decision variables $\mathcal{D}_i$. ■

Proposition 2 shows the privacy preservation of the proposed algorithm against corrupted clouds. Note that cloud servers can be provided by single or multiple vendors, but the collaboration of at least d clouds is required to retrieve any secret. A brief proof of Proposition 2 is given as follows.

Proof: Under the collusion, $d-1$ clouds can construct the following set of equations:

$$\begin{cases} \tilde{y}_i(\alpha_1) = \tilde{\omega} + \tilde{a}_{i,1}\alpha_1 + \cdots + \tilde{a}_{i,d-1}\alpha_1^{d-1}, \\ \qquad\qquad \vdots \\ \tilde{y}_i(\alpha_{d-1}) = \tilde{\omega} + \tilde{a}_{i,1}\alpha_{d-1} + \cdots + \tilde{a}_{i,d-1}\alpha_{d-1}^{d-1}, \end{cases} \tag{32}$$

where $\tilde{y}_i(z)$ is defined in (28) and $\tilde{\omega} = \pi_i \tilde{P}(t)$. In (32), $\tilde{a}_{i,\hat{\imath}}$, $\hat{\imath} = 1, \ldots, d-1$ and $\tilde{\omega}$ are unknown. Consequently, $d-1$ clouds can yield in total $d-1$ equations yet d unknowns that lead to underdetermined solutions. Therefore, at least d clouds are required to retrieve an aggregated secret. □

Assumption 2. During a single iteration, at least one communication link of an individual bus is safe from external eavesdroppers. □

Assumption 2 is essential and generically used in SS-based schemes. Given d pairs of shares sent via different communication links, i.e., $\{(\varsigma_1, y_1), \ldots, (\varsigma_d, y_d)\} \subseteq \mathbb{R}^2$, if an external eavesdropper wiretaps all communication links to gain access to all the shares, then the secret can simply be deduced by the Lagrangian interpolation.

Theorem 3 (*Privacy preservation against adversaries*). Algorithm 1 securely computes the decision variables between buses in the presence of honest-but-curious buses. Under Assumption 2, external eavesdroppers learn no private information about the buses. ■

The privacy preservation of Algorithm 1 can be proved from the SMC perspective.

Definition 1 (*Computational indistinguishability* [36]). Let $\{D_\varkappa\}_{\varkappa\in\mathbb{N}}$ and $\{E_\varkappa\}_{\varkappa\in\mathbb{N}}$ be two distribution ensembles with security parameter $\varkappa$. If for any non-uniform probabilistic polynomial-time algorithm $\mathcal{G}(\cdot)$, there exists a negligible function $\delta(\varkappa)$ such that for every $\varkappa \in \mathbb{N}$,

$$\left| \Pr_{x\leftarrow D_\varkappa}[\mathcal{G}(x)=1] - \Pr_{x\leftarrow E_\varkappa}[\mathcal{G}(x)=1] \right| \leq \delta(\varkappa), \tag{33}$$

where $\leftarrow$ denotes the sampling operation. We say that $\{D_\varkappa\}_{\varkappa\in\mathbb{N}}$ and $\{E_\varkappa\}_{\varkappa\in\mathbb{N}}$ are computationally indistinguishable, denoted as $D_\varkappa \overset{c}{\equiv} E_\varkappa$. ■

Definition 1 states that any polynomial-time algorithm cannot distinguish two computationally indistinguishable ensembles because the outputs of those algorithms do not significantly differ. That is, any non-uniform probabilistic polynomial-time algorithm cannot tell apart a sample from $D_\varkappa$ and $E_\varkappa$. Based on computational indistinguishability, Definition 2 presents the standard privacy notion of SMC.

Definition 2 (*SMC* [37], [38]). Let Π be an n-party protocol for computing the outputs of function $\Phi(\mathcal{X})$ where $\mathcal{X} = \{x_1, \ldots, x_n\}$ and $\mathcal{M} = \{m_1, \ldots, m_n\}$ denote the set of inputs and parties, respectively. Let $\Phi_\rho(\mathcal{X})$ denote the ρth output of $\Phi(\mathcal{X})$. The view of the ρth party during the execution of Π is denoted by $\text{VIEW}_\rho^\Pi(\mathcal{X})$. We say that Π privately computes $\Phi_\rho(\mathcal{X})$ if there exists a polynomial-time algorithm $\digamma$, such that for every party m_ρ in $\mathcal{M}$, we have

$$\digamma(\rho, x_\rho, \Phi_\rho(\mathcal{X})) \overset{c}{\equiv} \text{VIEW}_\rho^\Pi(\mathcal{X}). \tag{34}$$

■

Definition 2 states that the privacy of a n-party protocol can be evaluated based on computational indistinguishability, i.e., the view of any party can be efficiently simulated solely based on its inputs and outputs. In other words, SMC enables a set of participants to learn the correct outputs of an agreed-upon function applied to their private inputs without disclosing anything else. We next prove that Algorithm 1 securely computes $\boldsymbol{\pi}_1\tilde{\boldsymbol{P}}, \ldots, \boldsymbol{\pi}_n\tilde{\boldsymbol{P}}$ between the buses.

Proof: The privacy preservation of Algorithm 1 against an honest-but-curious bus is proven by showing that any messages an honest-but-curious bus receives can be efficiently simulated. Let $\mathcal{J} = \{j \mid j = 1, \ldots, c\}$ denote the index set of j, and $\mathcal{J}_{i^-} = \{j \mid j \in \mathcal{J}, j \neq i\}$ excludes the index i. We drop the index ℓ for clarity. Therefore, bus i has a view of:

$$\begin{aligned}\text{VIEW}_i^{\text{Alg1}} = \{&\alpha_1, \ldots, \alpha_c, \theta, \gamma, \zeta, \boldsymbol{\pi}_i\tilde{\boldsymbol{P}}, y_i(z), \boldsymbol{p}_i, \bar{\mathcal{A}}_i,\\ &\mathcal{O}_i, \tilde{y}_i(\alpha_j), j \in \mathcal{J}\}.\end{aligned} \tag{35}$$

Then it is required to prove the existence of a polynomial-time algorithm, denoted as the simulator $\digamma$, that can simulate $\text{VIEW}_i^{\text{Alg1}}$ from the standpoint of bus i, i.e.,

$$\digamma(\Xi_i) \overset{c}{\equiv} \text{VIEW}_i^{\text{Alg1}}, \tag{36}$$

where $\Xi_i \triangleq \{\alpha_1, \ldots, \alpha_c, \theta, \gamma, \zeta, \boldsymbol{\pi}_i\tilde{\boldsymbol{P}}, y_i(z), \boldsymbol{p}_i, \bar{\mathcal{A}}_i, \mathcal{O}_i, \tilde{y}_i(\alpha_j), j \in \mathcal{J}\}$ denotes the set of data that bus i has access to. Manifesting (36) shows that any message received by bus i can be efficiently reconstructed based on its own knowledge. The simulator only needs to generate $\tilde{y}_i'(\alpha_j)$'s that satisfy:

$$\tilde{y}_i'(\alpha_j) \overset{c}{\equiv} \tilde{y}_i(\alpha_j), \forall j \in \mathcal{J}. \tag{37}$$

To achieve this goal, the simulator firstly generates secrets $\boldsymbol{p}'_{j\in\mathcal{J}_{i^-}} \in \mathbb{E}$ of other buses such that:

$$\boldsymbol{\pi}_i\tilde{\boldsymbol{P}} = \boldsymbol{p}_i + \sum_{j\in\mathcal{J}_{i^-}} \boldsymbol{p}'_j. \tag{38}$$

Then it generates a set of random polynomials to obtain $y_j'(z)$, $j \in \mathcal{J}_{i^-}$ with $\boldsymbol{p}'_j$ as the corresponding constant terms by:

$$y_i(z) = p_i(t) + a_{i,1}z + \cdots + a_{i,d-1}z^{d-1}, j = i, \tag{39a}$$

$$y_j'(z) = p_j'(t) + a_{i,1}'z + \cdots + a_{i,d-1}'z^{d-1}, j \in \mathcal{J}_{i^-}. \tag{39b}$$

Consequently, the simulator can use $\{\alpha_1, \ldots, \alpha_c\}$ as inputs for (39) to obtain:

$$\tilde{\mathcal{A}}_i' = \left\{\alpha_{\hat{\jmath}}, y_i(\alpha_{\hat{\jmath}}) + \sum_{j\in\mathcal{J}_{i^-}} y_j'(\alpha_{\hat{\jmath}}), \hat{\jmath} \in \mathcal{J}\right\}. \tag{40}$$

Based on the correctness analysis from Theorem 2, $\tilde{\mathcal{A}}_i'$ is sufficient to construct a new polynomial of:

$$\tilde{y}_i'(x) = (\pi_i\tilde{P}(t))' + \tilde{a}_{i,1}'z + \cdots + \tilde{a}_{i,d-1}'z^{d-1}, \tag{41}$$

where $(\pi_i\tilde{P}(t))' = \pi_i\tilde{P}(t)$. Therefore, (36) is proved. Consequently, an honest-but-curious bus cannot retrieve any useful information from others using the received data, due to the indistinguishable data outputs. By Definition 2, Algorithm 1 securely computes $\boldsymbol{\pi}_1\tilde{\boldsymbol{P}}, \ldots, \boldsymbol{\pi}_n\tilde{\boldsymbol{P}}$ between the buses.

We next prove the privacy preservation of Algorithm 1 against external eavesdroppers. Under Assumption 2, assume the communications between Cloud 1 and all buses are safe from external eavesdroppers. By wiretapping any other communication channels, an external eavesdropper can at most have access to:

$$\Xi_e = \left\{\alpha_1, \ldots, \alpha_c, y_i(\alpha_u), \bar{\mathcal{A}}_{u,i}, i \in \mathcal{B}, u \in \mathcal{J}_{1^-}\right\}. \tag{42}$$

However, the accessible information in (42) is insufficient for any external eavesdropper to infer either $y_i(z)$'s or $\tilde{y}_i'(z)$'s, by comparing with the required clouds' output data in (27). Therefore, the bus's private information $\boldsymbol{p}_i$'s or the aggregated message $\boldsymbol{\pi}_i\tilde{\boldsymbol{P}}$'s are safe from external eavesdroppers. □

V. Simulation Results

The proposed decentralized privacy-preserving DER control strategy is verified on a simplified single-phase IEEE 13-bus test feeder [39]. Without loss of generality, suppose the distribution network shown in Fig. 1 serves an area where all customers are situated in the region with identical solar irradiance. The slack bus voltage magnitude is $V_0 = 4.16$ kV. Each bus, except the slack bus, is assumed to be connected with 2 houses, and each house is equipped with an ESS and 5 solar panels that can generate a maximum of 2.5 kW solar output to meet the daily electricity demand. The maximum capacity of all residential ESSs is set to be 10 kWh, and the maximum charging and discharging power of ESSs are ± 3 kW, respectively. The initial SoCs of all ESSs are uniformly set to be 4 kWh and lower-bounded by it for the provision of emergent backup power supply [40]. The forecasted solar PV power generation is chosen from 01/01/2021 on a sunny day with $\Delta T = 15$ mins from California Independent System Operator (CAISO) [41].

The privacy-preserving DER control platform consists of in total $c = 4$ cloud servers. In the SS-based privacy-preserving algorithm, the degree of all polynomials is uniformly set to be 3 and the integer field is chosen as $\mathbb{E} = [0, 2^{31} - 1)$. For the fixed-point number quantization, the basis, magnitude, and resolution are selected to be $\theta = 2$, $\gamma = 27$, and $\zeta = 4$, respectively. In the selected resolution, the quantization error *w.r.t.* the real number to integer transformation is $\theta^{-\zeta} = 2^{-4}$. Therefore, the real numbers are mapped onto the integer set $\mathcal{Z}_{\theta,\gamma,\zeta} = \{-2^{31}, -2^{31}+1, \ldots, 2^{31}-1\}$. Finally, the integer set is mapped onto the integer field $\mathbb{E}$. The primal and dual step sizes were empirically chosen to be $\gamma^v_{\nu,\ell} = 2.3$, $\gamma^e_{\sigma,\ell} = 1.8$, and $\beta_{\mu_{l\iota},\ell} = 5 \times 10^{-4}$, respectively.

In Fig. 5, the daily baseline loads of the 24 houses connected to the distribution network are presented by the solid lines where the load profile of each house is obtained by scaling the residential load data from CAISO [41]. The actual solar power injections from the solar PVs are presented in the dashed lines where the solar power injections remain zero between 5 PM to 7 AM the next day when there is no sunlight. During the daytime, the solar power generation peaks around 12 PM and is consumed by the loads and stored in the ESSs. Only a small amount of solar power is curtailed compared to the forecasted available solar power. Fig. 6 presents the charging and discharging behaviors of the ESSs. The ESSs charge at the peak rate around noon to store the solar power and discharge most of their stored power during peak hours between 5-10 PM. The energy stored in ESSs is extracted to supply in-home use and compensate for the power loss. The power flows of 12 lines are shown in Fig. 7 where no reverse flows occur. The power flows reach the lower limit during noon time as a result of the abundant solar power generation, leading to the balance between active power generation and consumption at each bus. By solving the optimization problem in (**P2**) via the proposed algorithm, the decision variables of DERs are updated iteratively to the optimal solutions. Both the optimal primal and dual solutions are achieved concurrently with the privacy preservation guarantees. Fig. 8 presents the converging process of all decision variables from the solar PVs in around 50 iterations. Fig. 9 presents the evolution of the dual variable $\boldsymbol{\mu}_{l\iota}$ in 100 iterations. The convergence of the dual variable reflects that the corresponding lower power flow limits are actively bounded.

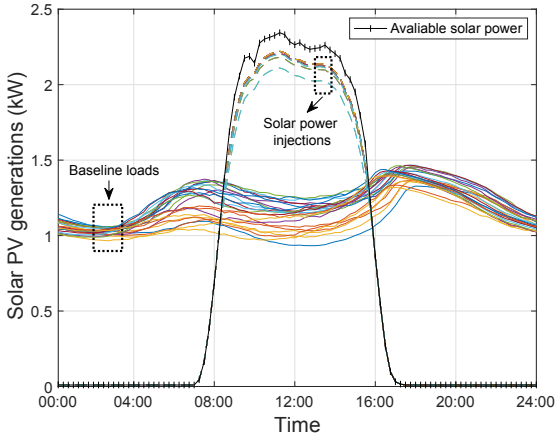


Fig. 5: Baseline loads of the 24 houses (solid lines) and actual solar power injections from the solar PVs (dashed lines).

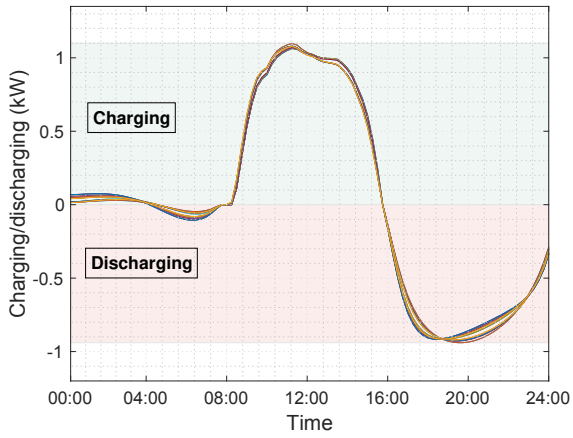


Fig. 6: Charging and discharging power from 24 ESSs.

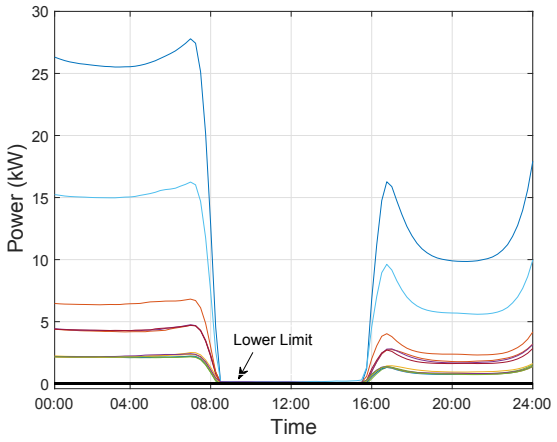


Fig. 7: Power flows of 12 lines in the distribution network.

Table I presents the CPU computing and communication efficiency comparison between the non-privacy PGM [28], the HE-based secure computing scheme using Paillier cryptosystem [42], and our proposed approach. In updating the PV's

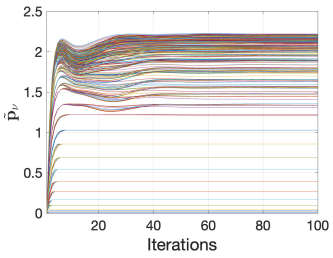


Fig. 8: Convergence of solar PVs' decision variables $\tilde{\mathbf{p}}_\nu$.

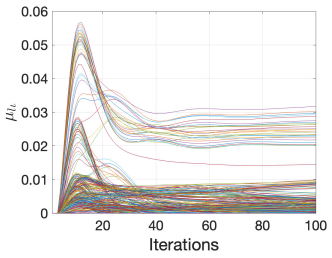


Fig. 9: Convergence of the dual variable $\boldsymbol{\mu}_{l_U}$.

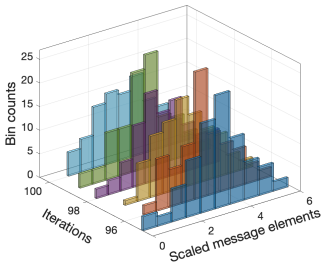


Fig. 10: Random shares generated by Bus 6 at different iterations (scaled by 6×10^9).

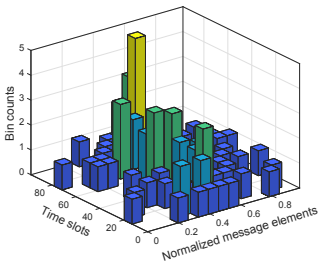


Fig. 11: Random shares generated by Bus 6 at a single iteration across different time slots (scaled by 6×10^9).

decision variable, the non-privacy PGM takes an average of 1.41×10^{-5}s to calculate the subgradient in (14a). In contrast, due to added privacy measures, the HE-based and proposed methods take an additional 2.41×10^{-3}s and 5.91×10^{-5}s, respectively. The proposed method demonstrates significantly higher computing efficiency in share generation and secret reconstruction compared to the encryption and decryptio operations from the Paillier cryptosystem. The PGM calculate on 32-bit single-precision floating point numbers, while bot the HE-based and proposed methods convert real numbers t 32-bit integers as inputs. However, the Paillier cryptosyster employs a 1024-bit key pair, resulting in 2048-bit ciphertext and significantly higher communication cost, as shown by th average length of transmitted messages. In a larger networ

TABLE I: Comparison of computing and communication effi ciency.

	HE [42]	Proposed	PGM
Avg. Time (10^{-5}s)	En† 187.68 De⋆ 53.45	Ge* 2.57 Re° 3.34	–
Total Time (10^{-5}s)	241.13	5.91	1.41
Avg. Length (bit)	2048	32	32

†Encryption ⋆Decryption *Share Generation °Secret Reconstructior

with more buses and DERs, the communication scalability between buses and cloud servers is maintained through the paralleled processing among buses. Additional computing costs occur only on the high-capacity cloud servers, thus not straining local resources. However, more DERs will require increased computing time at the local DER aggregation points. Experimental results show that aggregating 5, 20, and 100 solar PVs at each bus took on average only 0.59×10^{-5}s, 0.86×10^{-5}s, and 0.91×10^{-5}s, respectively, which are relatively minimal.

Fig. 10 presents normalized random shares generated by Bus 6 using its random polynomial $y_6^{(\ell)}(z)=\hat{\omega}_6^{(\ell)}+a_1^{(\ell)}z+a_2^{(\ell)}z^2+a_3^{(\ell)}z^3$ where the coefficients $a_i^{(\ell)}$, $i=1,2,3$ are randomized at each iteration for all time slots. The transmitted messages sent from Bus 6 are first scaled by 6×10^9 to better present the random distribution, then plotted during six consecutive iterations for $\ell=95,\ldots,100$. Moreover, random shares generated by Bus 6 at a single iteration across different time slots are given in Fig. 11. Both Fig. 10 and Fig. 11 prove the privacy preservation of Algorithm 1 against external eavesdroppers. Privacy is guaranteed because an external eavesdropper can at most have access to $\Xi_e=\{\alpha_1,\ldots,\alpha_4,y_i(\alpha_u),\bar{A}_{u,i},i\in\mathcal{B},u\in\mathcal{J}_{1^-}\}$, that is insufficient for any secret reconstruction. To further verify the privacy preservation of Algorithm 1 against honest-but-curious adversaries, we assume Bus 6 is an honest-but-curious adversary. In this case, Fig. 12 visualizes the 12

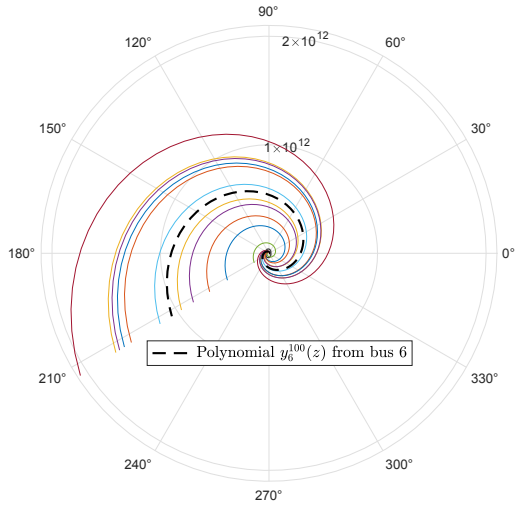


Fig. 12: Random polynomials generated by the buses in a polar plot.

random polynomials generated from all the buses at the 100th iteration. The polynomials are presented in a polar plot format where all polynomials share an order of 3. Specifically, the black dashed line represents the polynomial $y_6^{100}(z)$ that was generated by the honest-but-curious bus. The magnitudes of the outputs from random polynomials vary widely given the phase inputs. From the SMC perspective, Fig. 13 proves the existence of a simulator $\mathcal{F}$ that can generate true polynomial $\tilde{y}_6^{100}(z)$ and simulated polynomials $\tilde{y}_i'(z)$, $i=1,\ldots,12, i\neq6$, such that the computational indistinguishability $\tilde{y}_6'(\alpha_j)\overset{c}{\equiv}\tilde{y}_6(\alpha_j), j=1,\ldots,4$ is satisfied at any iteration or time slot. The ith bus, suppose honest-but-curious, can only access the information contained in its own view $\text{VIEW}_i^{\text{Alg1}}$, resulting in secure computation of $\boldsymbol{\pi}_1\tilde{\boldsymbol{P}},\ldots,\boldsymbol{\pi}_{12}\tilde{\boldsymbol{P}}$ among all buses.

VI. Conclusion

This paper developed a novel decentralized and privacy-preserving DER control algorithm for power distribution networks. The decision variables of DERs reached optimum while minimizing power line loss, PV curtailment cost, and ESS degradation cost through solving the constrained optimization problem. The developed approach preserved the privacy of

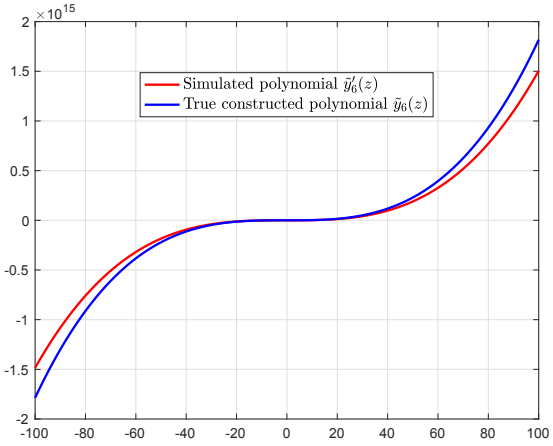


Fig. 13: Polynomials simulated by a simulator to achieve computational indistinguishability among buses.

DER owners' private data against honest-but-curious adversaries and external eavesdroppers. The developed privacy-preserving DER control framework guaranteed secure information exchange by synthesizing SS into decentralized cloud computing. Simulation results on a modified IEEE 13-bus test feeder verified the efficacy and efficiency of the proposed approach. Future work includes extending the developed method to handle nonlinear and discrete components that can lead to non-convex problem formulations.

Appendix I
Problem Reformulation

Let $\boldsymbol{Z} \in \mathbb{R}^{n\times n}$ denote the adjacency matrix and $\boldsymbol{Z}_\iota$ denote the ιth row of $\boldsymbol{Z}$. Let $\boldsymbol{Z}_\iota(i)$ denote the ith element of $\boldsymbol{Z}_\iota$, and $\boldsymbol{Z}_\iota(i)=1$ if the ιth power flow reaches edge of the network via bus i, e.g., $\boldsymbol{Z}_9=[0,0,0,0,0,0,0,0,1,1,1,0]$. Expand $\boldsymbol{Z}$ across T time slots, we have:

$$\tilde{\boldsymbol{Z}} = \begin{bmatrix} \boldsymbol{Z}_1(1)\boldsymbol{I} & \boldsymbol{Z}_1(2)\boldsymbol{I} & \cdots & \boldsymbol{Z}_1(n)\boldsymbol{I} \\ \vdots & \vdots & & \vdots \\ \boldsymbol{Z}_n(1)\boldsymbol{I} & \boldsymbol{Z}_n(2)\boldsymbol{I} & \cdots & \boldsymbol{Z}_n(n)\boldsymbol{I} \end{bmatrix}, \tag{43}$$

where $\boldsymbol{I}\in\mathbb{R}^{T\times T}$ denotes the identity matrix and $\tilde{\boldsymbol{Z}} \in \mathbb{R}^{nT\times nT}$ denotes the augmented adjacency matrix.

In what follows, let $\tilde{\boldsymbol{P}} \in \mathbb{R}^{nT}$ denote the augmented active power generations by aggregating $\boldsymbol{p}_i, i\in\mathcal{B}$, we have:

$$\tilde{\boldsymbol{P}} = \sum_{i=1}^{n} \boldsymbol{\Delta}_i \left(\tilde{\boldsymbol{p}}_i - \hat{\boldsymbol{p}}_i - \boldsymbol{p}_i^c\right), \tag{44}$$

where $\boldsymbol{\Delta}_i$ denotes the aggregation matrix whose ith block is represented by an identity matrix, and all other blocks are zeros, e.g., $\boldsymbol{\Delta}_1=[\boldsymbol{I},\boldsymbol{0},\ldots,\boldsymbol{0}]^\mathsf{T}\in\mathbb{R}^{nT\times T}$. Then, the active power flow of the ιth line can be calculated by:

$$\boldsymbol{P}_\iota = \tilde{\boldsymbol{Z}}_\iota \tilde{\boldsymbol{P}}. \tag{45}$$

where $\tilde{\boldsymbol{Z}}_\iota$ denotes the ιth block of $\tilde{\boldsymbol{Z}}$. Consequently, the power flow limit constraint in (3) becomes:

$$\boldsymbol{0} \le \tilde{\boldsymbol{Z}}_\iota \tilde{\boldsymbol{P}} \le \overline{\boldsymbol{P}}_\iota. \tag{46}$$

Appendix II
Derivation of the PGM Updates

Take the IEEE 13-bus test feeder for example, we give the PGM updates under BDAC. The power loss objective is:

$$f_1(\boldsymbol{p}_1^g,\ldots,\boldsymbol{p}_n^g) = \delta_1 \sum_{l_{ij}\in\mathcal{I}} r_{ij}\left(\frac{\|\boldsymbol{P}_{ij}\|_2^2}{V_0^2}\right) = \frac{\bar{\delta}_1}{2}\sum_{\iota\in\mathcal{I}}\|\boldsymbol{P}_\iota\|_2^2. \tag{47}$$

Take (45) into (47), we have:

$$f_1(\boldsymbol{p}_1^g,\ldots,\boldsymbol{p}_n^g) = \frac{\bar{\delta}_1}{2}\sum_{\iota\in\mathcal{I}}\|\tilde{\boldsymbol{Z}}_\iota\tilde{\boldsymbol{P}}\|_2^2. \tag{48}$$

Suppose the νth PV is connected at bus i, then its subgradient *w.r.t.* the power loss objective is:

$$\begin{aligned}\nabla_{\tilde{\boldsymbol{p}}_\nu}\mathcal{L}(\cdot) = {}& \delta_1\nabla_{\tilde{\boldsymbol{p}}_\nu} f_1(\boldsymbol{p}_1^g,\ldots,\boldsymbol{p}_n^g) + \delta_2\nabla_{\tilde{\boldsymbol{p}}_\nu} f_2(\tilde{\boldsymbol{p}}_\nu) \\ & + \sum_{\iota\in\mathcal{I}}\nabla_{\tilde{\boldsymbol{p}}_\nu}\boldsymbol{\mu}_{u\iota}^\mathsf{T}(\tilde{\boldsymbol{Z}}_\iota\tilde{\boldsymbol{P}}-\overline{\boldsymbol{P}}_\iota) - \sum_{\iota\in\mathcal{I}}\nabla_{\tilde{\boldsymbol{p}}_\nu}\boldsymbol{\mu}_{l\iota}^\mathsf{T}\tilde{\boldsymbol{Z}}_\iota\tilde{\boldsymbol{P}}. \end{aligned}\tag{49}$$

Substitute (44) and (47) into the first term of (49), we have:

$$\begin{aligned}\delta_1\nabla_{\tilde{\boldsymbol{p}}_\nu} f_1(\cdot) &= \frac{\bar{\delta}_1}{2}\nabla_{\tilde{\boldsymbol{p}}_\nu}\sum_{\iota\in\mathcal{I}}\|\tilde{\boldsymbol{Z}}_\iota\tilde{\boldsymbol{P}}\|_2^2 \\ &= \bar{\delta}_1\sum_{\iota\in\mathcal{I}}\left(\tilde{\boldsymbol{Z}}_\iota\boldsymbol{\Delta}_i\right)^\mathsf{T}\left(\tilde{\boldsymbol{Z}}_\iota\tilde{\boldsymbol{P}}\right). \end{aligned}\tag{50}$$

Take the subgradient of (5), the second term in (49) becomes:

$$\delta_2\nabla_{\tilde{\boldsymbol{p}}_\nu} f_2(\tilde{\boldsymbol{p}}_\nu) = 2\delta_2\left(\tilde{\boldsymbol{p}}_\nu - \overline{\boldsymbol{p}}_\nu^v\right). \tag{51}$$

Then, substitute (44) into the third term of (49) on the right hand side, we have:

$$\sum_{\iota\in\mathcal{I}}\nabla_{\tilde{\boldsymbol{p}}_\nu}\boldsymbol{\mu}_{u\iota}^\mathsf{T}(\tilde{\boldsymbol{Z}}_\iota\tilde{\boldsymbol{P}}-\overline{\boldsymbol{P}}_\iota) = \sum_{\iota\in\mathcal{I}}(\tilde{\boldsymbol{Z}}_\iota\boldsymbol{\Delta}_i)^\mathsf{T}\boldsymbol{\mu}_{u\iota}. \tag{52}$$

Similarly, the last term of (49) can be readily obtained as:

$$-\sum_{\iota\in\mathcal{I}}\nabla_{\tilde{\boldsymbol{p}}_\nu}\boldsymbol{\mu}_{l\iota}^\mathsf{T}(\tilde{\boldsymbol{Z}}_\iota\tilde{\boldsymbol{P}}) = -\sum_{\iota\in\mathcal{I}}(\tilde{\boldsymbol{Z}}_\iota\boldsymbol{\Delta}_i)^\mathsf{T}\boldsymbol{\mu}_{l\iota}. \tag{53}$$

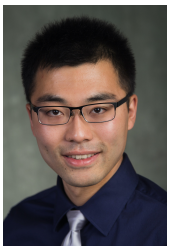
Finally, by substituting (50), (51), (52), (53) into (49), (13a) is readily obtained. The subgradients of $\hat{\boldsymbol{p}}_\sigma$ in (13b) for BDAC can also be derived similarly.

References

[1] J. Campbell, "Ancillary services provided from DER," Oak Ridge National Lab, Oak Ridge, TN, United States, Tech. Rep., 2005.
[2] J. R. Aguero, E. Takayesu, D. Novosel, and R. Masiello, "Modernizing the grid: Challenges and opportunities for a sustainable future," *IEEE Power and Energy Magazine*, vol. 15, no. 3, pp. 74–83, 2017.
[3] D. K. Molzahn, F. Dörfler, H. Sandberg, S. H. Low, S. Chakrabarti, R. Baldick, and J. Lavaei, "A survey of distributed optimization and control algorithms for electric power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2941–2962, 2017.
[4] M. Zeraati, M. E. H. Golshan, and J. M. Guerrero, "Distributed control of battery energy storage systems for voltage regulation in distribution networks with high PV penetration," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3582–3593, 2016.
[5] Y. Pan, A. Sangwongwanich, Y. Yang, and F. Blaabjerg, "Distributed control of islanded series PV-battery-hybrid systems with low communication burden," *IEEE Transactions on Power Electronics*, vol. 36, no. 9, pp. 10 199–10 213, 2021.
[6] T. Navidi, A. El Gamal, and R. Rajagopal, "A two-layer decentralized control architecture for DER coordination," in *Proceedings of the IEEE Conference on Decision and Control*, Miami, FL, USA, Dec. 17-29 2018, pp. 6019–6024.

[7] X. Huo and M. Liu, "Two-facet scalable cooperative optimization of multi-agent systems in the networked environment," *IEEE Transactions on Control Systems Technology*, vol. 30, no. 6, pp. 2317–2332, 2022.
[8] W. Lin and E. Bitar, "Decentralized stochastic control of distributed energy resources," *IEEE Transactions on Power Systems*, vol. 33, no. 1, pp. 888–900, 2017.
[9] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Proceedings of the Theory of Cryptography Conference*, New York, NY, USA, Mar. 4-7 2006, pp. 265–284.
[10] Y. Zhao and J. Chen, "A survey on differential privacy for unstructured data content," *ACM Computing Surveys*, vol. 54, no. 10s, pp. 1–28, 2022.
[11] V. Dvorkin, F. Fioretto, P. Van Hentenryck, P. Pinson, and J. Kazempour, "Differentially private optimal power flow for distribution grids," *IEEE Transactions on Power Systems*, vol. 36, no. 3, pp. 2186–2196, 2020.
[12] V. Dvorkin, P. Van Hentenryck, J. Kazempour, and P. Pinson, "Differentially private distributed optimal power flow," in *Proceedings of the IEEE Conference on Decision and Control*, Jeju, Korea (South), Dec. 14-18 2020, pp. 2092–2097.
[13] M. Ryu and K. Kim, "A privacy-preserving distributed control of optimal power flow," *IEEE Transactions on Power Systems*, vol. 37, no. 3, pp. 2042–2051, 2021.
[14] J. Dong, T. Kuruganti, S. Djouadi, M. Olama, and Y. Xue, "Privacy-preserving aggregation of controllable loads to compensate fluctuations in solar power," in *Proceedings of the IEEE Electronic Power Grid*, Charleston, SC, USA, Nov. 12-14 2018, pp. 1–5.
[15] S. Han, U. Topcu, and G. J. Pappas, "Differentially private distributed constrained optimization," *IEEE Transactions on Automatic Control*, vol. 62, no. 1, pp. 50–64, 2016.
[16] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, 2012.
[17] C. Zhang and Y. Wang, "Enabling privacy-preservation in decentralized optimization," *IEEE Transactions on Control of Network Systems*, vol. 6, no. 2, pp. 679–689, 2018.
[18] T. Wu, C. Zhao, and Y.-J. A. Zhang, "Privacy-preserving distributed optimal power flow with partially homomorphic encryption," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4506–4521, 2021.
[19] Y. Lu, J. Lian, and M. Zhu, "Privacy-preserving transactive energy system," in *Proceedings of the American Control Conference*, Denver, CO, USA, Jul. 1-3 2020, pp. 3005–3010.
[20] S. Wang, Q. Hu, Y. Sun, and J. Huang, "Privacy preservation in location-based services," *IEEE Communications Magazine*, vol. 56, no. 3, pp. 134–140, 2018.
[21] R. Gilad-Bachrach, K. Laine, K. Lauter, P. Rindal, and M. Rosulek, "Secure data exchange: A marketplace in the cloud," in *Proceedings of the ACM SIGSAC Conference on Cloud Computing Security Workshop*, London, UK, Nov. 11 2019, pp. 117–128.
[22] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
[23] M. Nabil, M. Ismail, M. M. Mahmoud, W. Alasmary, and E. Serpedin, "PPETD: Privacy-preserving electricity theft detection scheme with load monitoring and billing for AMI networks," *IEEE Access*, vol. 7, pp. 96 334–96 348, 2019.
[24] H. Zhang, J. Yu, C. Tian, P. Zhao, G. Xu, and J. Lin, "Cloud storage for electronic health records based on secret sharing with verifiable reconstruction outsourcing," *IEEE Access*, vol. 6, pp. 40 713–40 722, 2018.
[25] M. Baran and F. F. Wu, "Optimal sizing of capacitors placed on a radial distribution system," *IEEE Transactions on Power Delivery*, vol. 4, no. 1, pp. 735–743, 1989.
[26] J. Li, Z. Xu, J. Zhao, and C. Zhang, "Distributed online voltage control in active distribution networks considering PV curtailment," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 10, pp. 5519–5530, 2019.
[27] J. Forman, J. Stein, and H. Fathy, "Optimization of dynamic battery parameter characterization experiments via differential evolution," in *Proceedings of the American Control Conference*, Washington, DC, USA, Jun. 17-19 2013, pp. 867–874.
[28] D. Bertsekas and J. Tsitsiklis, *Parallel and Distributed Computation: Numerical Methods*. Athena Scientific, 2015.
[29] T. Hargreaves, M. Nye, and J. Burgess, "Making energy visible: A qualitative field study of how householders interact with feedback from smart energy monitors," *Energy Policy*, vol. 38, no. 10, pp. 6111–6119, 2010.
[30] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security & Privacy*, vol. 7, no. 3, pp. 75–77, 2009.
[31] M. T. Hale, A. Nedić, and M. Egerstedt, "Asynchronous multiagent primal-dual optimization," *IEEE Transactions on Automatic Control*, vol. 62, no. 9, pp. 4421–4435, 2017.
[32] J. Koshal, A. Nedić, and U. V. Shanbhag, "Multiuser optimization: Distributed algorithms and error analysis," *SIAM Journal on Optimization*, vol. 21, no. 3, pp. 1046–1081, 2011.
[33] H. D. Fernando, H. Shen, M. Liu, S. Chaudhury, K. Murugesan, and T. Chen, "Mitigating gradient bias in multi-objective learning: A provably convergent approach," in *Proceedings of the 11th International Conference on Learning Representations*, Kigali, Rwanda, May 1-5 2023.
[34] M. S. Daru and T. Jager, "Encrypted cloud-based control using secret sharing with one-time pads," in *Proceedings of the IEEE Conference on Decision and Control*, Nice, France, Dec. 11-13 2019, pp. 7215–7221.
[35] J. Humpherys and T. J. Jarvis, *Foundations of Applied Mathematics, Volume I: Mathematical Analysis*. Society for Industrial and Applied Mathematics, 2020.
[36] O. Goldreich, *Foundations of Cryptography: Volume 2, Basic Applications*. Cambridge University Press, 2009.
[37] D. Evans, V. Kolesnikov, and M. Rosulek, "A pragmatic introduction to secure multi-party computation," *Foundations and Trends in Privacy and Security*, vol. 2, no. 2-3, pp. 70–246, 2018.
[38] O. Goldreich, "Secure multi-party computation," *Manuscript. Preliminary Version*, vol. 78, p. 110, 1998.
[39] M. Liu, P. K. Phanivong, Y. Shi, and D. S. Callaway, "Decentralized charging control of electric vehicles in residential distribution networks," *IEEE Transactions on Control Systems Technology*, vol. 27, no. 1, pp. 266–281, 2019.
[40] National Renewable Energy Laboratory. Residential battery storage. [Online]. Available: https://atb.nrel.gov/electricity/2021/residential_battery_storage
[41] U.S. Energy Information Administration. Electric power annual. [Online]. Available: https://www.eia.gov/todayinenergy/detail.php?id=49276
[42] Y. Lu and M. Zhu, "Privacy preserving distributed optimization using homomorphic encryption," *Automatica*, vol. 96, pp. 314–325, 2018.

Xiang Huo (M'20) received the B.S. degree in automation and the M.S. degree in control science and engineering from Harbin Institute of Technology, Harbin, China, in 2017 and 2019, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Utah, Salt Lake City, UT, USA, in 2024. He is currently a Postdoctoral Researcher with the department of electrical and computer engineering, Texas A&M University, College Station, TX, USA. His research interests lie in multi-agent optimization and learning, privacy, and security, with applications to cyber-physical power systems.



Mingxi Liu (M'14) received the Ph.D. degree in mechanical engineering from the University of Victoria, Canada, in 2016. He is currently an Associate Professor of Electrical and Computer Engineering at the University of Utah, USA. Before joining the University of Utah, he was an NSERC Postdoctoral Fellow with the Energy & Resources Group, UC Berkeley. His research interests include control and optimization theories and their applications in power and energy systems, smart grid, and cyber-physical systems, focusing on scalability, privacy, and cyber security.

Dr. Liu is an NSF CAREER awardee, class of 2022. He received the NSERC Postdoctoral Fellowship and NSERC PostGraduate Scholarship-Doctoral from the Natural Sciences and Engineering Research Council of Canada in 2016 and 2014, respectively. He is an Associate Editor of the IEEE Open Journal of the Industrial Electronics Society and the IEEE Canadian Journal of Electrical and Computer Engineering. He serves on the IEEE CSS Conference Editorial Board.