Distributed Energy Management for Microgrids: When Privacy Preservation Meets Multiple Mechanisms

Jinliang Liu, *Senior Member, IEEE*, Enyu Ma, Lijuan Zha, and Engang Tian, *Senior Member, IEEE*

***Abstract*— The increasing demand for privacy preservation of modern power grids is constantly expanding. A single privacy-preserving mechanism is gradually unable to cope with the problem of privacy leakage in distributed energy management of microgrids. To solve this problem, a multiple privacy preservation scheme for distributed energy management of microgrids is proposed. The proposed scheme integrates attenuated differential privacy (ADP) with fully homomorphic encryption (FHE), and is embedded within the distributed alternating direction method of multipliers (ADMM), with the objective of minimizing power generation costs while preserving sensitive information from distributed generators (DGs). The convergence of the algorithm under mixed noise and encryption mechanism is strictly proved by constructing an extended Lyapunov function, and multiple indicators are used to reflect the advantages of multiple privacy preservation mechanism in privacy-cost trade-off. The efficacy and scalability of the proposed scheme is verified by the simulations on IEEE 30-bus system and IEEE 118-bus system. It is demonstrated by the simulation results that despite the additional time cost, the privacy preservation efficacy and economy of the proposed scheme are better than a single mechanism.**

***Index Terms*— Microgrids, smart grids, multiple privacy preservation, distributed energy management, alternating direction multiplier method (ADMM).**

I. Introduction

MICROGRIDS, as a power system aimed at a wide range of consumers, have the characteristics of flexibility and intelligence to enable efficient collaboration and optimized operation of energy equipment [1]. With the rise of low-carbon initiatives and the increasing demand for affordable energy solutions, an increasing number of consumers choose distributed generation equipment based on microgrids such as solar panels, battery storage systems, and electric vehicles [2]. Furthermore, the deployment of microgrids enhances the resilience, scalability, and efficiency of power systems.

Received 29 August 2025; revised 29 November 2025; accepted 31 December 2025. Date of publication 6 January 2026; date of current version 25 March 2026. This work was supported in part by the National Natural Science Foundation of China under Grant 62373252 and Grant 62273174 and in part by the Startup Foundation for Introducing Talent of Nanjing University of Information Science and Technology (NUIST) under Grant 2024r063. *(Corresponding author: Jinliang Liu.)*

Jinliang Liu and Enyu Ma are with the School of Computer Science, Nanjing University of Information Science and Technology, Nanjing 210044, China (e-mail: liujinliang@vip.163.com; maenyu99791013@163.com).

Lijuan Zha is with the School of Science, Nanjing Forestry University, Nanjing 210037, China (e-mail: zhalijuan@njfu.edu.cn).

Engang Tian is with the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China (e-mail: tianengang@163.com).

Digital Object Identifier 10.1109/TCE.2026.3651619

In the past, centralized control was widely adopted in microgrids, which works by aggregating various necessary information to the control center and using this information to solve economic dispatch problems [3], [4]. However, centralized methods are critically limited by their vulnerability to single-point failures, which pose a significant risk of systemic paralysis and thus constrain their broader development and application [5]. Therefore, distributed implementation solutions have received increasing attention and become a research hotspot due to their advantages of decentralization, autonomy, reliability, and scalability with the continuous integration of distributed energy into modern power grids [6], [7], [8]. For example, the Stackelberg game approach has been adopted in [9] to analyze the dynamic pricing behavior of integrated distributed energy system operators and optimize system operation strategies. A distributed consensus alternating direction multiplier algorithm has been developed to solve the problem of differential privacy energy management in microgrids collaboration [10]. In [11], a fully distributed approximate dynamic programming algorithm framework has been proposed to achieve real-time economic dispatch of microgrids.

In recent years, with the rapid development of data-driven technologies such as reinforcement learning [12], [13], many consumers oriented applications and systems have gradually become dependent on these technologies. However, this also leads to them suffering new complex vulnerabilities from AI attacks [14], [15]. For example, malicious attackers and interceptors have the potential to disrupt the stability of electricity market and even threaten the smooth operation of the power system infrastructure through leaked sensitive information [16], [17]. Competitors can also gain insights into consumers' behavior patterns and lifestyle habits based on their electricity consumption data, and predict their subsequent activities [18]. Therefore, the implementation of privacy preservation has become particularly crucial.

In order to address the privacy crisis in microgrids, researchers have adopted various methods. For example, the differential privacy strategy by injecting noise into the transmitted data to mask sensitive details [19], [20], [21]. However, the introduction of noise requires a compromise between privacy preservation and the accuracy of optimization results. To address this issue, some studies have developed methods that combine attenuated differential privacy (ADP) to maintain convergence accuracy [22]. Nevertheless, the privacy-preserving efficacy of this method may decrease with

iteration [23]. Some researchers adopt homomorphic encryption because it does not compromise the convergence accuracy and optimality of algorithms. Most of them are only based on semi homomorphic encryption such as Paillier. However, Paillier can only handle integer calculations and does not support multiplication calculations [24], [25], [26]. Though fully homomorphic encryption (FHE) such as Cheon-Kim-Kim-Song (CKKS) supports arbitrary calculations on floating-point numbers [27], comparison operations cannot be performed in the encrypted state and optimal energy management cannot be achieved in the encrypted state. It is worth noting that none of the above mentioned research works consider multiple privacy preservation.

Therefore, considering the issues of privacy preservation and the accuracy of optimization results, in this article, a multiple privacy preservation scheme that combines ADP and FHE is proposed. Candidate solutions are locally perturbed using Laplace noise integrated with an attenuation strategy, thereby establishing formal differential privacy guarantees to mitigate iterative reconstruction and inference attacks. Fully homomorphic encryption (FHE) is employed during the transmission and aggregation phases to ensure that intermediate data remains unreadable both at the network level and by the aggregator.

II. Problem Formulation and Preliminaries

A multiple privacy preservation scheme combining ADP and FHE is proposed and integrated into the distributed ADMM. ADP noise is injected during the local optimization to preserve the sensitive information of distributed generators (DGs) and encrypted transmission via FHE, which aims at coping with the problem of privacy leakage in distributed energy management of microgrids while minimizing the cost of power generation. The structure of proposed scheme is shown in Fig.1.

The problem formulation and preliminaries for achieving distributed energy management in microgrids, along with the required objective function and state of charge (SOC) update equation, are presented in this section.

A. Objective Function

The goal of the system is to minimize the power generation costs of the microgrids while meeting the load requirements and equipment operation constraints. The objective function [25] is

$$\min_{\{p_i, P_{ch,j}, P_{dis,j}\}} \left(\sum_{i=1}^{N} f_i(p_i) + \sum_{j=1}^{M} g_j\left(P_{ch,j},\ P_{dis,j}\right) \right) \tag{1}$$

where $f_i(p_i) = a_i p_i^2 + b_i p_i + c_i$ is the generation cost function of each DG. a_i, b_i, and c_i are cost coefficients and $a_i > 0$ ensures the convexity of the function. $g_j(P_{ch,j}, P_{dis,j}) = \alpha_{ch,j} P_{ch,j} + \beta_{dis,j} P_{dis,j}$ is the cost function of battery energy storage systems (BESSs). $\alpha_{ch,j} > 0$ and $\beta_{dis,j} > 0$ are the cost coefficients of unit charge and discharge power respectively. $P_{dis,j}$ is the discharge power of the j-th BESS and $P_{ch,j}$ is the charging power of the j-th BESS.

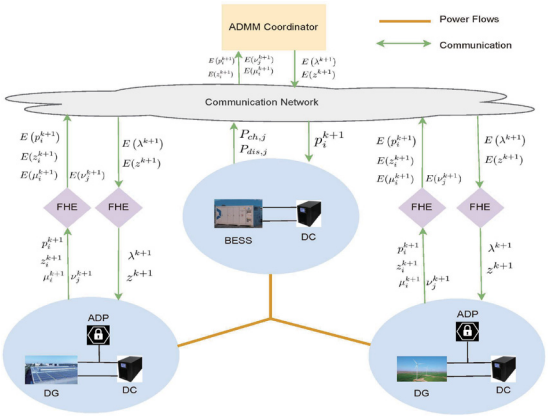


Fig. 1. Structure of distributed energy management for microgrids based on multiple privacy preservation scheme.

B. Constraints and State of Charge Update Equation

The sum of the generated power and the charging and discharging power of BESSs in microgrids needs to meet the load demand, and the formula is

$$\sum_{i=1}^{N} p_i + \sum_{j=1}^{M} P_{dis,j} - \sum_{j=1}^{M} P_{ch,j} = P_{load} \tag{2}$$

P_{load} is the total load demand of the microgrids. M is the total number of BESSs.

The power generation of each distributed power source has upper and lower limits:

$$p_{i,\min} \le p_i \le p_{i,\max}, \quad i = 1, 2, \ldots, N \tag{3}$$

$p_{i,\min}$ and $p_{i,\max}$ are the minimum and maximum power generation of the i-th distributed power source, respectively.

The charging and discharging power of each BESS also has upper and lower limits:

$$\begin{cases} 0 \le P_{ch,j} \le P_{ch,j,\max}, & j = 1, 2, \ldots, M \\ 0 \le P_{dis,j} \le P_{dis,j,\max}, & j = 1, 2, \ldots, M \end{cases} \tag{4}$$

where $P_{ch,j,\max}$ and $P_{dis,j,\max}$ are the maximum charging and discharging power of the j-th BESS.

The SOC of BESS updates over iterations, and the update formula [4] is

$$SOC_j(t+1) = SOC_j(t) + \frac{\eta_{ch,j} P_{ch,j}(t) \triangle t}{E_j} - \frac{P_{dis,j}(t) \triangle t}{\eta_{dis,j} E_j}$$
$$\text{s.t. } SOC_{j,\min} \le SOC_j \le SOC_{j,\max}, \quad j = 1, 2, \ldots, M \tag{5}$$

where $\eta_{ch,j}$ and $\eta_{dis,j}$ are the charging and discharging efficiency of the j-th BESS, respectively. E_j is the rated capacity of the j-th BESS. $\triangle t$ is the time step. $SOC_{j,\min}$ and $SOC_{j,\max}$ are the minimum and maximum values of the charge state of the j-th BESS.

Problem: How to develop a multiple privacy preservation scheme to cope with the problem of privacy leakage in microgrids while minimizing power generation costs.

Before introducing the scheme, the following definitions are needed.

Definition 1 [10]: Suppose that a random variable X has the following probability density function

$$Lap\,(x|\mu,\sigma) = \frac{1}{2\sigma} exp\left(-\frac{|x-\mu|}{\sigma}\right) \tag{6}$$

where μ is the mean and σ is the scaling parameter. Then, we say that X obeys the Laplace distribution and denotes as $X \sim \text{Lap}(x|\mu,\sigma)$. Furthermore, the expectation and variance of X are μ and $2\sigma^2$, respectively.

FHE allows for arbitrary computation of encrypted data without decryption and obtaining the encrypted result. The value obtained by decrypting the result is completely consistent with the result obtained by performing the same calculation directly on the original plaintext.

Definition 2 [24]: Suppose that the encryption function is as follows

$$E(m) = FHE.Encrypt(m, pk) \tag{7}$$

where pk is the public key and m is the plaintext information to be encrypted. Its characteristics are as follows [27]

$$\begin{cases} E(a) \oplus E(b) = E(a+b) \\ E(a) \otimes E(b) = E(a \times b) \\ k \otimes E(a) = E(k \cdot a) \end{cases} \tag{8}$$

where $E(\cdot)$ represents the encryption primitive. $\oplus$ represents additive homomorphism and $\otimes$ represents multiplicative homomorphism.

III. ADMM Algorithm Based on Multiple Privacy Preservation Scheme

Consider the optimization problem of microgrids with N DGs and M BESSs:

$$\begin{aligned} &\min_{\{p_i, P_{ch,j}, P_{dis,j}\}} \sum_{i=1}^{N} f_i(p_i) + \sum_{j=1}^{M} g_j\left(P_{ch,j},\ P_{dis,j}\right) \\ &\text{s.t.} \sum_{i=1}^{N} p_i + \sum_{j=1}^{M} (P_{dis,j} - P_{ch,j}) = P_{\text{load}}, \\ &\quad p_{i,\min} \le p_i \le p_{i,\max}, \\ &\quad 0 \le P_{ch,j} \le P_{ch,j,\max}, \\ &\quad 0 \le P_{dis,j} \le P_{dis,j,\max}, \\ &\quad SOC_{j,\min} \le SOC_j \le SOC_{j,\max}, \quad \forall i, j. \end{aligned} \tag{9}$$

In the following, the specific implementation process of the proposed distributed ADMM under multiple privacy preservation is presented.

A. Original Variable Update

Since FHE does not support local optimization structural formula operations such as arg min, if arg min is completed directly in the clear text domain, core business secrets such as cost coefficient will be exposed in the local memory in clear text for a short time, and there is a risk of being obtained by local memory leakage or side channel attack. In order to solve this problem, we adopt the hybrid scheme of symmetric authentication encryption and trusted execution environment (TEE) at the engineering implementation level.

Firstly, the sensitive information such as cost coefficients encrypt static storage and transmission with symmetric authentication:

$$\begin{cases} C_i = Enc_{K_i}^{AEAD} = (a_i, b_i, c_i, meta) \\ C_j = Enc_{K_j}^{AEAD} = (\alpha_{ch,j}, \beta_{dis,j}, meta) \end{cases} \tag{10}$$

where K_i and K_j are the key held only by the i/j-th agent and the trusted key management system.

Then, the agent and the coordinator establish a short-term session through remote certification and complete it in the TEE. The TEE decrypts with the session key in the proven trusted state, executes the argmin operation, and completes the local optimization:

$$\begin{cases} p_i^{k+1} = \arg\min\limits_{p_i} \Big\{ f_i(p_i) + \mu_i^k (p_i - z_i^k) \\ \quad + \frac{\rho}{2}(p_i - z_i^k)^2 \Big\} + \zeta_i^k, \quad \forall i \text{ without BESS} \\ p_i^{k+1} = \arg\min\limits_{p_i, P_{ch,j}, P_{dis,j}} \Big\{ f_i(p_i) + g_j(P_{ch,j}, P_{dis,j}) \\ \quad + \mu_i^k (p_i - z_i^k) + \nu_j^k \left(P_{dis,j} - P_{ch,j} - z_i^k\right) + \frac{\rho}{2}(p_i - z_i^k)^2 \\ \quad + \frac{\rho}{2}\left(P_{dis,j} - P_{ch,j} - z_i^k\right)^2 \Big\} + \zeta_i^k, \quad \forall i \text{ has BESS} \end{cases} \tag{11}$$

where z_i^k is the local auxiliary variable of the i-th DG in the k-th iteration. μ_i^k is the local Lagrange multiplier of the i-th DG in the k-th iteration. ν_j^k is local Lagrange multiplier corresponding to BESS, respectively. $\zeta_i^k \sim \text{Lap}\left(0, \sigma_i^k\right)$ is the Laplace noise that decays with iteration. ρ is the penalty parameter.

Remark 1: It should be noted that TEE provides engineering credibility rather than mathematically indestructible guarantees. Channel, firmware and supply chain level vulnerabilities on the micro architecture side may still threaten TEE's security. Therefore, the purpose of this process is to expose plaintext in trusted hardware for the shortest time so that greatly reducing the risk of memory leakage and local attacks.

Afterwards, the locally optimized results will be transmitted through FHE:

$$E\left(p_i^{k+1}\right) = FHE.Encrypt(p_i^{k+1}, pk). \tag{12}$$

B. Auxiliary Variable Update

The local auxiliary variable z_i is used to store the status information of each DG. According to the properties of FHE, the update formula in the encrypted state is

$$\begin{aligned} E(z_i^{k+1}) = \tfrac{1}{2} \otimes \Big[& E(p_i^{k+1}) \oplus \tfrac{1}{\rho} \otimes E(\mu_i^k) \oplus E(z_i^k) \oplus \\ & (-\tfrac{1}{N\rho}) \otimes E(\lambda^k) \oplus \mathbf{1}_{\{i \text{ has BESS}\}} E(P_{dis,j} - P_{ch,j}) \Big]. \end{aligned} \tag{13}$$

The global auxiliary variable z is introduced to aggregate all local information to enforce global consistency and its update

formula in encrypted state is

$$E(z^{k+1}) = \frac{1}{N} \otimes E(P_{load}) \oplus (-\frac{1}{\rho}) \otimes E(\lambda^k) \oplus \bigoplus_{i=1}^{N} E(z_i^{k+1}) \tag{14}$$

where p_i^{k+1} is the updated original variable. z^k is the global auxiliary variable in the k-th iteration. λ^k is the global Lagrange multiplier in the k-th iteration.

C. Lagrange Multiplier Update

In the process of distrubuted ADMM Algorithm, Global Lagrange multiplier λ is applied to adjust global consistency through penalty terms and its update formula in the encrypted state is as follows

$$E\left(\lambda^{k+1}\right) = E\left(\lambda^k\right) \oplus \rho \otimes \left(\bigoplus_{i=1}^{N} E\left(z_i^{k+1}\right) \oplus E\left(-P_{load}\right) \right). \tag{15}$$

To prevent deviation of local decisions from global objectives, the local Lagrange multiplier μ and ν are introduced. Their update formulas in encrypted state are

$$\begin{cases} E(\mu_i^{k+1}) = E(\mu_i^k) \oplus \rho \otimes \left(E(p_i^{k+1}) \oplus E(-z_i^{k+1})\right) \\ E(\nu_j^{k+1}) = E(\nu_j^k) \oplus \rho \otimes \left(E(P_{dis,j} - P_{ch,j}) \oplus E(-z_i^{k+1})\right). \end{cases} \tag{16}$$

D. Termination Conditions

When the norm of both the original residual and the dual residual is less than the given threshold, it is considered that the algorithm has converged.

The original residual calculation formula is

$$||\mathcal{R}^k||_2 = ||\mathcal{P}^k - \mathcal{Z}^k||_2 \le \epsilon_{pri}. \tag{17}$$

The dual residual calculation formula is

$$||\mathcal{S}^k||_2 = \rho||(\mathcal{Z}^k - \mathcal{Z}^{k-1})||_2 \le \epsilon_{dual} \tag{18}$$

where $\mathcal{P}^k = [p_1^k, p_2^k, \ldots, p_N^k]^T \in \mathbb{R}^N$ is the column vector composed of all original variables at the k-th iteration, and $\mathcal{Z}^k = [z_1^k, z_2^k, \ldots, z_N^k]^T \in \mathbb{R}^N$ is the column vector composed of all auxiliary variables at the k-th iteration. ϵ_{pri} and ϵ_{dual} are the original residual threshold and dual residual threshold, respectively. Their calculation formulas are as follows

$$\begin{cases} \epsilon_{pri} = \dfrac{A_1}{k} + A_2 \max\limits_{t \le k} \|\zeta_t\| + A_3 \max\limits_{t \le k} \|\delta_t\| \\ \epsilon_{dual} = \dfrac{Q_1}{k} + Q_2 \max\limits_{t \le k} \|\zeta_t\| + Q_3 \max\limits_{t \le k} \|\delta_t\| \end{cases} \tag{19}$$

where ζ_t and δ_t are the introduced ADP noise and FHE noise of the t-th iteration, respectively. A_i and Q_i $(i = 1, 2, 3)$ are constants.

In the distributed energy management of microgrids under multiple privacy preservation scheme, ADP noise is injected during local optimization processes in accordance with (9) to simultaneously ensure sensitive information preservation and optimization accuracy. Concurrently, FHE is integrated into the ADMM algorithm through (10)-(14) for encrypted variable transmission and update. Therefore, the problem of achieving multiple privacy preservation for DGs data while satisfying load demand and minimizing generation costs is addressed. The implementation process of the proposed algorithm is shown in Algorithm 1.

Algorithm 1 ADMM Algorithm Under Multiple Privacy Preservation Scheme

Input: System parameters a_i, b_i, c_i, $P_{ch,j}$ and $P_{dis,j}$, etc;
ADP parameters π_i, κ_i;
FHE key pairs pk, sk;
Initial values z^0, z_i^0, λ^0, μ_i^0, ν_j^0;
Penalty parameter ρ;
Residual threshold ϵ_{pri}, ϵ_{dual}.
Initialization:
Encrypt initial variables:
$E(z^0) \leftarrow$ FHE.Encrypt(z^0, pk);
$E(z_i^0) \leftarrow$ FHE.Encrypt(z_i^0, pk) for all i;
$E(\lambda^0) \leftarrow$ FHE.Encrypt(λ^0, pk);
$E(\mu_i^0) \leftarrow$ FHE.Encrypt(μ_i^0, pk) for all i;
$E(\nu_j^0) \leftarrow$ FHE.Encrypt(ν_j^0, pk) for all j;
$k \leftarrow 0$;
converged $\leftarrow$ false.
while not converged **do**
  Original variables update:
  for $i = 1$ to N **do**
    step 1: Generate the ADP noise $\zeta^k \sim \text{Lap}\left(0, \sigma^k\right)$.
    step 2: Start remote authentication with TEE and establish short-term session key K_i, K_j.
    step 3: Decrypt the local ciphertext parameters using K_i, K_j within the TEE.
    step 4: Performing local optimization within TEE to obtain p_i^{k+1}.
    step 5: Output is immediately encrypted with the FHE public key within the TEE accroding to (12).
  end for
  Auxiliary variables update:
  for $i = 1$ to N **do**
    Update the z_i^{k+1} according to (13).
  end for
  Update the z^{k+1} according to (14).
  Lagrange multipliers update:
  Update the λ^{k+1} according to (15).
  for $i = 1$ to N **do**
    Update the μ_i^{k+1} and ν_j^{k+1} according to (16).
  end for
  if $||\mathcal{R}_k||_2 \le \epsilon_{\text{pri}}$ and $||\mathcal{S}_k||_2 \le \epsilon_{\text{dual}}$ and $k >$ iterations **then**
    converged $\leftarrow$ true.
  else
    $k \leftarrow k + 1$.
  end if
end while
Output: p_i^*, z^*, z_i^*, λ^*, μ_i^*, ν_j^*.

IV. Convergence Analysis

Given the residual second-order moment and noise accumulation term together, it is demonstrated that ADMM iteration still converges in the expected sense under mixed noise and encryption architectures by constructing an extended Lyapunov function.

A. Extended Lyapunov Function

In the distributed optimization framework, the impact of mixed noise introduced by privacy preservation mechanisms

on algorithm convergence needs to be analyzed from two levels: residual constraints and function drift. Theorem 1 is given to quantify the disturbance of noise on the original residual and dual residual, and proves the correlation between the upper bound of the second-order moment of the residual and the noise accumulation term.

Theorem 1: Consider the ADP and FHE hybrid noise architecture in the microgrids of distributed energy management, if $\zeta^k \sim \text{Lap}(0, \sigma^k)$ satisfies $\sum_{k=1}^{\infty}(\sigma^k)^2 < +\infty$, $\sigma^{k+1} = \kappa^k\sigma^0 (0 < \kappa < 1)$. FHE noise ε_{enc}^k satisfies $\mathbb{E}\left[\varepsilon_{enc}^k\right] = 0$, $\mathbb{E}\left[\left(\varepsilon_{enc}^k\right)^2\right] \le \delta^2$ and $\varepsilon_{enc}^k \perp \zeta^k$. Then, there is an upper bound for the second moment $\mathbb{E}\left[\left\|\mathbf{R}^{k+1}\right\|_2^2 + \left\|\mathbf{S}^{k+1}\right\|_2^2\right]$ of the original residual and the dual residual.

Remark 2: According to the classical combination theorem of differential privacy, the overall privacy budget after t iterations satisfies $\epsilon_{total} \le \sum_{k=1}^{t}\epsilon_k$.

For ADP, the attenuation noise $\sigma^{k+1} = \kappa^k\sigma^0 (0 < \kappa < 1)$ is used in each round. Therefore, the privacy budget for each round is $\epsilon_k = \frac{\Delta}{\sigma^{k+1}} = \frac{\Delta}{\kappa^k\sigma^0}$. So the accumulated privacy budget is $\epsilon_{\text{total}} = \sum_{k=1}^{t}\frac{\Delta}{\kappa^k\sigma_0} = \frac{\Delta}{\sigma_0}\cdot\frac{1-\kappa^{-t}}{1-\kappa^{-1}}$. Because $0 < \kappa < 1$, κ^{-t} eventually tends towards a finite upper bound as t increases. Therefore: $\epsilon_{\text{total}} = O\left(\frac{1}{1-\kappa}\right)$. Therefore, it can be concluded that the cumulative privacy budget of ADP is bounded, rather than infinite growth.

Remark 3: In the distributed energy management problem, although there are differences in physical characteristics and cost functions between DGs and BESSs, they have the same mathematical structure in the optimization framework. Therefore, this paper considers the convergence of the algorithm as a whole.

Proof: Based on mixed noise and encryption architecture, the following extended Lyapunov function is given

$$V^k = \mathbb{E}\left[||\mathbf{R}^k||_2^2 + ||\mathbf{S}^k||_2^2\right] + C\sum_{i=1}^{N}\sum_{n=1}^{k}(\sigma_i^n)^2 + D\sum_{i=1}^{N}\sum_{n=1}^{k}\delta_i^2 \tag{20}$$

For the i-th component, the update formula for the original variable $\mathbf{P}_i^{k+1}$ and auxiliary variable $\mathbf{Z}_i^{k+1}$ with noise are as follows

$$\begin{cases} \mathbf{P}_i^{k+1} = \tilde{p}_i^* + \zeta_i^k + \varepsilon_{i,enc}^k \\ \mathbf{Z}_i^{k+1} = \frac{1}{2}\left(\tilde{p}_i^* + \frac{\tilde{\mu}_i^k}{\rho} + z_i^k - \frac{\lambda^k}{N\rho}\right) + \frac{1}{2}\left(\zeta_i^k + \varepsilon_{i,enc}^k\right) + \varepsilon_{i,z}^k \end{cases} \tag{21}$$

where

$$\begin{cases} \tilde{p}_i^* = p_i^* + \sum_{j\in\mathcal{B}(i)}\left(P_{dis,j} - P_{ch,j}\right), \\ \tilde{\mu}_i^k = \mu_i^k + \sum_{j\in\mathcal{B}(i)} v_j^k \end{cases}$$

$\mathcal{B}(i)$ represents the BESS set connected to node i. If node i has no BESS, then the null sum is 0, and the combined noise term is only equal to the noise term contained in the DG.

Therefore, we have

$$\mathbf{R}_i^{k+1} = \mathbf{P}_i^{k+1} - \mathbf{Z}_i^{k+1} = r_i^* + \tilde{\varepsilon}_{i,r}^k \tag{22}$$

where $r_i^* = \frac{1}{2}\left[\tilde{p}_i^* - \tilde{\mu}_i^k/\rho - z_i^k + \lambda^k/(N\rho)\right]$ represents the half step residual in the ideal state without noise.$\tilde{\varepsilon}_{i,r}^k = \frac{1}{2}(\zeta_i^k + \varepsilon_{i,enc}^k) - \varepsilon_{i,z}^k$ represents the random part of the original linear system affected by both ADP noise and FHE noise. It can be inferred from $\mathbb{E}\left[\zeta_i^k\right] = 0$ and $\mathbb{E}\left[\varepsilon_\cdot^k\right] = 0$ that $\mathbb{E}\left[\tilde{\varepsilon}_{i,r}^k\right] = 0$. According to the Laplace noise distribution variance $\mathbb{E}\left[\left(\zeta_i^k\right)^2\right] = 2\left(\sigma_i^k\right)^2$ and FHE noise second-order moment bounded $\mathbb{E}\left[\left(\varepsilon_\cdot^k\right)^2\right] \le \delta_i^2$, it can be inferred that $\mathbb{E}\left[\left(\tilde{\varepsilon}_{i,r}^k\right)^2\right] \le c_1(\sigma_i^k)^2 + c_2\delta_i^2$, where c_1 and c_2 are constants. From this, it can be concluded that

$$\begin{aligned} \mathbb{E}\left[\left\|\mathbf{R}^{k+1}\right\|_2^2\right] &= \sum_{i=1}^{N}\left\{(r_i^*)^2 + \mathbb{E}\left[\left(\tilde{\varepsilon}_{i,r}^k\right)^2\right]\right\} \\ &\le \sum_{i=1}^{N}\frac{1}{4}\left\|\tilde{p}_i^* - z_i^k - \left(\tilde{\mu}_i^k/\rho - \lambda^k/(N\rho)\right)\right\|^2 \\ &\quad + N\left(c_1\left(\sigma_{\max}^k\right)^2 + c_2\delta_{\max}^2\right) \end{aligned} \tag{23}$$

where $\sigma_{\max}^k = \max_i \sigma_i^k$, $\delta_{\max} = \max_i \delta_i$ are the boundary.

According to [28], the noise free residual satisfies the linear convergence property, and the local solution $\tilde{p}_i^*$ satisfies the optimality condition:

$$\tilde{p}_i^* = z_i^k + \frac{1}{\rho}(\tilde{\mu}_i^k - \nabla f_i(\tilde{p}_i^*)) \tag{24}$$

∇f_i is the gradient of the cost function. For the quadratic cost function, the gradient is linear, which can be obtained by substituting into the residual definition:

$$\left\|\tilde{p}_i^* - z_i^k - \left(\frac{\tilde{\mu}_i^k}{\rho} - \frac{\lambda^k}{N\rho}\right)\right\|^2 \le \alpha_i\|R_i^k\|^2 + \beta_i\|S_i^k\|^2 \tag{25}$$

α_i and β_i are constants that depend on penalty parameter ρ, number of nodes N and cost function convexity $a_i > 0$. Among them, increasing the penalty parameter ρ can accelerate local convergence but easily enhance the influence of noise. The more nodes N, the closer α and β are to 1, and the convergence will slow down. If the strong convexity of the cost function $a_i > 0$, it can make α and β less than 1. Because the global residual is the sum of the local residual, it can be inferred that

$$\sum_{i=1}^{N}\frac{1}{4}\left\|\tilde{p}_i^* - z_i^k - \left(\frac{\tilde{\mu}_i^k}{\rho} - \frac{\lambda^k}{N\rho}\right)\right\|^2 \le \frac{1}{4}\alpha\|R^k\|_2^2 + \frac{1}{4}\beta\|S^k\|_2^2 \tag{26}$$

where $\alpha = \max_i \alpha_i$ and $\beta = \max_i \beta_i$ are global shrinkage constants and depend on system parameters. It can be obtained by combining the noise term:

$$\mathbb{E}\left[\left\|\mathbf{R}^{k+1}\right\|_2^2\right] \le \frac{1}{4}\alpha\left\|\mathbf{R}^k\right\|_2^2 + \frac{1}{4}\beta\left\|\mathbf{S}^k\right\|_2^2 + Nc_1\left(\sigma_{\max}^k\right)^2 + Nc_2\delta_{\max}^2 \tag{27}$$

where $0 < \alpha < 1$ and $0 < \beta < 1$.

For the i-th component, dual residual update formula with additional noise is $\mathbf{S}_i^{k+1} = \rho(\mathbf{Z}_i^{k+1} - \mathbf{Z}_i^k)$. Similar to (23), it can be obtained that

$$\mathbb{E}\left[\left\|\mathbf{S}^{k+1}\right\|_2^2\right] = \rho^2 \sum_{i=1}^{N} \mathbb{E}\left[B_i^k + \tilde{\varepsilon}_{i,s}^k\right] \leq \rho^2 \sum_{i=1}^{N} B_i^k + N\rho^2\left(c_3\left(\sigma_{\max}^k\right)^2 + c_4\delta_{\max}^2\right) \quad (28)$$

where $B_i^k = \frac{1}{4}\left\|\mathbf{P}_i^{k+1} - \mathbf{Z}_i^k + \left(\tilde{\mu}_i^k/\rho - \lambda^k/(N\rho)\right)\right\|^2$, which is the decisive part of the dual residual in the absence of noise. $\tilde{\varepsilon}_{i,s}^k = \varepsilon_{i,z}^k\left[\mathbf{P}_i^{k+1} - \mathbf{Z}_i^k + \left(\tilde{\mu}_i^k/\rho - \lambda^k/(N\rho)\right)\right] + \left(\varepsilon_{i,z}^k\right)^2$ represents the random deviation related to noise, satisfying $\mathbb{E}\left[\tilde{\varepsilon}_{i,z}^k\right] = 0$ and $\mathbb{E}\left[\left(\tilde{\varepsilon}_{i,z}^k\right)^2\right] \leq c_3\left(\sigma_{\max}^k\right)^2 + c_4\delta_{\max}^2$. Among them, c_3 and c_4 are constants. Similarly, according to [28], there exists constants $\alpha' < 1$, $\beta' < 1$ such that

$$\mathbb{E}\left[\left\|\mathbf{S}^{k+1}\right\|_2^2\right] \leq \rho^2\alpha'\left\|\mathbf{R}^k\right\|_2^2 + \rho^2\beta'\left\|\mathbf{S}^k\right\|_2^2 + N\rho^2\left(c_3\left(\sigma_{\max}^k\right)^2 + c_4\delta_{\max}^2\right). \quad (29)$$

By combining the previous (27), we can obtain

$$\mathbb{E}\left[\left\|\mathbf{R}^{k+1}\right\|_2^2 + \left\|\mathbf{S}^{k+1}\right\|_2^2\right] \leq \left(\frac{1}{4}\alpha + \rho^2\alpha'\right)\left\|\mathbf{R}^k\right\|_2^2 + \left(\frac{1}{4}\beta + \rho^2\beta'\right)\left\|\mathbf{S}^k\right\|_2^2 + N\left[c_1 + \rho^2 c_3\right]\left(\sigma_{\max}^k\right)^2 + N\left[c_2 + \rho^2 c_4\right]\delta_{\max}^2. \quad (30)$$

Theorem 1 completes the proof. ■

Remark 4: In terms of engineering implementation, adopting the bootstrapping operation can ensure that the FHE noise ε_{enc}^k is independent across iterations, and independent of the ADP noise ζ^k.

Remark 5: In engineering implementation, to prevent excessive noise growth, relinearization or modulus switching operations are usually used to ensure that the noise variance is less than δ^2.

The existence of upper bounds on the second-order moments of residuals is proved in Theorem 1 by analyzing the efficacy of mixed noise on the original residuals and dual residuals. However, the convergence of the system is not demonstrated therein. Furthermore, relying on the established upper bounds of residuals in Theorem 1, Theorem 2 is given to transform residual constraints into a monotonic analysis of function drift, with the result that the convergence of the system is proven.

Theorem 2: Under the condition of Theorem 1, there exists $\gamma > 0$ so that the drift of Lyapunov function satisfies

$$\mathbb{E}\left[V^{k+1} - V^k\right] \leq -\gamma\mathbb{E}\left[\left\|\mathbf{R}^k\right\|_2^2 + \left\|\mathbf{S}^k\right\|_2^2\right]. \quad (31)$$

Then, V^k monotonically decreases and converges.

Proof: According to (20), we can obtain

$$V^{k+1} - V^k = \mathbb{E}\left[\left\|\mathbf{R}^{k+1}\right\|_2^2 + \left\|\mathbf{S}^{k+1}\right\|_2^2\right] - \mathbb{E}\left[\left\|\mathbf{R}^k\right\|_2^2 + \left\|\mathbf{S}^k\right\|_2^2\right] + C\sum_{i=1}^{N}(\sigma_i^{k+1})^2 + D\sum_{i=1}^{N}\delta_i^2. \quad (32)$$

Substituting (30) into (32), (32) can be rewritten as

$$V^{k+1} - V^k \leq (\alpha_{\text{eff}} - 1)\left\|\mathbf{R}^k\right\|_2^2 + (\beta_{\text{eff}} - 1)\left\|\mathbf{S}^k\right\|_2^2 + N\left[c_1 + \rho^2 c_3\right]\left(\sigma_{\max}^k\right)^2 + N\left[c_2 + \rho^2 c_4\right]\delta_{\max}^2 + CS_\sigma^{k+1} + DS_\delta \quad (33)$$

where $\alpha_{\text{eff}} = \frac{1}{4}\alpha + \rho^2\alpha'$, $\beta_{\text{eff}} = \frac{1}{4}\beta + \rho^2\beta'$, $S_\sigma^k = \sum_{i=1}^{N}\left(\sigma_i^k\right)^2$, $S_\delta = \sum_{i=1}^{N}\delta_i^2$.

Since $\alpha', \beta' < 1$, as long as ρ is not too large, it can satisfy $\alpha_{\text{eff}} < 1, \beta_{\text{eff}} < 1$. At this point, let $\gamma = \min\{1 - \alpha_{\text{eff}}, 1 - \beta_{\text{eff}}\} > 0$, then

$$V^{k+1} - V^k \leq -\gamma\left\|\mathbf{R}^k\right\|_2^2 - \gamma\left\|\mathbf{S}^k\right\|_2^2 + N\left[c_1 + \rho^2 c_3\right]\left(\sigma_{\max}^k\right)^2 + N\left[c_2 + \rho^2 c_4\right]\delta_{\max}^2 + C\,S_\sigma^{k+1} + D\,S_\delta. \quad (34)$$

where $S_\sigma^k = \sum_{i=1}^{N}(\sigma_i^k)^2$ and $S_\delta = \sum_{i=1}^{N}\delta_i^2$. To ensure that the noise item is not positive, that is

$$CS_\sigma^{k+1} + DS_\delta - N[c_1 + \rho^2 c_3](\sigma_{\max}^k)^2 - N[c_2 + \rho^2 c_4]\delta_{\max}^2 \leq 0. \quad (35)$$

Remark 6: In drift analysis, the influence of the disturbance is usually quantified and accumulated into Lyapunov function, and then compared with the positive contribution of the current wheel disturbance to the residual in the drift inequality, the appropriate constant is selected to make the overall drift negative, so as to ensure that the system can still converge to a small area or expected convergence under the disturbance [29].

For ADP noise part, from attenuation strategy $\sigma^{k+1} = \kappa^k\sigma^0 (0 < \kappa < 1)$, there is $S_\sigma^{k+1} \leq \kappa_{\max}^2 S_\sigma^k$ and $\kappa_{\max} = \max_i \kappa_i$, it can be obtained that:

$$CS_\sigma^{k+1} - N\left[c_1 + \rho^2 c_3\right]\left(\sigma_{\max}^k\right)^2 \leq C\kappa_{\max}^2 S_\sigma^k - N\left[c_1 + \rho^2 c_3\right]\left(\sigma_{\max}^k\right)^2 \leq 0 \quad (36)$$

To ensure the above formula ≤ 0, the sufficient condition is

$$C\kappa_{\max}^2 S_\sigma^k \leq N[c_1 + \rho^2 c_3](\sigma_{\max}^k)^2. \quad (37)$$

According to $S_\sigma^k \geq (\sigma_{\max}^k)^2$, it can be inferred that

$$C\kappa_{\max}^2 \leq N[c_1 + \rho^2 c_3]\frac{(\sigma_{\max}^k)^2}{S_\sigma^k} \leq N[c_1 + \rho^2 c_3]. \quad (38)$$

From the above equation, it can be concluded that $C \leq \frac{N[c_1+\rho^2 c_3]}{\kappa_{\max}^2}$ and $0 < \kappa_{\max} < 1$. Therefore, taking stricter conditions can lead to $C \leq N[c_1 + \rho^2 c_3]$.

For the FHE noise part, the FHE noise variance is bounded $E[(\varepsilon_{i,\text{enc}}^k)^2] \leq \delta_i^2$ and $\delta_{\max} = \max_i \delta_i$. According to $S_\delta = \sum_{i=1}^{N}\delta_i^2 \leq N\delta_{\max}^2$, it can be obtained by substituting the condition:

$$DS_\delta - N[c_2 + \rho^2 c_4]\delta_{\max}^2 \leq DN\delta_{\max}^2 - N[c_2 + \rho^2 c_4]\delta_{\max}^2. \quad (39)$$

To ensure the function drift ≤ 0, it is necessary to obtain: $D \leq N[c_2 + \rho^2 c_4]$

In conclusion, as long as constants $C \leq N[c_1 + \rho^2 c_3]$ and $D \leq N\left[c_2 + \rho^2 c_4\right]$ are selected, it can be ensured that the noise related term is non positive in (34), that is

$$C S_\sigma^{k+1} + D S_\delta - \left[N\left[c_1 + \rho^2 c_3\right]\left(\sigma_{\max}^k\right)^2 + N\left[c_2 + \rho^2 c_4\right]\delta_{\max}^2\right] \leq 0. \tag{40}$$

At this point, (34) is converted into

$$V^{k+1} - V^k \leq -\gamma \left\|\mathbf{R}^k\right\|_2^2 - \gamma \left\|\mathbf{S}^k\right\|_2^2 \tag{41}$$

That is

$$\mathbb{E}\left[V^{k+1} - V^k\right] \leq -\gamma \mathbb{E}\left[\left\|\mathbf{R}^k\right\|_2^2 + \left\|\mathbf{S}^k\right\|_2^2\right]. \tag{42}$$

Note that $V^k \geq 0$, and $\mathbb{E}[V^{k+1}]$ has a lower bound of 0, then the right-hand side of the above equation cannot infinitely approach negative infinity, otherwise it contradicts $\mathbb{E}[V^{k+1}] \geq 0$. Therefore, there must be

$$\sum_{k=0}^{\infty} \mathbb{E}\left[\|\mathbf{R}^k\|_2^2 + \|\mathbf{S}^k\|_2^2\right] < +\infty \Longrightarrow \lim_{k\to\infty} \mathbb{E}\left[\|\mathbf{R}^k\|_2^2 + \|\mathbf{S}^k\|_2^2\right] = 0. \tag{43}$$

At this point, the system has reached convergence and the proof is complete. ■

Remark 7: Given a certain iteration k, in order for the residual to converge to a given tolerance, according to (30) the necessary and sufficient conditions must be satisfied

$$N\left(c_1 + \rho^2 c_3\right)\left(\sigma_{\max}^k\right)^2 + N\left(c_2 + \rho^2 c_4\right)\delta_{\max}^2 \leq (1 - \alpha_{\text{eff}})\,\epsilon_{\text{tot}}$$

where $\epsilon_{\text{tot}} = \epsilon_{\text{pri}} + \epsilon_{\text{dual}}$ is a target residual tolerance. So for a given target threshold ϵ_{tot}, the upper bound of noise must satisfy

$$\left(\sigma_{\max}^k\right)^2 \leq \frac{(1 - \alpha_{\text{eff}})\,\epsilon_{\text{tot}}}{N(c_1 + \rho^2 c_3)}, \quad \delta_{\max}^2 \leq \frac{(1 - \alpha_{\text{eff}})\,\epsilon_{\text{tot}}}{N(c_2 + \rho^2 c_4)}.$$

Conversely, if the noise is fixed, the above equation gives the minimum feasible adjustment of the convergence threshold:

$$\epsilon_{\text{tot}} \geq \frac{N(c_1 + \rho^2 c_3)\left(\sigma_{\max}^k\right)^2 + N(c_2 + \rho^2 c_4)\delta_{\max}^2}{1 - \alpha_{\text{eff}}}.$$

If σ_i^k or δ_i^2 increases, the thresholds ϵ_{pri}, ϵ_{dual} must be increased accordingly to remain feasible and if σ_i^k decreases over time, the required thresholds shrink automatically, enabling convergence. The quantitative relationship between different noise intensities and convergence boundaries can be obtained by combining (19).

Remark 8: It is worth noting that classical differential privacy, which injects a constant noise scale at every iteration, is incompatible with the convergence guarantees established in Theorem 1 and Theorem 2. Since the noise term would not vanish, the Lyapunov recursion cannot contract to zero residuals. In contrast, ADP provides a diminishing perturbation sequence that preserves convergence while the FHE mechanism ensures strong long-term privacy preservation.

V. Simulation Studies

The efficacy of the ADMM algorithm under multiple privacy preservation scheme is verified through two parts. Firstly, multiple indicators are used to compare the privacy-cost trade-off between different mechanisms. Secondly, conventional operations have been implemented on the IEEE 30-bus system and 118-bus system. Among them, the IEEE 30-bus system includes 4 DGs and 2 BESSs and the IEEE 118-bus system consists of 40 DGs and 7 BESSs. Overall, these case studies were conducted in a Python 3.9.6 environment on a computer running on an Intel Core i7-10750 CPU at 2.60 GHz, with FHE implemented using TenSEAL 0.3.16. In the following text, a clear description is provided.

Remark 9: In our simulations, we used TenSEAL and CKKS scheme as the practical FHE backend. The exact TenSEAL context used in the experiments is:

```
ctx = ts.context(ts.SCHEME_TYPE.CKKS,
poly_modulus_degree=8192,
coeff_mod_bit_sizes=[60, 40, 40, 60])
ctx.global_scale = 2**40
ctx.generate_galois_keys()
```

These parameters were chosen to balance three factors: (i) numerical precision of approximate real arithmetic, (ii) allowable multiplicative depth, and (iii) practical security. At the same time, to ensure the correctness and to quantify the effect of CKKS approximation, we performed the following checks in all experiment runs: (i) Plaintext-vs-decrypted equality test, (ii) Noise budget monitoring, (iii) End-to-end consistency. These implementation details and validation steps ensure the authenticity of the homomorphic-encryption-based results reported in this paper.

A. Comparison of Privacy-Cost Trade-off

The comparison results of different metrics among the multiple privacy preservation mechanism, ADP and FHE in the first 50 iterations of the IEEE 30-bus system are presented in Table I. Table II compares the computational overhead of three mechanisms on IEEE 30-bus system and IEEE 118-bus system. The time for different operations in the entire iteration process of FHE is shown in Table III.

From Table I, it can be seen that compared to lightweight ADP, although multiple privacy preservation mechanism possesses huge computational overhead, its improvement in information uncertainty and data attack resistance is significant. Shannon entropy and Root Mean Square Error (RMSE) are 40.5523 and 10.5708 respectively, significantly higher than ADP's 0.3672 and 0.2681. Similarly, Shannon entropy and RMSE of multiple privacy preservation mechanism has increased by 0.91% and 53.4% in comparison to FHE respectively, indicating that multiple privacy preservation mechanism also has better privacy preservation efficacy. In terms of total cost of system optimization, multiple privacy preservation mechanism reduces ADP by about 0.68% and FHE by about 0.43%, reflecting better economic efficacy.

Remark 10: RMSE represents the root mean square difference between the attacker's reconstruction of confidential

TABLE I

PERFORMANCE INDICATORS OF DIFFERENT PRIVACY-PRESERVING MECHANISMS

Mechanism	Shannon Entropy	RMSE	Cost	Time
ADP	0.3672	0.2681	63588	0.0019
FHE	40.1851	6.9366	63007	3.3166
Multi-Privacy	40.5523	10.5708	62499	3.3371

TABLE II

COMPUTATIONAL OVERHEAD OF DIFFERENT PRIVACY-PRESERVING MECHANISMS

System	Multi-Privacy	ADP	FHE
IEEE 30-bus	15.0554	0.4732	14.7836
IEEE 118-bus	59.6097	1.9582	59.3053

TABLE III

TIME FOR DIFFERENT OPERATIONS IN FHE

System	Total	Key Generation	Encryption	Decryption
IEEE 30-bus	14.7836	0.4333	10.6779	3.6724
IEEE 118-bus	59.3053	0.2826	41.9825	17.0402

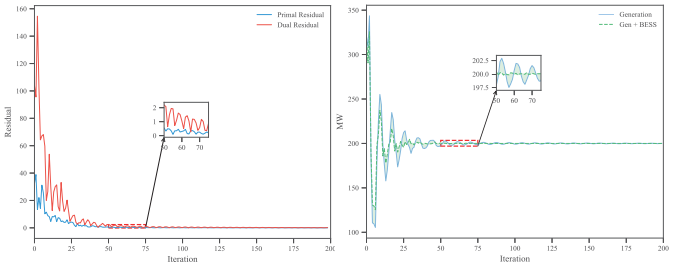
data and the true value, and is a direct indicator of the attacker's ability to resist attacks. The larger the RMSE, the more difficult it is for attackers to recover the original data and the stronger the privacy preservation. Shannon entropy reflects the overall increase in data uncertainty. The higher the entropy, the more chaotic the information, and the more difficult it is for attackers to extract structures from statistical distributions.

From Table II, it can be inferred that the computation time increases significantly with the increase of system size. Specifically, the computation time for ADP, FHE, and multiple privacy preservation mechanisms increased by approximately 4.13 times, 4.01 times, and 3.96 times, respectively, from IEEE 30-bus system to IEEE 118-bus system. This indicates that as the number of nodes increases, the computational complexity is mainly dominated by the number of participating nodes N, which is in line with the theoretical expectation of distributed ADMM algorithm. Meanwhile, the results in Table II also indicate that FHE operation occupies the main bottleneck in overall computation. The results in Table III indicate that encryption operations occupy the main bottleneck in the overall FHE operation.

From Table III, it can be seen that as the system scale expands from IEEE 30-bus system to IEEE 118-bus system. The number of buses increases by about 10 times, while the total FHE computation time increases from 14.7836 seconds to 59.3053 seconds, an increase of about 3.01 times. Further analysis of the overhead ratio of key operations reveals that encryption operations are an absolute time bottleneck, accounting for 72.2% and 70.7% of the time consumption in IEEE 30-bus system and IEEE 118-bus system, respectively, while decryption and key generation have relatively small proportions.

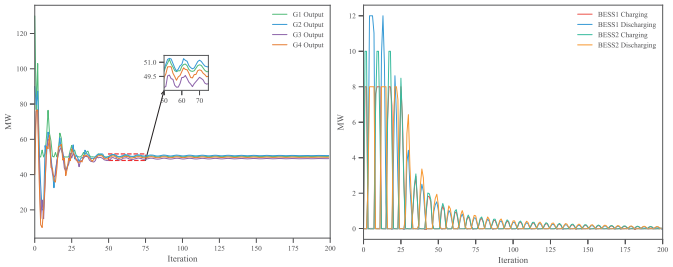
B. Simulated Results

The simulated results on the IEEE 30-bus system and IEEE 118-bus system are presented.



(a) (b)

Fig. 2. Simulated results on IEEE 30-bus system: (a) Residual convergence curves. (b) Power compensation for BESSs.



(a) (b)

Fig. 3. Simulated results on IEEE 30-bus system: (a) Generator power trajectory. (b) BESSs charging and discharging trajectory.

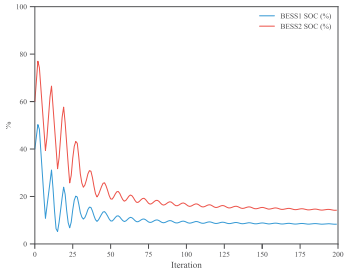
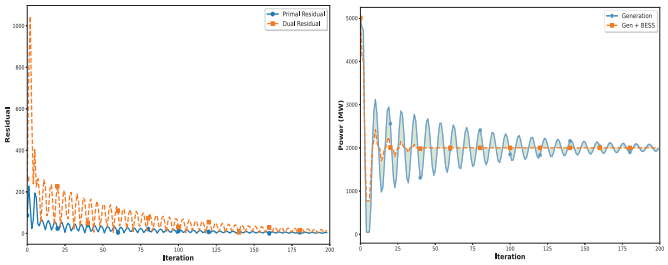


Fig. 4. SOC trajectory of BESSs on IEEE 30-bus system.

The parameters of generators and BESSs can be referred to [10]. The related privacy-preserving parameters are given as follows $\pi_i = 10$, $\kappa_i = 0.93$, $\rho = 3$, $P_{load_{30}} = 200$, $P_{load_{118}} = 2000$. Then, by applying multiple privacy-preserving ADMM algorithm with (11)-(16) to solve the problem of achieving minimum power generation cost and collaborative optimization of DGs under multiple privacy preservation scheme for the objective function. The corresponding simulation results are shown in Figs.2-5.

Fig.2.(a) depicts both the original residual and dual residual values decrease continuously over iterations and approach zero. Furthermore, Fig.2.(b) illustrates that the power generation and energy storage gradually converge to a stable value with the iteration progresses.

Fig.3.(a) and Fig.3.(b) show that during the iteration process, the output power of each generator and the charging and discharging power of BESS gradually stabilize, verifying the effectiveness of minimizing the objective function. It can be inferred from Fig.4 that the SOC curves of BESS1 and BESS2 exhibit certain fluctuations during the iteration process, but overall remains within a reasonable range (5).



(a) (b)

Fig. 5. Simulated results on IEEE 118-bus system: (a) Residual convergence curves. (b) Power compensation for BESSs.

Fig.5 demonstrates that the proposed scheme is still applicable to large-scale systems with many nodes, proving that the algorithm proposed in this paper has strong scalability.

Remark 11: Although FHE has the problems of high computational overhead and slow encryption/decryption speed, by using the TenSEAL library and CKKS scheme, and utilizing batch processing and parallelization optimization, acceptable encryption/decryption speed has been achieved for small and medium-sized systems under conservative parameters with polynomial modulus of 8192. Meanwhile, the design allows each computing node to autonomously perform local encryption updates and occasional synchronous communication, supporting flexible addition and deletion of nodes without the need for significant reconstruction. The simulation results on IEEE 30-bus system and IEEE 118-bus system validated the scalability of the designed framework.

VI. Conclusion

In this article, a multiple privacy preservation scheme that combines FHE and ADP for ADMM algorithm is proposed to cope with the limitations of a single mechanism in privacy preservation for microgrids. The core goal is to minimize power generation costs while preserving sensitive information of DGs. The algorithm achieves dual privacy preservation by adding ADP noise in the local optimization and encrypting the transmitted data through FHE. An extended Lyapunov function is constructed to prove the convergence of the algorithm under noise interference and the efficacy of the mechanism is verified through simulation experiments on IEEE 30-bus system and IEEE 118-bus system. In future work, we will mainly focus on designing strategies for adaptive noise intensity and encryption levels, and how to speed up convergence, such as introducing dynamic event triggering mechanism [30], [31].

References

[1] Y. Li, S. Liu, L. Zhu, and H. Wang, "Neural fictitious-self play-based cyber-layer defense for frequency control in microgrids against FDI attacks," *IEEE Trans. Consum. Electron.*, vol. 71, no. 2, pp. 6109–6119, May 2025.

[2] D. Zhang, R. Han, W. Fu, L. Ran, and J. Qin, "Bi-level robust optimal energy management of a community microgrid via Stackelberg game," *IEEE Trans. Consum. Electron.*, vol. 71, no. 2, pp. 6889–6899, May 2025.

[3] H. Bai, S. Weng, D. Yue, and C. Dou, "Distributed privacy-preserving economic dispatch of isolated microgrid based on event-triggered mechanism," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 55, no. 8, pp. 5477–5490, Aug. 2025.

[4] Z. Zhao et al., "Distributed robust model predictive control-based energy management strategy for islanded multi-microgrids considering uncertainty," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 2107–2120, May 2022.

[5] W. Zhang, T. Qian, X. Chen, K. Huang, W. Tang, and Q. Wu, "Resilient economic control for distributed microgrids under false data injection attacks," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4435–4446, Sep. 2021.

[6] S. Mao et al., "A finite-time distributed optimization algorithm for economic dispatch in smart grids," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 4, pp. 2068–2079, Apr. 2021.

[7] R. Wang, Q. Li, and H. Liu, "Distributed economic dispatch under random time-varying digraph," *IEEE Trans. Ind. Informat.*, vol. 20, no. 9, pp. 11139–11148, Sep. 2024.

[8] Z. Bai, D. Xu, B. Zhou, X. Yang, H. Yang, and J. Liu, "Computing optimal resilience-oriented operation of distribution systems considering heterogenous consumer-side microgrids," *IEEE Trans. Consum. Electron.*, vol. 71, no. 2, pp. 5866–5875, May 2025.

[9] Y. Zhang, H. Zhao, B. Li, and X. Wang, "Research on dynamic pricing and operation optimization strategy of integrated energy system based on Stackelberg game," *Int. J. Electr. Power Energy Syst.*, vol. 143, Dec. 2022, Art. no. 108446.

[10] D. Zhao et al., "Differential privacy energy management for islanded microgrids with distributed consensus-based ADMM algorithm," *IEEE Trans. Control Syst. Technol.*, vol. 31, no. 3, pp. 1018–1031, May 2023.

[11] X. Xue et al., "A fully distributed ADP algorithm for real-time economic dispatch of microgrid," *IEEE Trans. Smart Grid*, vol. 15, no. 1, pp. 513–528, Jan. 2024.

[12] J. Liu, N. Zhang, L. Zha, X. Xie, and E. Tian, "Reinforcement learning-based decentralized control for networked interconnected systems with communication and control constraints," *IEEE Trans. Autom. Sci. Eng.*, vol. 21, no. 3, pp. 4674–4685, Jul. 2024.

[13] J. Liu, N. Zhang, Y. Li, X. Xie, E. Tian, and J. Cao, "Learning-based event-triggered tracking control for nonlinear networked control systems with unmatched disturbance," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 53, no. 5, pp. 3230–3240, May 2023.

[14] J. Liu, Y. Dong, L. Zha, X. Xie, and E. Tian, "Reinforcement learning-based tracking control for networked control systems with DoS attacks," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 4188–4197, 2024.

[15] Y. Gan, Z. Xiao, T. Ke, and Z. Liang, "UAV application with XAI and soft computing methods to protect privacy of power-data in smart grids," *IEEE Trans. Consum. Electron.*, vol. 71, no. 2, pp. 3921–3929, May 2025.

[16] L. Zha, J. Miao, J. Liu, E. Tian, and C. Peng, "Data-driven decentralized resilient control for large-scale systems under DoS attacks," *IEEE Trans. Consum. Electron.*, vol. 71, no. 2, pp. 5310–5320, May 2025.

[17] A. Mubarak et al., "FPGA-driven secure energy routing and attack detection in decentralized microgrids with SREM-based dynamic path optimization," *IEEE Trans. Consum. Electron.*, vol. 71, no. 4, pp. 11279–11288, Nov. 2025.

[18] L. Yan, X. Chen, and Y. Chen, "A consensus-based privacy-preserving energy management strategy for microgrids with event-triggered scheme," *Int. J. Electr. Power Energy Syst.*, vol. 141, Oct. 2022, Art. no. 108198.

[19] L. Sun, D. Ding, H. Dong, and X. Bai, "Privacy-preserving distributed economic dispatch for microgrids based on state decomposition with added noises," *IEEE Trans. Smart Grid*, vol. 15, no. 3, pp. 2424–2433, May 2024.

[20] W. Chen, Z. Wang, J. Hu, and G.-P. Liu, "Differentially private average consensus with logarithmic dynamic encoding–decoding scheme," *IEEE Trans. Cybern.*, vol. 53, no. 10, pp. 6725–6736, Oct. 2023.

[21] R. Tian, Z. Zuo, Q. Han, Y. Wang, and W. Zhang, "Differential privacy for second-order bipartite consensus over signed digraph," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 54, no. 6, pp. 3652–3664, Jun. 2024.

[22] D. Zhao, D. Liu, and L. Liu, "Distributed privacy preserving algorithm for economic dispatch over time-varying communication," *IEEE Trans. Power Syst.*, vol. 39, no. 1, pp. 643–657, Jan. 2024.

[23] L. Pan, H. Shao, Y. Lu, M. Mesbahi, D. Li, and Y. Xi, "Privacy-preserving average consensus via matrix-weighted inter-agent coupling," *Automatica*, vol. 174, Apr. 2025, Art. no. 112094.

[24] H. Zhang et al., "Homomorphic encryption-based resilient distributed energy management under cyber-attack of micro-grid with event-triggered mechanism," *IEEE Trans. Smart Grid*, vol. 15, no. 5, pp. 5115–5126, Sep. 2024.

[25] W. Chen, Z. Wang, Q. Ge, H. Dong, and G.-P. Liu, "Quantized distributed economic dispatch for microgrids: Paillier encryption–decryption scheme," *IEEE Trans. Ind. Informat.*, vol. 20, no. 4, pp. 6552–6562, Apr. 2024.

[26] Z.-P. Yuan, P. Li, Z.-L. Li, and J. Xia, "A fully distributed privacy-preserving energy management system for networked microgrid cluster based on homomorphic encryption," *IEEE Trans. Smart Grid*, vol. 15, no. 2, pp. 1735–1748, Mar. 2024.

[27] Z. Cheng, F. Ye, X. Cao, and M.-Y. Chow, "A homomorphic encryption-based private collaborative distributed energy management system," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5233–5243, Nov. 2021.

[28] S. Boyd, "Distributed optimization and statistical learning via the alternating direction method of multipliers," *Found. Trends Mach. Learn.*, vol. 3, no. 1, pp. 1–122, 2010.

[29] T. Huang, S. Gao, and L. Xie, "A neural Lyapunov approach to transient stability assessment of power electronics-interfaced networked microgrids," *IEEE Trans. Smart Grid*, vol. 13, no. 1, pp. 106–118, Jan. 2022.

[30] F. Yang, J. Liu, Y. Du, and C.-B. Yan, "Predefined-time secure distributed energy management for microgrids against DoS attack based on dynamic event-triggered approach," *IEEE Trans. Autom. Sci. Eng.*, vol. 22, pp. 12791–12801, 2025.

[31] F. Yang, J. Liu, and X. Guan, "Distributed fixed-time optimal energy management for microgrids based on a dynamic event-triggered mechanism," *IEEE/CAA J. Automatica Sinica*, vol. 11, no. 12, pp. 2396–2407, Dec. 2024.

Jinliang Liu (Senior Member, IEEE) received the Ph.D. degree in control theory and control engineering from the School of Information Science and Technology, Donghua University, Shanghai, China, in 2011.

He was a Post-Doctoral Research Associate with the School of Automation, Southeast University, Nanjing, China, from December 2013 to June 2016. He was a Visiting Researcher/Scholar with the Department of Mechanical Engineering, The University of Hong Kong, Hong Kong, from October 2016 to October 2017. He was a Visiting Scholar with the Department of Electrical Engineering, Yeungnam University, Gyeongsan, South Korea, from November 2017 to January 2018. From June 2011 to May 2023, he was an Associate Professor and then a Professor with Nanjing University of Finance and Economics, Nanjing, China. In June 2023, he joined Nanjing University of Information Science and Technology, Nanjing, where he is currently a Professor with the School of Computer Science. His research interests include cyber-physical systems, autonomous systems, privacy preservation, and game theory.

Enyu Ma received the B.S. degree in computer science and technology from Jiangsu Ocean University, Lianyungang, China, in 2024. He is currently pursuing the M.S. degree in computer technology with the College of Computer Science, Nanjing University of Information Science and Technology, Nanjing, China. His research interests include privacy preservation, microgrids, and optimization algorithms.

Lijuan Zha received the Ph.D. degree in control science and engineering from Donghua University, Shanghai, China, in 2018.

From December 2017 to March 2024, she was an Associate Professor with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing, China. From 2018 to 2023, she was a Post-Doctoral Research Associate with the School of Mathematics, Southeast University, Nanjing. Since April 2024, she has been a Professor with the College of Science, Nanjing Forestry University, Nanjing. Her current research interests include networked control systems, neural networks, and complex dynamical systems.

Engang Tian (Senior Member, IEEE) received the B.S. degree in mathematics from Shandong Normal University, Jinan, China, in 2002, the M.Sc. degree in operations research and cybernetics from Nanjing Normal University, Nanjing, China, in 2005, and the Ph.D. degree in control theory and control engineering from Donghua University, Shanghai, China, in 2008.

From 2011 to 2012, he was a Post-Doctoral Research Fellow with The Hong Kong Polytechnic University, Hong Kong. From 2015 to 2016, he was a Visiting Scholar with the Department of Information Systems and Computing, Brunel University London, Uxbridge, U.K. From 2008 to 2018, he was an Associate Professor and then a Professor with the School of Electrical and Automation Engineering, Nanjing Normal University. In 2018, he was appointed as an Eastern Scholar by the Municipal Commission of Education, Shanghai, and joined the University of Shanghai for Science and Technology, Shanghai, where he is currently a Professor with the School of Optical-Electrical and Computer Engineering. He has published more than 100 articles in refereed international journals. His research interests include networked control systems, cyber attacks, and nonlinear stochastic control and filtering.