Privacy-Preserving Distributed Economic Dispatch of Microgrids
A Dynamic Quantization-Based Consensus Scheme With Homomorphic Encryption

Chen, Wei; Liu, Lu; Liu, Guo-Ping

Published in:
IEEE Transactions on Smart Grid

Published: 01/01/2023

Document Version:
Post-print, also known as Accepted Author Manuscript, Peer-reviewed or Author Final version

Published version (DOI):
10.1109/TSG.2022.3189665

Publication details:
Chen, W., Liu, L., & Liu, G.-P. (2023). Privacy-Preserving Distributed Economic Dispatch of Microgrids: A Dynamic Quantization-Based Consensus Scheme With Homomorphic Encryption. *IEEE Transactions on Smart Grid*, *14*(1), 701-713. https://doi.org/10.1109/TSG.2022.3189665

Chen, W., Liu, L., & Liu, G-P. (2023). Privacy-Preserving Distributed Economic Dispatch of Microgrids: A Dynamic Quantization-Based Consensus Scheme With Homomorphic Encryption. IEEE Transactions on Smart Grid, 14(1), 701-713. https://doi.org/10.1109/TSG.2022.3189665.

Privacy-Preserving Distributed Economic Dispatch of Microgrids: A Dynamic Quantization Based Consensus Scheme with Homomorphic Encryption

Wei Chen, Lu Liu, *Senior Member, IEEE*, and Guo-Ping Liu, *Fellow, IEEE*

***Abstract*—This paper is concerned with the privacy-preserving distributed economic dispatch problem (ED) of microgrids. A homomorphically encrypted consensus algorithm is developed in the absence of a third party to achieve optimal power distribution with the least cost while preventing sensitive information leakage during the entire communication process. For ease of data encryption, a novel estimator-like dynamic quantizer is first constructed, where the information to be transmitted is converted into a series of finite-level codewords. Then, a sufficient condition is derived, taking advantage of mathematical induction and the properties of matrix norms, to ensure that the quantization output is unsaturated and *exact* consensus is reached. Furthermore, by means of the additive homomorphic property of the Paillier algorithm to embed secrecy in pairwise interaction dynamics, the confidential communication strategy is adopted to ensure that the distributed algorithm converges to the optimal value without disclosing private or sensitive state information of agents. Finally, case studies are provided to illustrate the feasibility and validity of the adopted privacy-preserving ED scheme in IEEE 39-bus power systems.**

***Index Terms*—Microgrids, economic dispatch, consensus algorithm, privacy preservation, dynamic quantization, homomorphic cryptography.**

I. Introduction

With the growing global energy crisis and environmental pollution, the past years have seen an increasing interest in intelligent microgrids, where distributed generators (DGs) offer a promising approach to facilitate the integration of renewable energy [1]–[3]. As one of the fundamental issues of energy management, economic dispatch (ED) plays an important role in the operation and control of microgrids, whose main aim is to schedule power outputs of all DGs to meet the load demand at the lowest operating cost under practical system constraints [4], [5]. In recent decades, some optimization methods, such as the lambda-iteration method [4], the Newton-Raphson method [6], the interior-point method [7], and heuristic algorithms (e.g., particle swarm optimization [8] and genetic algorithm [9]), have been successfully applied to address various ED problems. However, the aforementioned centralized methods are far difficult to meet the operation and control demand of microgrids because of the increasing network scale [10]. Hence, considerable research attention has turned to develop distributed ED algorithms owing to their merits in robustness, reliability, and scalability [5].

Thanks to the consensus theory of multi-agent systems, some distributed algorithms have been developed to solve the ED problem of microgrids [5], [11]–[16]. For example, a "consensus+innovation" framework has been established [11], where an innovation term, which is introduced to a consensus update, is regarded as a feedback mechanism to adjust the incremental cost of each generator to the optimal value. The feedback gain sequence is required to be decaying to ensure the convergence of the distributed algorithm. Subsequently, a fully distributed algorithm with a fixed gain has been developed to solve the optimal ED problem [5], which can collaboratively estimate the total mismatch between demand and supply. Moreover, the convergence of the employed consensus-based scheme has been analyzed by using the eigenvalue perturbation approach. In addition, a novel consensus-based approach has been proposed to improve the convergence rate of the distributed algorithm [16].

To achieve optimal ED in a distributed manner, agents need to communicate with their neighboring nodes over a relatively open network, which inevitably leads to privacy disclosure. Some malicious adversaries or eavesdroppers may exploit sensitive information to disturb the electricity market, even destroy the reliability and stability of microgrids, resulting in severe security threats. Therefore, it is urgently crucial to design a privacy-preserving distributed scheme to prevent privacy leakage. Recently, some privacy-preserving consensus schemes have been proposed to address distributed optimization problem [15], [17]–[21]. For instance, a differentially private distributed algorithm has been developed via adding the independent Laplacian noise [15], [18]. However, the adopted approach cannot reach the exact convergence due to the intrinsic tradeoff between the privacy level and convergence accuracy. To tackle such a tradeoff, a sequence of correlated noises has been injected into sensitive information to preserve privacy [17], [19]. Such a scheme may be vulnerable, given that external eavesdroppers can infer the initial value by constructing an appropriate observer. Instead of adding random noises, an observability-based approach has been proposed in [20], [21] by designing interaction topology to weaken the

This work was supported by the National Natural Science Foundation of China under Grant 61773327, and the Research Grants Council of the Hong Kong Special Administrative Region of China under Project CityU/11217619. (*corresponding author: Lu Liu*)

W. Chen is with the City University of Hong Kong Shenzhen Research Institute, City University of Hong Kong, Shenzhen 518057, China, (Email: chenweibro@163.com).

L. Liu is with the Department of Mechanical and Biomedical Engineering, City University of Hong Kong, Kowloon, Hong Kong, (Email: luliu45@cityu.edu.hk).

G.-P. Liu is with the Center for Control Science and Technology, Southern University of Science and Technology, Shenzhen 518055, China, (Email: liugp@sustech.edu.cn).

observability of a compromised agent. Although the ability of the compromised agent is minimized to estimate the initial states of other agents, this scheme cannot provide privacy preservation for the direct neighboring nodes.

To improve the privacy-preserving performance of the aforementioned approaches, an alternative approach is to adopt cryptography to encrypt sensitive data. By means of algebraic number theory, the main idea of encryption is confusion where a data is transformed into a huge number to confuse an eavesdropper and make deciphering nearly impossible without the private key. Compared with widely employed noise-injected privacy-preserving schemes [15], [19], the cryptography-based one, despite its weakness in computational complexity, preserves the structure of the original data since its encryption/decryption process is an invertible transformation. The cryptography-based method can provide privacy and security for confidential communication when a trustworthy third party is available (e.g., cloud-based control or computation [22], [23]). However, such a scheme is a centralized one with centralized key management in multi-agent networks where a central authority is required. To achieve a completely decentralized and third-party free confidential communication, a homomorphically encrypted average consensus algorithm has been first developed in [24], which combined the homomorphic encryption with the random weight construction in data exchange to prevent two parties in a pairwise interaction from exposing information to each other. In addition, a mechanism similar to the communication request and return has been introduced to achieve decentralized key management, where the node sent its public key and encrypted state to neighboring nodes, and then returned encrypted weighted differences after a two-step homomorphic encryption operation.

Typically, the distributed algorithms are designed to operate with real numbers, while cryptography-based encryption only operates on the set of integers. To bridge this gap, a natural idea is to introduce a quantization scheme to achieve transformation from real numbers to integers before data encryption. Due to limited communication resources and computational ability, finite quantization levels inevitably cause quantization errors. The existing static quantization scheme [12], [24] need to increase quantization levels to improve the convergence accuracy of the distributed algorithm, resulting in more data release. Furthermore, the computational complexity of the encryption algorithm and the data communication traffic of the distributed scheme are inevitably increased since the increasing bit length of quantized/encoded outputs [25]. Therefore, exploring an applicable cryptography-based distributed ED algorithm with an appropriate quantization scheme is of practical importance in ensuring both convergence accuracy and implementation efficiency of the distributed algorithm, and this motivates our current investigation.

In summary, three essential challenges of this paper are identified as follows: *(1) How to design a quantization strategy to deal with the tradeoff between quantization accuracy and system performance? (2) How to analyze the convergence of the distributed algorithm under the quantization scheme? and (3) How to develop a cryptography-based confidential communication scheme under the dynamic quantization mechanism to achieve privacy-preserving consensus without any third parties?* To handle the above-mentioned difficulties, in this paper, we develop a homomorphic cryptography-based consensus algorithm with a dynamic quantization scheme to solve the optimal distributed ED problem of microgrids *without* quantization error effects. The main contributions of this paper are highlighted as follows:

1) A novel dynamic quantizer is proposed to effectively eliminate the quantization error effects by constructing an estimator-like auxiliary equation, where the quantized signal is a "prediction error" rather than the state. Intuitively speaking, the amplitude of the prediction error is smaller than that of the state itself, which results in less data release.
2) A sufficient condition concerning the finite-level quantizer design is derived to ensure bounded quantization output and exact convergence of the distributed algorithm by means of mathematical induction and matrix norm analysis. In addition, the convergence rate of the developed algorithm is also analyzed in light of the defined asymptotic convergence factor.
3) A cryptography-based consensus algorithm under the dynamic quantization scheme is developed to prevent the leakage of private information of microgrids by resorting to the additive homomorphic property of the Paillier algorithm. Furthermore, the analysis of privacy and security shows that the proposed scheme provides resilience against external and honest-but-curious adversaries aiming to eavesdrop exchanged information.

The rest of this paper is listed as follows. Section II presents some preliminaries in terms of microgrid structure and classic consensus-based ED algorithm. In Section III, a novel dynamic quantization scheme is proposed, and a sufficient condition is derived to ensure exact consensus. Section IV gives a confidential communication scheme by means of the additive homomorphic property of the Paillier algorithm. Section V provides simulation studies to verify the theoretical results. Finally, Section VI states the conclusions.

Notation: $\mathbb{R}$, $\mathbb{R}^n$, and $\mathbb{R}^{p\times q}$ are the set of real numbers, n-dimensional real vectors, and $n\times m$ real matrices, respectively. $|a|$ is the absolute value of a. $\|A\|_\infty$ refers to the ∞-norm of matrix A. Functions $\gcd(x,y)$ and $\mathrm{lcm}(x,y)$ stand for the greatest common divisor of x and y and the least common multiple of x and y, respectively. $\mathbb{Z}$ is the set of prime numbers. $\mathbb{Z}_n = \{z|z \in \mathbb{Z}, 0 \leq z < n\}$ means that the set of prime numbers less than n. $\mathbb{Z}_n^* = \{z|z \in \mathbb{Z}, 0 \leq z < n, \gcd(z,n) = 1\}$ is the set of numbers less than and co-prime to n. $\mathrm{diag}\{A_1, A_2, \cdots, A_N\}$ represents the block-diagonal matrix. $\mathbf{0}_n$ is the n-dimensional zero vector.

II. Preliminaries

A. Microgrid Structure

As shown in Fig. 1, the structure of microgrids involves a physical layer and a cyber communication layer. The physical layer is an interconnected electrical grid for the purpose of transmitting electric power from DGs to loads. The cyber communication layer, which can be described by a sparse

communication network, supports some applications, such as dynamic monitoring, fault diagnosis, ED, cyber security, and privacy preservation (see e.g., [3], [19], [26]).

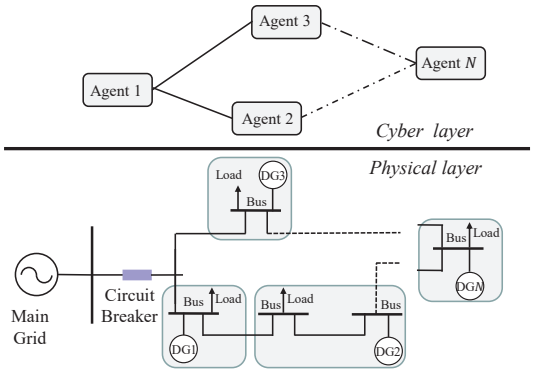

Fig. 1. Microgrid Structure.

1) Physical Layer: The microgrid mainly consists of local loads and DGs. In this paper, without loss of generality, we assume that the microgrid has N DGs. The DGs may include photovoltaic panels, fuel cells, micro-turbines, oil- and coal-fired steam, and wind turbines [1], [3], [10]. These DGs are of flexible structure, which can be freely plugged and played into microgrids. Furthermore, the microgrid can be integrated into the main grid through a circuit breaker; hence, it can be operated in two modes (i.e., the grid-connected mode and the islanded mode). In the islanded mode, the microgrids need to maintain the balance of power supply and load demand to achieve autonomous operation, which is the main focus of this paper.

2) Cyber Communication Layer: In this paper, it is assumed that each agent owns a certain number of loads and a DG locally, which can collect local power supply and local demand information, and also provide optimal reference power to DG via data exchange with its neighboring agents. In this case, the communication network has N agents which can be described by a weight undirected graph $\mathscr{G} = (\mathcal{V}, \mathcal{E})$ with the node set $\mathcal{V} = \{1, 2, \cdots, N\}$ and the edge set $\mathcal{E} = \{(i,j)|i,j \in \mathcal{V}\} \subseteq \mathcal{V} \times \mathcal{V}$. The edge (i,j) means that agent i and j can communicate with each other. Denote the neighboring set of node i as $\mathcal{N}_i = \{j|(i,j) \in \mathcal{E}, i \neq j\}$. In addition, it is assumed that the undirected graph is connected. Note that the physical network and communication network can be of different topologies.

B. Standard Consensus-Based ED Algorithm

In islanded microgrids, the purpose of the distributed ED is to achieve a balance between global power output and load demand in minimizing total generation cost via local communication between agents. For ease of analysis processing, we assume that practical power loss is ignored. Specific details are presented in the following.

For agent i $(i \in \mathcal{V})$, the collected local load demand is P_{Di} and the local power generation is $P_i \in [P_i^m, P_i^M]$. The generation cost of agent i (i.e., DG i) is denoted by the following quadratic function:

$$C_i(P_i) = a_i P_i^2 + b_i P_i + c_i, \tag{1}$$

where a_i, b_i, and c_i are the fitting cost coefficients of DG i. Furthermore, the function (1) can be transformed as

$$C_i(P_i) = \frac{(P_i - \vartheta_i)^2}{2\theta_i} + \kappa_i, \tag{2}$$

where $\theta_i = \frac{1}{2a_i}$, $\vartheta_i = -\frac{b_i}{2c_i}$, and $\kappa_i = c_i - \frac{b_i^2}{4a_i}$. The physical explanation or related practical examples on cost function (1) can refer to e.g., [4] for more details. The ED problem, which is to minimize the global generation cost under generator constraints, is described as

$$\begin{aligned} \underset{\{P_1,\ldots,P_N\}}{\arg\min} \ & \sum_{i\in\mathcal{V}} C_i\left(P_i\right) \\ \text{s.t.} \quad & \sum_{i\in\mathcal{V}} P_i = \sum_{i\in\mathcal{V}} P_{Di} = P_D, \\ & P_i^m \le P_i \le P_i^M, \end{aligned} \tag{3}$$

where P_D is the total power demand satisfying $\sum_{i\in\mathcal{V}} P_i^m \le P_D \le \sum_{i\in\mathcal{V}} P_i^M$.

To solve the above optimal ED problem, let us first denote the incremental cost of agent i by

$$\lambda_i = \frac{dC_i(P_i)}{dP_i} = \frac{P_i - \vartheta_i}{\theta_i}. \tag{4}$$

Then, the standard consensus algorithm is developed as follows [5]:

$$\begin{cases} \lambda_{i,k+1} = \displaystyle\sum_{j\in\mathcal{N}_i\cup\{i\}} l_{ij}\lambda_{j,k} + \epsilon\phi_{i,k} \\ P_{i,k+1} = \begin{cases} P_i^M, & \lambda_{i,k+1} \le \lambda_i^M \\ \theta_i\lambda_{i,k+1} + \vartheta_i, & \lambda_i^m < \lambda_{i,k+1} < \lambda_i^M \\ P_i^m, & \lambda_{i,k+1} \ge \lambda_i^m \end{cases} \\ \phi_{i,k+1} = \displaystyle\sum_{j\in\mathcal{N}_i\cup\{i\}} w_{ij}\phi_{j,k} - (P_{i,k+1} - P_{i,k}), \end{cases} \tag{5}$$

for $\forall i \in \mathcal{V}$, where $\epsilon > 0$ is a small gain parameter, $\lambda_i^m = \frac{P_i^m - \vartheta_i}{\theta_i}$, $\lambda_i^M = \frac{P_i^M - \vartheta_i}{\theta_i}$, $\phi_{i,k}$ is the local power estimation error between the demand and the supply. Here, l_{ij} and w_{ij} are the connection weight associated with graph $\mathscr{G}$, which can be selected as follows:

$$l_{ij} = w_{ij} = \begin{cases} (1 + \max\{d_i, d_j\})^{-1}, & j \in \mathcal{N}_i \\ 1 - \sum_{j\in\mathcal{N}_i} w_{ij}, & i = j \\ 0, & \text{otherwise}, \end{cases}$$

where d_i is the number of neighbors of agent i except itself. Note that $L = [l_{ij}]_{N\times N}$ and $W = [w_{ij}]_{N\times N}$ are doubly stochastic matrices. Furthermore, the initial state of agent i $(i \in \mathcal{V})$ can be given as follows:

$$\begin{cases} P_{i,0} = \begin{cases} P_i^m, & P_{Di} \le P_i^m \\ P_i, & P_i^m < P_i < P_i^M \\ P_i^M, & P_i^M \le P_{Di} \end{cases} \\ \lambda_{i,0} = \frac{P_{i,0} - \vartheta_i}{\theta_i} \\ \phi_{i,0} = P_{Di} - P_{i,0}. \end{cases} \tag{6}$$

Remark 1: So far, two types of weights have been widely applied in recent literature, namely, the maximum-degree weights [14] and Metropolis weights [27]. The Metropolis weights, the selected rule in this paper, have huge merit in fully distributed implementation given that the global information, including the number of agents, is not required. In addition, the parameter ϵ is also named as learning gain, which plays an important role in the convergence of the consensus algorithm (5). Recently, some approaches have been provided to design parameter ϵ. For example, the iterative numerical method developed in [5] can find a sub-optimal solution via a few iterations. In [14], the upper bound $\bar{\epsilon}$ has been obtained by virtue of the related conclusion of optimal matching distance. In our paper, the selected $\epsilon \in (0, \bar{\epsilon})$ follows from Proposition 2 in [14].

Lemma 1: [5] Consider the consensus algorithm (5) with initial condition (6) under connected undirected graph $\mathscr{G}$. If $\epsilon > 0$ is a sufficiently small constant, then the algorithm (5) can converge to the optimal solution of the ED problem (3), i.e.,

$$\lim_{k\to\infty} \lambda_{i,k} = \lambda^\star, \lim_{k\to\infty} P_{i,k} = P_i^\star, \lim_{k\to\infty} \phi_{i,k} = 0,\ i \in \mathcal{V}, \quad (7)$$

where the optimal incremental cost $\lambda^\star$ and the optimal power $P_i^\star$ are further expressed as

$$\begin{cases} \lambda^\star = \dfrac{\sum_{i=1}^N P_{i,0} + \sum_{i=1}^N \phi_{i,0} - \sum_{i=1}^N \vartheta_i}{\sum_{i=1}^N \theta_i} \\ \qquad = \dfrac{\sum_{i=1}^N P_{Di} - \sum_{i=1}^N \vartheta_i}{\sum_{i=1}^N \theta_i} \\ P_i^\star = \begin{cases} P_i^m, & \lambda^\star \le \lambda_i^m \\ \theta_i\lambda^\star + \vartheta_i, & \lambda_i^m < \lambda^\star < \lambda_i^M \\ P_i^M, & \lambda^\star \ge \lambda_i^M. \end{cases} \end{cases} \quad (8)$$

In consensus algorithm (5), the agent needs to communicate with its neighbors, during which some sensitive information may be eavesdropped by malicious attackers or leaked by its neighbors. Hence, the purpose of this paper is to provide a homomorphically encrypted communication scheme such that the distributed algorithm achieves optimal ED without quantization error effects under conditions that (i) the actual communication information is not disclosed to eavesdroppers; and (ii) the *real* initial state $\lambda_{i,0} \in \mathbb{R}$ and $\phi_{i,0} \in \mathbb{R}$ is not inferred or computed by neighboring agents.

Remark 2: In the smart grid, the generation power, the cost function parameters, and the local load demand are privacy sensitive data, which are reflected in initial values $\lambda_{i,0} = \frac{P_{i,0}-\vartheta_i}{\theta_i}$ and $\phi_{i,0} = P_{Di} - P_{i,0}$ in our paper. In the market, the generation power P_i and the cost function parameters (a_i, b_i, c_i) are important business information. When these information is revealed to other competitors, they can generate more power and reduce their own operational cost to disrupt the market in pursuit of more profit. In addition, the local load demand P_{Di} can reflect the electricity habits and behaviors of some consumers. If this sensitive information is learned by the thief, he can enter the consumer's house when the house is empty, which may cause property losses for individuals.

III. Dynamic quantization based Consensus Scheme

In this section, a dynamic quantization scheme is first provided for ease of computation and communication given that the encryption/decryption and encoding/decoding procedures need to be carried out on integers. In other words, the practical analog signal is required to be converted into a digital signal. Then, a sufficient condition is obtained to reach the exact consensus by means of the mathematical induction and the properties of matrix norms. Furthermore, the convergence rate is evaluated. More details are provided as follows.

A. Consensus Analysis

The consensus analysis is divided into two parts: the distributed ED algorithm without and with generation constraints.

Let us first investigate the scenario that consensus algorithm (5) without generation constraints. To achieve confidential communication, the consensus algorithm with time-varying weights can be described by

$$\begin{cases} \lambda_{i,k+1} = \lambda_{i,k} + \sum_{j\in\mathcal{N}_i} l_{ij,k}(\lambda_{j,k} - \lambda_{i,k}) + \epsilon\phi_{i,k} \\ \phi_{i,k+1} = (1-\epsilon\theta_i)\phi_{i,k} + \sum_{j\in\mathcal{N}_i} w_{ij,k}(\phi_{j,k} - \phi_{i,k}) \\ \qquad\qquad - \theta_i \sum_{j\in\mathcal{N}_i} l_{ij,k}(\lambda_{j,k} - \lambda_{i,k}), \end{cases} \quad (9)$$

where $l_{ij,k}$ and $w_{ij,k}$ are the time-varying weights, and can be constructed by $l_{ij,k} = l_{i\to j,k} l_{j\to i,k}$, $w_{ij,k} = w_{i\to j,k} w_{j\to i,k}$ with $l_{i\to j,k}$ ($l_{j\to i,k}$), $w_{i\to j,k}$ ($w_{j\to i,k}$) randomly generated by and only known to agent i (j). Furthermore, the selection of these random variables can follow

$$l_{i\to j,k}(w_{i\to j,k}) \begin{cases} \in (0, \sqrt{(1+\max\{d_i, d_j\})^{-1}}], & j \in \mathcal{N}_i \\ = 0, & \text{otherwise.} \end{cases}$$

Note that $l_{ij,k} = l_{ji,k}$ and $w_{ij,k} = w_{ji,k}$ for $i, j \in \mathcal{V}$, which mean that time-varying matrices $L_k = [l_{ij,k}]_{N\times N}$, $W_k = [w_{ij,k}]_{N\times N}$ are doubly stochastic.

Remark 3: The adopted weight construction method can not only ensure the convergence of the consensus algorithm but also achieve confidential communication [24]. To be more specific, the weight constructed by the product of two random variables can ensure symmetry (i.e., $l_{ij,k} = l_{ji,k}$), which is necessary for consensus. Furthermore, the generated coupling weights are completely independent of communication channels. In other words, such a weight is unknown to both agents in a pairwise interaction, which can ensure that the node does not directly infer the neighboring information and further facilitate the realization of privacy preservation without a third party.

Due to network bandwidth constraints, only finite number bits are transmitted over communication channels. To this end, a finite-level uniform quantizer is described as follows:

$$q_S(x) = \begin{cases} s\delta, & (s-\frac{1}{2})\delta \le x < (s+\frac{1}{2})\delta \\ S\delta, & x \ge (S+\frac{1}{2})\delta \\ -q_S(-x), & x \le -\frac{1}{2}\delta, \end{cases} \quad (10)$$

where δ is the quantization accuracy, $s = 0, 1, \cdots, S$, and thus the quantizer has $(2S+1)$ quantization levels. If $|x| \leq (S+\frac{1}{2})\delta$, then the quantization error satisfies $|x - q_S(x)| \leq \frac{1}{2}\delta$.

The dynamic quantization scheme is designed as:

$$\begin{cases} \hat{\lambda}_{i,k+1} = \hat{\lambda}_{i,k} + \epsilon\hat{\phi}_{i,k} + \varphi_k u^1_{i,k} \\ \hat{\phi}_{i,k+1} = (1-\epsilon\theta_i)\hat{\phi}_{i,k} + \varphi_k u^2_{i,k} \\ u^1_{i,k} = q_S\big(\frac{\lambda_{i,k+1} - \hat{\lambda}_{i,k} - \epsilon\hat{\phi}_{i,k}}{\varphi_k}\big) \\ u^2_{i,k} = q_S\big(\frac{\phi_{i,k+1} - (1-\epsilon\theta_i)\hat{\phi}_{i,k}}{\varphi_k}\big) \\ \hat{\lambda}_{i,0} = \hat{\phi}_{i,0} = 0, \end{cases} \tag{11}$$

where $u^1_{i,k}$ and $u^2_{i,k}$ are the quantization output, and $\hat{\lambda}_{i,k}$ and $\hat{\phi}_{i,k}$ are the estimation of $\lambda_{i,k}$ and $\phi_{i,k}$, respectively. Notably, dynamic equation (11) is simultaneously updated by two agents in a pairwise interaction. In addition, φ_k is the scaling function designed as $\varphi_k = \varphi_0\tau^k$ where φ_0 and τ are unknown parameters to be determined.

Hence, the dynamic quantization based consensus algorithm can be written as:

$$\begin{cases} \lambda_{i,k+1} = \lambda_{i,k} + \sum\limits_{j\in\mathcal{N}_i} l_{ij,k}(\hat{\lambda}_{j,k} - \hat{\lambda}_{i,k}) + \epsilon\phi_{i,k} \\ \phi_{i,k+1} = (1-\epsilon\theta_i)\phi_{i,k} + \sum\limits_{j\in\mathcal{N}_i} w_{ij,k}(\hat{\phi}_{j,k} - \hat{\phi}_{i,k}) \\ \qquad\qquad - \theta_i \sum\limits_{j\in\mathcal{N}_i} l_{ij,k}(\hat{\lambda}_{j,k} - \hat{\lambda}_{i,k}). \end{cases} \tag{12}$$

For simplicity, denote

$$\begin{aligned} \lambda_k &= [\ \lambda_{1,k} \quad \lambda_{2,k} \quad \cdots \quad \lambda_{N,k}\ ]^T, \\ \phi_k &= [\ \phi_{1,k} \quad \phi_{2,k} \quad \cdots \quad \phi_{N,k}\ ]^T, \\ \hat{\lambda}_k &= [\ \hat{\lambda}_{1,k} \quad \hat{\lambda}_{2,k} \quad \cdots \quad \hat{\lambda}_{N,k}\ ]^T, \\ \hat{\phi}_k &= [\ \hat{\phi}_{1,k} \quad \hat{\phi}_{2,k} \quad \cdots \quad \hat{\phi}_{N,k}\ ]^T, \\ x_k &= [\ \lambda_k^T \quad \phi_k^T\ ]^T, \quad \hat{x}_k = [\ \hat{\lambda}_k^T \quad \hat{\phi}_k^T\ ]^T, \\ \Theta &= \text{diag}\{\theta_1, \theta_2, \cdots, \theta_N\},\ \varsigma = \mathbf{1}_N^T\Theta\mathbf{1}_N, \\ \theta_{\max} &= \ \max\{\theta_1, \theta_2, \cdots, \theta_N\}. \end{aligned}$$

Denote the estimation error as $e_k = x_k - \hat{x}_k$, the distributed algorithm (12) can be written in the following augmented form:

$$x_{k+1} = (A^{(\epsilon)} - B_k)x_k + B_k e_k, \tag{13}$$

where

$$A^{(\epsilon)} \triangleq \begin{bmatrix} I_N & \epsilon I_N \\ \mathbf{0}_{N\times N} & I_N - \epsilon\Theta \end{bmatrix},$$

$$B_k \triangleq \begin{bmatrix} I_N - L_k & \mathbf{0}_{N\times N} \\ \Theta(L_k - I_N) & I_N - W_k \end{bmatrix}.$$

For the sake of simplicity, the superscript ϵ in $A^{(\epsilon)}$ is omitted in following parts.

Similarly, it follows from (11) that

$$\hat{x}_{k+1} = A\hat{x}_k + \varphi_k Q_S\Big(\frac{1}{\varphi_k}(x_{k+1} - A\hat{x}_k)\Big), \tag{14}$$

where $Q_S(\cdot) = [\ q_S(\cdot), \cdots, q_S(\cdot)\ ]^T$.

Before deriving our main results, let us present related assumption and lemma as follows.

Assumption 1: There exists a constant Υ such that $\|x_0\|_\infty \leq \Upsilon$.

Lemma 2: For any time instant k, if L_k and W_k are doubly stochastic matrices, there exist two instants $\epsilon > 0$ and $\rho \in (0,1)$ such that time-varying matrix $A - B_k$ has a simple eigenvalue 1 and corresponding left and right eigenvectors are $[\mathbf{1}_N^T\Theta\ \mathbf{1}_N^T]^T$ and $[\mathbf{1}_N^T\ \mathbf{0}_N^T]^T$, and the remaining $2N-1$ eigenvalues of $(A - B_k)$ have norms upper bounded by $\rho < 1$.

Proof: The proof is similar to that of *Lemma 1* in [12] and hence is omitted here. ■

Theorem 1: Under Assumption 1, if the quantizer satisfies the following conditions:

1) The quantization level satisfies

$$S \geq \frac{\|A\|_\infty + 2(1+\theta_{\max})}{2\tau} + \frac{2(1+\theta_{\max})^2}{(\tau-\rho)\tau} - \frac{1}{2};$$

2) The scaling function are designed as $\tau \in (\rho, 1)$ and

$$\varphi_0 \geq \max\Big\{\frac{\|A\|_\infty\Upsilon}{\big(S+\frac{1}{2}\big)\delta}, \frac{(2\varsigma+N)(\tau-\rho)\tau\Upsilon}{(1+\theta_{\max})\varsigma\delta}\Big\},$$

then there exists a sufficiently small constant $\epsilon > 0$ such that distributed algorithm (12) with dynamic quantization scheme (11) under connected and undirected graph $\mathscr{G}$ converges to the optimal solution (7) of the ED problem (3).

Proof: Define two vectors as $\nu \triangleq [\mathbf{1}_N^T\Theta\ \mathbf{1}_N^T]^T/\varsigma$, $\mu \triangleq [\mathbf{1}_N^T\ \mathbf{0}_N^T]^T$. In light of *Lemma 2*, it is observed that ν and μ are the left and right eigenvectors of $A - B_k$ corresponding to the eigenvalue 1 satisfying $\nu^T\mu = 1$. Moreover, there exists a nonsingular matrix $T_k \in \mathbb{R}^{2N\times 2N}$ of the following form

$$T_k = [\mu\ \ V_k], \quad T_k^{-1} = [r\ \ U_k^T]^T$$

such that $T_k^{-1}(A - B_k)T_k = \text{diag}\{1, J_k\}$, where $J_k = U_k(A - B_k)V_k$ is the Jordan block, and its spectral radius satisfies $\sup_{k\geq 0}\rho(J_k) = \rho < 1$.

Denote the consensus error as $\bar{x}_k = (I - \mu\nu^T)x_k$, it follows from $\mu\nu^T(A - B_k) = (A - B_k)\mu\nu^T = \mu\nu^T\mu\nu^T = \mu\nu^T$ and $(I_{2N} - \mu\nu^T)B_k = B_k(I_{2N} - \mu\nu^T) = B_k$ that

$$\begin{aligned} \bar{x}_{k+1} &= (A - B_k - \mu\nu^T)x_k + B_k e_k \\ &= (A - B_k - \mu\nu^T)(x_k - \mu\nu^T x_k) + B_k e_k \\ &= (A - B_k - \mu\nu^T)\bar{x}_k + B_k e_k. \end{aligned} \tag{15}$$

Note that $\text{rank}(\mu\nu^T) = \text{rank}(\nu^T\mu) = 1$ and $\nu^T\mu = 1$, it is verified that matrix $\mu\nu^T$ has a simple eigenvalue 1 and the remaining $2N-1$ eigenvalues are zeros, that is, $T_k^{-1}\mu\nu^T T_k = \text{diag}\{1, \underbrace{0, 0, \cdots, 0}_{2N-1}\}$. Hence, $A - B_k - \mu\nu^T = T_k\text{diag}\{0, J_k\}T_k^{-1}$ and its spectral radius is upper bounded by the constant $\rho < 1$.

Furthermore, the dynamical evolution of the estimation error is expressed as

$$\begin{aligned} e_{k+1} &= x_{k+1} - \hat{x}_{k+1} \\ &= (A - B_k)x_k + B_k e_k - A\hat{x}_k \\ &\quad - \varphi_k Q\Big(\frac{1}{\varphi_k}((A - B_k)x_k + B_k e_k - A\hat{x}_k)\Big) \end{aligned}$$

$$= (A+B_k)e_k - B_k\bar{x}_k - \varphi_k Q\Big(\frac{1}{\varphi_k}\big((A+B_k)e_k - B_k\bar{x}_k\big)\Big). \quad (16)$$

Let $\xi_k = \frac{1}{\varphi_k}\bar{x}_k$ and $\psi_k = \frac{1}{\varphi_k}e_k$, it follows from (15) and (16) that

$$\tau\xi_{k+1} = (A - B_k - \mu\nu^T)\xi_k + B_k\psi_k \quad (17a)$$

$$\tau\psi_{k+1} = (A+B_k)\psi_k - B_k\xi_k - Q\big((A+B_k)\psi_k - B_k\xi_k\big). \quad (17b)$$

Now, we are in a position to show that the quantization output is not saturated at each time instant k by mathematical induction. First, consider the initial instant (i.e., $k=0$). Due to the fact that $\hat{x}_0 = B_k\mu\nu^T x_0 = \mathbf{0}_{2N}$, one has

$$\begin{aligned}
&\frac{1}{\varphi_0}\|(A+B_0)e_0 - B_0\bar{x}_0\|_\infty \\
&= \frac{1}{\varphi_0}\|(A+B_0)x_0 - B_0(x_0 - \mu\nu^T x_0)\|_\infty \\
&\le \frac{1}{\varphi_0}\|A\|_\infty\Upsilon \\
&\le (S+\frac{1}{2})\delta. \quad (18)
\end{aligned}$$

Then, assume that quantization output is unsaturated before time $k>0$. On the one hand, in light of (17b), one obtains that

$$\sup_{1\le i\le k+1}\|\psi_i\|_\infty \le \frac{\delta}{2\tau}.$$

On the other hand, it follows from (17a) that

$$\begin{aligned}
\xi_{k+1} &= \frac{A-B_k-\mu\nu^T}{\tau}\xi_k + \frac{B_k}{\tau}\psi_k \\
&= \Big(\frac{A-B_k-\mu\nu^T}{\tau}\Big)^{k+1}\xi_0 \\
&\quad + \sum_{i=0}^{k}\Big(\frac{A-B_k-\mu\nu^T}{\tau}\Big)^{k-i}\frac{B_k}{\tau}\psi_i \\
&\le \Big(\frac{\rho}{\tau}\Big)^{k+1}\xi_0 + \Big(\sum_{i=0}^{k}\Big(\frac{\rho}{\tau}\Big)^{k-i}\Big)\sup_{1\le i\le k+1}\Big\|\frac{B_k}{\tau}\psi_i\Big\|_\infty\mathbf{1}_N \\
&= \Big(\frac{\rho}{\tau}\Big)^{k+1}\xi_0 + \frac{\tau}{\tau-\rho}\Big(1-\Big(\frac{\rho}{\tau}\Big)^{k+1}\Big) \\
&\quad \times \sup_{1\le i\le k+1}\Big\|\frac{B_i}{\tau}\psi_i\Big\|_\infty\mathbf{1}_N. \quad (19)
\end{aligned}$$

Before analyzing the upper bound of $\|\xi_{k+1}\|_\infty$, let us discuss $\sup_{k\ge0}\big\|B_k\|_\infty$ and $\|\xi_0\|_\infty$. Note that matrix B_k can be divided into

$$B_k = B_{1,k} - B_{2,k},$$

where

$$B_{1,k} \triangleq \begin{bmatrix} I_N & \mathbf{0}_{N\times N} \\ -\Theta & I_N \end{bmatrix},\ B_{2,k} \triangleq \begin{bmatrix} L_k & \mathbf{0}_{N\times N} \\ -\Theta L_k & W_k \end{bmatrix}.$$

In light of the property of infinite norm on matrix, one has

$$\sup_{k\ge0}\big\|B_k\big\|_\infty \le \|B_{1,k}\|_\infty + \sup_{k\ge0}\big\|B_{2,k}\big\|_\infty = 2 + 2\theta_{\max},$$

where $\theta_{\max} = \max\{\theta_1,\theta_2,\cdots,\theta_N\}$.

Similarly, we have the following inequality

$$\begin{aligned}
\|\xi_0\|_\infty &= \frac{1}{\varphi_0}\|\bar{x}_0\|_\infty \\
&\le \frac{1}{\varphi_0}\|(I-\mu\nu^T)\|_\infty\|x_0\|_\infty \\
&\le \frac{1}{\varphi_0}\big(\|I\|_\infty + \|\mu\nu^T\|_\infty\big)\|x_0\|_\infty \\
&\le \frac{2+N/\varsigma}{\varphi_0}\|x_0\|_\infty \\
&\le \frac{2\varsigma+N}{\varsigma\varphi_0}\Upsilon. \quad (20)
\end{aligned}$$

It is observed from (19) that

$$\begin{aligned}
\|\xi_{k+1}\|_\infty &\le \Big(\frac{\rho}{\tau}\Big)^{k+1}\|\xi_0\|_\infty + \frac{\delta}{2\tau(\tau-\rho)}\Big(1-\Big(\frac{\rho}{\tau}\Big)^{k+1}\Big) \\
&\quad \times \sup_{1\le i\le k+1}\big\|B_i\big\|_\infty \\
&\le \frac{2\varsigma+N}{\varsigma\varphi_0}\Upsilon\Big(\frac{\rho}{\tau}\Big)^{k+1} \\
&\quad + \frac{(1+\theta_{\max})\delta}{(\tau-\rho)\tau}\Big(1-\Big(\frac{\rho}{\tau}\Big)^{k+1}\Big). \quad (21)
\end{aligned}$$

Given that $\rho/\tau<1$, one has

$$\|\xi_{k+1}\|_\infty \le \max\Big\{\frac{2\varsigma+N}{\varsigma\varphi_0}\Upsilon, \frac{(1+\theta_{\max})\delta}{(\tau-\rho)\tau}\Big\}. \quad (22)$$

At time instant $k+1$, according to the consistency property (or sub-multiplicative property) of matrix norms, we arrive at

$$\begin{aligned}
&\big\|(A+B_{k+1})\psi_{k+1} - B_{k+1}\xi_{k+1}\big\|_\infty \\
&\le \big\|(A+B_{k+1})\psi_{k+1}\big\|_\infty + \big\|B_{k+1}\xi_{k+1}\big\|_\infty \\
&\le \big(\big\|A\big\|_\infty + \big\|B_{k+1}\big\|_\infty\big)\|\psi_{k+1}\|_\infty + \big\|B_{k+1}\big\|_\infty\|\xi_{k+1}\|_\infty \\
&\le \frac{\big(\big\|A\big\|_\infty + 2(1+\theta_{\max})\big)\delta}{2\tau} + \frac{2(1+\theta_{\max})^2\delta}{(\tau-\rho)\tau} \\
&\le (S+\frac{1}{2})\delta. \quad (23)
\end{aligned}$$

Furthermore, based on the results in (22), we derive that

$$\begin{aligned}
\lim_{k\to\infty}\|\bar{x}_k\|_\infty &= \lim_{k\to\infty}\|\varphi_k\xi_k\|_\infty \\
&\le \sup_{k\ge0}\|\xi_k\|_\infty\lim_{k\to\infty}\varphi_k = 0, \quad (24)
\end{aligned}$$

which concludes that consensus algorithm (12) with dynamic quantization scheme (11) is convergent without quantization error effects.

Moreover, recall relationships $\mu\nu^T(A-B_k) = \mu\nu^T$ and $\mu\nu^T B_k = \mathbf{0}_{2N}$, it follows from (13) that

$$\mu\nu^T x_{k+1} = \mu\nu^T x_k = \cdots = \mu\nu^T x_0 = \nu^T x_0\mu,$$

which means that the optimally incremental cost $\lambda^\star = \lim_{k\to\infty}\lambda_{i,k} = \nu^T x_0 = \frac{\mathbf{1}_N^T\Theta\lambda_0 + \mathbf{1}_N^T\phi_0}{\varsigma}$ and $\lim_{k\to\infty}\phi_{i,k} = 0$ for $\forall i\in\mathcal{V}$. The proof is completed. ■

Theorem 1 provides a sufficient condition to show that consensus algorithm (12) with dynamic quantization scheme (11) converges to the optimally incremental cost $\lambda^\star$ under limited data rate.

In what follows, we are in a position to address the general case with power generation constraints. If all generations operate in the unsaturated region (i.e., $P_{i,k} \in [P_i^m,\ P_i^M], \forall k \geq 0$), the main results completely follow *Theorem 1*. Hence, we only consider the saturated case. The corresponding consensus algorithm becomes

$$\begin{cases} \lambda_{i,k+1} = \lambda_{i,k} + \sum\limits_{j\in\mathcal{N}_i} l_{ij,k}(\hat{\lambda}_{j,k} - \hat{\lambda}_{i,k}) + \epsilon\phi_{i,k} \\ \phi_{i,k+1} = \phi_{i,k} + \sum\limits_{j\in\mathcal{N}_i} w_{ij,k}(\hat{\phi}_{j,k} - \hat{\phi}_{i,k}) \\ \qquad\qquad - (P_{i,k+1} - P_{i,k}) \\ P_{i,k+1} = \begin{cases} P_i^m, & \lambda_{i,k+1} \leq \lambda_i^m \\ P_i^M, & \lambda_{i,k+1} \geq \lambda_i^M. \end{cases} \end{cases} \tag{25}$$

Motivated by [5], denote the sum of all incremental cost as $\Lambda_k = \sum_{i=1}^N \lambda_{i,k}$. Then, it follows from (25) that

$$\Lambda_{k+1} = \Lambda_k + \epsilon E_k, \tag{26}$$

where $E_k \triangleq \left(P_D - \sum_{i=1}^N P_{i,k}\right)$ is the error between total demand and total supply. Note that total power demand condition $\sum_{i\in\mathcal{V}} P_i^m \leq P_D \leq \sum_{i\in\mathcal{V}} P_i^M$, there exists at least one generator being not saturated. Without loss of generality, assume $E_k > 0$, and then Λ_k will increase and the total power generation will also increase in light of the relationship between incremental cost and power generation. Furthermore, the error E_k will decrease. After a certain time K_t, if $P_{i,k}$ reaches its saturation value, then $P_{i,k}$ is always saturated for $k > K_t$. To analyze the behavior for $k > K_t$, the algorithm (13) can be rewritten as

$$x_{k+1} = (\tilde{A} - \tilde{B}_k)x_k + B_k e_k, \tag{27}$$

where

$$\begin{aligned} \tilde{A} &\triangleq \begin{bmatrix} I_N & \epsilon I \\ \mathbf{0}_{N\times N} & I - \epsilon\tilde{\Theta} \end{bmatrix}, \\ \tilde{B}_k &\triangleq \begin{bmatrix} I_N - L_k & \mathbf{0}_{N\times N} \\ \tilde{\Theta}(L_k - I_N) & I_N - W_k \end{bmatrix}, \\ \tilde{\Theta} &\triangleq \text{diag}\{\tilde{\theta}_1, \tilde{\theta}_2, \cdots, \tilde{\theta}_N\}, \\ \tilde{\theta}_i &\triangleq \begin{cases} 0, & \text{if } P_{i,k} \text{ is saturated,} \\ \theta_i, & \text{otherwise.} \end{cases} \end{aligned}$$

Recall condition $\sum_{i\in\mathcal{V}} P_i^m \leq P_D \leq \sum_{i\in\mathcal{V}} P_i^M$, we can conclude that at least one generator is not saturated (i.e., $\exists\ \tilde{\theta}_i \neq 0,\ i \in \mathcal{V}$). Next, along with similar line of *Theorem 1* combining with the eigenvalue perturbation approach [5], [12], we can derive that the proposed scheme can solve the optimal ED problem under generation constraints.

B. Convergence Rate Analysis

First, to evaluate the convergence rate, the *asymptotic convergence factor* [28] is defined as

$$r_{asym} = \sup_{x_0\neq x^*} \lim_{k\to\infty} \left(\frac{\|x_k - x^*\|_2}{\|x_0 - x^*\|_2}\right)^{1/k}$$

where $x^* = \lim_{k\to\infty} x_k$.

In what follows, pre- and post-multiplying (19) by φ_{k+1}, the consensus error is rewritten as

$$\begin{aligned} \bar{x}_{k+1} &= (A - B_k - \mu\nu^T)\bar{x}_k + B_k e_k \\ &= (A - B_k - \mu\nu^T)^{k+1}\bar{x}_0 \\ &\quad + \sum_{i=0}^{k}(A - B_k - \mu\nu^T)^{k-i}B_i e_i \\ &\leq \rho^{k+1}\bar{x}_0 + \frac{(1+\theta_{\max})\delta}{(\tau-\rho)\tau}\Big(\rho^{k+1} - \tau^{k+1}\Big)\mathbf{1}_N. \end{aligned}$$

In light of the definition of asymptotic convergence factor, we have that $r_{asym} = \max\{\tau, \rho\}$. Note that $\rho < \tau < 1$, one has $r_{asym} = \tau$ which concludes that the convergence rate of the developed distributed algorithm only depends on the parameter τ. It should be pointed out that the communication topology $\mathscr{G}$ and the value of parameter ϵ determine the upper bound on norm of matrix $(A - B_k - \mu\nu)$ (i.e., the value of ρ), and further affect the selection of τ in light of obtained results in Theorem 1.

Remark 4: This section introduces a new dynamic quantization strategy to the consensus algorithm and analyzes the convergence of algorithm under a limited data rate. Compared with existing results (e.g., [12], [24]), the proposed dynamic quantization scheme presents prominent features in the following three folds: (1) the consensus algorithm with the adopted quantization scheme can reach exact consensus without quantization error effects; (2) bounded quantization outputs reduce the size of data transmission and relieve the calculation and communication burden; and (3) uncertain quantization outputs increase the security of the transmitted data.

IV. Privacy-Preserving Scheme

In this section, the Paillier cryptosystem and its additive homomorphic property are first introduced. Then, based on the quantization output, the confidential communication scheme is presented by using the homomorphic property of the Paillier cryptosystem. Next, the security and privacy of the proposed communication scheme are discussed.

A. Homomorphic Encryption

To preserve data privacy and implement communication security, this paper adopts a public-key cryptosystem, which is widely used in open networks in the absence of a third party for key management. In general, the public-key cryptosystem owns two keys, namely, a public key k_s, which is distributed publicly for encryption, and a private key k_p, which is authorized individually for decryption. In the public-key cryptosystem, any individual (agent) can use the public key to encrypt the plaintext while the corresponding ciphertext can only be recovered by agents with the corresponding private key.

Algorithm 1 Paillier Cryptosystem

- ***Key Generation*** (k_p, k_s)
  Step 1: Choose two large prime numbers p and q ($p \neq q$) such that $\gcd\big(pq,\ (p-1)(q-1)\big) = 1$.
  Step 2: Compute $n = pq$ and $\lambda = \text{lcm}(p-1, q-1)$.
  Step 3: Select a random $r \in \mathbb{Z}_{n^2}^*$ such that n divides the order of g.
  Step 4: Compute modular multiplicative inverse $\nu = \big(L(r^\lambda \bmod n^2)\big)^{-1} \bmod n$ where $L(x) = \frac{x-1}{n}$.
  Step 5: Generate the public key $k_p = (n, r)$ and the private key $k_s = (\lambda, \nu)$.
- ***Encryption*** $(c = \mathbf{E}(m))$
  a) Choose a random g ($g \in [0, n)$ and $g \in \mathbb{Z}_{n^2}^*$).
  b) Generate the ciphertext $c = r^m g^n \bmod n^2$ where $m \in \mathbb{Z}_n, c \in \mathbb{Z}_{n^2}^*$.
- ***Decryption*** $(m = \mathbf{D}(c))$
  The plaintext $m = L(c^\lambda \bmod n^2) \bmod n$.

So far, some of the classic public-key cryptosystems include RSA [29], Paillier [30], and ELGamal [31] algorithms. As one of the probabilistic asymmetric cryptosystems, the Paillier cryptosystem is believed to be highly secure and is thus adopted in this paper. The corresponding algorithm is outlined in Algorithm 1. In addition, the Paillier cryptosystem is of the additive homomorphic property, which permits to perform computations on encrypted data directly. Specifically, the ciphertext of $m_1 + m_2$ (i.e., $\mathbf{E}(m_1 + m_2)$) can be obtained by $\mathbf{E}(m_1 + m_2) = \mathbf{E}(m_1)\mathbf{E}(m_2)$. Furthermore, one has $(\mathbf{E}(m_1))^n = \mathbf{E}(nm_1)$, where n is a positive integer. Notably, the additive homomorphic property plays an important role in ensuring communication security and privacy preservation of the consensus algorithm.

B. Confidential Communication Scheme

In this subsection, a secure communication scheme is introduced by taking full advantage of the additive homomorphic property of Paillier cryptosystem. To facilitate encryption and decryption, variable $l_{i\to j,k}(w_{i\to j,k})$ is selected by

$$l_{i\to j,k} = \sqrt{(1 + \max\{d_i, d_j\})^{-1}} \sum_{i=1}^{l} 2^{i-l-1} \pi_{i,k}, \qquad (28)$$

where $\pi_{i,k} \in \{0, 1\}$ is randomly generated, l refers to the length of bit string. Moreover, $\Pi_k \triangleq \{\pi_{l,k}, \pi_{l-1,k}, \cdots, \pi_{1,k}\}$ can be regarded as the binary bit string.

Denote

$$s_{ij,k}^1 = l_{ij,k}(u_{j,k}^1 - u_{i,k}^1),\ \Delta\hat{\lambda}_{ij,k} = l_{ij,k}(\hat{\lambda}_{j,k} - \hat{\lambda}_{i,k}),$$
$$s_{ij,k}^2 = w_{ij,k}(u_{j,k}^2 - u_{i,k}^2),\ \Delta\hat{\phi}_{ij,k} = w_{ij,k}(\hat{\phi}_{j,k} - \hat{\phi}_{i,k}).$$

The dynamic quantization based consensus algorithm (12) can be rewritten as

$$\lambda_{i,k+1} = \lambda_{i,k} + \sum_{j\in\mathcal{N}_i} \Delta\hat{\lambda}_{ij,k} + \epsilon\phi_{i,k},$$
$$\phi_{i,k+1} = (1 - \epsilon\theta_i)\phi_{i,k} + \sum_{j\in\mathcal{N}_i} \Delta\hat{\phi}_{ij,k} - \theta_i \sum_{j\in\mathcal{N}_i} \Delta\hat{\lambda}_{ij,k} \qquad (29)$$

where

$$\Delta\hat{\lambda}_{ij,k+1} = \Delta\hat{\lambda}_{ij,k} + \epsilon\Delta\hat{\phi}_{ij,k} + \varphi_k s_{ij,k}^1,$$
$$\Delta\hat{\phi}_{ij,k+1} = (1 - \epsilon\theta_i)\Delta\hat{\phi}_{ij,k} + \varphi_k s_{ij,k}^2.$$

Now, the confidential implementation between agent i and its neighboring agent j is presented by Algorithm 2.

Algorithm 2 Confidential Implementation Scheme

- ***Initialization*** (agent i)
  Generate public and private key pairs (k_{pi}, k_{si}) as well as random variable $l_{i\to j,k}$ and $w_{i\to j,k}$ via (28).
- ***Encryption and Transmission*** (the flow $i \to j \to i$)
  Step 1: Encrypt plaintexts $-u_{i,k}^1$, $-u_{i,k}^2$ as $\mathbf{E}(-u_{i,k}^1)$, $\mathbf{E}(-u_{i,k}^2)$, respectively, and transmit both and public key k_{pi} to neighboring node j.
  Step 2: Encrypt plaintexts $u_{j,k}^1$, $u_{j,k}^2$ as $\mathbf{E}(u_{j,k}^1)$, $\mathbf{E}(u_{j,k}^1)$ via using public key k_{pi}, and compute the differences via
  $$\mathbf{E}(u_{j,k}^1 - u_{i,k}^1) = \mathbf{E}(u_{j,k}^1)\mathbf{E}(-u_{i,k}^1),$$
  $$\mathbf{E}(u_{j,k}^2 - u_{i,k}^2) = \mathbf{E}(u_{j,k}^2)\mathbf{E}(-u_{i,k}^2),$$
  and further
  $$\mathbf{E}\big(l_{j\to i,k}(u_{j,k}^1 - u_{i,k}^1)\big) = \big(\mathbf{E}(u_{j,k}^1 - u_{i,k}^1)\big)^{l_{j\to i,k}},$$
  $$\mathbf{E}\big(w_{j\to i,k}(u_{j,k}^2 - u_{i,k}^2)\big) = \big(\mathbf{E}(u_{j,k}^2 - u_{i,k}^2)\big)^{w_{j\to i,k}}.$$
  Step 3: Return $\mathbf{E}\big(l_{j\to i,k}(u_{j,k}^1 - u_{i,k}^1)\big)$, $\mathbf{E}\big(w_{j\to i,k}(u_{j,k}^2 - u_{i,k}^2)\big)$ to agent i.
- ***Decryption and Update***
  Step 1: Decrypt ciphertexts $\mathbf{E}\big(l_{j\to i,k}(u_{j,k}^1 - u_{i,k}^1)\big)$, $\mathbf{E}\big(w_{j\to i,k}(u_{j,k}^2 - u_{i,k}^2)\big)$ as $l_{j\to i,k}(u_{j,k}^1 - u_{i,k}^1)$, $w_{j\to i,k}(u_{j,k}^2 - u_{i,k}^2)$ via using the private key k_{si}.
  Step 2: Multiply the results with $l_{i\to j,k}$, $w_{i\to j,k}$ to get weighted differences $s_{ij,k}^1$, $s_{ij,k}^2$, respectively. Compute the difference $\Delta\lambda_{ij,k}$, $\Delta\phi_{ij,k}$, and then carry out state update via (29).

C. Analysis of Security and Privacy

The proposed confidential communication scheme is secure against external eavesdroppers. First, we observe that, in light of Algorithm 2, an eavesdropper who does not have access to the secret key cannot figure out the encrypted information. Second, some malicious attackers may inject some additive deception signals to affect the convergence of the consensus algorithm. An alternative scheme to attach a digital signature against possible attackers can be used to detect the possible data tampering during communication (for more details, see [24]).

The following part provides a discussion on privacy preservation against honest-but-curious adversaries who can be agents or observers eavesdropping communication links. First, according to the communication flow from agent i to agent j, agent j cannot decrypt the received $\mathbf{E}\{-u_{i,k}^1\}$ and $\mathbf{E}\{-u_{i,k}^2\}$ without private key k_{si} due to the semantic security of the Paillier algorithm. Then, connection weights are unknown to

all agents in light of the generation rule of random weights. Hence, agent i neither infers to $\hat{\lambda}_{j,k}$, $\hat{\phi}_{j,k}$ by

$$\hat{\lambda}_{j,k} = \Delta\hat{\lambda}_{ij,k}/l_{ij,k} + \hat{\lambda}_{i,k},\ \hat{\phi}_{j,k} = \Delta\hat{\phi}_{ij,k}/w_{ij,k} + \hat{\phi}_{i,k},$$

nor obtains/estimates $\lambda_{j,k}$ and $\phi_{j,k}$.

Next, to specifically analyze the privacy-preserving performance, let us give the following definition.

Definition 1: For communication network of N agents, the initial state $\lambda_{i,0}$ and $\phi_{i,0}$ of node i is preserved if an honest-but-curious adversary cannot estimate the values of $\lambda_{i,0}$ and $\phi_{i,0}$ with any accuracy.

According to the convention in cryptography, the legitimate participants are denoted as $\mathcal{A}$ (Alice) and $\mathcal{B}$ (BoB), and the adversary is denoted as $\mathcal{E}$ (Eve).

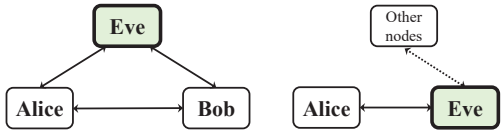

Fig. 2. Two connection configurations

Theorem 2: Consider distributed algorithm (12) with dynamic quantization scheme (11) under connected and undirected graph $\mathscr{G}$. Under Theorem 1, assume that all data transmission follows the confidential communication scheme illustrated in Algorithm 2. An honest-but-curious node, who can receive messages from neighboring nodes, cannot estimate the initial state of legitimate node.

Proof: The proof includes two cases.

• *Case 1. Alice is connected to at least a legitimate node Bob*

There is no loss of generality that the connection configuration is considered as illustrated in Fig. 2(a) where Eve is connected to both Alice and Bob.

In what follows, a privacy-proving approach is proposed to show that variationally private values are indistinguishable to Eve. Define the information available to Eve at time instant k as

$$\begin{aligned} I_{\mathcal{E},k} = \{\ & s^1_{\mathcal{E}\mathcal{A},k}, s^1_{\mathcal{E}\mathcal{B},k}, s^2_{\mathcal{E}\mathcal{A},k}, s^2_{\mathcal{E}\mathcal{B},k}, \lambda_{\mathcal{E},k}, \phi_{\mathcal{E},k}, \\ & l_{\mathcal{E}\to\mathcal{A},k}, l_{\mathcal{E}\to\mathcal{B},k}, w_{\mathcal{E}\to\mathcal{A},k}, w_{\mathcal{E}\to\mathcal{B},k}\}. \end{aligned}$$

The cumulated information available to Eve in whole time horizon is described by $I_{\mathcal{E}} = \bigcup_{k=0}^{\infty} I_{\mathcal{E},k}$.

To show that initial values $\lambda_{\mathcal{A},0}$, $\phi_{\mathcal{A},0}$ are not leaked to Eve, or Eve cannot estimate the value of $\lambda_{\mathcal{A},0}$, $\phi_{\mathcal{A},0}$ with any accuracy, we need to prove that $\bar{I}_{\mathcal{E}} = I_{\mathcal{E}}$ could hold for any $\bar{\lambda}_{\mathcal{A},0} \neq \lambda_{\mathcal{A},0}$, $\bar{\phi}_{\mathcal{A},0} \neq \phi_{\mathcal{A},0}$. The reason is that Eve infers $\lambda_{\mathcal{A},0}$, $\phi_{\mathcal{A},0}$ based on the only information available $I_{\mathcal{E},k}$, and if $I_{\mathcal{E},k}$ is unchanged for different initial values, then Eve has no way to infer/estimate initial values $\lambda_{\mathcal{A},0}$, $\phi_{\mathcal{A},0}$.

Next, we present that there exist initial values of $\bar{\lambda}_{\mathcal{A},0}$, $\bar{\phi}_{\mathcal{A},0}$ and coupling weights such that $\bar{I}_{\mathcal{E}} = I_{\mathcal{E}}$ holds under $\bar{\lambda}_{\mathcal{A},0} \neq \lambda_{\mathcal{A},0}$, $\bar{\phi}_{\mathcal{A},0} \neq \phi_{\mathcal{A},0}$. To more specific, to ensure that all agents converge to the original optimal value, the local load demand $\bar{P}_{D\mathcal{B}}$ satisfies

$$\bar{P}_{D\mathcal{B}} = P_{D\mathcal{A}} + P_{D\mathcal{B}} - \bar{P}_{D\mathcal{A}},$$

and coupling weights can be selected as

$$\begin{aligned} \bar{l}_{\mathcal{E}\to\mathcal{A},0} &= l_{\mathcal{E}\to\mathcal{A},0},\ \bar{w}_{\mathcal{E}\to\mathcal{A},0} = w_{\mathcal{E}\to\mathcal{A},0}, \\ \bar{l}_{\mathcal{E}\to\mathcal{B},0} &= l_{\mathcal{E}\to\mathcal{B},0},\ \bar{w}_{\mathcal{E}\to\mathcal{B},0} = w_{\mathcal{E}\to\mathcal{B},0}, \\ \bar{l}_{\mathcal{A}\to\mathcal{E},0} &= l_{\mathcal{A}\to\mathcal{E},0}(u^1_{\mathcal{A},0} - u^1_{\mathcal{E},0})/(\bar{u}^1_{\mathcal{A},0} - u^1_{\mathcal{E},0}), \\ \bar{w}_{\mathcal{A}\to\mathcal{E},0} &= w_{\mathcal{A}\to\mathcal{E},0}(u^2_{\mathcal{A},0} - u^2_{\mathcal{E},0})/(\bar{u}^2_{\mathcal{A},0} - u^2_{\mathcal{E},0}), \\ \bar{l}_{\mathcal{B}\to\mathcal{E},0} &= l_{\mathcal{B}\to\mathcal{E},0}(u^1_{\mathcal{B},0} - u^1_{\mathcal{E},0})/(\bar{u}^1_{\mathcal{B},0} - u^1_{\mathcal{E},0}), \\ \bar{w}_{\mathcal{B}\to\mathcal{E},0} &= w_{\mathcal{B}\to\mathcal{E},0}(u^2_{\mathcal{B},0} - u^2_{\mathcal{E},0})/(\bar{u}^2_{\mathcal{B},0} - u^2_{\mathcal{E},0}), \\ \bar{l}_{i\to j,k} &= l_{i\to j,k},\ \bar{w}_{i\to j,k} = w_{i\to j,k}, \\ & \forall i,j \in \{\mathcal{A},\mathcal{B},\mathcal{E}\},\ k = 1,2,\cdots. \end{aligned}$$

Moreover, select suitable $\bar{l}_{\mathcal{A}\to\mathcal{B},0}$, $\bar{l}_{\mathcal{B}\to\mathcal{A},0}$, $\bar{w}_{\mathcal{A}\to\mathcal{B},0}$, $\bar{w}_{\mathcal{B}\to\mathcal{A},0}$ such that $\bar{\lambda}_{\mathcal{A},1} = \lambda_{\mathcal{A},1}$, $\bar{\phi}_{\mathcal{A},1} = \phi_{\mathcal{A},1}$, $\bar{\lambda}_{\mathcal{B},1} = \lambda_{\mathcal{B},1}$, $\bar{\phi}_{\mathcal{B},1} = \phi_{\mathcal{B},1}$. We observe that $\bar{I}_{\mathcal{E}} = I_{\mathcal{E}}$ holds under $\bar{\lambda}_{\mathcal{A},0} \neq \lambda_{\mathcal{A},0}$, $\bar{\phi}_{\mathcal{A},0} \neq \phi_{\mathcal{A},0}$, which shows that the honest-but-curious node Eve cannot infer the initial value of node Alice if Alice is connected to a legitimate node Bob.

• *Case 2. All neighbors of Alice are honest-but-curious*

Since multiple honest-but-curious neighboring nodes can collude with each other to cooperatively estimate Alice's initial state, these nodes can be regarded as one node. Hence, without loss of generality, we only consider that Alice is connected to an honest-but-curious node Eve as shown in Fig. 2(b).

Denote $x_{i,k} = [\lambda_{i,k} \quad \phi_{i,k}]^T$, $\Delta x_{ij,k} = [\Delta\lambda_{ij,k} \quad \Delta\phi_{ij,k}]^T$, one has

$$\begin{aligned} x_{\mathcal{A},k+1} &= T_{\mathcal{A}} x_{\mathcal{A},k} + V_{\mathcal{A}} \Delta x_{\mathcal{A}E,k} \\ &= T^{k+1}_{\mathcal{A}} x_{\mathcal{A},0} + \sum_{i=0}^{k} T^{k-i}_{\mathcal{A}} V_{\mathcal{A}} \Delta x_{\mathcal{A}E,i} \end{aligned}$$

where

$$T_{\mathcal{A}} = \begin{bmatrix} 1 & \epsilon \\ 0 & 1-\epsilon\theta_{\mathcal{A}} \end{bmatrix}, V_{\mathcal{A}} = \begin{bmatrix} 1 & 0 \\ -\theta_{\mathcal{A}} & 1 \end{bmatrix}.$$

Note that $\lim_{k\to\infty} x_{\mathcal{A},k} = \lim_{k\to\infty} x_{\mathcal{E},k}$ in light of the constructed consensus scheme. However, Eve is unknown to the sensitive information $\theta_{\mathcal{A}}$, and further the value of $x_{\mathcal{A},0}$ cannot be estimated by

$$\hat{x}_{\mathcal{A},0} = \lim_{k\to\infty} \big((T^{k+1}_{\mathcal{A}})^{-1}(x_{\mathcal{E},k+1} - \sum_{i=0}^{k} T^{k-i}_{\mathcal{A}} V_{\mathcal{A}} \Delta x_{\mathcal{E}A,i})\big).$$

Hence, Eve cannot infer the initial value of node Alice, even if all neighbors of Alice are honest-but-curious. ■

Remark 5: In this paper, we have developed a homomorphically encrypted consensus algorithm with a dynamic quantization strategy. In comparison to the existing results in [12], our results present the following merits: (1) the proposed dynamic quantization scheme is new in reducing the size of the data transmission by introducing an estimator-like auxiliary equation; (2) the established sufficient condition is new in achieving exact convergence by virtue of mathematical induction and matrix norm analysis; and (3) the adopted confidential

TABLE I
COMPARISON AMONG EXISTING PRIVACY-PRESERVING APPROACHES

	ours	[12]	[15]	[19]	[20]
time-varying graph	✓	✓	×	×	×
convergence accuracy	✓	×	×	✓	✓
honest-but-curious nodes	✓	✓	✓	✓	×
external eavesdroppers	✓	✓	✓	×	×

TABLE II
GENERATION PARAMETERS FOR IEEE 39-BUS

DGi	$1,6$	$2,7$	$3,8$	$4,9$	$5,10$
a_i $(\$/KW^2h)$	0.105	0.074	0.078	0.082	0.094
b_i $(\$/KWh)$	2.53	3.17	3.41	4.02	1.22
c_i $(\$/h)$	78	62	31	42	51
P_i^m (KW)	3.8	4.2	8	5.4	10
P_i^M (KW)	40	18	60	45	80

communication strategy is new in preventing sensitive information disclosure by using the additive homomorphic property, and extended analysis shows privacy-preserving performance. To sum up, our paper proposes a new dynamic quantization scheme to eliminate quantization error effects and reduce computational complexity and data communication traffic of the homomorphically encrypted distributed ED algorithm.

Remark 6: It is observed in Table I that, compared with differential-privacy-based [15], correlated-noise-injected [19], and observability-based [20] privacy-preserving approaches, our approach can be suitable for time-varying graphs with weak topological restrictions, which covers a wider range of practical applications. In comparison with [12], [15], our approach exhibits better system performance in exact convergence due to the constructed dynamic quantization scheme. In contrast to [19], [20], our privacy-preserving method is effective against external and honest-but-curious eavesdroppers in view of the generation rule of unknown random weights and the semantic security of the Paillier algorithm. Hence, our proposed algorithm has comprehensive merits in topological condition, convergence accuracy, and privacy preservation.

V. SIMULATION STUDY

This section provides simulation examples to evaluate the effectiveness of the proposed privacy-preserving ED scheme under different cases.

Consider IEEE 39-bus systems with 10 generation units and 18 demands. Assume that the cyber communication layer consists of 10 agents, where each agent only owns one generation unit and some local loads. The communication link is described by the red dotted lines in Fig. 3. The related parameters of generation units are presented in Table II, which are borrowed from [10], [14]. The modular bits of the Paillier cryptosystem is selected as 32, and the test platform is MATLAB (R2014a) in a PC of Intel Core CPU i7-5500U at 2.40 Hz and 8-GB RAM.

Set $\epsilon = 0.03$, $S = 30$, $\tau = 0.94$, and $\delta = 1$. The local power demand $P_{Di}(i \in \mathcal{V})$ is selected as $P_{D1} = 25KW$, $P_{D2} = 10KW$, $P_{D3} = 20KW$, $P_{D4} = 30KW$, $P_{D5} = 35KW$, $P_{D6} = 20KW$, $P_{D7} = 15KW$, $P_{D8} = 20KW$, $P_{D9} = 25KW$, and $P_{D10} = 40KW$. Hence, the total demand is $P_D = 120KW$. The initial power of each generation is set as $P_{1,0} = 10KW$, $P_{2,0} = 12KW$, $P_{3,0} = 20KW$, $P_{4,0} = 8KW$, $P_{5,0} = 20KW$, $P_{6,0} = 15KW$, $P_{7,0} = 13KW$, $P_{8,0} = 18KW$, $P_{9,0} = 16KW$, and $P_{10,0} = 25KW$.

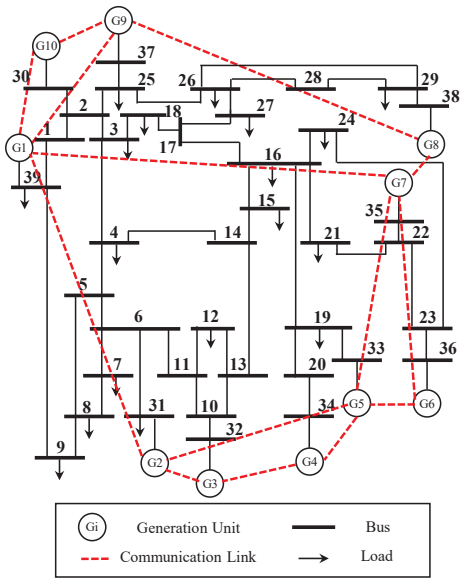

Fig. 3. IEEE 39-Bus test system

A. Case Study 1: Without Generator Constraints

In this case study, we do not take generator constraints into consideration. The initial power of each generation is set as $P_{1,0} = 25KW$, $P_{2,0} = 10KW$, $P_{3,0} = 20KW$, $P_{4,0} = 30KW$, and $P_{5,0} = 35KW$. Furthermore, the optimal power $P_i^\star(i \in \mathcal{V})$ is calculated as $P_1^\star = P_6^\star = 21.43KW$, $P_2^\star = P_7^\star = 26.09KW$, $P_3^\star = P_8^\star = 23.21KW$, $P_4^\star = P_9^\star = 18.36KW$, and $P_5^\star = P_{10}^\star = 30.91KW$, respectively.

Then, we carry out the homomorphically encrypted consensus scheme (i.e., Algorithm 2). The simulation results are shown in Figs. 4–6. In Fig. 4, we can see that all incremental costs converge to the optimal value $\lambda^\star = 7.03\$/KWh$, the mismatch between demand and generation approaches 0, the local power outputs $P_{i,k}$ converge to the optimal $P_i^\star$, respectively, and the global power generation matches the total demand. Fig. 5 presents the dynamical evolution of quantization outputs $u_{i,k}^1$, $u_{i,k}^2$ and estimation errors $e_{i,k}^1$, $e_{i,k}^2$. We observe that estimation error between the actual state and estimated state approaches 0, which shows that the developed dynamic quantization scheme has merit in eliminating quantization error effects. Fig. 6 plots the encrypted weighted differences $\mathbf{E}(l_{j\to i,k}(u_{j,k}^1 - u_{i,k}^1)$, $\mathbf{E}(w_{j\to i,k}(u_{j,k}^2 - u_{i,k}^2)$. The total simulation time is $4.07s$ for 101 instants of 10 nodes. It implies that the average calculation time for each control instant is $4.03ms$, which is applicable for constrained low-cost microprocessors. Notably, the received encrypted messages (ciphertext) are disordered to external eavesdroppers though

the states have converged to the optimal value, which verifies the effectiveness of obtained theoretical results.

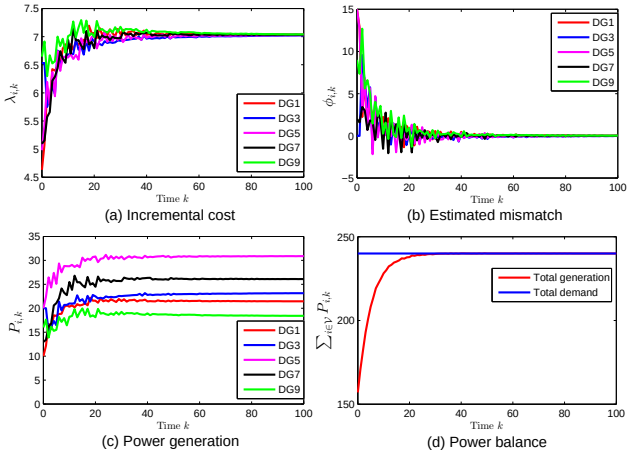

Fig. 4. Test results of consensus algorithm without generation constraints

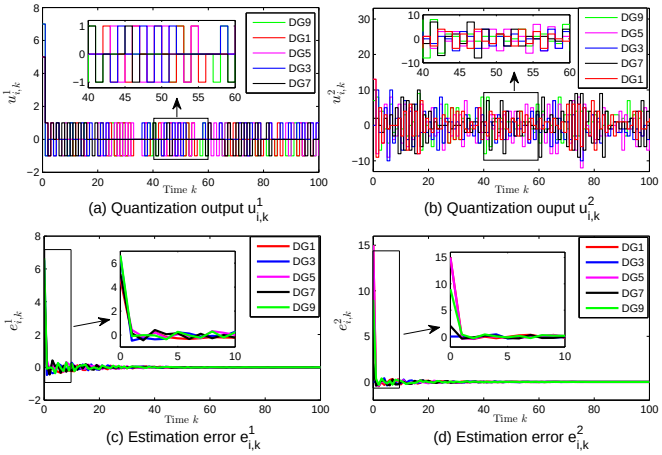

Fig. 5. Quantization outputs and estimation errors

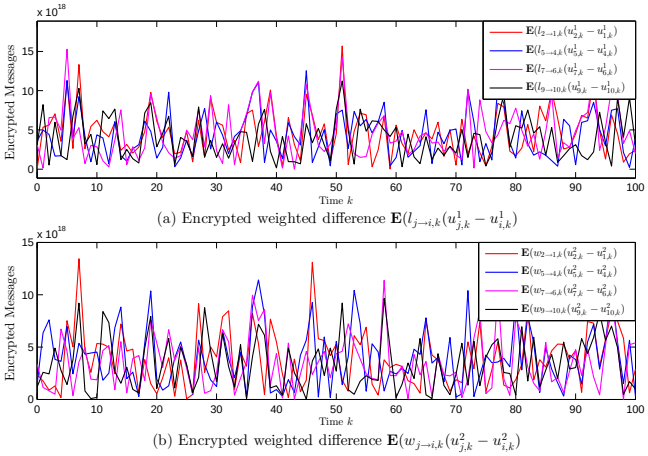

Fig. 6. Encrypted weighted differences

The test results verify that the proposed privacy-preserving consensus algorithm can achieve exact consensus while ensuring secure communication and privacy preservation.

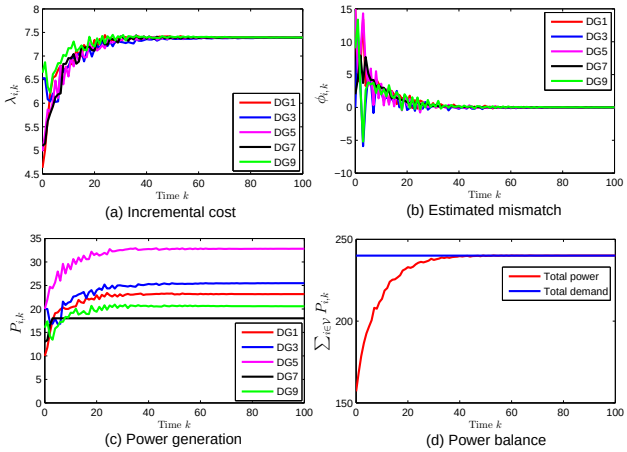

Fig. 7. Test results of consensus algorithm with generation constraints

B. Case Study 2: With Generator Constraints

In this case study, the generator constraints are involved. It is calculated that the optimal incremental cost $\lambda^\star = 7.39\$/KWh$, and the optimal power generation is $P_1^\star = P_6^\star = 23.14KW$, $P_2^\star = P_7^\star = 18KW$, $P_3^\star = P_8^\star = 25.51KW$, $P_4^\star = P_9^\star = 20.54KW$, and $P_5^\star = P_{10}^\star = 32.81KW$, respectively.

The test results are shown in Figs. 7–9. In Fig. 7, we observe that all variables converge to the optimal values, which are within the operation domains. Fig. 8 shows that quantization outputs are bounded and estimation errors converge to 0, which verifies theoretical results in Section III-A. It is observed from Fig. 9 that the received encrypted messages are still random to external eavesdroppers though the consensus algorithm has converged to the optimal value. The total simulation time is $4.03s$ for 101 instants of 10 nodes, which implies that the average calculation time for each control instant is $3.99ms$.

C. Case Study 3: Comparison with Existing Result

In this subsection, we compare the performance of our proposed ED algorithm with that of static quantization based distributed scheme in [12] under the same quantization accuracy. Fig. 10 plots the dynamic evolution of incremental cost $\lambda_{i,k}$, power mismatch $\phi_{i,k}$, and corresponding quantization errors under the static quantization scheme via setting quantization accuracy or resolution as $m = 1$ [12]. Note that all incremental costs cannot converge to exact optimal value, which further shows the superiority of the proposed dynamic quantization scheme in achieving exact convergence.

D. Case Study 4: Convergence Rate for Different τ

In this part, we set τ as 0.94, 0.96, 0.98, 0.995 to test the dynamic evolution of λ_i. Fig. 11 shows that a smaller τ leads to a faster convergence speed, which verifies the obtained theoretical results.

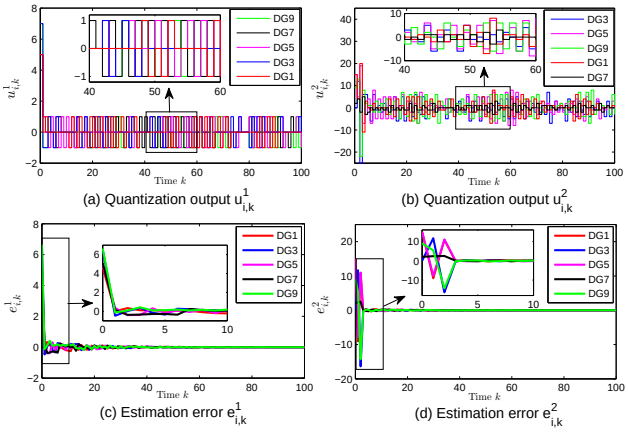

Fig. 8. Quantization outputs and estimation errors

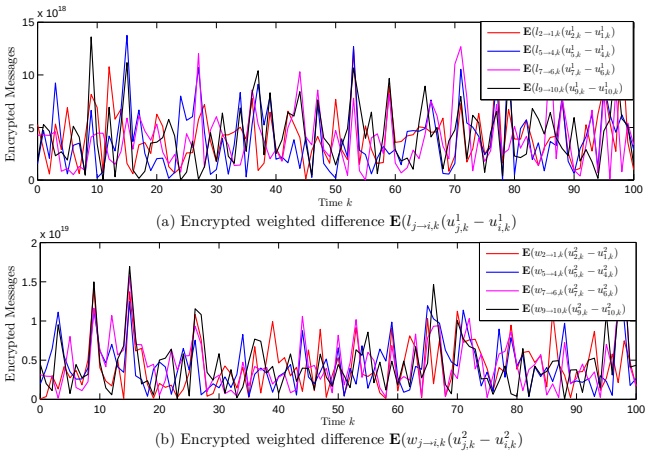

Fig. 9. Encrypted weighted differences

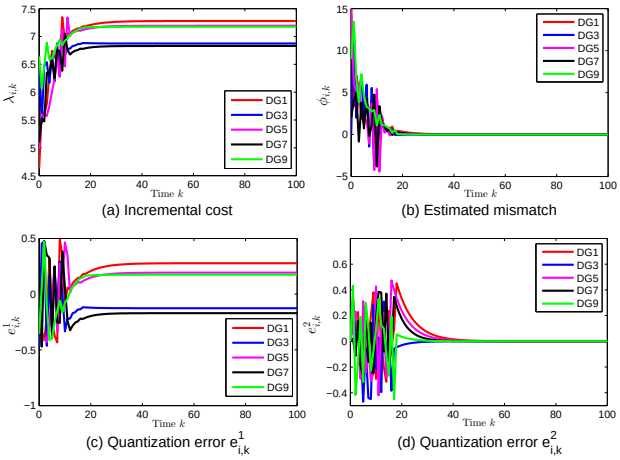

Fig. 10. Test results of consensus algorithm with static quantization scheme [12]

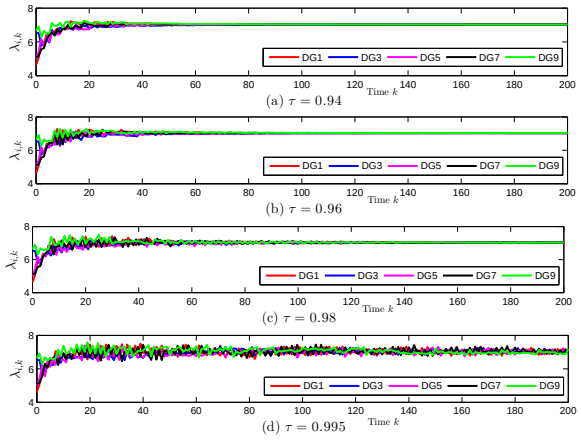

Fig. 11. The dynamic evolution of incremental cost with different τ.

VI. Conclusions

In this paper, we have addressed the privacy-preserving distributed ED issue of microgrids by a homomorphically encrypted consensus scheme. A novel estimator-like quantizer has been first constructed to facilitate data encryption and signal transmission. Then, a sufficient condition, in terms of quantization parameters, has been derived via taking full advantage of mathematical induction and matrix norm analysis. Furthermore, to preserve privacy and achieve secure communication, we have proposed a confidential interaction protocol in the absence of a third party with the help of the additive homomorphic property of the Paillier cryptosystem. Finally, the simulation results have shown the validity and superiority of the developed consensus algorithm. In comparison with static quantization scheme, the proposed dynamic one has merits in less data release and exact convergence. In addition, in contrast to the noise-injected scheme, the adopted homomorphically encrypted scheme exhibits better privacy-preserving performance against external and honest-but-curious eavesdroppers. Future directions would be the extensions of other type of privacy-preserving distributed ED algorithms with the power flow and thermal constraints.

References

[1] L.-Y. Lu and C.-C. Chu, Consensus-based droop control synthesis for multiple DICs in isolated micro-grids, *IEEE Trans. Power Syst.*, vol. 30, no. 5, pp. 2243–2256, Sept. 2015.

[2] W. Meng, X. Wang, and S. Liu, Distributed load sharing of an inverter-based microgrid with reduced communication, *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1354–1364, Mar. 2018.

[3] H. Zhang, W. Meng, J. Qi, X. Wang, and W.-X. Zheng, Distributed load sharing under false data injection attack in an inverter-based microgrid, *IEEE Trans. Indus. Electron.*, vol. 66, no. 2, pp. 1543–1551, Feb. 2019.

[4] A. J. Wood, B. F. Wollenberg, and G. B. Sheblé, *Power Generation, Operation, and Control*. Hoboken, NJ, USA: Wiley, 2013.

[5] S. Yang, S. Tan, and J.-X. Xu, Consensus based approach for economic dispatch problem in a smart grid, *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4416–4426, Nov. 2013.

[6] J.-F. Chen and S.-D. Chen, Multiobjective power dispatch with line flow constraints using the fast Newton-Raphson method, *IEEE Trans. Energy Convers.*, vol. 12, no. 1, pp. 86–93, Mar. 1997.

[7] X. Yan and V. H. Quintana, An efficient predictor-corrector interior point algorithm for security-constrained economic dispatch, *IEEE Trans. Power Syst.*, vol. 12, no. 2, pp. 803–810, May 1997.

[8] Z.-L. Gaing, Particle swarm optimization to solving the economic dispatch considering the generator constraints, *IEEE Trans. Power Syst.*, vol. 18, no. 3, pp. 1187–1195, Aug. 2003.

[9] P. Chen and H. Chang, Large-scale economic dispatch by genetic algorithm, *IEEE Trans. Power Syst.*, vol. 10, no. 4, pp. 1919–1926, Nov. 1995.

[10] G. Chen, F. L. Lewis, E. N. Feng, and Y. Song, Distributed optimal active power control of multiple generation systems, *IEEE Trans. Indus. Electron.*, vol. 62, no. 11, pp. 7079–7090, Nov. 2015.
[11] G. Hug, S. Kar, and C. Wu, Consensus+innovations approach for distributed multiagent coordination in a microgrid, *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1893–1903, Jul. 2015.
[12] Y. Yan, Z. Chen, V. Varadharajan, M. J. Hossain, and G. E. Town, Distributed consensus-based economic dispatch in power grids using the Paillier cryptosystem, *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3493–3502, Jul. 2021.
[13] N. R.-Asr, U. Ojha, Z. Zhang, and M.-Y. Chow, Incremental welfare consensus algorithm for cooperative distributed generation/demand response in smart grid, *IEEE Trans. Smart Grid*, vol. 5, no. 6, pp. 2836–2845, Nov. 2014.
[14] R. Wang, Q. Li, B. Zhang, and L. Wang, Distributed consensus based algorithm for economic dispatch in a microgrid, *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3630–3640, Jul. 2019.
[15] A. Wang, W. Liu, T. Dong, X. Liao, and T. Huang, DisEHPPC: Enabling heterogeneous privacy-preserving consensus-based scheme for economic dispatch in smart grids, *IEEE Trans. Cybern.*, to be published, doi: 10.1109/TCYB.2020.3027572.
[16] Z. Tang, D. J. Hill, and T. Liu, A novel consensus-based economic dispatch for microgrids, *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3920–3922, Jul. 2018.
[17] Y. Mo and R. M. Murray, Privacy preserving average consensus, *IEEE Trans. Autom. Control*, vol. 62, no. 2, pp. 753–765, Feb. 2017.
[18] E. Nozari, P. Tallapragada, and J. Cortes, Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design, *Automatica*, vol. 81, pp. 221–231, Jul. 2017.
[19] C. Zhao, J. Chen, J. He, and P. Cheng, Privacy-preserving consensus-based energy management in smart grids, *IEEE Trans. Signal Process.*, vol. 66, no. 23, pp. 6162–6176, Dec. 2018.
[20] S. Pequito, S. Kar, S. Sundaram, and A. P. Aguiar, Design of communication networks for distributed computation with privacy guarantees, in *Proc. IEEE 53rd Annu. Conf. Decis. Control*, 2014, pp. 1370–1376.
[21] S. S. Kia, J. Cortes, and S. Martínez, Dynamic average consensus under limited control authority and privacy requirements, *Int. J. Robust Nonlinear Control*, vol. 25, no. 13, pp. 1941–1966, 2015.
[22] A. B. Alexandru, K. Gatsis, Y. Shoukry, S. A. Seshia, P. Tabuada, and G. J. Pappas, Cloud-based quadratic optimization with partially homomorphic encryption, *IEEE Trans. Autom. Control*, vol. 66, no. 5, pp. 2357–2364, May 2021.
[23] R. L. Lagendijk, Z. Erkin, and M. Barni, Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation, *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 82–105, Jan. 2013.
[24] M. Ruan, H. Gao, and Y. Wang, Secure and privacy-preserving consensus, *IEEE Trans. Autom. Control*, vol. 64, no. 10, pp. 4035–4049, Oct. 2019.
[25] O. Goldreich, *Foundations of Cryptography: Volume 1*, Basic Tools. New York, NY, USA: Cambridge Univ. Press, 2007.
[26] M. Rostami and S. Lotfifard, Distributed dynamic state estimation of power systems, *IEEE Trans. Indus. Informat.*, vol. 14, no. 8, pp. 3395–3404, Aug. 2018.
[27] C. Zhao, J. He, P. Cheng, and J. Chen, Analysis of consensus-based distributed economic dispatch under stealthy attacks, *IEEE Trans. Indus. Electron.*, vol. 64, no. 6, pp. 5107–5117, Jun. 2017.
[28] L. Xiao and S. Boyd, Fast linear iterations for distributed averaging, *Syst. Control Lett.*, vol. 53, no. 1, pp. 65-78, Sept. 2004.
[29] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.
[30] P. Paillier, *Public-Key cryptosystems based on composite degree residuosity classes*. Berlin, Germany: Springer, 1999, pp. 223–238.
[31] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms.* Berlin, Germany: Springer, 1985, pp. 10–18.