A Privacy-preserving Energy Management System Based on Homomorphic Cryptosystem for IoT-enabled Active Distribution Network

Qian Hu, Siqi Bu, Wencong Su, and Vladimir Terzija

Abstract—**Active distribution network (ADN), as a typically cyber-physical system, develops with the evolution of Internet of Things (IoTs), which makes the network vulnerable to cybersecurity threats. In this paper, the eavesdropping attacks that lead to privacy breaches are addressed for the IoT-enabled ADN. A privacy-preserving energy management system (EMS) is proposed and empowered by secure data exchange protocols based on the homomorphic cryptosystem. During the information transmission among distributed generators and load customers in the EMS, private information including power usage and electricity bidding price can be effectively protected against eavesdropping attacks. The correctness of the final solutions, e.g., optimal market clearing price and unified power utilization ratio, can be deterministically guaranteed. The simulation results demonstrate the effectiveness and the computational efficiency of the proposed homomorphically encrypted EMS.**

Index Terms—**Eavesdropping attack, energy management system, homomorphic cryptosystem, Internet of Things (IOTs), active distribution network (ADN), privacy-preserving.**

I. Introduction

THE deployment of digital smart sensing, distributed generators (DGs), and advanced information and communication technology has been accelerated in the past few decades to drive the power grid toward a more interconnected network. Along with the emerging control strategy, various components and devices in the power grid can be managed in a distributed and connected manner through the internet or communication platforms [1], [2]. Such an evolution into a big Internet of Things (IoT) extensively boosts the growing functionalities of modern power grids [3]. However, potential cybersecurity threats are inevitably posed to power networks. Among different types of cybersecurity threats, eavesdropping attack has received increasing attention [4]-[8]. It can be provoked by an unauthorized and corrupted entity to obtain confidential information of legitimate components when the information is transmitted between two components.

An IoT-enabled active distribution network (ADN) comprises a wide range of physical components, e.g., DGs and load customers, and devices, e.g., advanced sensors and metering infrastructures, that require interactive communications to realize a bunch of functions in a distributed manner. It is a typical multi-agent cyber-physical system. Consensus theory is the foundation of most of the existing distributed algorithms. With several advantages, e.g., robustness to the single-point failure and scalability in computation and communication, consensus-based algorithm has been widely applied to facilitate multi-agent distributed operations in the cyber-physical power network with different network-wide objectives such as economic dispatch, cost minimization, loss minimization, and accurate power sharing [9]-[17]. To achieve an effective and flexible operation of IoT-enabled ADN, it is necessary to apply promising distributed algorithms like consensus algorithm in a well-designed energy management system (EMS).

In the context of the IoT evolution, the deployment of distributed EMS in the ADN will be greatly facilitated through peer-to-peer communications. Nevertheless, in an IoT-enabled ADN, confidential data are more easily inferred and collected by eavesdropping attacks during the distributed decision-making process because of the collaborative and connective nature of agents. For instance, hackers who successfully eavesdrop on the cyber network of an ADN can steal power usage data of load customers and bidding price information of DGs, and may even disclose important decisions or control actions for illegal purposes [18], [19]. Private information such as power usage is at a high confidential level as it can imply personal preferences and activities. Hence, measures to keep private data of agents secure are extremely essential in the IoT-enabled ADN.

Generally, two common approaches with regard to data-processing are used for preventing privacy disclosure in the

Manuscript received: August 10, 2022; revised: November 30, 2022; accepted: May 3, 2023. Date of CrossCheck: May 3, 2023. Date of online publication: June 20, 2023.

This work was supported by the National Natural Science Foundation of China (No. 52077188), Guangdong Science and Technology Department (No. 2019A1515011226), and Hong Kong Research Grant Council (No. 15219619).

Q. Hu is with the Department of Physics, Hong Kong Baptist University, Hong Kong, China (e-mail: qianhu@hkbu.edu.hk).

S. Bu (corresponding author) is with the Department of Electrical and Electronic Engineering, Shenzhen Research Institute, The Hong Kong Polytechnic University, Hong Kong, China (e-mail: siqi.bu@polyu.edu.hk).

W. Su is with the Department of Electrical and Computer Engineering, University of Michigan-Dearborn, Dearborn, MI 48128, USA (e-mail: wencong@umich.edu).

V. Terzija is with the School of Engineering, Newcastle University, Newcastle, UK (e-mail: Vladimir.Terzija@newcastle.ac.uk).

DOI: 10.35833/MPCE.2022.000507

literature. One approach is to implement differential privacy to protect data, and the other is to use cryptographic techniques. For differential privacy, randomized noises are added to an individual's data to make sure that an eavesdropper cannot infer the original information. Some studies have applied differential privacy for information privacy in the power sector. In [20]-[22], privacy-preserving algorithms are developed based on differential privacy for energy management and economic dispatch problems in smart grids and microgrids. To protect the confidentiality of private loads, differential privacy is also implemented in [23] for optimal power flow calculation. However, by utilizing differential privacy, the injected perturbations will potentially affect the exact accuracy of the algorithm convergence and deteriorate the control system performance. There exists an inherent tradeoff between correctness and privacy in the differential privacy scheme [24]. The injected noise should follow strict mathematical requirements. Otherwise, the convergence cannot be ensured.

By contrast, cryptographic techniques do not inject any perturbation in the power network and are capable of finding the exact solution to the problem after the decryption [18]. In particular, a homomorphic cryptosystem allows certain computations to be carried out on the ciphertext, i.e., the encrypted data, to maintain the confidentiality of the original data. After decrypting the encrypted data, the decrypted result exactly matches the computation result performed on the plaintext [25]. Thanks to the advantage of semantically secure encryption and efficient decryption, the homomorphic cryptosystem has been employed to create privacy-preserving distributed control schemes lately in the field of control. For example, privacy-preserving average consensus algorithms are developed to ensure the accurate average consensus without disclosing the initial states of agents in [26] and [27]. In addition, homomorphic encryption has been used in smart grid such as secure data aggregation in [24], privacy protection of customer usage information in the forecast prediction in [25], and the data security of smart meters in [26]. All of them only need one-step data aggregation, which makes the application of HE relatively simple. However, the application of the homomorphic cryptosystem in energy management has not been sufficiently investigated for IoT-enabled power networks, especially distribution networks, with high requirement for data exchange.

Therefore, to address the pressing demand for privacy preservation in the IoT-enabled ADN, this paper develops a privacy-preserving EMS by utilizing the homomorphic cryptosystem. The core task is to protect data privacy against eavesdropping attacks during the information exchange needed for distributed optimization and coordination in the EMS. The privacy preservation is empowered by secure data exchange protocols based on the homomorphic cryptosystem. The contributions of the paper are summarized as follows.

1) For IoT-enabled ADNs highly relying on the communications among heterogeneous components, a two-level EMS is proposed to maximize the social welfare of DGs and load customers and achieve cooperative power sharing among DGs.

2) Privacy concerns and risks subject to eavesdropping attacks in the IoT-enabled ADN with distributed consensus-based EMS are comprehensively analyzed and mitigated. Secure data exchange protocols are developed based on the homomorphic cryptosystem to prevent the leakage of private information of each agent during the distributed operation of the EMS. The operation of secure protocols is fully distributed without the supervision of a third party, which is cost-effective and efficient to be implemented.

3) The proposed two-level EMS based on the homomorphic cryptosystem can accomplish two advantageous properties at the same time: privacy preservation and correctness, guaranteeing the effectiveness of the EMS.

The remaining paper is organized as follows. Section II presents the proposed two-level EMS and its associated information privacy concerns. Section III introduces the preliminaries on the homomorphic cryptosystem. Section IV presents the homomorphically encrypted EMS based on secure exchange protocols. Simulation results are demonstrated in Section V. The discussion and conclusion are presented in Sections VI and VII.

II. Proposed Two-level EMS and Its Associated Information Privacy Concerns

In this section, a two-level EMS is first introduced for the IoT-enabled ADN. To realize its functions in a distributed way, distributed consensus-based algorithms are then presented. The privacy concerns and potential risks are discussed.

A. Proposed Two-level EMS for IoT-enabled ADN

The schematic diagram of ADN structure and proposed two-level EMS is illustrated in Fig. 1, including three types of entities: virtual power plants (VPPs), DGs, and load customers. VPP consists of multiple DGs. A group of DGs are aggregated as a VPP to provide flexible power generation and multiple VPPs work cooperatively as power suppliers to quickly respond to changing power demand of load customers. Dash lines indicate the communication connections among different entities. The economic dispatch of VPPs, demand response of customers, and the cooperative control of DGs can be realized through a proposed two-level EMS, which is demonstrated in Fig. 1, where P_{VPP}^{*} is the optimal power generation.

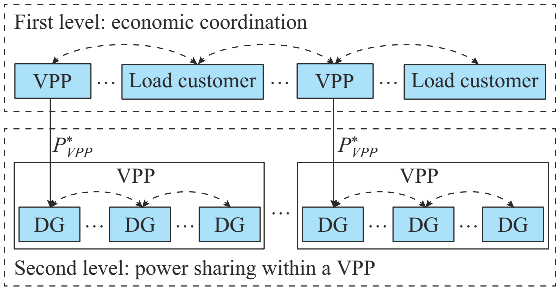

Fig. 1. Schematic diagram of ADN structure and proposed two-level EMS.

During the first-level operation of EMS, the information of each VPP (or load customer) is encrypted by the local VPP operator (or customer) and then transmitted to other

VPPs (or customers). Similarly, the information of each DG in a VPP is encrypted by DG itself and then transmitted to other DGs for the encrypted data processing in the second-level operation.

Economic operation of a distribution network should involve active participations of both supply and demand sides in energy market. In a deregulated energy market, both parties are supposed to be self-interested and have optimal strategies to participate in the market. The self-interested market model describes the essential objectives of suppliers and customers, which are discussed below. Let us consider VPPs belonging to the set $\mathcal{V}_{VPP}=\{1,2,\ldots,N_s\}$ and load customers belonging to the set $\mathcal{V}_c=\{1,2,\ldots,N_c\}$. The active power loss is incorporated into the market model. For each VPP operator $i\in\mathcal{V}_{VPP}$ and each customer $j\in\mathcal{V}_c$, the energy selling price and bidding price are denoted by $\lambda_{s,i}$ and $\lambda_{b,j}$, respectively, and the objective of the self-interested market model is to maximize VPP profit and customer utility, respectively, formulated as:

$$\max_{P_{VPP}} (\lambda_{s,i}P_{VPP,i}(1-\gamma_i)-C_i(P_{VPP,i})) \tag{1}$$

$$\max_{P_D} ((U_j(P_{D,j})-\lambda_{b,i}P_{D,j}(1+\gamma_j)) \tag{2}$$

where $P_{VPP,i}$ and $P_{D,j}$ are the power generation of the VPP and the power demand of the customer, respectively; γ_i and γ_j are the loss coefficients in a range of $[0,1]$ that can be defined by $\gamma_i=\partial P_{LOSS}/\partial P_{VPP,i}$ and $\gamma_j=\partial P_{LOSS}/\partial P_{D,j}$ for the i^{th} VPP and j^{th} customer, respectively [28], and P_{LOSS} is the total active power loss; $C_i=\frac{1}{2}a_iP^2_{VPP,i}+b_iP_{VPP,i}+c_i$ is the cost function of the VPP, and a_i, b_i, c_i are the cost coefficients of the i^{th} VPP; and $U_j=\frac{1}{2}\alpha_jP^2_{D,j}+\beta_jP_{D,j}$ is the utility function of the customer [11], and α_j and β_j are the utility coefficients of the j^{th} customer. The marginal cost function $R_{c,i}$ for the i^{th} VPP and the marginal utility function $R_{u,j}$ for the j^{th} customer are defined as (3) and (4), respectively.

$$R_{c,i}(P_{VPP,i})=\frac{\partial C_i(P_{VPP,i})}{\partial P_{VPP,i}}=a_iP_{VPP,i}+b_i \tag{3}$$

$$R_{u,j}(P_{D,j})=\frac{\partial U_j(P_{D,j})}{\partial P_{D,j}}=\alpha_jP_{D,j}+\beta_j \tag{4}$$

At the first level of the EMS, to maximize social welfare and to reduce energy costs from the perspective of the entire ADN, based on (1) and (2), the economic coordination problem can be formulated as:

$$\max\left(\sum_{j\in\mathcal{V}_c}U_j(P_{D,j})-\sum_{i\in\mathcal{V}_{VPP}}C_i(P_{VPP,i})\right) \tag{5a}$$

s.t.

$$\sum_{i=1}^{N_s}P_{VPP,i}=\sum_{j=1}^{N_c}P_{D,j}+P_{LOSS} \tag{5b}$$

$$P^{\min}_{VPP,i}\le P_{VPP,i}\le P^{\max}_{VPP,i} \tag{5c}$$

$$P^{\min}_{D,j}\le P_{D,j}\le P^{\max}_{D,j} \tag{5d}$$

where $P^{\min}_{VPP,i}$ and $P^{\max}_{VPP,i}$ are the lower and upper limits of the VPP generation, respectively; and $P^{\min}_{D,j}$ and $P^{\max}_{D,j}$ are the lower and upper limits of the load demand, respectively.

P_{LOSS} can be written as:

$$P_{LOSS}=\gamma_i\sum_{i=1}^{N_s}P_{VPP,i}+\gamma_j\sum_{j=1}^{N_c}P_{D,j} \tag{6}$$

Through the self-interested model, each VPP operator will find an optimal power generation for the i^{th} VPP $P^*_{VPP,i}$ such that the marginal cost equals the energy selling price $\lambda_{s,i}$. The optimal solution of (1) therefore can be found by:

$$\lambda_{s,i}(1-\gamma_i)-R_{c,i}(P_{VPP,i})=0 \tag{7}$$

Similarly, the customer will find the optimal solution $P^*_{D,j}$ of (2) by equating the marginal utility to its bidding price:

$$\lambda_{b,i}(1+\gamma_j)-R_{u,j}(P_{D,j})=0 \tag{8}$$

Considering constraints (5c) and (5d), the generation of the VPP and consumption of the customer can be determined based on (7) and (8) as:

$$P_{VPP,i}=\begin{cases}P^{\min}_{VPP,i} & \lambda_{s,i}<\dfrac{R^{\min}_{c,i}}{1-\gamma_i}\\ P^{\max}_{VPP,i} & \lambda_{s,i}>\dfrac{R^{\max}_{c,i}}{1-\gamma_i}\\ \dfrac{\lambda_{s,i}(1-\gamma_i)-b_i}{a_i} & \text{otherwise}\end{cases} \tag{9}$$

$$P_{D,j}=\begin{cases}P^{\min}_{D,j} & \lambda_{b,i}<\dfrac{R^{\min}_{u,j}}{1+\gamma_j}\\ P^{\max}_{D,j} & \lambda_{b,i}>\dfrac{R^{\max}_{u,j}}{1+\gamma_j}\\ \dfrac{\lambda_{b,i}(1+\gamma_j)-\beta_j}{\alpha_j} & \text{otherwise}\end{cases} \tag{10}$$

where $R^{\min}_{c,i}$ and $R^{\max}_{c,i}$ are the lower and upper bounds of the marginal cost, respectively; and $R^{\min}_{u,j}$ and $R^{\max}_{u,j}$ are the lower and upper bounds of the utility, respectively. They can be known from (3) and (4) by giving $P^{\min}_{VPP,i}$ (or $P^{\min}_{D,j}$) and $P^{\max}_{VPP,i}$ (or $P^{\max}_{D,j}$). Social welfare is maximized at the equilibrium of the market, i.e., $\lambda_{s,i}$ and $\lambda_{b,j}$ both settle at a unique price denoted by λ^*. This optimum will also result in an identical marginal cost and utility for all participants.

At the second level of the proposed two-level EMS, a cooperative power sharing strategy will be subsequently conducted by all DGs in each VPP once the optimal power generation P^*_{VPP} is determined. Consider DGs belonging to the set $\mathcal{V}_{DG}=\{1,2,\ldots,N_d\}$. For each DG $m\in\mathcal{V}_{DG}$, the following problem is formulated to satisfy the power generation requirement and meanwhile to ensure accurate power sharing among DGs:

$$\min_{P_{DG}}\left(\frac{1}{2}(P^{total}-P^*_{VPP})^2\right) \tag{11a}$$

s.t.

$$P^{total}=\sum_{m=1}^{N_d}\delta_mP^{\max}_{DG,m} \tag{11b}$$

$$0 \le \delta_1 = \ldots = \delta_m = \frac{P_{DG,m}}{P_{DG,m}^{\max}} \le 1 \tag{11c}$$

$$0 \le P_{DG,m} \le P_{DG,m}^{\max} \tag{11d}$$

where $P_{DG,m}$ and $P_{DG,m}^{\max}$ are the power output and its upper limit, respectively; and $\delta_m \in [0,1]$ is defined as the power utilization ratio. A VPP manager only participates in the first level of the EMS, so when conducting (11a)-(11d), VPP operator does not know $P_{DG,m}$ of each DG. This value is only determined by each DG itself through communications with other neighboring DGs in the second-level EMS operation.

B. Consensus-based Distributed Algorithms for EMS

A graph $\mathcal{G}=(\mathcal{V},\mathcal{E})$ is used to capture the communication network of an IoT-enabled system. Nodes belonging to the set $\mathcal{V}=\{\mathcal{V}_1,\mathcal{V}_2,\ldots,\mathcal{V}_N\}$ represent the agent in the ADN. A finite edge set $\mathcal{E}=\{(p,q)\}\in\mathcal{V}\times\mathcal{V}$ consists of all communication links between any pair of connecting agents, where agent $\mathcal{V}_q$ can receive the information from agent $\mathcal{V}_p$. For agent $\mathcal{V}_p\in\mathcal{G}$, the agents that can directly receive information from it are defined as its out-neighbors, denoted by $N_p^{out}=\{\mathcal{V}_q|(p,q)\in\mathcal{E}\}$. The cardinality of N_p^{out} is called as out-degree and is denoted by $\mathcal{D}_p^{out}$. The agents that can directly send information to the agent $\mathcal{V}_p\in\mathcal{G}$ are defined as its in-neighbors, denoted by $N_p^{in}=\{\mathcal{V}_q|(q,p)\in\mathcal{E}\}$. The cardinality of N_p^{in} is called the in-degree and denoted by $\mathcal{D}_p^{in}$.

At the first level of the EMS, a strongly connected graph $\mathcal{G}_{ADN}=(\mathcal{V}_{ADN},\mathcal{E}_{ADN})$ is introduced to describe the communication network of the IoT-enabled ADN. $\mathcal{V}_{ADN}=\{\mathcal{V}_{VPP}\cup\mathcal{V}_c\}$. For any $i,j\in\mathcal{V}_{ADN}$, the associated weighting factors for the communication link between a pair of communicating neighbors are defined as [10]:

$$\phi_{ij}=\begin{cases}\dfrac{1}{\mathcal{D}_i^{in}} & j\in N_i^{in}\\ 0 & \text{otherwise}\end{cases} \tag{12}$$

$$\omega_{ij}=\begin{cases}\dfrac{1}{\mathcal{D}_j^{out}} & i\in N_j^{out}\\ 0 & \text{otherwise}\end{cases} \tag{13}$$

where i and j represent either a VPP or a load customer. An operator $[\cdot]_-$ is used to define the mathematical operation as:

$$[a]_-=\begin{cases}a & a\ge 0\\ 0 & a<0\end{cases} \tag{14}$$

Based on the weighting factor, the economic coordination for the VPPs and load customers at the first level of the proposed two-level EMS is solved by a consensus-based distributed algorithm, formulated as:

$$\lambda_i(k+1)=\lambda_i(k)+\left[\sum_{j\in N_i^{in}}\phi_{ij}(\lambda_j(k)-\lambda_i(k))\right]_-+\sigma y_i(k) \tag{15a}$$

$$y_i(k+1)=\sum_{j\in N_i^{in}}\omega_{ij}y_j(k)-(P_i(k+1)-P_i(k)) \tag{15b}$$

where $\lambda_i(k)$ is a compact set of the energy selling price and energy bidding price for the VPP and the load customer; $y_i(k)$ is the local estimation of the power imbalance, which is the feedback item driving $\lambda_i(k)$ to the optimal value; and $P_i(k)$ is updated by (9) if $i\in\mathcal{V}_{VPP}$ and by (10) if $i\in\mathcal{V}_c$ at every step k. By introducing (14), $\sum_{j\in N_i^{in}}\phi_{ij}(\lambda_j(k)-\lambda_i(k))$ in (15a) is guaranteed to be nonnegative, which ensures convergence.

From (13), it is not difficult to find that $\sum_{j\in N_i^{in}}\phi_{ij}=1$ and $\sum_{i\in N_j^{out}}\omega_{ij}=1$, which is a sufficient condition for convergence. And the following theorem holds.

Theorem 1 [29]: considering the algorithm (15) with the weighting factors in (13), the algorithm achieves an optimal global solution $\lim_{k\to\infty}\lambda_i(k)=\lambda^*$ and $\lim_{k\to\infty}y_i(k)=0$, provided that the communication graph is strongly connected and there exists a sufficiently small gain σ.

At the second level of the EMS, a strongly connected graph $\mathcal{G}_{DG}=(\mathcal{V}_{DG},\mathcal{E}_{DG})$ is adopted to describe the communication network for a single VPP consisting of multiple DGs. For any $m,n\in\mathcal{V}_{DG}$, the element of the weighted adjacency matrix $\boldsymbol{D}$ can be defined as:

$$D_{mn}=\begin{cases}d_{mn} & n\in N_m^{in}\text{ and }m\ne n\\ 1-\sum\limits_{n\in N_m^{in}}d_{mn} & m=n\\ 0 & \text{otherwise}\end{cases} \tag{16}$$

where d_{mn} is the element at the m^{th} row and the n^{th} column of $\boldsymbol{D}$.

Obviously, $\boldsymbol{D}$ is a row-stochastic matrix, i.e., $\sum_{n\in N_m^{in}}d_{mn}=1$. All entries should be positive and satisfy $\varepsilon\le d_{mn}\le 1$ for all $n\in N_m^{in}$, where $0<\varepsilon\le\min_m\{1/D_m^{in}\}$. A leader-follower consensus algorithm is used to solve the self-organizing power sharing problem (11) in the VPP. Without loss of generality, DG1 is assigned as the leader that has access to the reference P_{VPP}^* as well as a global variable P^{total}. Even though DG1 can collect the power output of each DG, such information will only be received in an encrypted form (data encryption processes will be introduced in the next section). Denote t as the iteration step of the second-level cooperative control in the EMS. The utilization ratio of the leader DG is updated by (17a). To achieve a unified power utilization ratio for each DG in the VPP, the utilization ratio of the follower DG is updated by (17b).

$$\delta_1(t+1)=\delta_1(k)+\rho(P_{VPP}^*-P^{total}(t)) \tag{17a}$$

$$\delta_m(t+1)=\sum_{n\in N_m^{in}}d_{mn}\delta_n(t)\quad m,n\ne 1 \tag{17b}$$

where $\rho>0$ is the control gain.

The convergence of the cooperative power sharing problem is guaranteed with a sufficiently small gain ρ, as stated in the following theorem.

Theorem 2 [30]: the cooperative control (11) solved by the leader-follower consensus (17) guarantees that all DGs asymptotically converge to the optimal solution, $\lim_{t\to\infty}\delta_m(t)=\delta^*$ and $\lim_{t\to\infty}P^{total}(t)=P_{VPP}^*$, provided that the communication graph is strongly connected and there exists a sufficiently small gain ρ.

The solution of (5) and (11) in a privacy-preserving manner and against eavesdropping attacks is our focus, so a detailed convergence analysis is not provided here.

C. Privacy Concerns in IoT-enabled ADNs

In an IoT-enabled ADN, due to the strong communicative connections among agents, significant concerns are raised that the privacy of individual agents can be leaked during the information sharing under eavesdropping attacks. Note that the eavesdropping attacks can be launched not only by an extraneous observer but also by a corrupted entity in the cyber network. Curious and adversarial attackers can collect private data or sensitive information for illegal purposes.

In particular, the consensus-based distributed algorithms discussed above relying on the information exchange among different entities through iterative communications will pose the risk of unintentional information disclosure. At the first level of the EMS, the initial price $\lambda_i(0)$ and the initial load demand/power supply $P_i(0)$ are regarded as the privacy of the participating VPP and customer. It cannot be revealed to others during the distributed decision-making process in the communication network. In fact, it is crucial to keep participants' parameters, e.g., coefficients of the cost/utility function, private from unauthorized parties by protecting the information of initial bidding/selling price and the power demand/supply. Besides, load demand and power supply should be maintained at a high-security level as the exposure of such information may reveal much about the personal preference of the load customer and the business secret of the VPP. Therefore, necessary measures for privacy preservation should be taken in the EMS to prevent the curious entity from gathering the personal information of others during the information exchange.

III. Preliminaries on Homomorphic Cryptosystem

The homomorphic cryptosystem, as one of the cryptographic techniques, empowers a distinguished feature to maintain data confidentiality during both information transmission and processing. Compared with the approach of differential privacy, the correctness of the results and the privacy of agents can be both ensured by applying a homomorphic cryptosystem. Such functionalities make it a suitable candidate to be implemented in the distributed EMS to prevent agents' private information from being disclosed.

A homomorphic cryptosystem comprises three main functions to prevent data leakage during the entire process of data transmission and processing: ① key generation K, ② data encryption E, and ③ data decryption. A public key Key^{pub} and a private key Key^{pri} are generated through the key generation process. Based on the public key, an original message α can be turned into a ciphertext β by encryption function E. Oppositely, the ciphertext β can be decrypted by decryption function D to the original message α based on the private key. Any agent can use the same public key to encrypt original messages to cipher ones while only the trustworthy entity with the corresponding private key can decrypt the ciphertext.

The Paillier cryptosystem, as one of the homomorphic cryptosystems, is implemented in this paper. The functions of the Paillier cryptosystem are introduced below to facilitate the development of the proposed homomorphically encrypted EMS in the next section.

Notations. Denote the set of positive real numbers in the format of floating-point and integer as $\mathbb{R}_F$ and $\mathbb{R}_I$, respectively. $gcd(a,b)$ and $lcm(a,b)$ denote the greatest common divisor and the least common multiple of integers a and b, respectively; mod denotes the modular operation; $\lfloor a \rfloor$ denotes the floor of a real number a, i.e., the largest integer smaller or equal to a.

Key generation. Randomly select two large prime numbers c and v and calculate $h=cv$ and $\varphi=lcm(c-1,v-1)$. A random integer g is chosen such that $gcd(Z(g^{\varphi} \bmod h^2),h)=1$, where $Z(t)=\left\lfloor \frac{t-1}{h} \right\rfloor$. The public key is denoted as $Key^{pub}(g,h)$ and the private key is $Key^{pri}(\varphi)$.

Encryption. A natural integer number $\alpha \in \mathbb{R}_I$ can be encrypted using the public key as:

$$E(\alpha)=g^{\alpha} r^{h} \bmod h^2 \tag{18}$$

where $r \in \mathbb{R}_I$ is a random positive integer.

Decryption. Ciphertext β can be decrypted using the private key as:

$$D(\beta)=\frac{Z(\beta^{\varphi} \bmod h^2)}{Z(g^{\varphi} \bmod h^2)} \bmod h \tag{19}$$

The correctness, semantic security, and homomorphic property of the Paillier cryptosystem are demonstrated as follows [31].

1) Correctness: for any nonnegative integer $\alpha \in \mathbb{R}_I$, (20) holds.

$$D(E(\alpha))=\alpha \tag{20}$$

2) Semantic security: if the decisional composite residuosity assumption holds (DCRA), the Paillier cryptosystem is semantically secure.

3) Homomorphic properties: define any $\alpha_1,\alpha_2,\ldots,\alpha_n \in \mathbb{R}_I$.

a) Additively homomorphic property:

$$D\left(\prod_{i=1}^{n} E(\alpha_i)\right)=\sum_{i=1}^{n}\alpha_i \tag{21}$$

b) Multiplicatively semi-homomorphic property:

$$D(E(\alpha_1)^{\alpha_2})=\alpha_1\alpha_2 \tag{22}$$

The homomorphic properties allow in-network algebraic operations on encrypted values without the need for decryption, which is vital for developing the proposed homomorphically encrypted EMS in the next section.

IV. Homomorphically Encrypted EMS Based on Secure Exchange Protocols

This section presents a detailed design and practical deployment for the privacy-preserving EMS. The Paillier cryptosystem is implemented to construct the secure information exchange protocol to maintain confidentiality for each participant during the information exchange. It is fully distributed without adding noise to the state variables. The proposed secure exchange protocol can prevent information leakage to the eavesdropping attacker while achieving the deterministic convergence to the optimal solution of (15) and (17). The objective of the secure exchange protocol is twofold.

1) Privacy preservation: for each participant (can be either VPP $i \in \mathcal{V}_{VPP}$ or a load customer $i \in \mathcal{V}_c$ or a DG $m \in \mathcal{V}_c$), its information $\lambda_i(k)$, $y_i(k)$ and $\delta_m(t)$ cannot be inferred by any semi-honest eavesdropping attacker in each iteration during data exchange.

2) Correctness: at the first level of EMS, when $k \rightarrow \infty$, $\lambda_{s,i}(k)$ and $\lambda_{b,i}(k)$ can settle at an optimal solution λ^* for each VPP and load customer. At the second level of EMS, when $t \rightarrow \infty$, the power utilization ratio $\delta_m(t)$ can converge to a unified ratio for each DG.

A. Random Weight Reconstruction

As shown in (15), participant i needs the information on the weighted difference $\phi_{ij}(\lambda_j(k)-\lambda_i(k))$ for the local update. To ensure that any participant obtains the weighted difference between itself and any of its neighbors without revealing each other's information, the state information can be encrypted and broadcasted to neighbors at every iteration step. However, without a third party secretly distributing ϕ_{ij}, the privacy of both interacting participants cannot be protected even with state encryption. For example, participant j' s state $\lambda_j(k)$ can be still inferred through $\lambda_j(k)=\phi_{ij}(\lambda_j(k)-\lambda_i(k))/\phi_{ij}+\lambda_i(k)$ by its communicating neighbor i as the weight ϕ_{ij} is constant and available to participant i. To address this issue, a random weight construction approach [27] is extended to the homomorphically encrypted EMS, preventing a pair of communicating participants from inferring each other's states through the information exchange. The weight can be represented by the product of two random numbers, as given by:

$$\phi_{ij}=\phi_{i\rightarrow j}\phi_{j\rightarrow i} \tag{23a}$$

$$\omega_{ij}=\omega_{i\rightarrow j}\omega_{j\rightarrow i} \tag{23b}$$

where $\phi_{i\rightarrow j}(\omega_{i\rightarrow j})$ is the random weight generated by and only known to participant i; and $\phi_{j\rightarrow i}(\omega_{j\rightarrow i})$ is the random weight generated by and only known to participant j. As defined in [32], the random weight $\phi_{i\rightarrow j}(\phi_{j\rightarrow i})$ and $\omega_{i\rightarrow j}(\omega_{j\rightarrow i})$ should be selected in the feasible range of $[\epsilon_1, 1/\mathcal{D}_i^{in}-\epsilon_2]$ and $[\epsilon_1, 1/\mathcal{D}_j^{out}-\epsilon_2]$, respectively, where ϵ_1 and ϵ_2 are the positive numbers that satisfy $\epsilon_1+\epsilon_2< 1\Big/\max\limits_i \{\mathcal{D}_i^{in}\}$. Similarly, for the weight (16), we can obtain:

$$d_{mn}=d_{m\rightarrow n}d_{n\rightarrow m} \tag{24}$$

The random weight should be selected in the feasible range of $[\underline{d}, \bar{d}]$ [27], to ensure convergence, the feasible range must satisfy $0<\underline{d}<\bar{d}< 1\Big/\sqrt{\rho\cdot\max\limits_m \{\mathcal{D}_m^{in}\}}$.

B. Transformation Between Floating-point Numbers and Integers

The Paillier cryptosystem relying on certain modular operations only works for integers. However, the state values of electrical variables are primarily in the form of floating-point numbers [33]. Thus, the transformation between the floating-point number and the integer is necessary before the encryption. According to floating-point arithmetic, a floating-point number $x_F \in \mathbb{R}_F$ can be simply transformed to an integer $x_I \in \mathbb{R}_I$ by $x_I=10^\tau x_F$, where τ denotes the preserved decimal fraction digits. After the decryption, the following functions can be applied to convert an integer x_I to a signed real number x_F with τ decimal fraction digits, where $\mu \in \mathbb{R}_I$ is a positive odd integer [18].

C. Secure Exchange Protocols

Next, without loss of generality, a pair of communicating participants $(\mathcal{V}_1, \mathcal{V}_2)$ is used to illustrate the design process of the secure exchange protocol for the first level of EMS, as shown in Fig. 2.

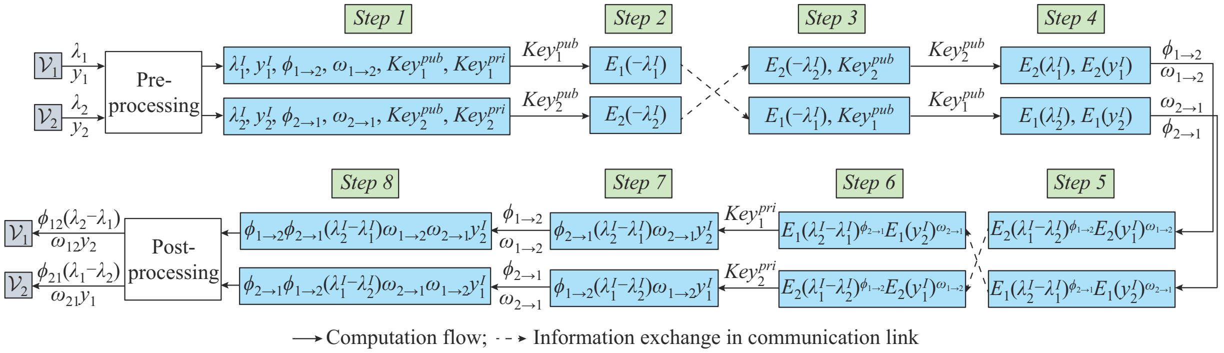
Step 1
Step 2
Step 3
Step 4
$\mathcal{V}_1$
λ_1
y_1
$\mathcal{V}_2$
λ_2
y_2
Pre-processing
$\lambda_1^I, y_1^I, \phi_{1\rightarrow 2}, \omega_{1\rightarrow 2}, Key_1^{pub}, Key_1^{pri}$
$\lambda_2^I, y_2^I, \phi_{2\rightarrow 1}, \omega_{2\rightarrow 1}, Key_2^{pub}, Key_2^{pri}$
Key_1^{pub}
Key_2^{pub}
$E_1(-\lambda_1^I)$
$E_2(-\lambda_2^I)$
$E_2(-\lambda_2^I), Key_2^{pub}$
$E_1(-\lambda_1^I), Key_1^{pub}$
Key_2^{pub}
Key_1^{pub}
$E_2(\lambda_1^I), E_2(y_1^I)$
$E_1(\lambda_2^I), E_1(y_2^I)$
$\phi_{1\rightarrow 2}$
$\omega_{1\rightarrow 2}$
$\omega_{2\rightarrow 1}$
$\phi_{2\rightarrow 1}$
Step 8
Step 7
Step 6
Step 5
$E_2(\lambda_1^I-\lambda_2^I)^{\phi_{1\rightarrow 2}}E_2(y_1^I)^{\omega_{1\rightarrow 2}}$
$E_1(\lambda_2^I-\lambda_1^I)^{\phi_{2\rightarrow 1}}E_1(y_2^I)^{\omega_{2\rightarrow 1}}$
$E_1(\lambda_2^I-\lambda_1^I)^{\phi_{2\rightarrow 1}}E_1(y_2^I)^{\omega_{2\rightarrow 1}}$
$E_2(\lambda_1^I-\lambda_2^I)^{\phi_{1\rightarrow 2}}E_2(y_1^I)^{\omega_{1\rightarrow 2}}$
Key_1^{pri}
Key_2^{pri}
$\phi_{2\rightarrow 1}(\lambda_2^I-\lambda_1^I)\omega_{2\rightarrow 1}y_2^I$
$\phi_{1\rightarrow 2}(\lambda_1^I-\lambda_2^I)\omega_{1\rightarrow 2}y_1^I$
$\phi_{1\rightarrow 2}$
$\omega_{1\rightarrow 2}$
$\phi_{2\rightarrow 1}$
$\omega_{2\rightarrow 1}$
$\phi_{1\rightarrow 2}\phi_{2\rightarrow 1}(\lambda_2^I-\lambda_1^I)\omega_{1\rightarrow 2}\omega_{2\rightarrow 1}y_2^I$
$\phi_{2\rightarrow 1}\phi_{1\rightarrow 2}(\lambda_1^I-\lambda_2^I)\omega_{2\rightarrow 1}\omega_{1\rightarrow 2}y_1^I$
Post-processing
$\phi_{12}(\lambda_2-\lambda_1)$
$\omega_{12}y_2$
$\phi_{21}(\lambda_1-\lambda_2)$
$\omega_{21}y_1$
$\mathcal{V}_1$
$\mathcal{V}_2$
Computation flow; Information exchange in communication link

Fig. 2. Illustration of secure exchange protocol based on homomorphic cryptosystem for first level of EMS.

$\mathcal{V}_1$ and $\mathcal{V}_2$ represent either the VPP or load customer. The subscript k is omitted next for the sake of a clear demonstration. The step-by-step details of Fig. 2 are explained next. Note that the operation at the k^{th} iteration is described.

1) Pre-processing: Key Generation

Before conducting the privacy-preserving interaction protocol, $\mathcal{V}_1$ (or $\mathcal{V}_2$) generates a public key Key_1^{pub} (or Key_2^{pub}) and a private key Key_1^{pri} (or Key_2^{pri}).

2) Step 1: Initialization

Integer transformation: state variables of $\mathcal{V}_1$ and $\mathcal{V}_2$ are transformed into integers by multiplying 10^τ, denoted by $\lambda_1^I, \lambda_2^I, y_1^I, y_2^I \in \mathbb{R}_I$.

Random weight selection: $\mathcal{V}_1$ randomly selects weight $\phi_{1\rightarrow 2}$ and $\omega_{1\rightarrow 2}$; and $\mathcal{V}_2$ randomly selects weight $\phi_{2\rightarrow 1}$

and $\omega_{2\to 1}$.

3) Step 2: Encryption Using Own Public Key

$\mathcal{V}_1$ uses public key Key_1^{pub} to encrypt $-\lambda_1^I$ to $E_1(-\lambda_1^I)$; and $\mathcal{V}_2$ uses public key Key_2^{pub} to encrypt $-\lambda_2^I$ to $E_2(-\lambda_2^I)$.

4) Step 3: Transmission of Encrypted States and Public Key

$\mathcal{V}_1$ sends $E_1(-\lambda_1^I)$ and Key_1^{pub} to $\mathcal{V}_2$; and $\mathcal{V}_2$ sends $E_2(-\lambda_2^I)$ and Key_2^{pub} to $\mathcal{V}_1$ (private keys are kept as secret on their own and do not share with others).

5) Step 4: Encryption Using Neighbor's Public Key

$\mathcal{V}_1$ uses public key Key_2^{pub} to encrypt λ_1^I and y_1^I to $E_2(\lambda_1^I)$ and $E_2(y_1^I)$, respectively; and $\mathcal{V}_2$ uses public key Key_1^{pub} to encrypt λ_2^I and y_2^I to $E_1(\lambda_2^I)$ and $E_1(y_2^I)$, respectively.

6) Step 5: Computation on Encrypted States

According to additively homomorphic property (21) and multiplicatively semi-homomorphic property (22), $\mathcal{V}_1$ computes the encrypted difference as $E_2(\lambda_1^I-\lambda_2^I)=E_2(\lambda_1^I)E_2(-\lambda_2^I)$, then multiplying the weight to acquire $E_2(\lambda_1^I-\lambda_2^I)^{\phi_{1\to 2}}$ and $E_2(y_1^I)^{\omega_{1\to 2}}$. Similarly, $E_1(\lambda_2^I-\lambda_1^I)^{\phi_{2\to 1}}$ and $E_1(y_2^I)^{\omega_{2\to 1}}$ are acquired by $\mathcal{V}_2$.

7) Step 6: Transmission of Processed Encrypted Results

$\mathcal{V}_1$ returns $E_2(\lambda_1^I-\lambda_2^I)^{\phi_{1\to 2}}$ and $E_2(y_1^I)^{\omega_{1\to 2}}$ to $\mathcal{V}_2$; and $\mathcal{V}_2$ returns $E_1(\lambda_2^I-\lambda_1^I)^{\phi_{2\to 1}}$ and $E_1(y_2^I)^{\omega_{2\to 1}}$ to $\mathcal{V}_1$.

$$x_F=\begin{cases} x_I/10^{\tau} & 0\le x_I\le \dfrac{\mu-1}{2} \\ (x_I-\mu)/10^{\tau} & \dfrac{\mu+1}{2}\le x_I<\mu \end{cases} \tag{25}$$

8) Step 7: Decryption Using Own Private Key

$\mathcal{V}_1$ uses private key Key_1^{pri} to decrypt $D(E_1(\lambda_2^I-\lambda_1^I)^{\phi_{2\to 1}})=\phi_{2\to 1}(\lambda_2^I-\lambda_1^I)$ and $D(E_1(y_2^I)^{\omega_{2\to 1}})=\omega_{2\to 1}y_2^I$; and $\mathcal{V}_2$ uses private key Key_2^{pri} to decrypt $D(E_2(\lambda_1^I-\lambda_2^I)^{\phi_{1\to 2}})=\phi_{1\to 2}(\lambda_1^I-\lambda_2^I)$ and $D(E_2(y_1^I)^{\omega_{1\to 2}})=\omega_{1\to 2}y_1^I$.

9) Step 8: Weight Multiplication

$\mathcal{V}_1$ multiplies the decrypted result with its own generated weight to get: $\phi_{12}(\lambda_2^I-\lambda_1^I)=\phi_{1\to 2}\phi_{2\to 1}(\lambda_2^I-\lambda_1^I)$ and $\omega_{12}y_2^I=\omega_{1\to 2}\omega_{2\to 1}y_2^I$; and $\mathcal{V}_2$ multiplies the decrypted result with its own generated weight to get: $\phi_{21}(\lambda_1^I-\lambda_2^I)=\phi_{2\to 1}\phi_{1\to 2}(\lambda_1^I-\lambda_2^I)$ and $\omega_{21}y_1^I=\omega_{2\to 1}\omega_{1\to 2}y_1^I$.

10) Post-processing: Floating-point Number Transmission

The states are converted to floating-point numbers using (25).

Similarly, a secure exchange protocol is designed to find a unified power utilization ratio for all DGs in the VPP to prevent information disclosure, which is shown in Fig. 3. In summary, Fig. 4 illustrates the execution process of the homomorphically encrypted EMS based on the secure exchange protocols to achieve different objectives at each level. It should be noted that: ① the key generation process is only required once at the beginning of the iteration. Generated public and private keys are reused in subsequent iterations till the convergence; ② the conversion between floating-point numbers and integers is performed at each iteration; ③ since the homomorphic encryption scheme is already computation-intensive, we use a pre-set condition to stop the iterative convergence. $k_{\max}$ is set to be the a reasonable value through a trial-and-error approach to make sure the proposed approach converges each time.

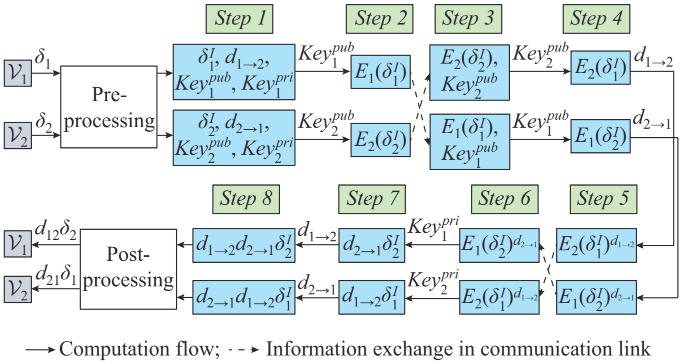

Fig. 3. Illustration of secure exchange protocol based on homomorphic cryptosystem for second level of EMS.

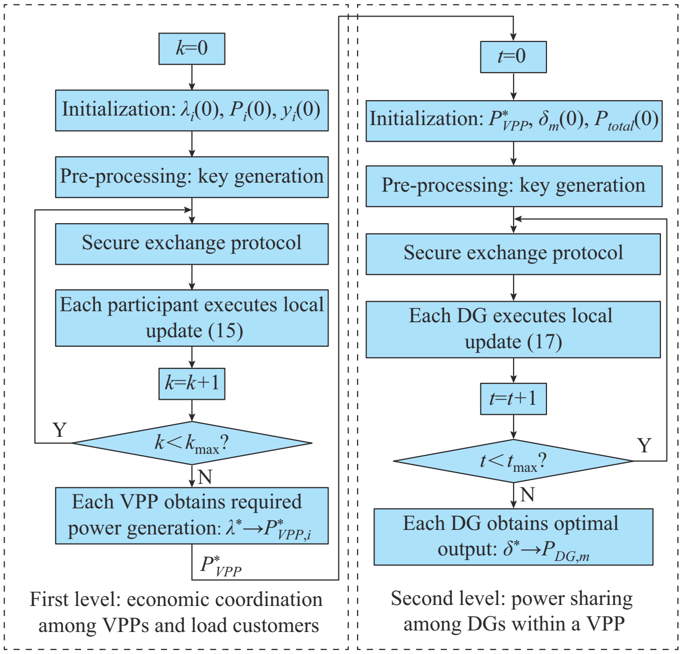
k=0
Initialization: $\lambda_i(0)$, $P_i(0)$, $y_i(0)$
Pre-processing: key generation
Secure exchange protocol
Each participant executes local update (15)
k=k+1
$k<k_{\max}$?
Y
N
Each VPP obtains required power generation: $\lambda^*\to P^*_{VPP,i}$
P^*_{VPP}
First level: economic coordination among VPPs and load customers
t=0
Initialization: P^*_{VPP}, $\delta_m(0)$, $P_{total}(0)$
Pre-processing: key generation
Secure exchange protocol
Each DG executes local update (17)
t=t+1
$t<t_{\max}$?
Y
N
Each DG obtains optimal output: $\delta^*\to P_{DG,m}$
Second level: power sharing among DGs within a VPP

Fig. 4. Flowchart of execution process of homomorphically encrypted EMS based on secure exchange protocols.

V. Simulation Results

In this section, the effectiveness of the proposed secure exchange protocols for two-level EMS is verified. The impact of key length on computational efficiency is examined in the following simulation studies. The functions of the Paillier cryptosystem and the proposed privacy-preserving protocols are developed and implemented in MATLAB running on an Intel Core i5 CPU at 3.5 GHz with a 16 GB RAM computer.

A. Case 1: IEEE 5-bus Test Network

An IEEE 5-bus test network, as shown in Fig. 5(a), consists of two VPPs and three load customers. The ring-circle with undirected links is used as the communication topology for the VPPs and loads. The communications among DGs in the VPP2 are illustrated in Fig. 5(b) and DG1 is set as the leader DG which can access the power reference P^*_{VPP}. Solid lines represent the information exchange among DGs. Corresponding parameter configurations are shown in Tables I and II.

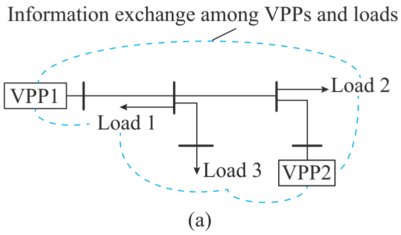

Fig. 5. Schematic diagram of 5-bus test network and communication configuration for DGs in VPP1. (a) 5-bus network. (b) DGs in VPP1.

TABLE I
PARAMETER CONFIGURATION OF VPP FOR CASE 1

VPP	a_i	b_i	c_i	$P^{\min}_{VPP,i}$ (kW)	$P^{\max}_{VPP,i}$ (kW)	$P_i(0)$ (kW)	γ_i
1	0.0016	4.26	40	180	255	220	–0.025
2	0.0017	4.54	60	150	355	206	0.016

TABLE II
PARAMETER CONFIGURATION OF LOAD FOR CASE 1

Load	α_j	β_j	$P^{\min}_{D,j}$ (kW)	$P^{\max}_{D,j}$ (kW)	$P_i(0)$ (kW)	γ_i
1	–0.065	15.86	100	160	160	0.017
2	–0.061	17.45	150	200	180	0.022
3	–0.056	19.35	180	250	230	0.013

The effectiveness of homomorphically encrypted economic coordination under the secure exchange protocols is first evaluated. Set $\tau=5$. The bit length of public and private keys is set to be 256. Variable states in the format of the floating-point number are converted to 64-bit integers before the encryption. The feedback gain σ is set to be 0.5×10^{-3} for (15). The weights $\phi_{i\to j}$ and $\omega_{i\to j}$ are also scaled up and represented by 64-bit integers. The obtained results are shown in Figs. 6 and 7. The optimal value of λ_i is found to be 5.6 and the power balance between generation and demand approaches zero when the algorithm converges.

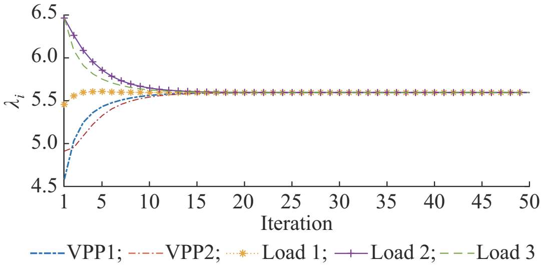

Fig. 6. Convergence to optimal market-clearing price.

Figure 8 visualizes the encrypted state difference transmitted to communicating neighbors. At each iteration, the encrypted difference $E_i(\lambda_j^I-\lambda_i^I)^{\phi_{j\to i}}$ is exchanged as a random big integer between a pair of communicating participants (i,j). It should be underlined that the convergence is still achieved although the encrypted messages appear to be random, verifying that an eavesdropping attacker cannot infer any information during the entire distributed operation.

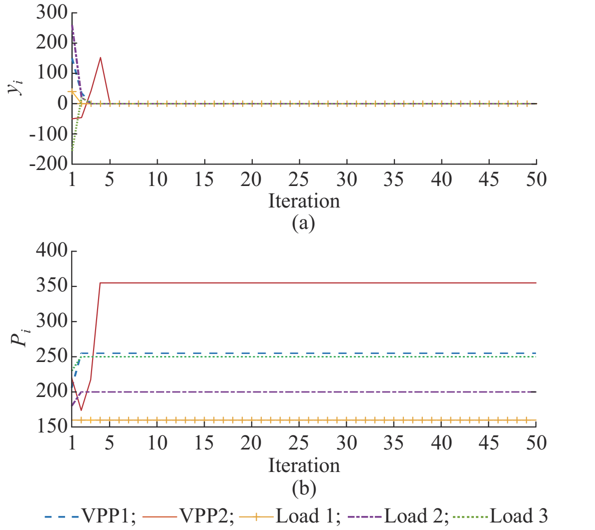

Fig. 7. Updates of local power mismatch y_i and generation/demand P_i at first level of EMS. (a) Local power mismatch update in response to price update. (b) Generation/demand adjustment in response to price update and limited by constraints.

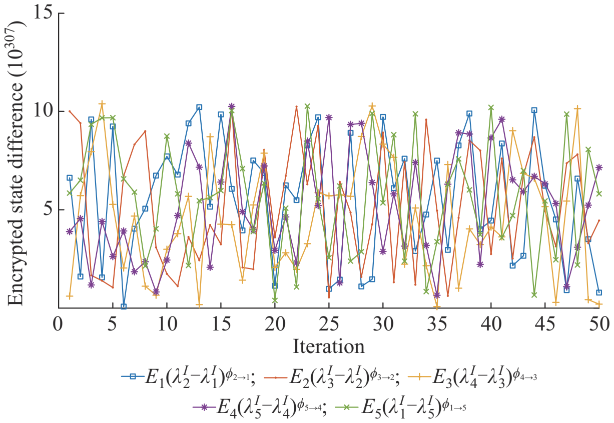

Fig. 8. Encrypted state difference transmitted to communicating neighbors.

Once the optimal power generation of the VPP, i. e., $P^*_{VPP,1}=255$ kW and $P^*_{VPP,2}=350$ kW, is determined at the first level of EMS, the second level of the EMS is activated within a VPP. Here, VPP2 is taken as an example to demonstrate the process of cooperative power sharing. Choose the control gain $\rho=0.004$ for (17). As shown in Fig. 5(b), DG1 has the most communicating neighbors, which lead to $\max\limits_i\{D_i^{in}\}=7$. Hence, $0<\underline{d}<\bar{d}<1\Big/\sqrt{\rho\cdot\max\limits_i\{D_i^{in}\}}=\sqrt{0.004\times7}=0.167$ and the permissible range for the weight $d_{i\to j}$ is set as $[\underline{d},\bar{d}]=[0.01,0.16]$. The objective is to meet $P^*_{VPP,2}=350$ kW and to ensure that the unified power utilization ratio is achieved.

Figure 9 shows the cooperative power sharing among DGs at the second level of EMS within VPP2. The reference in Fig. 9 is $P^*_{VPP,2}=350$ kW that is acquired from the first level of EMS, which is to be satisfied by all DGs in the VPP2. The difference between the power output reference value and the total amount of DG power output gradually approaches zero when the consensus algorithm iterates to find the convergence. Each DG approaches a unified power utilization ratio $\delta_i = 0.8$ while the total power output of all DGs satisfies the required power reference when the algorithm converges.

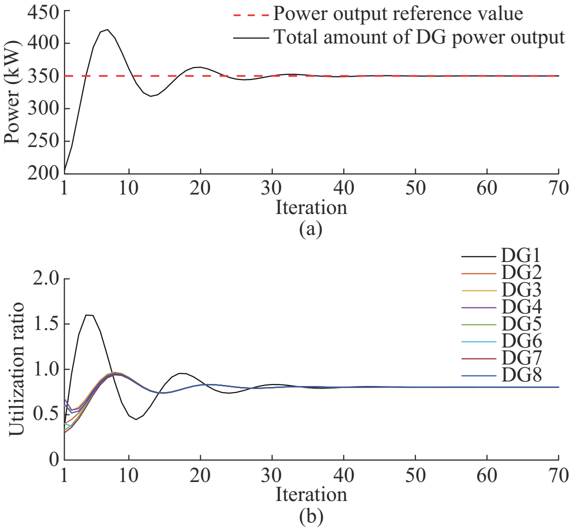

Fig. 9. Cooperative power sharing among DGs at second level of EMS within VPP2. (a) Update of total amount of DG power output. (b) Update of power utilization ratio for each DG.

DG2 is taken as an example to examine its received encrypted states from communicating neighbors, as shown in Fig. 10. The disorderliness verifies that the privacy is protected.

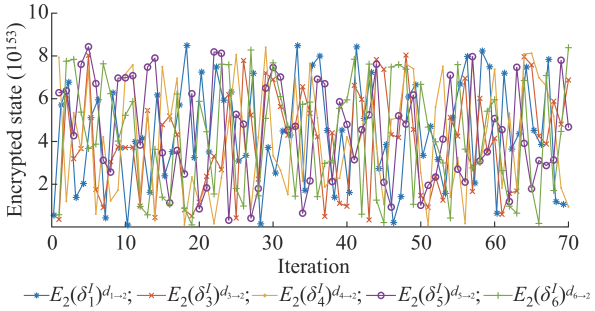

Fig. 10. Encrypted states received by DG2 from communicating neighbors.

B. Case 2: IEEE 34-bus Test Network

IEEE 34-bus test network is used as the second test distribution network, including 10 VPPs and 19 load customers, as shown in Fig. 11. The parameter configurations of VPP and load for case 2 are presented in Tables AI and AII in Appendix A, respectively. The communication configuration for 29 participants in the IEEE 34-bus test network is shown in Fig. 12.

The performance of the first-level economic coordination under a secure exchange protocol is investigated. In the simulation, the bit length of the key is set to be 256. The feedback gain σ is set to be 0.1×10^{-4} for (15). The results are shown in Fig. 13, revealing that the consensus on λ^* is achieved within 150 iterations and the generation and load demand are adjusted in response to the price. The encrypted state difference $E_i(\lambda_j^I - \lambda_i^I)^{\phi_{j\to i}}$ is shown in Fig. 14. The random big integers verify that the privacy of each agent is adequately protected as it is difficult for the attackers to obtain or infer any useful information from such unreadable patterns.

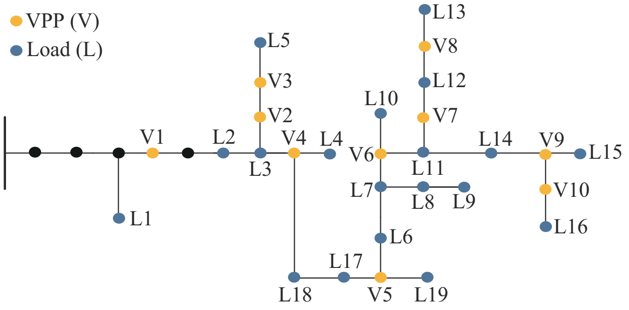

Fig. 11. Schematic diagram of IEEE 34-bus test network.

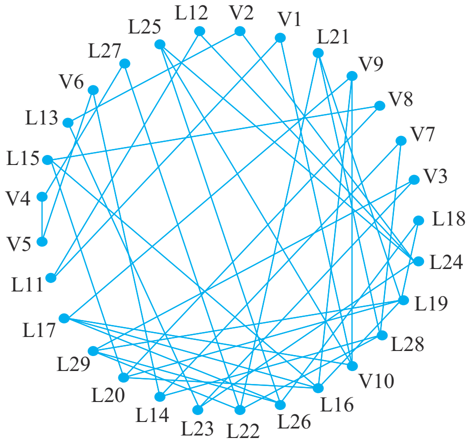

Fig. 12. Communication configuration for 29 participants in IEEE 34-bus test network.

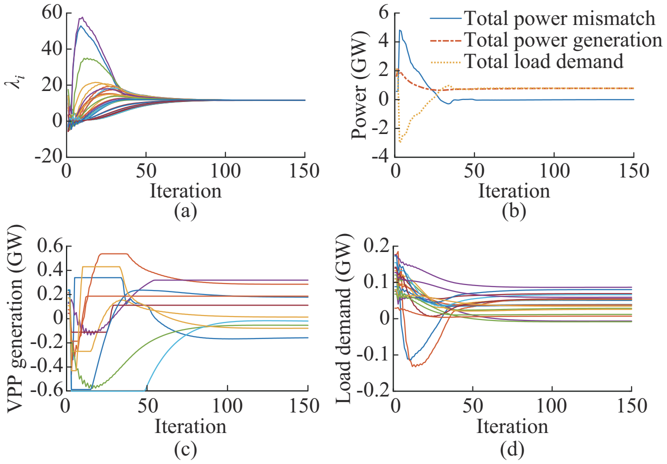

Fig. 13. State evolution. (a) Update of prices (all VPPs and loads). (b) Power mismatch. (c) Generation adjustment in response to price update (10 VPPs). (d) Demand adjustment in response to price update (19 loads).

The computational efficiency under different key lengths is compared, as shown in Table III. It takes a longer total simulation time to run homomorphic cryptosystem based algorithm (15) with a longer key length. Overall, the simulation time is still acceptable and efficient enough for the EMS operation even under the longer key length.

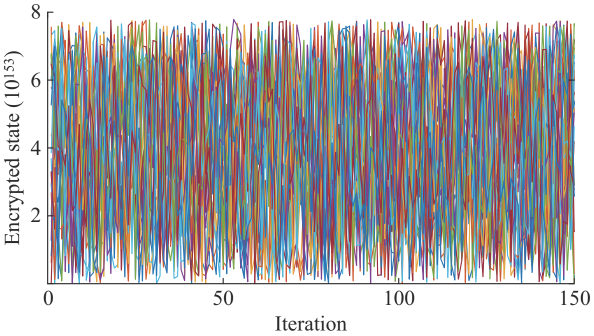

Fig. 14. Encrypted state difference transmitted to communicating neighbors (total 29 encrypted state differences).

TABLE III
COMPUTATIONAL EFFICIENCY UNDER DIFFERENT KEY LENGTHS

Key length (bit)	Total simulation time (s)	Computation time per agent (s)
64	6.12	0.21
128	8.48	0.29
256	10.86	0.27
512	14.65	0.51
1024	17.21	0.59
Unencrypted	4.56	0.15

VI. DISCUSSION

A. Properties of Secure Exchange Protocols

The proposed secure exchange protocol has two main properties: privacy preservation and correctness. The comparison between privacy-preserving EMS under two approaches is given in Table IV. As the working principle of differential privacy is to inject perturbations and noises into the original signal, the convergence and optimality of the final value may not be guaranteed if the injected perturbations and noises are not carefully selected. But for the proposed secure exchange protocols based on the homomorphic cryptosystems, the property of privacy preservation follows the semantic security of the Paillier cryptosystem (introduced in Section III) so that absolute correctness of the final value can be achieved all the time.

TABLE IV
COMPARISON BETWEEN PRIVACY-PRESERVING EMS UNDER TWO APPROACHES

Approach	Correctness	Privacy preservation
EMS based on homomorphic cryptosystem	√	√
EMS based on differential privacy [17]	Only guaranteed with proper noise selection	√

Next, we take λ_i^I as an example to explain the privacy preservation between two communicating participants at each iteration step. For agent $\mathcal{V}_1$, after receiving encrypted information $E_1(\lambda_2^I-\lambda_1^I)^{\phi_{2\to1}}$ from $\mathcal{V}_2$, $\mathcal{V}_1$ decrypts it with Key_1^{pri} so that decrypted information $\phi_{2\to1}(\lambda_2^I-\lambda_1^I)$ is obtained. Nevertheless, $\mathcal{V}_1$ cannot infer λ_2^I through $\phi_{2\to1}(\lambda_2^I-\lambda_1^I)$ as $\phi_{2\to1}$ is only known to $\mathcal{V}_1$. For agent $\mathcal{V}_2$, after receiving encrypted information $E_1(-\lambda_1^I)$ from $\mathcal{V}_1$, it cannot see λ_1^I as it does not have the private key Key_1^{pri} to decrypt it. For an extraneous eavesdropper that eavesdrops on the communication link between participants, it cannot infer λ_i^I as the information is encrypted to $E_i(-\lambda_i^I)$ by the corresponding agent itself, and then transmitted over the communication link. The information privacy on y_i^I and δ_i^I is protected in the same way through the secure exchange protocol. Therefore, it can be concluded that the privacy of all participants is preserved against eavesdropping attacks.

B. Quantization Error and Computation Complexity

The conversion between the floating-point and the integer number will bring unavoidable quantization error Δ, as follows:

$$\Delta=\left|x_F-x_I\right|=x_F\left|(1-10^{\tau})\right| \tag{26}$$

Such a quantization error can be neglected if we choose a sufficiently large preserved digital number τ.

The computation overhead, i.e., the algorithmic complexity, indicates how the computation complexity depends on the input size, which is specified using the Big-O notation. The bit length of the key is denoted by l. Under the proposed secure exchange protocol, for an agent i, the total computation overhead of each iteration is $O(\mathcal{D}_i^{in}l)$ [27]. The computational complexity of the secure exchange protocol based on the Paillier cryptosystem is increased with the number of in-neighbors of a certain agent rather than network size. Hence, the homomorphically encrypted EMS can be applied on large networks with moderate connections.

C. Implementation Considerations of Proposed Privacy-preserving EMS

Since homomorphic encryption allows computation directly on encrypted data which makes the computation speed slower compared with operating on non-encrypted data, it is not suitable to be applied in computational-heavy applications and real-time applications. In this paper, the proposed privacy-preserving EMS is not intended to be applied in real-time operation. Instead, it is conducted every 15 min in the ADN to accommodate the stochastic demand and accordingly update the market-clearing price and DG power output.

VII. CONCLUSION

In this paper, a homomorphically encrypted EMS for economic coordination and power sharing in the IoT-enabled ADN is developed to guarantee the data privacy of DGs and load customers during the information transmission. As a typical homomorphic cryptosystem, the Paillier cryptosystem is applied to develop secure exchange protocols by encoding randomness into the system dynamics so that enhanced privacy security and deterministic convergence of the consensus-based algorithms can be achieved. Private information such as price information, load demand, and power utilization is successfully protected against eavesdropping attackers. The effectiveness and the computational efficiency of the proposed encrypted approach are verified by two test networks.

Appendix A

TABLE AI
Parameter Configuration of VPP for Case 2

VPP	a_i	b_i	$P_i(0)$ (kW)
1	0.0046	13.060	135.880
2	0.0111	5.295	214.920
3	0.0099	11.370	108.040
4	0.0095	3.360	127.690
5	0.0104	12.790	232.560
6	0.0029	11.750	240.000
7	0.0021	3.375	44.628
8	0.0062	9.435	234.480
9	0.0077	6.450	74.600
10	0.0048	12.390	172.090

TABLE AII
Parameter Configuration of Load for Case 2

Load	α_j	β_j	$P_i(0)$ (kW)
1	–0.140	25.750	110.15
2	–0.062	18.420	176.75
3	–0.151	27.630	109.69
4	–0.084	10.590	75.55
5	–0.081	16.275	120.64
6	–0.212	28.365	80.26
7	–0.119	28.140	142.02
8	–0.159	23.550	88.57
9	–0.127	21.420	100.80
10	–0.069	15.225	132.38
11	–0.097	28.560	175.75
12	–0.082	10.305	75.13
13	–0.092	23.940	154.69
14	–0.094	22.050	139.30
15	–0.091	26.250	172.85
16	–0.340	16.455	28.98
17	–0.183	24.375	79.67
18	–0.132	26.295	127.37
19	–0.130	14.760	67.92

Reference

[1] D. Du, M. Zhu, X. Li *et al.*, "A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems," *Journal of Modern Power Systems and Clean Energy*, vol. 11, no. 3, pp. 727-743, May 2023.

[2] O. Dzobo, B. Malila, and L. Sithole, "Proposed framework for blockchain technology in a decentralised energy network," *Protection and Control of Modern Power Systems*, vol. 6, no. 1, pp. 1-11, Dec. 2021.

[3] H. Shahinzadeh, J. Moradi, G. B. Gharehpetian *et al.*, "IoT Architecture for smart grids," in *Proceedings of 2019 International Conference on Protection and Automation of Power System (IPAPS)*, Tehran, Iran, Jan. 2019, pp. 22-30.

[4] F. Meneghello, M. Calore, D. Zucchetto *et al.*, "IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182-8201, Oct. 2019.

[5] Y. Mo，T. H.-J. Kim, K. Brancik *et al.*, "Cyber-physical security of a smart grid infrastructure," *Proceedings of IEEE*, vol. 100, no. 1, pp. 195-209, Jan. 2012.

[6] J. Lin, W. Yu, N. Zhang *et al.*, "A survey on Internet of Things: architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125-1142, Oct. 2017.

[7] Y. Lu and L. Xu, "Internet of Things (IoT) cybersecurity research: a review of current research topics," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2103-2115, Apr. 2019.

[8] J. Yang, G. Sun, and J. Yin, "Coordinated cyber-physical attack considering false overload of lines," *Protection and Control of Modern Power Systems*, vol. 7, no. 1, pp. 1-13, Dec. 2022.

[9] T. Yang, D. Wu, H. Fang *et al.*, "Distributed energy resource coordination over time-varying directed communication networks," *IEEE Transactions on Control of Network Systems*, vol. 6, no. 3, pp. 1124-1134, May 2019.

[10] D. Yang, S. Member, S. Zhang *et al.*, "Consensus-based decentralized optimization for distributed generators power allocation over time-varying digraphs in microgrids," *IEEE Systems Journal*, vol. 15, no. 1, pp. 1-12, Jan. 2020.

[11] R. A. Jabr and I. Džafić, "Distribution management systems for smart grid: architecture, work flows, and interoperability," *Journal of Modern Power Systems and Clean Energy*, vol. 10, no. 2, pp. 300-308, Mar. 2022.

[12] M. H. Ullah, B. Babaiahgari, A. Alseyat *et al.*, "A computationally efficient consensus-based multiagent distributed EMS for DC microgrids," *IEEE Transactions on Industrial Electronics*, vol. 68, no. 6, pp. 5425-5435, Jun. 2021.

[13] Q. Li, D. W. Gao, H. Zhang *et al.*, "Consensus-based distributed economic dispatch control method in power systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 941-954, Jan. 2019.

[14] N. Patari, V. Venkataramanan, A. Srivastava *et al.*, "Distributed optimization in distribution systems: use cases, limitations, and research needs," *IEEE Transactions on Power Systems*, vol. 37, no. 5, pp. 3469-3481, Sept. 2022.

[15] P. Li, J. Hu, L. Qiu *et al.*, "A distributed economic dispatch strategy for power-water networks," *IEEE Transactions on Control of Network Systems*, vol. 9, no. 1, pp. 356-366, Mar. 2022.

[16] Q. Hu, S. Bu, Z. Li *et al.*, "Cost-effective communication network planning considering performance of pinning-based secondary control in microgrids," *International Journal of Electrical Power & Energy Systems*, vol. 133, p. 107269, Dec. 2021.

[17] Q. Hu, Z. Zhu, S. Bu *et al.*, "A multi-market nanogrid P2P energy and ancillary service trading paradigm: mechanisms and implementations," *Applied Energy*, vol. 293, p. 116938, Jul. 2021.

[18] Y. Lu and M. Zhu, "Privacy preserving distributed optimization using homomorphic encryption," *Automatica*, vol. 96, pp. 314-325, Jun. 2018.

[19] Y. Lu, J. Lian, and M. Zhu, "Privacy-preserving transactive energy system," in *Proceedings of 2020 American Control Conference (ACC)*, Denver, USA, Jul. 2020, pp. 3005-3010.

[20] L. Yan, X. Chen, J. Zhou *et al.*, "Privacy-preserving economic dispatch for microgrids with a distributed event-triggered communication scheme," in *Proceedings of 2020 IEEE PES General Meeting (PESGM)*, Montreal, Canada, Aug. 2020, pp. 1-5.

[21] C. Zhao, J. Chen, J. He *et al.*, "Privacy-preserving consensus-based energy management in smart grids," *IEEE Transactions on Signal Processing*, vol. 66, no. 23, pp. 6162-6176, Jun. 2018.

[22] F. Ye, Z. Cheng, X. Cao *et al.*, "A random-weighted privacy-preserving distributed algorithm for energy management in microgrid with energy storage devices," in *Proceedings of 2020 2nd IEEE International Conference on Industrial Electronics for Sustainable Energy Systems (IESES)*, Cagliari, Italy, Sept. 2020, pp. 249-254.

[23] T. W. K. Mak, F. Fioretto, L. Shi *et al.*, "Privacy-preserving power system obfuscation: a bilevel optimization approach," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1627-1637, Mar. 2020.

[24] Y. Xiong, J. Xu, K. You *et al.*, "Privacy-preserving distributed online optimization over unbalanced digraphs via subgradient rescaling," *IEEE Transactions on Control of Network Systems*, vol. 7, no. 3, pp. 1366-1378, May 2020.

[25] X. Yi, R. Paulet, and E. Bertino, *Homomorphic Encryption and Applications*. Cham: Springer International Publishing, 2014.

[26] T. Yin, Y. Lv, and W. Yu, "Accurate privacy preserving average consensus," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 4, pp. 690-694, Jul. 2020.

[27] M. Ruan, H. Gao, and Y. Wang, "Secure and privacy-preserving consensus," *IEEE Transactions on Automatic Control*, vol. 64, no. 10, pp. 4035-4049, Oct. 2019.

[28] A. J. Wood and B. F. Wollenberg, *Power Generation, Operation and Control*. New York: Wiley, 2012.

[29] S. Yang, S. Tan, and J. Xu, "Consensus based approach for economic dispatch problem in a smart grid," *IEEE Transactions on Power Systems*, vol. 28, no. 4, pp. 4416-4426, Apr. 2013.

[30] Y. Liu, H. Xin, Z. Qu *et al*., "An attack-resilient cooperative control strategy of multiple distributed generators in distribution networks," *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2923-2932, Jun. 2016.

[31] P. Paillier, *Public-key Cryptosystems Based on Composite Degree Residuosity Classes*. Berlin: Springer Berlin Heidelberg, 2007.

[32] Y. Yan, Z. Chen, V. Varadharajan *et al*., "Distributed consensus-based economic dispatch in power grids using the Paillier cryptosystem," *IEEE Transactions on Smart Grid*, vol. 12, no. 4, pp. 3493-3502, Jul. 2021.

[33] J. Wang, D. Shi, J. Chen *et al*., "Privacy-preserving hierarchical state estimation in untrustworthy cloud environments," *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1541-1551, Mar. 2021.

Qian Hu received the bachelor's degree from The University of Manchester, Manchester, UK, and North China Electric Power University, Beijing, China, in 2016, the M.Sc. degree from The University of Manchester, and the Ph.D. degree from the Hong Kong Polytechnic University, Hong Kong, China, in 2021. She is currently a Lecturer with the Department of Physics, Hong Kong Baptist University, Hong Kong, China. Her research interests include distributed control and operation of smart grid and multi-energy systems, and the integration of distributed energy resources.

Siqi Bu received the Ph.D. degree from the Electric Power and Energy Research Cluster, The Queen's University of Belfast, Belfast, UK, where he continued his postdoctoral research work before entering industry. Then he was with National Grid UK as an experienced UK National Transmission System Planner and Operator. He is an Associate Professor with the Department of Electrical and Electronic Engineering, The Hong Kong Polytechnic University, Hong Kong, China, and also a Chartered Engineer with UK Engineering Council, London, UK. His research interests in clude power system stability analysis and operation control, considering renewable energy integration and smart grid application.

Wencong Su received the B.S. degree (Hons.) from Clarkson University, Potsdam, USA, in 2008, the M.S. degree from Virginia Tech, Blacksburg, USA, in 2009, and the Ph.D. degree from North Carolina State University, Raleigh, USA, in 2013. He is currently an Associate Professor and Chair of the Department of Electrical and Computer Engineering, University of Michigan-Dearborn, Dearborn, USA. He is a Fellow of IET. He is an Editor of IEEE Transactions on Smart Grid, an Editor of IEEE Power Engineering Letters, an Associate Editor of IEEE Access, and an Associate Editor of IEEE DATAPORT. He was the Guest Editor-in-Chief of IEEE Transactions on Smart Grid – Special Section on Power-Electronics-Enabled Smart Power Distribution Grid. He was a recipient of the 2015 IEEE Power and Energy Society (PES) Technical Committee Prize Paper Award and the 2013 IEEE Industrial Electronics Society (IES) Student Best Paper Award. His current research interests include power systems, transportation electrification, and cyber-physical systems.

Vladimir Terzija received the Dipl-Ing., M.Sc., and Ph.D. degrees in electrical engineering from the University of Belgrade, Belgrade, Serbia, in 1988, 1993, and 1997, respectively. He is a Professor of Energy Systems & Networks at the Newcastle University, Newcastle, UK. He is also a Distinguished Visiting Professor at Shandong University, Jinan, China, as well as a Guest Professor at the Technical University of Munich, Munich, Germany. In the period 2021-2022, he was a Full Professor at Skolkovo Institute of Science and Technology, Skoltech, Russian Federation. In the period 2006-2020, he was the EPSRC Chair Professor at The University of Manchester, Manchester UK. From 2000 to 2006, he was a Senior Specialist for switchgear and distribution automation with ABB, Ratingen, Germany. From 1997 to 1999, he was an Associate Professor with the University of Belgrade, Belgrade, Serbia. He is the Editor-in-Chief of the International Journal of Electrical Power and Energy Systems, Humboldt Fellow and the recipient of the National Friendship Award, China. His current research interests include smart grid applications, wide-area monitoring, protection and control, multi-energy systems, switchgear and transient processes, Internet and communication technology, data analytics, and digital signal processor applications in power systems.