PPSO: A Privacy-Preserving Service Outsourcing Scheme for Real-Time Pricing Demand Response in Smart Grid

Kaiping Xue, *Senior Member, IEEE*, Qingyou Yang, Shaohua Li, David S. L. Wei, *Senior Member, IEEE*, Min Peng, Imran Memon, and Peilin Hong

***Abstract*—In power utility service outsourcing, some time-sensitive computations (e.g., dynamic prices prediction) are outsourced to a third-party service provider. This brings in new privacy threats to customers. Although some existing works focus on achieving privacy-preserving temporal and spatial aggregation for one center, they basically cannot be directly applied to the scenario of service outsourcing with multiple centers (e.g., with power utility and service providers). We thus propose a privacy-preserving service outsourcing scheme, called PPSO, for real-time pricing demand response in smart grid with fault tolerance and flexible customers' enrollment and revocation. In our proposed PPSO, power utility can outsource the dynamic pricing prediction to a service provider, while still preserving customers' privacy. Extensive experiment results demonstrate that PPSO has less computation overhead and lower transmission delay compared with existing schemes.**

***Index Terms*—Privacy preservation, real-time pricing (RTP) demand response (DR), service outsourcing, smart grid.**

I. Introduction

SMART grid incorporates advanced information and communication technology to provide more reliable and economic electricity generation, transmission, and distribution. Intelligent devices, such as smart meters, are thus introduced for the architecture of smart grid. The smart meter is one of the core components in advanced metering infrastructure (AMI) which can collect various types of data and transmit them to other parties through the communication network. Power demand data collected by AMI is important for power utilities to project the demand response (DR) program to maintain the stability of supply and demand in the power system.

Manuscript received May 30, 2018; revised August 10, 2018; accepted September 11, 2018. Date of publication September 18, 2018; date of current version May 8, 2019. This work was supported in part by the National Natural Science Foundation of China under Grant 61671420, in part by the Fundamental Research Funds for the Central Universities, and in part by the Youth Innovation Promotion Association CAS under Grant 2016394. *(Corresponding author: Kaiping Xue.)*

K. Xue, Q. Yang, S. Li, and P. Hong are with the Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei 230027, China (e-mail: kpxue@ustc.edu.cn).

D. S. L. Wei is with the Computer and Information Science Department, Fordham University, New York, NY 10458 USA.

M. Peng is with the School of Computer Science and Information Engineering, Hefei University of Technology, Hefei 230601, China.

I. Memon is with the College of Computer Science, Zhejiang University, Hangzhou 310027, China.

Digital Object Identifier 10.1109/JIOT.2018.2870873

DR was defined by the U.S. Department of Energy as "a tariff or program established to motivate changes in electric use by end-use customers, in response to changes in the price of electricity over time, or to give incentive payments designed to induce lower electricity use at times of high market prices or when grid reliability is jeopardized" [1]. It is recognized as the most cost-effective and reliable solution for smoothing of the demand curve. In general, DR can be classified into two types: 1) price-based DR (PDR) program, which motivates customers to change their consumption patterns according to the dynamic (time-varying) electricity prices and 2) incentive-based DR program, which rewards participating customers for reducing their electricity usage in response to DR requests [2], [3].

In fact, real-time pricing (RTP) DR scheme, classified as a PDR scheme, has already been applied to a large number of industrial and commercial customers [4]. Under the RTP scheme, power utility determines electricity prices for the upcoming time period and announces them before the start of each time period (e.g., 15 min beforehand) [5], thereby improving customers' power usage patterns for shifting the demand curve. The price is subject to multiple factors, such as random events, total real-time power consumption, and the response of customers to the previous prices [6].

For power utility, it is difficult to securely collecting and correctly processing all the data that affect the price. On the one hand, the real-time power data have the characteristics of "3Vs": volume, velocity, and variety [7]. In the traditional way, securely collecting these massive data often uses symmetric encryption (e.g., AES) or asymmetric encryption (e.g., RSA) to encrypt/decrypt each individual data, which will introduce heavy load in communication and computation to power utility. On the other hand, compared with third parties, such as some enterprises specialized in large data analysis, power utilities may not be able to provide more efficient and accurate processing algorithms (such as electricity forecasting and dynamic pricing algorithms). Additionally, as a third party, some types of service providers have been formally introduced into the architecture of smart grid, which can remotely monitor and manage power usage based on customers' preference [8], [9]. For the above reasons, many existing RTP programs choose to outsource some complex operations to third-party service providers.

In fact, the practical demonstrations of services outsourcing have been conducted by companies, such as Oracle [10] and

ENERNOC [11], which act as the service provider and use statistical algorithms to derive information from customers' power data for utility customers. However, as power consumption data usually involves customers' privacy information (especially the real-time consumption data), service outsourcing would pose a significant threat to privacy, which will reduce the willingness of customers to participate in the DR programs.

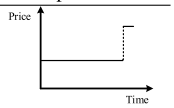
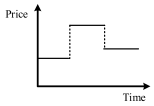
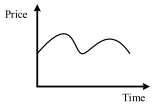
Recently, researchers have paid much attention to privacy preservation in smart grid. For the scenario of real-time data collection, Lu *et al.* [12] and Abdallah and Shen [13], respectively, used the homomorphic encryption to aggregate customers' power data, while avoiding the violation of customer's privacy. Chim *et al.* [14] used anonymous credentials to conceal customer's real ID for privacy preservation in power request. A survey of privacy preservation in V2G has been provided in [15]. However, till now, few researches have considered the privacy preservation problem of service outsourcing in RTP DR program, which is completely different from the above scenarios. It requires the service provider to have the capability of leveraging customers' energy consumption to carry out the dynamic pricing prediction, without leaking any privacy information of customers.

In this paper, motivated by the fact that the privacy preserving problem of service outsourcing in real-time demand respond is worthy to be studied and so far still there is no proposed method addressing it well, we conduct this paper to address this problem. In our scheme, a third-party service provider is introduced to collect and process customers' encrypted consumption data. The power utility can charge customers correctly even the electricity price is time-varying. Our contributions can be summarized as follows.

1) We propose a privacy-preserving service outsourcing scheme addressing RTP DR in smart grid. We realize an efficient DR with fault tolerance and flexible customers' enrollment and revocation. As far as we know, this paper is the first to address the privacy issue in the scenario of service outsourcing dealing with real-time pricing DR in smart grid.
2) To prevent users' privacy disclosing to the third-party service provider, we modify the Paillier cryptosystem to hold two different decryption keys: one is for the service provider to access the particular customer set's aggregation data, and the other one is for the power utility to access the encryption data of all customers.
3) A special billing mechanism is proposed for dynamic pricing of DR. The scheme not only provides each customer's correct electricity bill during the time-varying price periods but also prevents privacy from disclosing to other parties.

The rest of this paper is organized as follows. Section II discusses the related works. We review Paillier cryptosystem as our preliminary in Section III. In Section IV, we introduce our system architecture and security assumptions. Then, we present our proposed PPSO in Section V, followed by security and performance analysis in Sections VI and VII, respectively. Finally, Section VIII makes a conclusion on this paper.

TABLE I
PRICING STRATEGIES

Pricing Strategies	Description	Example
Flat Pricing	Price is fixed within a long time period, e.g., season, year...	
Time-of-Use pricing	Price changes according to the time of day.	
Real-Time Pricing (Dynamic Pricing)	Prices frequently changes (in hours, or minutes).	

II. RELATED WORKS

A. Time-Based Demand Response Programs

In the traditional power grid, the power utility adopts the *flat pricing* strategy to schedule the electricity load. Under this strategy, customers can reduce their electricity bills by using less electricity throughout the duration of the day [16]. Recently, time-of-use (TOU) pricing strategy has been widely adopted by utility companies, e.g., Hydro One [17] and Waterloo North Hydro [18]. Under TOU, electricity prices are changes according to the time of day [19]. The integration of two-way communication for the smart grid enables the RTP strategy for DR, in which the utility announces the dynamic prices at different time periods for users' dynamic demand [5]. Recent researches for RTP strategy mainly focus on maximization of electricity load. Tsui and Chan [20] optimized electricity loads for various household appliances in smart home under RTP. Namerikawa *et al.* [21] designed a distributed real-time electricity pricing mechanism by utilizing game-theoretic approach, which provides suppliers and consumers with a guaranteed incentive to participate in the RTP market. However, consumers are risk-averse, and the privacy disclosure issue discourages the widely deployment of the existing RTP programs [22]. In order to make the above pricing strategies easier to understand, we use Table I to summarize the main difference between them.

B. Security and Privacy in Smart Grid

The security and privacy issue is the main impediment for the development of smart grid, which has been identified in [23]–[25]. Generic security protection methods in traditional networks, such as source authentication and integrity protection mechanism, have thus been introduced to construct a more secure communication between different components in smart grid [26], [27]. However, owing to the distinctive features of smart grid, customers' privacy may still be leaked out unconsciously.

Therefore, recently, some new privacy-preserving mechanisms have been proposed for smart grid. The works in [14], [28], and [29] utilize anonymous credentials/permits

TABLE II
COMPARISON OF RELATED WORKS

Schemes	Advantages	Disadvantages
Credential based [14], [28], [29]	Provide billing and authentication functions	More interactions and higher communication overhead
Noise based [32–37]	Provide differential privacy and high efficiency on customer side	Inaccurate aggregation results
Homomorphism based [12], [38], [43], [44]	Provide secure data aggregation and accuracy aggregation results	Higher computation overhead

to conceal user's real ID during legality verifying of interactive messages. This can also be achieved by using zero-knowledge proof, which has been presented in [30] and [31]. Meanwhile, some other schemes focus on data obfuscation, which aim to hide individual metering data. One way is adding the given distribution noise (like Laplace distribution) into each customer's metering data [32]–[36], or securely generating the secret shares and sending them to two noncolluding cloud servers [37], so as to prevent user's privacy being compromised by differential attacks. Another way is implementing data aggregation technologies, which often utilize homomorphic encryption to get the sum of consumers' data, so that individual data cannot be revealed.

The homomorphism property of homomorphic encryption that allows computing on ciphertext has been implemented widely in smart grid to preserve privacy. Lu *et al.* [12] proposed a novel efficient and privacy-preserving aggregation (EPPA) scheme to process the data of all dimension as a whole rather than separately. Wang [38] proposed an identity-based data aggregation protocol which is more efficient when compared to the public-key-based schemes, and moreover the problem of forward security of key evolution were discussed in [39]. Several schemes about fault tolerance for smart grid, such as [32] and [34], have been proposed to construct a more robust system even when some user failures and server malfunctions occur. Meanwhile, Shi *et al.* [33] and Sun *et al.* [40], respectively, provided effective solutions to perform the error detection when some smart meters are malfunctioning. Considering potential internal attackers, Fan *et al.* [41] used blinding factors to create blinded data, while the works of [42] and [43] proposed a more efficient solution by using the Boneh–Goh–Nissim public key cryptography. Recently, Li *et al.* [44] also presented a aggregation scheme to collect multisubset data against internal attackers.

Specifically, we divide the related works into three categories and summarize their advantages and disadvantages in Table II.

Owing to the fact that service outsourcing scenario usually has multiple centers (e.g., power utility and service providers), directly implementing these existing schemes brings in a severe computation burden and may leak customers' privacy. Therefore, in this paper, we propose an efficient privacy-preserving scheme for service outsourcing with multiple centers in smart grid.

III. PRELIMINARIES

In this section, we review the Paillier cryptosystem [45] and give its extension which serves as the basic building block of our proposed scheme.

A. Paillier Cryptosystem

The Paillier cryptosystem is one of the popular public key encryption schemes, which can achieve homomorphism property and has been widely applied in many privacy-preserving applications [32], [40]. Let $E(\cdot)$, $D(\cdot)$, and r be the notations of encryption function, decryption function, and a random number in $\mathbb{Z}_N^*$, respectively. To generate the private key and public key, we first choose two secure prime numbers p and q, and let $N = pq$ be RSA modulus. We then choose a random element $g \in \mathbb{Z}_{N^2}^*$, and compute $\lambda = \text{lcm}(p-1, q-1)$, $\mu = (L(g^\lambda \bmod N^2))^{-1} \bmod N$, where function $L(x) = (x-1)/N$. Therefore, the private key prk is $\{\lambda, \mu\}$, and the public key puk is $\{N, g\}$. The operation for encrypting a message m is shown as

$$c = E(m) = g^m \cdot r^N \bmod N^2 \tag{1}$$

and the corresponding decryption process is

$$m = D(c) = L\left(c^\lambda \bmod N^2\right) \cdot \mu \bmod N. \tag{2}$$

While the additive homomorphism property is given as follows:

$$\begin{aligned} E(m_1) \cdot E(m_2) &= \left(g^{m_1} \cdot r_1^N\right)\left(g^{m_2} \cdot r_2^N\right) \bmod N^2 \\ &= g^{m_1+m_2} \cdot (r_1 r_2)^N \bmod N^2 \\ &= E(m_1 + m_2). \end{aligned} \tag{3}$$

B. M-Paillier: Modified Paillier Cryptosystem

We make some modifications on the traditional Paillier cryptosystem to deliver two different decryption keys for our proposed scheme, and we call them the *general decryption key* and the *particular decryption key*. Indeed, the general decryption key is the same as a traditional Paillier decryption key, which can be used to decrypt a single ciphertext or any aggregated ciphertext encrypted by the corresponding public key. The particular decryption key is a limited key, and is limited to decrypt the defined set of aggregated ciphertexts. The modified scheme contains the following five phases: 1) key generation; 2) encryption; 3) homomorphic aggregation; 4) general decryption; and 5) particular decryption.

1) *Key Generation:* Select two large and independent prime numbers p and q randomly, and compute $\lambda = \text{lcm}(p-1, q-1)$, where λ is the least common multiple (LCM) of $p-1$ and $q-1$, and let $N = p \cdot q$. Then, define a function $L(x) = [(x-1)/N]$ and choose a generator $g = (1+N)$, compute $\mu = (L(g^\lambda \bmod N^2))^{-1} \bmod N$. Additionally, n random numbers $\{x_1, x_2, \ldots, x_n\}$ in $\mathbb{Z}_N^*$ are generated, where n is the total number of system customers. Then compute $x_0 \in \mathbb{Z}_N^*$ to make it satisfy

$$x_0 + \sum_{i=1}^{n} x_i = 0 \mod \lambda. \tag{4}$$

Finally, let (N, g) be the public key, (λ, μ) be the general decryption key, and x_0 be the particular decryption key.

2) *Encryption:* To encrypt message $m \in \mathbb{Z}_N^*$ at the time point t, the ciphertext can be computed as follows:

$$c = E(m) = g^m \cdot H(t)^{N \cdot x_i} \mod N^2$$

where $H(\cdot)$ is a chosen hash function $H : \{0,1\}^* \rightarrow \{0,1\}^N$.

3) *Homomorphic Aggregation:* The property of additive homomorphism is still held in M-Paillier, which can be used in secure aggregation as follows:

$$\begin{aligned} c &= E(m_1) \cdot E(m_2) \cdots E(m_n) \\ &= g^{m_1+m_2+\cdots+m_n} \cdot H(t)^{N \cdot (x_1+x_2+\cdots+x_n)} \mod N^2 \\ &= E(m_1 + m_2 + \cdots + m_n). \end{aligned} \tag{5}$$

4) *General Decryption:* The encryption result is still in the form of the traditional Paillier cryptosystem, which can be decrypted by using the general decryption key (λ, μ) as follows:

$$\sum_{i=1}^{n} m_i = L(c^{\lambda} \mod N^2) \cdot \mu \mod N.$$

5) *Particular Decryption:* The particular decryption key x_0 is a limited key, which can only be utilized to decrypt the specified set of aggregation data (e.g., all n customers)

$$\sum_{i=1}^{n} m_i = \frac{c \cdot H(t)^{N \cdot x_0} - 1}{N} \mod N. \tag{6}$$

The correctness of the equation can be proved as follows:

$$\begin{aligned} c \cdot H(t)^{N \cdot x_0} &= g^{\sum_{i=1}^{n} m_i} \cdot H(t)^{x_0 + \sum_{i=1}^{n} x_i} \\ &= g^{\sum_{i=1}^{n} m_i} \cdot H(t)^{k\lambda} \mod N^2 \\ &= 1 + N \cdot \sum_{i=1}^{n} m_i. \end{aligned} \tag{7}$$

IV. Components, Security Assumptions, System Flow, and Design Goals

Here, we first describe the components and security assumptions for our proposed PPSO. Then, we demonstrate the system flow in detail. Finally, the design goals for our scheme are presented.

A. Components

Components in smart grid can communicate with each other, and take their respective responsibilities to construct a privacy-preserving demand request/response mechanism. The scheme involves four components, including *smart meter* (also mentioned as *customer*), *gateway*, *service provider*, and *power utility*, as shown in Fig. 1.

1) Smart Meter/Customer: Smart meters are intelligent devices that are installed at customer premises by utility companies. We assume that smart meters can implement basic cryptographic operations and control other intelligent devices in the house and response to the dynamic prices. For clarity, we can treat the smart meter and customer as the same component.

2) Gateway: Gateways are usually deployed by a third-party operator (e.g., telecom operator) to connect power utility, service providers, and smart meters into a network. They are usually physically locked from outside access so that attackers are relatively difficult to compromise them.

3) Service Provider: Service providers in smart grid are able to provide some special services for power utility or customers. In this paper, service providers are assumed to have a powerful algorithm for dynamic pricing prediction through the collected power consumption data and other valuable information.

4) Power Utility: Power utility buys and sells electricity, announces dynamic prices to customers during different time periods, and charges each customer after a billing period. It also takes the responsibility for system initialization and customers registration/revocation.

B. Threat Model

In this paper, we follow the same assumption of [46] and [47] and assume the power utility is fully trusted, while the service provider is assumed to be honest but curious. On the one hand, service provider will follow the defined protocols to provide its services correctly for gaining allowable benefits. On the other hand, it may attempt to violate customers' privacy for the purpose of crime or gaining illegal benefits. Additionally, we also assume that the service provider has no capability to collude with the customers under its serving scope. Since the gateways are usually deployed by a third-party operator, we also assume they are semi-honest, which means that they will follow the protocol but are interested in customers' privacy. The smart meters are tamper resistant such that the stored keys are difficult to be cracked or altered by outside parties.

C. System Flow

The system flow of our proposed scheme is shown in Fig. 1. Recently, the RTP DR has been applied to a large number of industrial and commercial customers [4]. However, in the residential domain, the existing RTP schemes have not been widely deployed, as many consumers are risk-averse. Also, in some cases the cost saving resulting from adopting the new pricing program exceeds what is imposed on customers to follow the program [48]. Therefore, the power utility tends to adopt a new pricing plan and allows customers to join in and quit the program voluntarily. Taking into account the above considerations, our scheme should contain two types of customers: 1) DR customers and 2) traditional customers. DR customers participate in the RTP DR program and are charged with the dynamic pricing strategy. Meanwhile, traditional customers can be charged with the flat pricing strategy. It is noted that the operations for this difference are only for power utility and gateways, and all customers in our scheme implement the same operations during the whole process. In addition, time is slotted in DR program, and we assume that a billing period contains T time slots. At each time slot, the electricity price is fixed, but the prices at different time slots are usually different.

The main procedure for DR customers consists of *metering process*, *submission process*, *price forecasting*, *price*

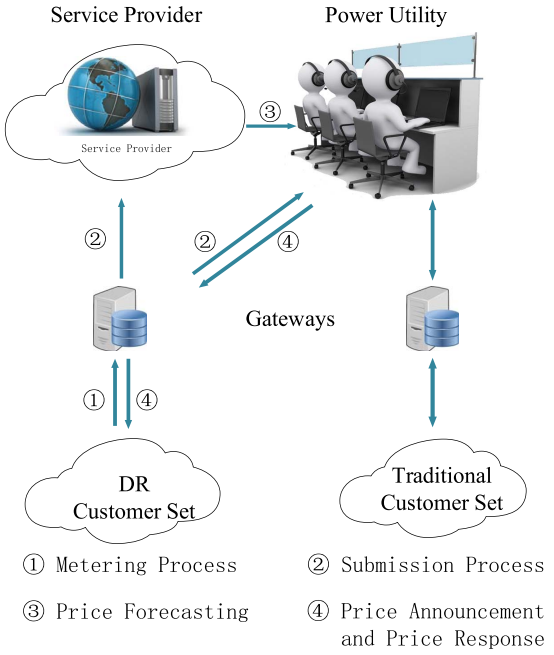


Fig. 1. System flow.

announcement and price response, and *billing*. At the beginning of each time slot, the metering process is first carried out, where each smart meter measures the power consumption data, encrypts the data, and sends the encrypted data to the corresponding gateway. Then the gateway duplicates the data into two copies, where one copy is submitted to the service provider for price forecasting, and the other one is submitted to the power utility for billing. After receiving all processed data of consumers from gateways, the service provider can predict the price for the next time slot, and sends the forecasted result to the power utility. Then the power utility announces the assessed power price to the involved customers. In the billing period, the power utility computes the accumulative electricity bill for each individual customer. It should be noted that, owing to the characteristics of 3Vs for real-time power consumption data [7], we allow the service provider to directly collect data from gateways, rather than the power utility, in order to avoid lots of complex cryptographic operations for the power utility. However, the proposed scheme should ensure that the service provider can only correctly handle the power consumption data from the customers involved in the specific DR program. For the traditional customers, the same as what proposed in [13] and [49], the power utility can directly collect aggregate data for billing or just monitoring the status of the system.

D. Design Goals

We intend to design an efficient scheme that can guarantee customers' privacy preserving when the power utility outsources some time-sensitive computation in the RTP DR program to a third-party service provider. Specifically, our design goals comprise the following four aspects.

1) *Data Confidentiality:* The proposed scheme should achieve the confidentiality of individual customer' real-time energy consumption data, even if an adversary eavesdrops the communication channel or compromise the gateways and service provider.
2) *Privacy Preservation:* Except the trusted power utility, no one, including the service provider, can be allowed to learn customers' privacy information from real-time energy consumption data.
3) *Fault Tolerance:* The proposed scheme should provide the capability of fault tolerance, in which even when some smart meters are malfunctioning and fail to submit real-time consumption data, the power utility and service provider should still be able to decrypt other customers' submitted data.
4) *Flexible Customers Enrollment and Revocation:* The proposed scheme should provide a flexible customer enrollment and revocation mechanism for supporting a customer to dynamicly join in/quit from the RTP DR program.

V. Proposed Scheme

In this section, we first give the system initialization. Then, two subprotocols, namely the privacy-preserving data metering for traditional customers and the privacy-preserving service outsourcing in RTP DR program for DR customers, of our scheme are provided in detail.

A. System Initialization

Let $\mathbb{U}$, $\mathbb{U}^a$, and $\mathbb{U}^b$ be the system customer set, DR customer set, and traditional customer set, respectively ($\mathbb{U} = \mathbb{U}^a \cup \mathbb{U}^b$). As stated in Section III-B, the power utility randomly chooses two different large primes p and q, where $|p| = |q| = l$, and then generates the public key ($N = pq$, g) and computes the general decryption key (λ, μ) for the Paillier cryptosystem. Then, the power utility generates n random numbers $\{x_1, \ldots, x_n\}$ in $\mathbb{Z}_N^*$ ($|\mathbb{U}| = n$), and computes the particular decryption key $x_0 \in \mathbb{Z}_N^*$ such that

$$x_0 + \sum_{i \in \mathbb{U}^a} x_i = 0 \mod \lambda. \tag{8}$$

In practice, the size of each random number should not be less than 1024 bits. Finally, the power utility sends x_0 to the service provider and x_i to each customer i in $\mathbb{U}$ via secure channels. In addition, a secure hash function $H : \{0,1\}^* \rightarrow \{0,1\}^N$ is selected. The system parameters are published as $\{N, g, H\}$.

B. Subprotocol I: Privacy-Preserving Data Metering for Traditional Customers

Considering that there are some customers (called traditional customers) who are not willing to participate in the DR program, the proposed scheme must be universal for both DR customers and traditional customers. As what traditional privacy-preserving data metering schemes, such as [13] and [49], are doing, our privacy-preserving data metering for traditional customers mainly consists of the following three steps.

1) *Encryption:* At the time for data collection (e.g., time slot t), customer $i \in \mathbb{U}^b$ reads the corresponding data

$m_{i,t}$, and encrypts it with x_i and N as follows, then sends the encryption result $c_{i,t}$ to the corresponding gateway

$$c_{i,t} = E(m_{i,t}) = g^{m_{i,t}} \cdot H(t)^{x_i \cdot N} \mod N^2. \quad (9)$$

2) *Aggregation:* After receiving the encryption results from customers, the gateway aggregates them into one message c_t, and submits c_t to the power utility

$$c_t = \prod_{i \in \mathbb{U}^b} E(m_{i,t}) = g^{\sum_{i \in \mathbb{U}^b} m_{i,t}} \cdot H(t)^{N \cdot \sum_{i \in \mathbb{U}^b} x_i} \mod N^2. \quad (10)$$

3) *Decryption:* After receiving the aggregated data from gateways, the power utility gets the sum of submitted data m_t by decrypting it with the general decryption key (λ, μ) as follows:

$$m_t = \sum_{i \in \mathbb{U}^b} m_{i,t} = L\left(c_t^{\lambda} \mod N^2\right) \cdot \mu \mod N. \quad (11)$$

It should be noted that the data metering scheme is flexible and fault-tolerant, meaning that even if some smart meters fail to submit their metering data to the gateway, the utility is still able to decrypt the aggregated data by using general decryption key (λ, μ).

C. Subprotocol II: Privacy-Preserving Service Outsourcing in RTP Demand Response for DR Customers

DR customers who participate in the proposed DR program should submit their real-time power consumption data to the third-party service provider. As shown in Fig. 1, the detailed processes are described as follows.

1) *Metering Process:* DR program should be implemented based on collected power consumption data, so the metering process is carried out first to collect customers' electricity usage. We elaborate the electricity usage collection with respect to a time slot t and a DR customer $i \in \mathbb{U}^a$. The customer i reports its electricity usage $m_{i,t}$ with the operation of encryption as follows:

$$c_{i,t} = E(m_{i,t}) = g^{m_{i,t}} \cdot H(t)^{x_i \cdot N} \mod N^2 \quad (12)$$

where x_i is the encryption key delivered by power utility in the phase of system initialization, and $c_{i,t}$ is the encryption form of electricity usage for customer i at time slot t. Then the customer sends $c_{i,t}$ to the corresponding gateway.

2) *Submission Process:* After receiving the encryption results from customers, the gateway first duplicates each data into two copies. One copy is used to implement the operation in (13) for charging the customer

$$b_{i,t} = {c_{i,t}}^{p_t}, \ i \in \mathbb{U}^a \quad (13)$$

where p_t is the predetermined electricity price at time slot t, $b_{i,t}$ is actually the encryption form of $m_{i,t} \cdot p_t$ and the corresponding plaintext of $b_{i,t}$ represents the electricity bill for customer i at time slot t. The encryption form of electricity bill for each customer will be sent to power utility for charging at the billing phase. The other copy is used to implement the operation in (14), and the result is submitted to the service provider for price forecasting

$$c_t = \prod_{i \in \mathbb{U}^a} c_{i,t} \quad (14)$$

where c_t is the encryption form of $\sum_{i \in \mathbb{U}^a} m_{i,t}$, which is the sum of all DR customers' electricity usage.

3) *Price Forecasting:* After receiving the aggregated data from gateway, the service provider first decrypts the data with its particular decryption key x_0 as follows:

$$m_t = \frac{c_t \cdot H(t)^{x_0 \cdot N} - 1}{N} \mod N \quad (15)$$

where $m_t = \sum_{i \in \mathbb{U}^a} m_{i,t}$ is the sum of all DR customers' electricity usage at time slot t.

After the decryption, the service provider utilizes its adopted algorithm, such as the algorithm in [50] (denoted as output $= \mathcal{A}$(input)), to generate the price p_{t+1} in the next time slot as follows:

$$p_{t+1} = \mathcal{A}(m_t, \text{other parameters}). \quad (16)$$

Then the service provider sends p_{t+1} to the power utility for ending this phase.

4) *Price Announcement and Price Response:* When the power utility receives the forecasted price p_{t+1} for the next time slot, it will broadcast/multicast it to all DR customers. After receiving the electricity price, DR customers can manually or automatically adjust its power usage pattern as the pricing response.

5) *Billing Process:* For charging customer i, the power utility first performs (17) to accumulate the total electricity bills in the form of ciphertext during the specific time period

$$b_i = \prod_{t=1}^{T} b_{i,t}. \quad (17)$$

The power utility gains the plaintext by decrypting it with its general decryption key (λ, μ)

$$M_i = L\left(b_i^{\lambda} \mod N^2\right) \cdot \mu \mod N. \quad (18)$$

In fact, M_i is equal to $\sum_{t=1}^{T} m_{i,t} \cdot p_t$ and represents the total electricity bills for customer i during the dynamic pricing period.

6) *Fault Tolerance:* Smart meters may be malfunctioning because of the limitations of its lifetime or natural disaster, and they require the power utility to remotely reset or reinstall them back to the normal status. However, during this maintenance period, the service provider would fail to get m'_t in *price forecasting* phase by decrypting the real-time aggregated data (assume that the malfunctioning smart meters set at time slot t is $\mathbb{U}^a_m$), since

$$c'_t = g^{\sum_{i \in \mathbb{U}^a / \mathbb{U}^a_m} m_{i,t}} \cdot H(t)^{\sum_{i \in \mathbb{U}^a / \mathbb{U}^a_m} x_i} \quad (19)$$

where $x_0 + \sum_{i \in \mathbb{U}^a / \mathbb{U}^a_m} x_i \neq 0 \mod \lambda$. Observing this problem, we design a fault tolerant mechanism to allow the service provider successfully decrypt the aggregated

data even when some smart meters are failed to submit their data. In detail, the power utility first implements the operation as (20) and sends the result H_{mal} to the service provider

$$H_{\text{mal}} = H(t)^{\sum_{i\in\mathbb{U}_m^a} x_i \cdot N}. \tag{20}$$

After receiving the aggregated data and H_{mal}, the service provider decrypts the ciphertext as follows:

$$\begin{aligned} m_t' &= \frac{c_t' \cdot H_{\text{mal}} \cdot H(t)^{x_0 \cdot N} - 1}{N} \mod N \\ &= \sum_{i\in\mathbb{U}^a/\mathbb{U}_m^a} m_{i,t}. \end{aligned} \tag{21}$$

D. Dynamic Customers' Enrollment and Evocation

Customer sets in the system may not always remain unchangeable, i.e., a new customer can be added into the customer set $\mathbb{U}$ or an existing one can be revoked from it. Therefore, the dynamic customer management is crucial to our scheme. The scheme is described as follows.

1) *Dynamic Customer Management for Traditional Customers:* When a customer U_b is added into the system as a traditional customer, the power utility first generates a random number $x_b \in \mathbb{Z}_N^*$ as the secret key for the newly joined customer, then delivers the key to this customer through the secure channel. Meanwhile, when a customer U_r is removed from traditional customer set $\mathbb{U}^b$, the power utility just deletes its secret key from the database.
2) *Dynamic Customer Management for DR Customers:* When a customer U_a is added into the system as a DR customer, the power utility first generates a random number $x_a \in \mathbb{Z}_N^*$ and sends it to U_a via the secure channel. Then the utility randomly selects a small number of DR customers from DR customer set $\mathbb{U}^a$ (denoted the selected DR customer set as $\mathbb{U}_{\text{sel}}^a \in \mathbb{U}^a$). For security consideration, $|\mathbb{U}_{\text{sel}}^a|$ should be larger than 2. Then the utility generates a new $x_i' \in \mathbb{Z}_N^*$ for each customer in $\mathbb{U}_{\text{sel}}^a$, such that

$$x_a + \sum_{i\in\mathbb{U}_{\text{sel}}^a} x_i' = \sum_{i\in\mathbb{U}_{\text{sel}}^a} x_i \mod \lambda.$$

Finally, the power utility sends each x_i' to the corresponding selected customer in $|\mathbb{U}_{\text{sel}}^a|$ through the secure channel. To remove a customer U_r from DR customer set $\mathbb{U}^a$, the procedure has to be more complicate than that of removing a traditional customer. The power utility randomly selects a subset $\mathbb{U}_{\text{sel}}^a$ ($|\mathbb{U}_{\text{sel}}^a| \geq 2$) from DR customer set, and generates a new random number $x_i' \in \mathbb{U}_N^*$ for each selected DR customer in $\mathbb{U}_{\text{sel}}^a$, such that

$$\sum_{i\in\mathbb{U}_{\text{sel}}^a} x_i' = \sum_{i\in\mathbb{U}_{\text{sel}}^a} x_i - x_r \mod \lambda.$$

Then the utility sends the newly generated number x_i' to the corresponding selected DR customers in $|\mathbb{U}_{\text{sel}}^a|$ via the secure channel.

VI. Security Analysis

In this section, we discuss the security issues of the proposed PPSO scheme via analysis. Our analysis mainly focuses on confidentiality and privacy preservation.

A. Confidentiality for Metering Data

In the proposed PPSO scheme, each customer i's electricity usage data in time slot t is encrypted as $c_{i,t} = g^{m_{i,t}} \cdot H(t)^{x_i \cdot N} \mod N^2$ by smart meters before being submitted to the gateway. To prove its confidentiality, we first give two assumptions as follows.

1) *The Problem of Deciding Nth Residuosity (DCR[N]):* A num x is said to be an Nth residue modulo N^2 if there exists a number $y \in \mathbb{Z}_{N^2}^*$ such that $x = y^N \mod N^2$. The problem of deciding Nth residuosity is to distinguishing Nth residues from non Nth residues, which is believed to be computationally hard.
2) *Decisional Composite Residuosity Assumption (DCRA):* There exists no polynomial time distinguisher for Nth residues modulo N^2, that is, DCR[N] is intractable.

Then, the confidentiality for metering data can be derived from the following lemma.

Lemma 1: The proposed M-Paillier scheme is semantically secure under DCRA.

Proof: Here, we use the IND-CPA game to prove our lemma. Proving the lemma is the same as proving that if M-Paillier is not secure, then DCRA does not hold. We assume a polynomial time adversary $\mathcal{A}$ against M-Paillier, then we can construct an adversary against DCR[N] as follows.

1) $\mathcal{A}$ chooses two messages $m_0, m_1 \in \mathbb{Z}_N$.
2) The challenger chooses $b \in \{0, 1\}$, and outputs $c = g^{m_b} \cdot H(t)^{x_i N} \mod N^2$. Meanwhile, we choose an instance $x \in$ DCR[N], and want to find out whether x is an N'th residue or not. Then, we compute $c' = cx$ and send c' to $\mathcal{A}$.
3) $\mathcal{A}$ decides if c' is an encryption of m_0 or m_1, and answers $b' \in \{0, 1\}$. If $b' = b$, we say x is Nth residue, otherwise it is not N'th residue.

Therefore, two cases are contained.

1) *x Is an Nth Residue:* Then c' is an encryption of m_0 or m_1. Thus, $\mathcal{A}$ has a non-negligible advantage. It means it has a probability non-negligible more than 1/2 to choose the right one. When $\mathcal{A}$ wins, we win as well. In other words, we also have a probability non-negligible higher than 1/2 to find Nth residues.
2) *x Is Not an Nth Residue:* Then x is an encryption of some random message, and c' is also an encryption of random message. Thus, $\mathcal{A}$ chooses with zero advantage, which means that it has only probability 1/2 to choose the right one. So when $\mathcal{A}$ wins, we lose, and this happens with probability 1/2.

In summary, we more often choose rightly when x is an Nth residue than wrongly when x is not an Nth residue. So we can solve DCR[n] with probability non-negligible more than 1/2, and accordingly break the DCRA assumption. In other words, our proposed M-Paillier is semantically secure if DCRA holds. Thus, the confidentiality of metering data is protected. ■

B. Privacy Preservation for Customers

In order to prevent the privacy of customers from disclosing, the service provider is not allowed to recover each individual customer's usage data, but can gain the aggregated data of a specific customer set. Here, we prove this goal by the following lemmas.

Lemma 2: Suppose that the number of participating customers satisfies $|\mathbb{U}^a| \geq 2$ and service provider cannot compromise each individual customer's private key x_i ($i \in \mathbb{U}^a$). Service provider cannot violate individual customer's privacy.

Proof: First, from Lemma 1, we know that service provider is unable to access each individual customer's metering data without knowing each customer's private key. Since service provider holds decryption key x_0 which satisfies $x_0 + \sum_{i\in\mathbb{U}^a} x_i = 0 \mod \lambda$, it can recovered the aggregated data $\sum_{i\in\mathbb{U}^a} m_{i,t}$ from the ciphertext as

$$\prod_{i\in\mathbb{U}^a} c_{i,t} \cdot H(t)^{x_0} = g^{\sum_{i\in\mathbb{U}^a} m_{i,t}} \cdot H(t)^{x_0+\sum_{i\in\mathbb{U}^a} x_i}. \tag{22}$$

However, it is still impossible for service provider to infer individual customer metering data from the aggregated result $\sum_{i\in\mathbb{U}^a} m_{i,t}$ since $|\mathbb{U}^a| \geq 2$. In fact, the decryption capability for the service provider is totally decided by the fully trusted power utility. Without any individual x_i, the service provider is impossible to access any individual customer's electricity usage data. ■

Lemma 3: Suppose that the service provider collude with customer set $\mathbb{U}^c$, and $|\mathbb{U}^c| < |\mathbb{U}^a| - 1$, service provider is unable to infer other noncolluding individual customer's metering data.

Proof: By colluding with customer set $\mathbb{U}^c$, service provider can obtain the aggregated result $\sum_{i\in\mathbb{U}^c} m_{i,t}$ and $\sum_{i\in\mathbb{U}^a} m_{i,t}$. Since $|\mathbb{U}^a| - |\mathbb{U}^c| \geq 2$, service provider cannot infer other noncolluding individual customer's metering data as proven in Lemma 2. On the other hand, service provider may try to recover the private key $\{\lambda, \mu\}$. However, the private key λ can be recovered only with all of the DR customers' secret keys as

$$x_0 + \sum_{i\in\mathbb{U}^a} x_i = z\lambda, \ z \in \mathbb{Z}. \tag{23}$$

Thus,

$$x_0 + \sum_{i\in\mathbb{U}^c} x_i = z\lambda - \sum_{j\in\mathbb{U}^a/\mathbb{U}^c} x_j. \tag{24}$$

As $\mathbb{U}^a/\mathbb{U}^c \neq \varnothing$ and x_j is a random number in $\mathbb{Z}^*_{\mathbb{N}}$, the service provider cannot obtain the private key $\{\lambda, \mu\}$. ■

Lemma 4: In the phase of customers' enrollment and revocation, service provider is unable to infer customers' private key.

Proof: In the dynamic customers' enrollment and revocation, when a customer U_a is added into or removed from DR customer set $\mathbb{U}^a$, the power utility chooses to update a random subset of DR customers' secret keys. Therefore, the added/removed customer key still would not be leaked to the service provider, and the forward security is also achieved after updating secret keys. ■

TABLE III
SECURITY COMPARISON WITH RELATED SCHEMES

Scheme	Data Confidentiality	Accurate Results	Dynamic Customers	Privacy-Preserving Service Outsourcing
EPPA [12]	Yes	Yes	Yes	No
PPFA [36]	Yes	No	Yes	No
EPPDR [39]	Yes	Yes	Yes	No
DPAFT [51]	Yes	No	Yes	No
3PDA [43]	Yes	Yes	No	No
our proposed PPSO	Yes	Yes	Yes	Yes

C. Security Comparisons

We compare the proposed PPSO with several other representative data aggregation schemes for smart grid in terms of the aspects of data confidentiality, accurate results, dynamic customers, and privacy-preserving service outsourcing. As shown in Table III, these existing works have not yet taken the issue of privacy-preserving service outsourcing into consideration in smart grid, and the issue is well addressed in our proposed PPSO.

VII. PERFORMANCE EVALUATION

In this section, we evaluate the performance of the proposed PPSO in terms of computation overhead, transmission delay, and communication overhead. As shown in Section V, our proposed PPSO consists of two subprotocols: 1) PPSO for traditional customers (denoted as PPSO-TRAD) and 2) PPSO for DR customers (denoted as PPSO-DR).

A. Experiment Setup

The privacy-preserving issue for service outsourcing in smart grid has not been explored in depth. As far as we know, there is still no existing scheme similar to ours that can be introduced for performance comparison. To specifically evaluate the performance with related works, we choose three representative works EPPA [12], PPFA [36], and 3PDA [43], and make a suitable modifications so that they can be applicable to the scenario of service outsourcing in DR. Without loss of generality, we use EPPA for illustration of our modifications, PPFA and 3PDA are also made the same changes. For the traditional customers who do not participate in the DR program, the original EPPA scheme can be directly implemented to replace PPSO-TRAD (denoted as EPPA-TRAD). While for the DR customers, there are generally two approaches to utilize EPPA for constructing PPSO-DR liked protocol. One approach (denoted as EPPA-DR1) is that the power utility directly collects all DR customers's real-time consumption data by using EPPA, then the utility securely sends specific data to the service provider (e.g., encrypted by AES algorithm). The other approach (denoted as EPPA-DR2) is that the gateways directly submit the real-time consumption data to the service provider as in our scheme. However, for preventing customers' private information from leaking to the service provider, each DR customer should, respectively, encrypt data twice by using different public key.

B. Computation Overhead

To evaluate the computation overhead for our scheme, we first investigate the time costs of the primitive cryptography

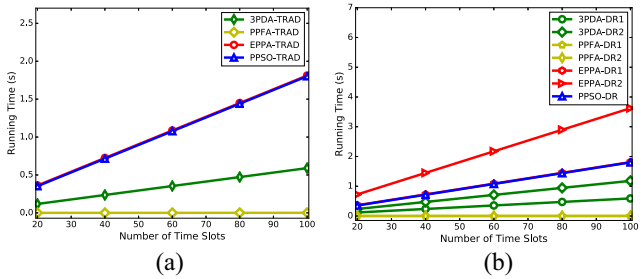


Fig. 2. Computation overhead for customer. (a) Comparison for TRAD protocol. (b) Comparison for DR protocol.

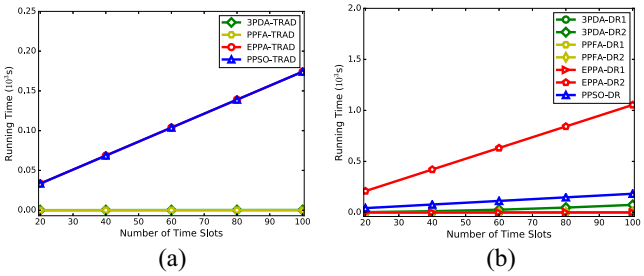


Fig. 3. Computation overhead for gateway. (a) Comparison for TRAD protocol. (b) Comparison for DR protocol.

operations as in 3PDA [43], in which the experiments are conducted in a laptop with the Intel Core i5–2450M CPU@2.50 GHz and 8 GB RAM, based on the PBC and Openssl library. Their experiment results show that the time costs for the pairing operation, point multiplication, Paillier encryption, Paillier decryption, and homomorphic addition are 2.187, 1.476, 18.114, 16.768, and 17.589 ms, respectively. Based on these data, we respectively, compare our computation overhead of customer, gateway, and power utility with the related works as follows.

1) Computation Overhead for Customer: As shown in Fig. 2, our scheme is more efficient than EPPA, but is inferior to 3PDA and PPFA, in terms of running time. However, it is acceptable since whether in TRAD protocol or DR protocol, the running time for customer in our scheme is less than 2 s even when the time slot is set as 100.

2) Computation Overhead for Gateway: As shown in Fig. 3, our scheme is more efficient than EPPA, but inferior to PPFA and 3PDA schemes, in terms of the time cost of gateway. It should be noted that the running time is not too high for each individual time slot and it is acceptable for gateways which usually has a certain computing power to execute these operations.

3) Computation Overhead for Power utility: We compare the computation overhead of our scheme with that of related works which is shown in Fig. 4. From the figure, it can be seen that our scheme is equally good to EPPA and more efficient than 3PDA in both TRAD and DR protocol in terms of the time cost. Although PPFA is more efficient than our proposed PPSO, it cannot get the accurate result since noise is added to perturb metering data.

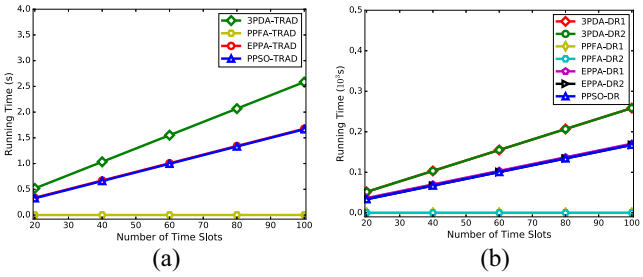


Fig. 4. Computation overhead for power utility. (a) Comparison for TRAD protocol. (b) Comparison for DR protocol.

TABLE IV
COMPARISON OF COMMUNICATION OVERHEAD

Overhead(MB)	EPPA		PPFA		3PDA		PPSO
	DR1	DR2	DR1	DR2	DR1	DR2	DR
10 Customers	0.25	0.38	0.20	0.20	0.74	1.00	0.26
100 Customers	2.44	3.67	1.84	1.85	7.33	9.80	2.45
500 Customers	12.21	18.32	9.17	9.18	36.62	48.85	12.22
1000 Customers	24.42	36.63	18.33	18.33	73.25	97.68	24.43

C. Transmission Delay

In an RTP DR program, the transmission delay of consumption data is also a critical factor which can influence the effectiveness of DR. Therefore, we compare the transmission delay of our proposed PPSO with the modified related schemes for DR protocol. For clarity, we assume that the average transmission delay between any two components is σ, that is, the time cost of the signal transmission for customer-gateway, gateway-utility, gateway-service provider, and service provider-utility is σ. We can easily derive that the transmission delay for our DR protocol is $5 \cdot \sigma$, while the DR1 and DR2 protocol for EPPA, PPFA, and 3PDA have the same transmission delay, that is $6 \cdot \sigma$ and $5 \cdot \sigma$, respectively. In summary, our proposed PPSO is more efficient than related works in terms of the transmission delay.

D. Communication Overhead

Owing to the fact that the TRAD protocol for EPPA, PPFA, 3PDA, and our proposed PPSO all have the same procedure, the size of message are very similar. Therefore, in this part, we only compare the communication overhead of DR protocol of our scheme with that of the related works. Specifically, the size of ciphertexts encrypted by asymmetric encryption algorithms (e.g., Paillier) are set as 1024 bits, ciphertexts encrypted by symmetric encryption algorithms (e.g., AES) are set as 512 bits. We compare the communication overhead with different number of customers as shown in Table IV (the number of time slots are set to 100). It can be seen that our proposed PPSO is barely equally good to EPPA and PPFA, and is more efficient than 3PDA scheme, in terms of the communication overhead.

VIII. CONCLUSION

In this paper, we proposed a privacy-preserving service outsourcing scheme for DR in smart grid. In our scheme, time-sensitive computations in RTP DR, such as dynamic prices

predictions, are outsourced to a third-party service provider to improve the effectiveness of DR program and reduce the computation load on the power utility. Moreover, we further modified the traditional Paillier cryptosystem, which only generates a single decryption key, to derive two different decryption keys for the new demand. In our modification, the decryption keys can be used to preserve customers' privacy while sharing the consumption data with the service provider. Compared with two modified EPPA-based schemes, our proposed PPSO is more efficient in terms of the computation overhead and the transmission delay. In the future work, we will consider to add some special noises, such as Laplace noise, to customers' metering data to prevent the differential privacy attack in the case of outsourcing services to service provider.

ACKNOWLEDGMENT

The authors would like to thank the anonymous referees for their invaluable suggestions that have led to the present improved version of this paper.

REFERENCES

[1] "Benefits of demand response in electricity markets and recommendations for achieving them," U.S. Dept. Energy, Washington, DC, USA, Rep. lbnl-1252d, 2006.

[2] R. Deng, Z. Yang, M.-Y. Chow, and J. Chen, "A survey on demand response in smart grids: Mathematical models and approaches," *IEEE Trans. Ind. Informat.*, vol. 11, no. 3, pp. 570–582, Jun. 2015.

[3] Q. Yang *et al.*, "A privacy-preserving and real-time traceable power request scheme for smart grid," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, 2017, pp. 1–6.

[4] P. Cappers, C. Goldman, and D. Kathan, "Demand response in U.S. electricity markets: Empirical evidence," *Energy*, vol. 35, no. 4, pp. 1526–1535, 2010.

[5] C. Chen, S. Kishore, and L. V. Snyder, "An innovative RTP-based residential power scheduling scheme for smart grids," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, 2011, pp. 5956–5959.

[6] P. Luh, Y.-C. Ho, and R. Muralidharan, "Load adaptive pricing: An emerging tool for electric utilities," *IEEE Trans. Autom. Control*, vol. AC-27, no. 2, pp. 320–329, Apr. 1982.

[7] A. V. Vasilakos and J. Hu, "Energy big data analytics and security: Challenges and opportunities," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2423–2436, Sep. 2016.

[8] D. He *et al.*, "Secure service provision in smart grid communications," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 53–61, Aug. 2012.

[9] S. Li, X. Zhang, K. Xue, L. Zhou, and H. Yue, "Privacy-preserving prepayment based power request and trading in smart grid," *China Commun.*, vol. 15, no. 4, pp. 14–27, Apr. 2018.

[10] *Opower*. Accessed: Sep. 27, 2018. [Online]. Available: https://www.oracle.com/industries/utilities/products/opower-energy-efficiency-cloud-service/index.html

[11] *ENERNOC*. Accessed: Sep. 27, 2018. [Online]. Available: https://www.enernoc.com/

[12] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621–1631, Sep. 2012.

[13] A. Abdallah and X. S. Shen, "A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 396–405, Jan. 2018.

[14] T. W. Chim, S.-M. Yiu, L. C. K. Hui, and V. O. K. Li, "Privacy-preserving advance power reservation," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 18–23, Aug. 2012.

[15] W. Han and Y. Xiao, "Privacy preservation for V2G networks in smart grid: A survey," *Comput. Commun.*, vols. 91–92, no. 2016, pp. 17–28, 2016.

[16] M. Doostizadeh and H. Ghasemi, "A day-ahead electricity pricing model based on smart metering and demand-side management," *Energy*, vol. 46, no. 1, pp. 221–230, 2012.

[17] *Hydro One*. Accessed: Sep. 27, 2018. [Online]. Available: http://www.hydroone.com/Pages/default.aspx

[18] *Waterloo North Hydro*. Accessed: Sep. 27, 2018. [Online]. Available: https://www.wnhydro.com/en/index.asp

[19] P. Palensky and D. Dietrich, "Demand side management: Demand response, intelligent energy systems, and smart loads," *IEEE Trans. Ind. Informat.*, vol. 7, no. 3, pp. 381–388, Aug. 2011.

[20] K. M. Tsui and S.-C. Chan, "Demand response optimization for smart home scheduling under real-time pricing," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1812–1821, Dec. 2012.

[21] T. Namerikawa, N. Okubo, R. Sato, Y. Okawa, and M. Ono, "Real-time pricing mechanism for electricity market with built-in incentive for participation," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2714–2724, Nov. 2015.

[22] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, "UDP: Usage-based dynamic pricing with privacy preservation for smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 141–150, Mar. 2013.

[23] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, no. 1, pp. 81–85, Jan. 2010.

[24] F. M. Tabrizi and K. Pattabiraman, "A model for security analysis of smart meters," in *Proc. IEEE/IFIP 42nd Int. Conf. Depend. Syst. Netw. Workshops (DSN-W)*, 2012, pp. 1–6.

[25] N. Saxena and B. J. Choi, "State of the art authentication, access control, and secure integration in smart grid," *Energies*, vol. 8, no. 10, pp. 11883–11915, 2015.

[26] T. W. Chim, S.-M. Yiu, L. C. Hui, and V. O. Li, "PASS: Privacy-preserving authentication scheme for smart grid network," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2011, pp. 196–201.

[27] T. W. Chim, S.-M. Yiu, V. O. Li, L. C. Hui, and J. Zhong, "PRGA: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid," *IEEE Trans. Depend. Secure Comput.*, vol. 12, no. 1, pp. 85–97, Jan./Feb. 2015.

[28] F. Diao, F. Zhang, and X. Cheng, "A privacy-preserving smart metering scheme using linkable anonymous credential," *IEEE Trans. Smart Grid*, vol. 6, no. 1, pp. 461–467, Jan. 2015.

[29] Z. Yang, S. Yu, W. Lou, and C. Liu, "P^2: Privacy-preserving communication and precise reward architecture for V2G networks in smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 697–706, Dec. 2011.

[30] Y. Gong, Y. Cai, Y. Guo, and Y. Fang, "A privacy-preserving scheme for incentive-based demand response in the smart grid," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1304–1313, May 2016.

[31] D. Mashima and A. Roy, "Privacy preserving disclosure of authenticated energy usage data," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2014, pp. 866–871.

[32] L. Chen, R. Lu, Z. Cao, K. AlHarbi, and X. Lin, "MuDA: Multifunctional data aggregation in privacy-preserving smart grid communications," *Peer-to-Peer Netw. Appl.*, vol. 8, no. 5, pp. 777–792, 2015.

[33] Z. Shi *et al.*, "Diverse grouping-based aggregation protocol with error detection for smart grid communications," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2856–2868, Nov. 2015.

[34] L. Chen, R. Lu, and Z. Cao, "PDAFT: A privacy-preserving data aggregation scheme with fault tolerance for smart grid communications," *Peer-to-Peer Netw. Appl.*, vol. 8, no. 6, pp. 1122–1132, 2015.

[35] C. E. Kement, H. Gultekin, B. Tavli, T. Girici, and S. Uludag, "Comparative analysis of load-shaping-based privacy preservation strategies in a smart grid," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3226–3235, Dec. 2017.

[36] L. Lyu *et al.*, "PPFA: Privacy preserving fog-enabled aggregation in smart grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3733–3744, Aug. 2018.

[37] H. Chun, K. Ren, and W. Jiang, "Privacy-preserving power usage and supply control in smart grid," *Comput. Security*, vol. 77, no. 2018, pp. 709–719, Feb. 2018.

[38] Z. Wang, "An identity-based data aggregation protocol for the smart grid," *IEEE Trans. Ind. Informat.*, vol. 13, no. 5, pp. 2428–2435, Oct. 2017.

[39] H. Li *et al.*, "EPPDR: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 8, pp. 2053–2064, Aug. 2014.

[40] R. Sun, Z. Shi, R. Lu, M. Lu, and X. Shen, "APED: An efficient aggregation protocol with error detection for smart grid communications," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, 2013, pp. 432–437.

[41] C.-I. Fan, S.-Y. Huang, and Y.-L. Lai, "Privacy-enhanced data aggregation scheme against internal attackers in smart grid," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 666–675, Feb. 2014.

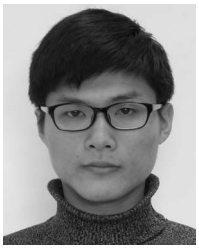
[42] D. He, N. Kumar, S. Zeadally, A. Vinel, and L. T. Yang, "Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2411–2419, Sep. 2017.
[43] Y. Liu, W. Guo, C.-I. Fan, L. Chang, and C. Cheng, "A practical privacy-preserving data aggregation (3PDA) scheme for smart grid," *IEEE Trans. Ind. Informat.*, to be published. [Online]. Available: https://doi.org/10.1109/TII.2018.2809672
[44] S. Li, K. Xue, Q. Yang, and P. Hong, "PPMA: Privacy-preserving multi-subset data aggregation in smart grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 462–471, Feb. 2018.
[45] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, 1999, pp. 223–238.
[46] Z. Sui, M. Niedermeier, and H. de Meer, "TAI: A threshold-based anonymous identification scheme for demand-response in smart grids," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3496–3506, Jul. 2018.
[47] D. Seo, H. Lee, and A. Perrig, "Secure and efficient capability-based power management in the smart grid," in *Proc. 9th IEEE Int. Symp. Parallel Distrib. Process. Appl. Workshops (ISPAW)*, 2011, pp. 119–126.
[48] B. R. Alexander, "Dynamic pricing? Not so fast! A residential consumer perspective," *Electricity J.*, vol. 23, no. 6, pp. 39–49, 2010.
[49] J. Ni, K. Alharbi, X. Lin, and X. Shen, "Security-enhanced data aggregation against malicious gateways in smart grid," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, 2015, pp. 1–6.
[50] P. Faria and Z. Vale, "Demand response in electrical energy supply: An optimal real time pricing approach," *Energy*, vol. 36, no. 8, pp. 5374–5384, 2011.
[51] H. Bao and R. Lu, "A new differentially private data aggregation with fault tolerance for smart grid communications," *IEEE Internet Things J.*, vol. 2, no. 3, pp. 248–258, Jun. 2015.

Kaiping Xue (M'09–SM'15) received the B.S. degree from the Department of Information Security, University of Science and Technology of China (USTC), Hefei, China, in 2003, and the Ph.D. degree from the Department of Electronic Engineering and Information Science (EEIS), USTC, in 2007.

From 2012 to 2013, he was a Post-Doctoral Researcher with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, USA. He is currently an Associate Professor with the Department of Information Security and the Department of EEIS, USTC. His current research interests include next-generation Internet, distributed networks, and network security.

Qingyou Yang received the B.S. degree in information security from the School of the Gifted Young, University of Science and Technology of China, Hefei, China, in 2016, where he is currently pursuing the graduation degree in communication and information system at the Department of Electronic Engineering and Information Science.

His current research interests include network security and cryptography.



Shaohua Li received the B.S. degree from the Department of Information Security, University of Science and Technology of China, Hefei, China, in 2016, where he is currently pursuing the graduation degree in communication and information system at the Department of Electronic Engineering and Information Science.

His current research interest includes network security protocol design and analysis.

David S. L. Wei (SM'07) received the Ph.D. degree in computer and information science from the University of Pennsylvania, Philadelphia, PA, USA, in 1991.

He is currently a Professor with the Computer and Information Science Department, Fordham University, New York, NY, USA. From 1993 to 1997, he was with the Faculty of Computer Science and Engineering, University of Aizu, Aizuwakamatsu, Japan (as an Associate Professor and then a Professor). He has authored or co-authored over 100 technical papers in various archival journals and conference proceedings. His current research interests include cloud computing, big data, IoT, and cognitive radio networks.

Dr. Wei was an Associate Editor of the IEEE TRANSACTIONS OF CLOUD COMPUTING, a Lead Guest Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS for the "Special Issue on Mobile Computing and Networking," the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS for the "Special Issue on Networking Challenges in Cloud Computing Systems and Applications," and the IEEE TRANSACTIONS ON CLOUD COMPUTING for the "Special Issue on Cloud Security," and a Guest Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS for the "Special Issue on Peer-to-Peer Communications and Applications." He is currently an Associate Editor of the *Journal of Circuits, Systems, and Computers* and a Guest Editor of the IEEE TRANSACTIONS ON BIG DATA for the "Special Issue on Trustworthiness in Big Data and Cloud Computing Systems." He served on the Program Committee and was a Session Chair for several international conferences.

Min Peng received the B.S. and Ph.D. degrees from the Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei, China, in 2005 and 2010, respectively.

From 2011 to 2013, he was a Research Engineer with the Huawei Nanjing Research Institute, Nanjing, China. In 2013, he joined the Department of Communication Engineering, Hefei University of Technology, Hefei. His current research interests include delay-tolerant networks, wireless communication, IoT, indoor positioning, and sensor networks.

Imran Memon received the B.S. degree in electronics from the IICT Building University of Sindh, Jamshoro, Pakistan, in 2008, the M.E. degree in computer engineering from the University of Electronic Science and Technology, Chengdu, China, and the Ph.D. degree from the College of Computer Science and Technology, Zhejiang University, Hangzhou, China.

He is currently a Research Assistant with Zhejiang University. He has authored or co-authored over 30 research papers. His current research interests include artificial intelligence systems, network security, embedded system, information security, peer to peer networks, location-based services, and road networks.

Peilin Hong received the B.S. and M.S. degrees from the Department of Electronic Engineering and Information Science (EEIS), University of Science and Technology of China (USTC), Hefei, China, in 1983 and 1986, respectively.

She is currently a Professor and an Advisor for Ph.D. candidates with the Department of EEIS, USTC. She has authored 2 books and over 150 academic papers in several journals and conference proceedings. Her current research interests include next-generation Internet, policy control, IP QoS, and information security.