ABDP: Accurate Billing on Differentially Private Data Reporting for Smart Grids

Jialing He, *Member, IEEE*, Ning Wang, *Member, IEEE*, Tao Xiang, *Senior Member, IEEE*, Yiqiao Wei, Zijian Zhang, *Senior Member, IEEE*, Meng Li, *Senior Member, IEEE*, and Liehuang Zhu, *Senior Member, IEEE*

***Abstract*—While smart grid significantly facilitates energy efficiency by using users' power consumption data, it poses privacy leakage risk for user personal behaviors. Differential privacy (DP) has emerged as a promising solution to address this issue. However, existing approaches suffer from severe data utility degradation due to the intensive noise introduced by DP. Additionally, some of these methods are vulnerable to security attacks. To bridge this gap, in this paper, we propose ABDP (accurate billing-enabled differentially private), a mechanism that achieves high-strength DP while ensuring accurate aggregation and billing operations without compromising security. In particular, we propose aggregated and individual noise cancellation algorithms to counteract the negative effects of noise on data utility. Specifically, our ABDP ensures precise aggregation and accurate billing calculations for the power grid and individual users, respectively Furthermore, we present a Blockchain smart contract exploiting the pseudo random function to enforce a fair and secure data reporting process. Theoretical analysis is provided to evaluate the privacy and security guarantees of ABDP. Experimental results on real-world datasets, namely NERL-DATA and REDD, demonstrate that ABDP achieves error-free aggregation and billing calculation, offers arbitrary intensity privacy protection against non-intrusive load monitoring and filtering attacks, and outperforms existing state-of-the-art approaches.**

***Index Terms*—Accurate aggregation, accurate billing, blockchain smart contract, differential privacy, smart grid.**

I. Introduction

POWER efficiency amounts to one of critical challenges facing humanity [1], [2]. Smart gird, through instruments such as demand-side management [3], [4] and dynamic pricing [5], [6], provides an integrative paradigm to regulate energy distribution, thereby achieving better power efficiency. Behind these instruments is the installed smart meter's ability to collect and transmit the energy usage data of end users. With the collected real-time energy usage data, smart grid utilities can perform analytics to determine the possible supplies for different districts and exploit appropriate strategies to improve power efficiency.

However, this operation raises a significant privacy concern for users. Existing research demonstrates that users' behavior patterns can be exposed through the collected power consumption data [7], [8]. For instance, filtering attacks [9] and the non-intrusive load monitoring (NILM) technique [10], [11], [12], [13] can recover the user's power signal and predict the usage of specific household appliances, enabling inferences about the occupant's presence at home, daily activities, and even dwelling size. Such personal information could be misused for malicious marketing or exploited by adversaries for home invasions, posing a serious threat to the user's personal safety.

To address this privacy concern, significant efforts have been devoted to this field. Traditionally, conventional solutions have relied on auxiliary devices and data encryption techniques to safeguard user privacy in the smart grid context. For instance, household rechargeable batteries and energy storage units can be employed to conceal users' actual power consumption data, thereby protecting their behavioral patterns [14], [15], [16]. However, the purchase of such rechargeable batteries and energy storage units is expensive. Additionally, their capacity limitations significantly impact the effectiveness of privacy preservation. Data encryption techniques [17], [18], [19], particularly homomorphic encryption, have emerged as another prevalent approach for privacy preservation [20], [21], [22], [23]. Homomorphic encryption schemes enable the aggregation of power signals from all users in a district without disclosing individual data, as these schemes support addition operations on ciphertexts. However, some of these solutions introduce security concerns, as they require trust in the power grid operator or a third party to provide the aggregated ciphertext. In reality, the power grid operator and the third party may misuse or sell users' private information for personal gain. Furthermore, encryption-based solutions generally entail high computation or communication complexity.

Recent advances in differential privacy (DP) [24] have provided promising approaches to address these limitations. DP

Manuscript received 6 June 2023; revised 2 June 2024; accepted 6 July 2024. Date of publication 15 July 2024; date of current version 9 October 2024. This work was supported in part by the National Key R&D Program of China under Grant 2022YFB3103500, in part by the National Natural Science Foundation of China under Grant 62302071, Grant 62101079, Grant U20A20176, Grant U23A20303, and Grant 62372149, and in part by the Natural Science Foundation of Chongqing, China, under Grant CSTB2023NSCQ-MSX0693. *(Corresponding author: Ning Wang.)*

Jialing He, Ning Wang, Tao Xiang, and Yiqiao Wei are with the College of Computer Science, Chongqing University, Chongqing 400044, China (e-mail: hejialing@cqu.edu.cn; nwang5@cqu.edu.cn).

Zijian Zhang and Liehuang Zhu are with the School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing 100081, China.

Meng Li is with the Key Laboratory of Knowledge Engineering with Big Data, Ministry of Education, Hefei University of Technology, Hefei 230002, China, also with the School of Computer Science and Information Engineering, Hefei University of Technology, Hefei 230002, China, and also with the Anhui Province Key Laboratory of Industry Safety and Emergency Technology; and Intelligent Interconnected Systems Laboratory of Anhui Province, Hefei University of Technology, Hefei 230002, China.

Digital Object Identifier 10.1109/TSC.2024.3428348

schemes involve the addition of carefully calibrated random noise to the user's power consumption data to ensure privacy. This strategy eliminates the need for costly auxiliary devices and reduces computation and communication costs. Additionally, DP offers a formal mathematical definition and proof for quantifying privacy. Several existing solutions [9], [17], [25], [26], [27] have adopted the DP mechanism to protect individual users' power consumption and appliance usage patterns. To support aggregation operations and preserve individual privacy in the aggregated data, [28], [29] propose DP-based mechanisms using the Boneh-Goh-Nissim cryptosystem and fog computing, respectively. However, these approaches require a trusted party to perform data sanitization, which raises security concerns. To overcome this reliance on a trusted third party, [30], [31] devise decentralized DP mechanisms that inject Laplace noise into the aggregated data in a distributed manner at each user's end, thus ensuring DP after aggregation. Zheng et al. [32] further enhance privacy protection by employing a random permutation algorithm to shuffle individual power measurement sequences.

However, existing DP-based solutions still face several critical issues:

• Privacy protection is limited as a trade-off to ensure the utility of power data. The introduction of noise in the DP mechanism obscures users' consumption patterns, but it also negatively impacts various essential operations such as load monitoring, dynamic pricing, and electricity billing due to the lack of accurate power data and aggregation. Gough et al. [33] have extensively studied the associated losses in load monitoring and users' electricity bills. Although they use cooperative game theory to distribute the additional costs among participants fairly, they are unable to completely eliminate the losses and costs. Therefore, achieving both accurate operations and high-level privacy preservation simultaneously remains a significant challenge.

• Collusion attacks pose a threat to DP mechanisms. Some DP schemes aim to enhance the utility of power data without compromising privacy protection. For example, Hafeez et al. [34], [35] proposed an aggregated-noise reduction strategy where a master or multiple masters are randomly selected from end users to collect the cumulative differential noise introduced by all other users. This allows the power grid to obtain accurate aggregation by subtracting the collected noise sum from the noisy aggregated power data. However, the absence of a secure master selection process makes the real users' power data vulnerable to compromise when corrupted masters collude with the power grid. Consequently, existing DP solutions still face significant security threats.

To address these challenges, we present an **A**ccurate **B**illing-enabled **D**ifferentially **P**rivate (ABDP) mechanism. ABDP is an innovative meter data reporting scheme that ensures both high-strength user privacy and accurate operations while resisting collusion attacks. By leveraging the infinite divisibility of the Laplace distribution, ABDP introduces Laplace noise into the power consumption data in a distributed manner at each end user, thereby ensuring DP after data aggregation and safeguarding users' behavior patterns. Through the design of novel noise cancellation strategies, ABDP significantly mitigates the trade-off between data utility and privacy protection, enabling accurate billing and aggregation operations while concurrently preserving privacy at a high level. Furthermore, the mathematical principle of additivity in the gamma distribution guarantees that our noise cancellation strategies do not violate user privacy. Additionally, we employ a Blockchain smart contract to ensure the security of ABDP. Blockchain technology [36] enhances the security and trustworthiness of ABDP in several ways. Its decentralized nature eliminates single points of failure and distributes control among multiple participants, reducing the risk of collusion. Smart contracts automate the execution of critical processes like master selection, ensuring they are carried out as specified without human intervention, minimizing errors and malicious alterations. Moreover, the immutability and transparency of Blockchain ensure that all operation results are permanently and verifiably The consensus mechanism further prevents collusion, preserving the integrity of the differential privacy guarantees. These features significantly enhance the security and reliability of our ABDP.

The technical contributions of our mechanism are shown as follows:

1) We introduce two novel noise cancellation strategies to mitigate the negative effects of added noise on data utility. From the perspective of end users, we propose a periodic noise cancellation algorithm that sets the added noise to zero for each period. This ensures accurate periodic power data for each customer, enabling precise billing calculations and supporting dynamic pricing. From the perspective of the power grid, we employ masters to collect real-time added noise data from all users. Consequently, the power grid can obtain accurate aggregated power data by subtracting the collected noise sum from the noisy aggregated data received.
2) To establish a secure and fair master selection process, we utilize a Blockchain smart contract and a pseudo-random function (PRF). This ensures that the selected masters are random and unpredictable to adversaries, and the selection result can be verified by any user. This process effectively prevents the master node from being compromised in advance by an adversary attempting to launch a collusion attack with the power grid and access users' real power consumption data.
3) We provide a formal theoretical analysis to validate the privacy and security of our ABDP scheme. Additionally, we evaluate our mechanism using two real-world datasets: NREL-DATA [37] and REDD [38]. The experimental results demonstrate that our ABDP scheme surpasses the state-of-the-art in achieving accurate aggregation and billing calculations, while maintaining a high level of privacy preservation effectiveness against NILM and filtering attacks.

The remainder of this paper is organized as below. We review related work in Section II. We introduce our system architecture, adversary model, and design objectives in Section IV. We give the preliminary in Section III, and our proposed scheme ABDP is presented in Section V. In Section VI, we formally analyze the security and privacy of ABDP. In Section VII, we show the implementation of ABDP and evaluate its performance against existing works on real-world datasets. Finally, Section VIII concludes this article.

II. Related Work

In this section, we review the underlying technologies which aim to protect user privacy in the meter data reporting.

Rechargeable batteries-based work: These solutions aim to safeguard end users' behavior patterns by concealing their actual power consumption data through the utilization of stored electricity in batteries or storage units. Tan et al. [14] employ a rechargeable battery with finite capacity to store excess energy for future use, thereby obfuscating the user's real power consumption data. They utilize a finite state model to represent the system and investigate the specific rate of information leakage between the input and output load, enabling measurement of user privacy. Farokhi and Sandberg [15] utilize Fisher information to quantify privacy and propose optimal policies for charging and discharging electricity from batteries to minimize Fisher information and maximize the power usage estimation error for adversaries. Subsequently, Sun et al. [16] propose the use of electric vehicles as a substitute for batteries to conceal the load. They employ Q-learning algorithms to optimize control policies for electricity storage units. However, the cost of these rechargeable batteries and energy storage units, as well as the control algorithms and storage capacity limitations, significantly impede the effectiveness of these schemes in preserving privacy.

Data encryption-based work: Data encryption is a widely used technology for protecting user privacy in smart grids. Ács and Castelluccia [17] propose a modulo addition-based encryption mechanism to encrypt each user's power consumption data. This ensures that the power grid can only decrypt the sum of all users' power data without accessing individual data. However, establishing pairwise keys between users using the Diffie-Hellman key exchange protocol incurs communication costs. Guan et al. [18] combine the RSA encryption algorithm, Bloom filter, and Blockchain to ensure data confidentiality and integrity, but it requires intensive communication and computation. Wang et al. [19] use the fill function and session keys to mask users' power consumption data, allowing the power grid to obtain aggregated power signals without revealing any user data. However, encryption introduces additional computation and communication overhead to resist internal attacks.

Many solutions opt for homomorphic encryption, as it enables aggregation on ciphertexts and reduces decryption computation for obtaining aggregated data. Liang et al. [20] incorporate homomorphic encryption to obtain aggregated power consumption data for each community while supporting dynamic pricing. Li et al. [21] scale this method to enable finer grid aggregations. However, these schemes require trusted gateways or control centers to collect aggregated ciphertexts, which can pose security risks. Epic [22] and NHP^3 [23] address this limitation by introducing key sharing and game theory technologies to remove the trusted assumption. Nevertheless, a significant drawback of all these data encryption-based solutions is the computation or communication overhead they entail.

DP-based work: To address computation limitations and formally measure privacy, several DP-based solutions have been proposed. Barbosa et al. [9] apply the DP mechanism to protect individual users' power consumption data, safeguarding their consuming patterns at the appliance level. Zhang et al. [25] ensure privacy by combining a household rechargeable battery with DP. Hassan et al. [26], [27] incorporate a Laplace-based DP mechanism to protect individual privacy and propose a usage-based algorithm to support dynamic pricing. To protect individual privacy in aggregated data, Bao et al. [28] propose the model DPAFT, which combines DP with a Boneh–Goh–Nissim cryptosystem. Lyu et al. [29] utilize the fog computing architecture and Gaussian mechanism to construct the PPFA system, achieving provable DP for aggregated data at fog and cloud levels. Both solutions require a trusted party for data sanitization, which can introduce security concerns. [30], [31] devise a decentralized DP mechanism where Laplace noise is injected at each user's end to add noise to aggregated data, eliminating the need for a trusted third party or aggregator assumption. Zheng et al. [32] further enhance protection strength by applying random permutation to individual user's data.

DP protects privacy by adding calibrated random noise to user data, but this compromises data utility. Gough et al. [33] extensively investigate the losses in operations such as load monitoring and bill calculation caused by the added noise of DP mechanisms. They employ cooperative game theory to distribute extra costs among participants fairly. However, the trade-off between privacy and data utility remains unresolved. Hafeez et al. [34], [35] propose introducing masters to collect all added noise data from users, enabling the power grid to acquire accurate real-time load information. However, there are two issues with this solution: 1) An insecure master selection process can lead to security concerns like collusion attacks; 2) While accurate aggregation is possible, precise periodic aggregation of power consumption for individual users is still lacking, hindering precise billing. Therefore, the trade-off between privacy preservation and data utility persists.

III. Preliminaries

A. Differential Privacy

Differential privacy (DP) [24] is a definition that supports learning useful information about a population while not revealing each individual's privacy. Down to the meter reporting scenario, DP ensures the protection of each individual's power-consuming privacy while supporting inquiring about the aggregated power consumption data of all users.

Definition 1 (ε-DP): A randomized mechanism $\mathcal{M}$ is ε-differential privacy if it satisfies that for all neighboring datasets x_0 and x_1 ($\|x_0 - x_1\|_1{}^1$) and all $\mathcal{S} \in Range(\mathcal{M})$:

$$\Pr\left[\mathcal{M}(x_0) \in \mathcal{S}\right] \leq e^{\varepsilon} \Pr\left[\mathcal{M}(x_1) \in \mathcal{S}\right], \tag{1}$$

where $Range(\mathcal{M})$ denotes all possible outputs of $\mathcal{M}$ and ε is a privacy budget. Further, the granularity of privacy protection of $\mathcal{M}$ is inversely proportional to the size of ε.

There exists a great number of mechanisms that guarantee ε-DP. We take the Laplace-DP mechanism (that is used to build our system) as an example to illustrate the details of a differentially private mechanism. We begin with a definition of the Laplace distribution:

Definition 2 (The Laplace distribution): The probability density function of the Laplace distribution (centered at 0) with scale λ is denoted as:

$$Lap\left(x|\lambda\right) = \frac{1}{2\lambda} exp\left(-\frac{|x|}{\lambda}\right). \tag{2}$$

We will use $Lap(\lambda)$ to denote a random variable $X \sim Lap(\lambda)$.

Now we can formally define the Laplace mechanism as follows.

Definition 3 (The Laplace-DP mechanism): Given any database x and query function f, the Laplace mechanism outputs sanitized query results by injecting i.i.d noise Y_i drawn from $Lap(\lambda)$:

$$\mathcal{M}_L(x, f(\cdot, \varepsilon)) = f(x) + (Y_1, \ldots, Y_k), \tag{3}$$

where k means k queries against the database.

To be more specific, the parameter λ for a Laplace mechanism is calculated as $\frac{\Delta f}{\varepsilon}$, where ε is a pre-determined privacy budget (see Definition 1) and Δf is the l_1-sensitivity of a query function f:

Definition 4 (l_1-sensitivity): Given a query function f and a pair of neighbor databases x_0 and x_1 ($\|x_0 - x_1\|_1 = 1^1$), the l_1-sensitivity of a function f is:

$$\Delta f = \max \|f(x_0) - f(x_1)\|_1, \tag{4}$$

where Δf can be seen as measuring the magnitude by which a single individual's data can alter the query result ($f(\cdot)$) at most.

Next, we introduce one common property concerning the composition of several differential private mechanisms. The property is further subdivided into *sequential composition* and *parallel composition* depending on the data to which the query functions are applied.

Property 1 (Sequential composition): Suppose $\mathcal{M}_i()$ each guarantees ε_i-differential privacy. Then we say that the sequence of $\mathcal{M}_i(x)$ supports $\sum_i \varepsilon_i$-differential privacy.

Property 2 (Parallel composition): Suppose $\mathcal{M}_i$ each guarantees ε_i-differential privacy. Let D_i be arbitrary disjoint subsets of the input domain D. Then the sequence of $\mathcal{M}_i(x \cap D_i)$ produces ε-differential privacy.

The properties above suggest that if an ε-differential private mechanism is run t times on a database x, the result is $\varepsilon \times t$-differentially private. Meanwhile, if an ε-differential private mechanism is run t times on disjoint subsets of x, the result remains ε-differential private.

IV. Problem Statement and Formulation

ABDP aims to protect the privacy of users' power consumption data while enabling essential operations like aggregation, billing calculation, and dynamic pricing. In this section, we provide an overview of the system architecture, adversary model, and design objectives of ABDP. Table I presents the frequently used notations in our paper.

TABLE I
Key Notations

Notation	Definition
U	Set of users
M	Set of masters
N	Number of users
m	Number of masters
z	Number of appliances
A	Power consumption with noise
X_i	The i-th appliance's power consumption
n	Noise data
C	Aggregated power consumption
q	Index number of the master
Δ	Regular time interval for data reporting
T	Time for data recoding
B	Time for bill calculation
H	Secure hash function
PRF	Pseudo random function
PPT	Probabilistic polynomial-time
$\mathcal{A}$	An adversary or a distinguisher
$\mathcal{C}$	A challenger to executes the mechanism
$F_k(\cdot)$	PRF with key k
NILM	Non-intrusive load monitoring
$\mathcal{N}$	NILM attack algorithm
$\mathcal{F}$	Filtering attack algorithm
DP	Differential privacy
$\mathcal{M}$	DP mechanism
Pdf	Probability density function
Δf	Sensitivity
$Lap(\lambda)$	Pdf of the Laplace distribution with scale λ
$G(\frac{1}{N}, \lambda)$	Gamma distribution with type $\frac{1}{N}$ and scale λ
ε	Privacy budget

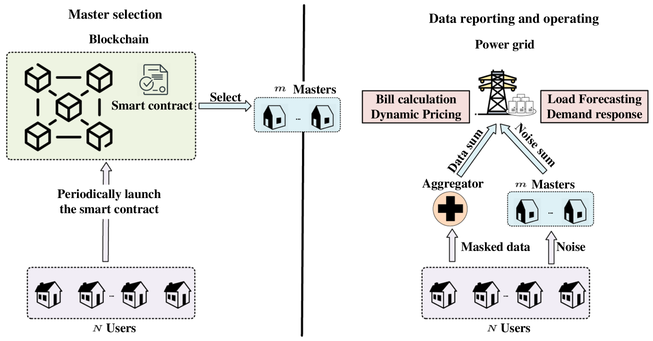


Fig. 1. System architecture.

A. System Architecture

The system model, depicted in Fig. 1, consists of the following entities: user, master, aggregator, power grid, and smart contract. Each user uploads their masked power data to the aggregator, and the corresponding added noise to the master. The aggregator and master then transmit the aggregated noisy data and the noise collected from all users in the region to the power grid. Subsequently, the power grid calculates the accurate aggregated power data by subtracting the sum of the noise from the received noisy aggregated data. Furthermore, the selection of masters is carried out fairly and securely using a Blockchain smart contract. In the following sections, we will provide a formal description of each entity in the system.

User: A user U_i (where $i \in [N]$) represents a residential customer equipped with a smart meter connected to the power grid. To protect the user's privacy, the real-time power consumption data d_i^t (where $t \in [T]$) recorded by the smart meter is masked by adding carefully calibrated random noise n_i^t. This process generates the masked data A_i^t, which is then reported.

Aggregator: The aggregator is responsible for collecting the masked data A_i^t (where $i \in [N]$ and $t \in [T]$) from the users and providing the sum $\sum_{i=1}^{N} A_i^t$ to the grid utility.

Master: A master M_i (where $i \in [m]$) is a user who is randomly selected through a public and fair election process. Their responsibility is to collect the added noise n_i^t from all other users. The sum of the noise $\sum_{i=1}^{N} n_i^t$ is then reported to the grid utility.

Power grid: The power grid is responsible for controlling the supply and distribution of electricity. By analyzing the received real-time power consumption data ($C_t = \sum_{i=1}^{N} A_i^t - \sum_{i=1}^{N} n_i^t$) from users, the grid can implement strategies such as dynamic pricing and load forecasting, which are essential for optimizing electricity usage. Additionally, the grid needs to calculate the individual electricity consumption and corresponding charges based on the dynamic pricing policy for each user.

Smart contract: We utilize an Ethereum smart contract to ensure a fair and secure process for electing masters. The smart contract contains the code or function responsible for randomly selecting m masters from the pool of N users. This election process occurs prior to the upload of power consumption data.

B. Adversary Model

External adversaries: These adversaries may eavesdrop on the system to acquire users' data (either from the user end, during transmission, or from the receiving end) and subsequently infer their actual power consumption information. They achieve this by launching differential attacks or filtering attacks. A filtering attack is a data reconstruction attack that aims to reduce the noise effect in the masked data. Additionally, adversaries may try to identify users' appliance usage patterns through the NILM attack, which involves extracting per-appliance power measurements from the user's aggregated power signal. The formal definitions of filtering attack and NILM attack are provided below.

Definition 5 (Filtering attack): Suppose an adversary has access to a power signal $A_i = A_i^1, A_i^2, \ldots, A_i^T$ from user U_i. The adversary applies the filtering attack algorithm $\mathcal{F}$ to reduce the noise effect in A_i and obtain a filtered power sequence $\hat{A}_i = \hat{A}_i^1, \hat{A}_i^2, \ldots, \hat{A}_i^T$.

$$\hat{A}_i = \mathcal{F}(A_i). \tag{5}$$

A typical filtering attack involves calculating the moving arithmetic mean of the masked data profile A_i[9].

Definition 6 (NILM attack): Suppose an adversary obtains a power signal $A_i = A_i^1, A_i^2, \ldots, A_i^T$ from user U_i. They then apply the NILM attack algorithm $\mathcal{N}$ to learn the power consumption data $X_i = x_i^1, x_i^2, \ldots, x_i^T$ of the appliances (z appliances are included) (where $i \in [z]$):

$$X_i = \mathcal{N}(A_i). \tag{6}$$

Moreover, the on-off state information of the appliances, denoted as $S_i = s_i^1, s_i^2, \ldots, s_i^T$, which indicates whether the appliance is turned on or off, can be deduced by comparing the power signal X_i of the appliance with thresholds.

A NILM attack algorithm can take the form of a statistical model, such as hidden Markov models [39], [40], or conditional random field-based models [41]. Recent advancements in deep learning techniques have opened new avenues for implementing NILM attacks, with deep neural networks being a popular choice [10], [11], [12], [13], [42].

Internal adversaries: An internal adversary refers to an operator within the power grid or the aggregator who has the potential to misuse and leak users' power consumption data. Additionally, they may collude with dishonest masters (users) to obtain system parameters and launch attacks to expose other users' consumption patterns. We assume that all adversaries are dishonest but non-intrusive, meaning they do not have permission to insert, modify, or delete user data.

C. Design Objectives

Our design objectives encompass three aspects: data privacy, operational accuracy, and system security. Regarding privacy and security, we construct cryptographic games where an adversary interacts with the algorithm, and the adversary's advantage in winning the game is formally defined. We consider the algorithm to be privacy-preserving and secure if the adversary's advantage in each game is limited or negligible. In terms of accuracy, our proposed scheme ensures precise aggregation and billing calculation.

1) Data Privacy: Data privacy can be divided into two aspects: 1) Power consumption data: Adversaries are unable to reveal the user's actual power consumption data from the aggregated power signal collected by the aggregator. 2) Power consumption patterns. Users' private information, such as appliance consumption patterns, remains undisclosed when they upload their power consumption measurements.

(1) Power consumption data: We calculate the advantage of a probabilistic adversary $\mathcal{A}$ in observing the execution of the differential privacy mechanism $\mathcal{M}(D, f, \varepsilon)$ and correctly guessing that a specific user's data was included in the dataset D based on the mechanism's result $f(D)$. We refer to this advantage as the *user data hiding* advantage ($Adv_{\mathcal{A}}^{user}(\mathcal{M})$). We formally define the *user data hiding* game $Game_{\mathcal{A},\mathcal{M}}^{user}$ as follows:

1) $\mathcal{A}$ generates two neighboring datasets x_0, x_1 such that $\|x_0 - x_1\|_1 \leq 1$[1], and gives them to $\mathcal{C}$.
2) $\mathcal{C}$ executes the mechanism $\mathcal{M}$ to obtain $y_0 = f(x_0)$ and $y_1 = f(x_1)$ on these two neighboring datasets.
3) $\mathcal{C}$ chooses a uniform bit $b \in \{0, 1\}$ and sends y_b to $\mathcal{A}$.
4) $\mathcal{A}$ outputs a bit b' and sends it to $\mathcal{C}$. We say $\mathcal{A}$ wins the game if $b' = b$.

[1] The l_1 norm of a database x is denoted as $\|x\|_1$ that measures how many records it contains, and $\|x_0 - x_1\|_1$ is a measure of how many records differ between x_0 and x_1.

$\mathcal{A}$ wins the game $Game^{user}_{\mathcal{A},\mathcal{M}}$ with the advantage $Adv^{user}_{\mathcal{A}}(\mathcal{M})$:

$$Adv^{user}_{\mathcal{A}}(\mathcal{M}) = \left|\Pr\left[\mathcal{A}\ wins\right] - \frac{1}{2}\right| = \left|\Pr\left[b' = b\right] - \frac{1}{2}\right|. \tag{7}$$

We consider the mechanism $\mathcal{M}$ to be privacy-preserving if the advantage of the adversary in the game is limited and controllable.

(2) Power consumption patterns: The system effectively safeguards users' private information and effectively resists NILM attacks. In our scenario, we consider an adversary who can access a target user's uploaded power consumption data, denoted as $A_i = A_i^1, A_i^2, \ldots, A_i^T$. By employing the NILM attack $\mathcal{N}(d_i)$, the adversary aims to infer information about the user's household appliances, represented as $\hat{X}_i$ (where $i \in [z]$). We can assert that the NILM attack is effectively resisted if there is a significant disparity between the learned power consumption data of the appliances, $\hat{X}_i = \mathcal{N}(A_i)$, and the actual power consumption data, X_i.

2) Operation Accuracy: Operation accuracy encompasses two aspects: 1) Billing accuracy, which ensures that each customer receives an accurate electricity bill for each billing period, reflecting their actual electricity consumption during that period; and 2) Aggregating accuracy, which enables the power grid to generate reliable load forecasts for future electricity usage in a specific region using historical (real-time) power consumption data. This accuracy is crucial for obtaining precise aggregated power consumption data for a given region.

3) System Security: The masters in the system are chosen through the utilization of a pseudo-random function (PRF) represented as $F_k(\cdot)$. It is of utmost importance for the system to prevent adversaries from accurately deducing which user or users are selected as masters. This ensures that they cannot collude with the aggregator and masters in advance to gain access to the actual consumption data of specific users. We assess the advantage of a distinguisher $\mathcal{A}$ in correctly determining the index number q of a master, whether it is generated by a random function $f(\cdot)$ or the PRF $F_k(\cdot)$. This advantage is referred to as the *master indistinguishable* advantage and denoted as $Adv^{Mas}_{\mathcal{A}}(\Pi)$. We formally define this advantage using the *master indistinguishable* game $Game^{Mas}_{\mathcal{A},\Pi}$ as follows:

1) A master choosing algorithm Π is initialized.
2) $\mathcal{A}$ chooses the current time t and queries it to challenger $\mathcal{C}$.
3) A uniform bit $b \in \{0, 1\}$ is chosen. If $b = 0$, $\mathcal{C}$ respond with q using random function $f(\cdot)$; otherwise, respond with q using PRF $F_k(\cdot)$.
4) $\mathcal{A}$ receives q and outputs a bit b'. $\mathcal{D}$ wins the game if $b' = b$.

$\mathcal{A}$ wins the game $Game^{Mas}_{\mathcal{A},\Pi}$ with the advantage $Adv^{Mas}_{\mathcal{A}}(\Pi)$:

$$Adv^{Mas}_{\mathcal{A}}(\Pi) = \left|\Pr\left[\mathcal{D}\ wins\right] - \frac{1}{2}\right| = \left|\Pr\left[b' = b\right] - \frac{1}{2}\right|. \tag{8}$$

For the master selection algorithm is secure, it must be that the advantage $Adv^{Mas}_{\mathcal{A}}(\Pi)$ is negligible.

V. Our Proposed ABDP Mechanism

The problem statement above has outlined the system architecture, adversary model, and design objectives of our ABDP scheme. In this section, we provide the technical details of ABDP, starting with an overview and followed by an explanation of the mechanisms and algorithms.

A. Overview

As shown in Fig. 1, the system operates in two main phases during each meter data reporting interval (e.g., every 10 minutes): *1) Master selection:* To achieve operational accuracy, the power grid selects certain users as masters to collect the aggregated noise data contributed by all users. Provided that all users' power data can be received, the power grid can obtain accurate aggregated power consumption data by subtracting this aggregated noise data from the data collected at the aggregator. Additionally, we introduce a Blockchain smart contract to ensure a fair, transparent, verifiable, and tamper-proof master selection process. *2) Data reporting and operations:* In this phase, a differential privacy (DP) mechanism is employed to protect the privacy of users' power consumption data. At each time point, users mask their real power consumption data by adding carefully designed noise. The masked data is then sent to the aggregator, while the added noise is sent to the masters. These data support subsequent grid operations such as dynamic pricing, load forecasting, and billing calculation. Further details of these two phases will be presented shortly in this section.

B. Master Selection

To achieve the objective of aggregating accuracy stated in Section IV-C, the system requires entities or nodes capable of collecting real-time noise data in a given area. Instead of introducing third-party entities that may lead to trust issues, we select a master from the system's users. To prevent data leakage from dishonest users selected as masters, we increase the number of masters and distribute the noise data among them. Moreover, to ensure a fair, public, and tamper-resistant master selection process, the Blockchain smart contract emerges as an ideal solution for implementation.

Furthermore, the selection function incorporated in the smart contract should satisfy two key properties: 1) randomness and unpredictability in master selection, and 2) verifiability of the selection result by any user in the system.

To fulfill these requirements and achieve a secure and equitable master selection process, we conduct the selection by periodically executing a smart contract that encompasses a pseudo-random function (PRF). Let $Q = q_1, q_2, \ldots, q_m$ denote the index set of masters $M_i (i \in [m])$, where $q_i \in [N]$. We utilize $F_k(\cdot)$ to represent the PRF, and $H()$ denotes a hash function. The index q_i for the ith master is determined as follows:

$$q_i = F_k\left(H\left(block_t.timestamp || block_t.difficulty || i\right)\right) \bmod N \tag{9}$$

$block_t.timestamp$ and $block_t.difficulty$ represent the timestamp and packing difficulty of the current block, respectively,

Algorithm 1: Master Selection.

```
Input: $block_t.timestamp$, $block_t.difficulty$, $m$, $N$
Output: $q_i$
Function Selct ($q_i$):
    for each $i$ in $m$ do
        set $temp$;
        set $k$;
        // hash function: $H'()$
        $k = H'(block_t.difficulty)$ ;
        // hash function: $H()$
        $temp =$
          $H(block_t.timestamp \parallel block_t.difficulty \parallel i)$ ;
        // PRF: $F_k()$
        $q_i = F_k(temp) modN$;
        for each $j$ in $i$ do
            if $q_i = q_j$ then
                $selct()$;
            end
        end
    end
return $q_i$
```

and $H()$ is a secure hash function. The key k of the PRF is a random number computed by a function in the smart contract at time point t and made public after all masters are selected. Specifically, $k = H'(block_t.difficulty)$, where $H'()$ is a secure hash function. The contract is executed each time power consumption data is reported. The pseudo code of the contract can be found in Algorithm 1. Unlike the traditional practice [35], where each user divides their data into m copies and sends each copy to a different master, in this paper, the user reports their noise data to the nearest master, i.e., the master with the closest serial number. This reduces the communication cost from $O(N \times m)$ to $O(N)$, resulting in significant communication cost savings, especially when m is large.

C. Data Report and Operation

An aggregator is responsible for collecting real-time power consumption data from all users in an area. To protect the privacy of users' power consumption, we employ a Laplace-DP mechanism $\mathcal{M}(D, f(\cdot), \varepsilon)$. Let's begin with the database D to explain this differential privacy mechanism $\mathcal{M}$. The power consumption data for N users ($U = U_1, U_2, \ldots, U_N$) over a time period $\Delta \cdot T$ (where Δ represents a regular time interval, e.g., 10 minutes, and $T \in \mathbb{N}$) is recorded as $d_i^1, d_i^2, \ldots, d_i^T$ for user U_i. The entire database of power data for all users is denoted as $D = (D^t)t \in [T]$, where $D^t = (d_i^t)i \in [N]$. The aggregator aims to obtain the aggregated time profile $f(D) = (f(D^1), f(D^2), \ldots, f(D^T)) \in \mathbb{R}^T$. At each time point, the aggregated data is computed as $f(D^t) = \sum_{i=1}^N d_i^t$. By applying a differential privacy mechanism $\mathcal{M}^t(D^t, f(\cdot), \varepsilon)$ at each time point t, we can achieve a mechanism $\mathcal{M}(D, f(\cdot), \varepsilon)$ for the entire time period T through the parallel composition property (see Property 2). We now formally define the mechanism $\mathcal{M}^t(D^t, f(\cdot), \varepsilon)$ as follows.

Definition 7 (Power data reporting mechanism): Given a database D^t and a query function (aggregating function) f, the power data reporting mechanism outputs a sanitized aggregated power data by injecting noise Y^t drawn from $Lap(\frac{\Delta f}{\varepsilon})$:

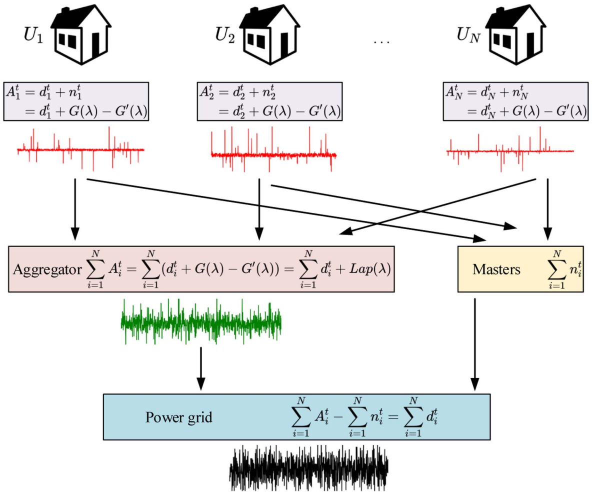

U_1
U_2
$\ldots$
U_N
$A_1^t = d_1^t + n_1^t = d_1^t + G(\lambda) - G'(\lambda)$
$A_2^t = d_2^t + n_2^t = d_2^t + G(\lambda) - G'(\lambda)$
$A_N^t = d_N^t + n_N^t = d_N^t + G(\lambda) - G'(\lambda)$
Aggregator $\sum_{i=1}^N A_i^t = \sum_{i=1}^N (d_i^t + G(\lambda) - G'(\lambda)) = \sum_{i=1}^N d_i^t + Lap(\lambda)$
Masters $\sum_{i=1}^N n_i^t$
Power grid $\sum_{i=1}^N A_i^t - \sum_{i=1}^N n_i^t = \sum_{i=1}^N d_i^t$

Fig. 2. Algorithmic framework of the data report and operation phase.

$$\mathcal{M}^t\left(D^t, f(\cdot), \varepsilon\right) = f\left(D^t\right) + Y^t. \tag{10}$$

We follow the previous studies [30], [32], [34] and use *point-wise sensitivity* to compute Δf as:

$$\Delta f = \max\left|f\left(D^t\right) - f\left(D^{t'}\right)\right| = \max_i \left|d_i^t\right|, \tag{11}$$

where D^t and $D^{t'}$ are a pair of neighboring databases that differ in one user's power data, Δf represents the maximum power consumption among all users at that specific time point.

To avoid introducing an additional trusted entity for adding noise drawn from $Lap(\frac{\Delta f}{\varepsilon})$, which could potentially lead to privacy and security concerns, the system employs a distributed approach. Specifically, each user U_i independently adds noise drawn from a Gamma distribution. The mathematical justification for this distributed approach is provided by the following theorem on the infinite divisibility of the Laplace distribution:

Theorem 1 (Infinite divisibility of the Laplace distribution): Suppose $Lap(\lambda)$ represents a random variable drawn from a Laplace distribution with probability density function $f(x, \lambda) = \frac{1}{2\lambda}\exp(-\frac{|x|}{\lambda})$. Then, for any integer $N \geq 1$, the distribution $Lap(\lambda)$ can be expressed as the sum of N Gamma distributions, $Lap(\lambda) = \sum_{i=1}^N (G(\frac{1}{N}, \lambda) - G'(\frac{1}{N}, \lambda))$, where $G(\frac{1}{N}, \lambda)$ and $G'(\frac{1}{N}, \lambda)$ are independent and identically distributed with probability density function $g(x, \frac{1}{N}, \lambda)$:

$$g\left(x, \frac{1}{N}, \lambda\right) = \frac{(1/\lambda)^{\frac{1}{N}}}{\Gamma(\frac{1}{N})} x^{\frac{1}{N}-1} e^{-x/\lambda}, \tag{12}$$

where $\Gamma(\frac{1}{N})$ is the Gamma function.

We can now formally describe the three steps (setup, distributed data generation, report and aggregation) of the data reporting and operation phase. The algorithmic framework for this phase is illustrated in Fig. 2.

1) Setup: In this step, the system initializes the necessary parameters. The privacy budget ε is set to 0.01, the number of

Algorithm 2: Distributed Data Generation in Each Period $\Delta \cdot B$.

```
Input: $d_i^t$, $\varepsilon$, $\Delta f$ and $B$ .
Output: $n_i^t$ and $A_i^t$
for each $i$ in $N$ do
    set $temp = 0$;
    while $t \leq B - 1$ do
        $n_i^t = G(\frac{1}{N}, \frac{\Delta f}{\varepsilon}) - G'(\frac{1}{N}, \frac{\Delta f}{\varepsilon})$;
        $A_i^t = d_i^t + n_i^t$;
        $temp = temp + n_i^t$;
    end
    $n_i^B = -temp$;
    $A_i^B = d_i^B + n_i^B$;
end
return $n_i^t$ and $A_i^t$
```

Algorithm 3: Dynamic Pricing-Supported Bill Calculation.

```
Input: $maxUnits$, $P_h$, $P_l$
Output: $Bill_i$
for each $i$ in $N$ do
    set $temp = 0$;
    while $t \leq B$ do
        $temp = temp + A_i^t$ ;
    end
    if $temp > maxUnits$ then
        Notice user $U_i$ that she/he is a high power
          consumption state. ;
        $Bill_i = maxUnits \times P_l + (temp - maxUnits) \times p_h$;
    end
    else
        $Bill_i = temp \times p_l$
    end
    return $Bill_i$
end
```

connected users to the aggregator is set to 200, and the regular time interval Δ for data reporting is set to 10 minutes.

2) Distributed data generation: For each time point t ($t \in [T]$), every user U_i generates two independent and identically distributed (i.i.d.) Gamma noises, denoted as $G(\frac{1}{N}, \lambda)$ and $G'(\frac{1}{N}, \lambda)$, with a probability density function (pdf) of $g(x, \frac{1}{N}, \lambda)$ (see (12)), where $\lambda = \frac{\Delta f}{\varepsilon}$. Each user U_i then computes their noise as $n_i^t = G(\frac{1}{N}, \lambda) - G'(\frac{1}{N}, \lambda)$. In this system, the aggregated power consumption from all users is denoted as f. Therefore, Δf represents the maximum power consumption of any user at this time point (see (11)). Consequently, user U_i obtains a noisy (masked) version of their power measurement as $A_i^t = d_i^t + n_i^t$, where d_i^t is the user's actual power consumption. However, in order to fulfill our objective of ensuring accurate billing (as stated in Section IV-C), further modifications are needed in the data generation approach. For each user U_i, achieving an accurate bill entails producing an accurate aggregated power consumption over each bill-calculation time period of $\Delta \cdot B$ (e.g., one hour), where $B \in \mathbb{N}$. To accomplish this goal, we introduce additional changes to the data generation process for user U_i as follows.

For each bill-calculation period of $\Delta \cdot B$, user U_i generates noise data n_i^t at each time point, as described in the previous statement. However, at the last time point of this period, the user changes the noise data to $-\sum_{t=1}^{t=B-1} n_i^t$. This adjustment ensures that the aggregated noise contributed by user U_i over each bill calculation period is $\sum_{t=1}^{t=B-1} n_i^t + (-\sum_{t=1}^{t=B-1} n_i^t) = 0$. As a result, an accurate aggregated power consumption over the bill-calculation period is achieved. Furthermore, the noise added in the last time point still follows a gamma distribution $(G(\frac{B-1}{N}, \frac{\Delta f}{\varepsilon}) - G'(\frac{B-1}{N}, \frac{\Delta f}{\varepsilon}))$ due to the additivity property of the gamma distribution. This ensures that the privacy guarantee of the scheme is not violated. The data generation process is presented in Algorithm 2.

3) Report and aggregation: After the data is generated in a distributed manner, each user reports their noisy (masked) data A_i^t to the aggregator and the corresponding added noise n_i^t to the master. Upon receiving the data, the aggregator and masters aggregate all the collected data, obtaining $\sum_{i=1}^N A_i^t$ and $\sum_{i=1}^N n_i^t$ respectively. Specifically, $\sum_{i=1}^N A_i^t = \sum_{i=1}^N (d_i^t + G(\lambda) - G'(\lambda)) = \sum_{i=1}^N d_i^t + Lap(\lambda)$, where the added noise follows a Laplace distribution $Lap(\lambda)$. The obtained data $\sum_{i=1}^N A_i^t$ and $\sum_{i=1}^N n_i^t$ are then reported to the power grid. As a result, the power grid can acquire accurate power consumption data $C^t = \sum_{i=1}^N A_i^t - \sum_{i=1}^N n_i^t$ for this area without revealing the real power consumption measurements of any individuals. With this real-time power consumption data C^t ($t \in [T]$), the power grid can perform various operations such as load forecasting, dynamic pricing, and bill calculation. However, approaches for load forecasting are beyond the scope of this paper. To demonstrate the dynamic-pricing supported bill calculation method, we provide Algorithm 3.

Here, $maxUnits$ represents the maximum power consumption threshold for each billing period $\Delta \cdot B$. Users whose power consumption is below $maxUnits$ are charged at the low tariff rate p_l, while users whose power consumption exceeds $maxUnits$ are charged at the high tariff rate p_h.

VI. Theoretical Analysis

In this section, we provide a formal proof of the privacy and security guarantees offered by our system, considering the adversary model and design objectives.

A. Security

Theorem 2: If $F_k : \{0,1\}^n \rightarrow \{0,1\}^n$ is a secure PRF and $H : \{0,1\}^* \rightarrow \{0,1\}^n$ is a secure hash function, then the master selection process Π of our ABDP scheme is $Adv_{\mathcal{A}}^{Mas}(\Pi)$-master indistinguishable against the probabilistic polynomial-time (PPT) adversary $\mathcal{A}$, where $Adv_{\mathcal{A}}^{Mas}(\Pi)$ is negligible, i.e., $Adv_{\mathcal{A}}^{Mas}(\Pi) \leq negl(n)$.

Proof: For simplicity, we denote the index number of the ith master as $q_i = \Pi(t) = F_k(H(t|i))$. Here, we replace the expression $block_t \cdot timestamp|block_t \cdot difficulty$ with t to represent the timestamp and packing difficulty of the current block. We omit the modulo operation as it does not affect the proof. Similarly, let $q_i' = \Pi'(t) = f(t|i)$ denote the index number chosen by a truly random function f instead of the pseudorandom function (PRF) F_k. To prove that $Adv_{\mathcal{A}}^{Mas}(\Pi) \leq negl(n)$, we aim to demonstrate the distinguishability between $F_k(H(t|i))$ and a random function $f(t|i)$. We accomplish this by showing that $F_k(H(t|i))$ is also a PRF when its input is $t|i$. Since i is a constant that has no impact on the proof, we omit it below for simplicity. We formally prove this proposition using the following lemma.

Lemma 1: If $F_k : \{0,1\}^n \rightarrow \{0,1\}^n$ is a secure PRF and $H : \{0,1\}^* \rightarrow \{0,1\}^n$ is a hash function family with negligible collision probability ϵ, then we say that $F'_k(t) := F_k(H(t))$ is also a PRF.

Proof of Lemma 1: Consider a distinguisher D' that has access to an oracle O', which could be either the PRF F'_k or a random function f'. The goal of D' is to determine which function the oracle represents. Now, let's introduce another distinguisher D, who is given an oracle O that is either F_k or f. D will call D' to attempt to break the PRF property of F_k, and it outputs the same bit as D'. Next, let's discuss their queries in detail. For D', if it is facing a random function f', it receives the following responses for q different queries $t_1, t_2, \ldots, t_q$:

$$\{f'(t_1), f'(t_2), \ldots, f'(t_q)\},$$

which is indistinguishable from

$$\{f\left(H(t_1)\right), f(H(t_2)), \ldots, f\left(H(t_q)\right)\}.$$

The reason for this is as follows: 1) If f' is a random function, then the values $f'(t_i)$ for $i \in 1, 2, \ldots, q$ are all independent and uniformly distributed n-bit strings. 2) If f is a random function and $H(t_i)$ values are distinct, then $f(H(t_i))$ are also independent and uniformly distributed n-bit strings.

We assume that H is a hash function with a negligible collision probability ϵ. Therefore, the values $H(t_i)$ for $i \in 1, 2, \ldots, q$ are indistinct with a probability of $\binom{q}{2}\epsilon$, which is negligible. Additionally, we assume that t_i values are distinct since they are time-related. Hence,

$$\begin{aligned}
&\left|\Pr\left[D'^{f'(\cdot)}(1^n) = 1\right] - \Pr\left[D'^{f'(H(\cdot))}(1^n) = 1\right]\right| \\
&= \left|\Pr\left[\exists i, j\ s.t.\ H(t_i) = H(t_j)\right]\right| \\
&\leq \tbinom{q}{2}\epsilon.
\end{aligned}$$

Since D calls D' to break the PRF property of F_k and outputs the same bit as D', the view of D' when run as a subroutine by D is distributed identically to the view of D. Therefore, the probability that D' successfully distinguishes between F_k and f is the same as the probability that D successfully distinguishes between F_k and f. Hence,

$$\begin{aligned}
&\left|\Pr\left[D'^{f'(\cdot)}(1^n) = 1\right] - \Pr\left[D'^{F'_k(\cdot)}(1^n) = 1\right]\right| \\
&= \left|\Pr\left[D'^{f'(\cdot)}(1^n) = 1\right] - \Pr\left[D'^{F_k(H(\cdot))}(1^n) = 1\right]\right| \\
&= |\Pr\left[D'^{f'(\cdot)}(1^n) = 1\right] - \Pr\left[D'^{f(H(\cdot))}(1^n) = 1\right] \\
&\quad + \Pr\left[D'^{f(H(\cdot))}(1^n) = 1\right] - \Pr\left[D'^{F_k(H(\cdot))}(1^n) = 1\right]| \\
&\leq \tbinom{q}{2}\epsilon + \left|\Pr[D'^{f(H(\cdot))}(1^n) = 1] - \Pr\left[D'^{F_k(H(\cdot))}\,(1^n) = 1\right]\right| \\
&= \tbinom{q}{2}\epsilon + \left|\Pr\left[D^{f(H(\cdot))}(1^n) = 1\right] - \Pr\left[D^{F_k(H(\cdot))}(1^n) = 1\right]\right| \\
&\leq \tbinom{q}{2}\epsilon + negl'(n) \\
&= negl(n),
\end{aligned}$$

where q is within PPT operations and $\binom{q}{2}\epsilon + negl'(n)$ is also negligible.

We have completed the proof of Lemma 1. Now we can proceed with the proof of Theorem 2, which shows that the advantage of adversary $\mathcal{A}$ is negligible. Let us assume that there is a distinguisher D in the *master indistinguishable* game $Game^{mas}_{D,\prod}$ who outputs $b_D = 1$ when they believe they are facing $\Pi(t) = F_k(H(t|i)) = F'k(t|i)$. Now, we will analyze the advantage of adversary $\mathcal{A}$ in breaking the $Game\mathcal{A}, \prod^{mas}$.

$$\begin{aligned}
Adv^{mas}_{\mathcal{A},\Pi} &= \left|\Pr\left[b' = b\right] - \frac{1}{2}\right| \\
&= |\Pr\left[b' = 1|b = 1\right] \cdot \Pr[b = 1] \\
&\quad + \Pr\left[b' = 0|b = 0\right] \cdot \Pr[b = 0] - \frac{1}{2}| \\
&= \frac{1}{2}\left|\Pr\left[b' = 1|b = 1\right] + \Pr\left[b' = 0|b = 0\right] - 1\right| \\
&= \frac{1}{2}\left|\Pr\left[b' = 1|b = 1\right] - (1 - \Pr\left[b' = 0|b = 0\right])\right| \\
&= \frac{1}{2}\left|\Pr\left[b' = 1|b = 1\right] - \Pr\left[b' = 1|b = 0\right]\right| \\
&= \frac{1}{2}\left|\Pr\left[D^{F'_k(\cdot)}(1^n) = 1\right] - \Pr\left[D^{f'(\cdot)}(1^n) = 1\right]\right| \\
&\leq \frac{1}{2}negl(n)
\end{aligned}$$

The key points to obtain the above equations are that:

1) If $b = 1$, then the view of $\mathcal{A}$ is distributed identically to the view of D in given F'_k. Thus $\Pr[b' = 1|b = 1] = \Pr[D^{F'_k(\cdot)}(1^n) = 1]$ holds.
2) If $b = 0$, then the view of $\mathcal{A}$ is distributed identically to the view of D in given f'. Thus $\Pr[b' = 1|b = 0] = \Pr[D^{f'(\cdot)}(1^n) = 1]$ holds.

Therefore the advantage for $\mathcal{A}$ for breaking $Game^{mas}_{\mathcal{A},\prod}$ is $\frac{1}{2}negl(n)$, i.e., negligible. We thus complete the proof of Theorem 2. □

B. Privacy

Theorem 3: The power data reporting mechanism (Definition 7) of our ABDP scheme can ensure ε-differential privacy. This means that the mechanism provides $Adv^{user}_{\mathcal{A}}(\mathcal{M})$-user data hiding against probabilistic adversaries, where $Adv^{user}_{\mathcal{A}}(\mathcal{M})$ is limited.

Proof: Let's consider a pair of neighboring databases D^t and $D^{t'}$ that differ in one user's power data, i.e., $\|D^t - D^{t'}\|_1 = 1$, $f(\cdot)$ denotes the query function. Let p_{D^t} denote the pdf of $\mathcal{M}^t(D^t, f(\cdot), \varepsilon)$ and $p_{D^{t'}}$ denote the pdf of $\mathcal{M}^t(D^{t'}, f(\cdot), \varepsilon)$. We compute the two at certain arbitrary string $R = \{R_1, R_2, \ldots R_l\}$ (length is l):

$$\frac{\Pr_{D^t}(R)}{\Pr_{D^{t'}}(R)} = \frac{\Pr[f(D^t) + < Y_1, Y_2, \ldots, Y_l >] = R}{\Pr[f(D^{t'}) + < Y'_1, Y'_2, \ldots, Y'_l >] = R}$$

$$
\begin{aligned}
&= \frac{\Pr[(Y_1 = R_1 - f(D^t)_1) \wedge \ldots (Y_l = R_l - f(D^t)_l)]}{\Pr[(Y'_1 = R_1 - f(D^{t'})_1) \wedge \ldots (Y'_l = R_l - f(D^{t'})_l)} \\
&= \frac{\prod_{i=1}^{l} \Pr[Y_i = R_i - f(D^t)_i]}{\prod_{i=1}^{l} \Pr[Y'_i = R_i - f(D^{t'})_i]} \\
&= \prod_{i=1}^{l} \left(\frac{exp(-\frac{\varepsilon |f(D^t)_i - R_i|}{\Delta f})}{exp\left(-\frac{\varepsilon |f(D^{t'})_i - R_i|}{\Delta f}\right)} \right) \\
&= \prod_{i=1}^{l} exp\left(\frac{\varepsilon(|f(D^{t'})_i - R_i| - |f(D^t)_i - R_i|)}{\Delta f} \right) \\
&\leq \prod_{i=1}^{l} exp\left(\frac{\varepsilon |f(D^{t'})_i - f(D^t)_i|}{\Delta f} \right) \\
&= exp\left(\frac{\varepsilon \cdot \|f(D^{t'}) - f(D^t)\|_1}{\Delta f} \right) \\
&\leq exp(\varepsilon),
\end{aligned}
$$

where the first inequality deduced from the triangle inequality, and the second deduced from the sensitivity definition(11). We also have $\frac{\Pr_{D^t}(R)}{\Pr_{D^{t'}}(R)} \geq exp(-\varepsilon)$ by symmetry. The advantage $Adv_{\mathcal{A}}^{user}(\mathcal{M})$ is computed as:

$$
\begin{aligned}
Adv_{\mathcal{A}}^{user}(\mathcal{M}) &= \frac{1}{exp(\varepsilon) + 1} - \frac{1}{2} \\
&= \frac{1 - exp(\varepsilon)}{2exp(\varepsilon) + 2},
\end{aligned}
$$

which is restricted and controllable. □

VII. Performance Evaluation

In this section, we develop a prototype of ABDP using a Laplace-based differential privacy mechanism and an Ethereum testnet. We evaluate the effectiveness of our ABDP using two commonly used residential power recording datasets. Our evaluation focuses on two main aspects: 1) Assessing the granularity of privacy protection provided by our ABDP model against filtering attacks and NILM attacks for varying privacy budgets ε. 2) Evaluating the accuracy of real-time aggregated power consumption calculation and individual billing calculation for our ABDP compared to five other DP-based baselines.

A. Experimental Settings

The data reporting and operation processes were implemented using Python and executed on a desktop PC with Intel(R) Core(TM) i9-12900 @2.4 GHz CPU and 21 GB RAM. Each experiment was conducted 30 times, and the average results were recorded. For the master selection process, we utilized the Solidity language to write our smart contract. The SHA256 hash function and HMAC-SHA256 were used as the hash and PRF, respectively. The smart contract code was developed using the browser-based tool Remix-Ethereum, compiled using the Solidity Compiler (Solc), and deployed on the Ethereum testnet Goerli.

Baselines: We compare our ABDP scheme against five DP-based baselines: 1) RSMD [30]: The first scheme that utilizes DP for real smart metering consumption data. 2) DPDR [27]: A modified usage-based dynamic pricing method that integrates DP to protect smart metering data. 3) DDP [32]: A decentralized privacy-preserving smart metering mechanism that employs DP and random permutation techniques. 4) DPNCT [34]: A DP-based smart metering approach with noise cancellation for load monitoring. 5) E-DPNCT [35]: An enhanced attack-resilient DP scheme for smart metering that utilizes split noise cancellation.

Datasets: We evaluate our ABDP scheme and the state-of-the-art by using two commonly used datasets: NREL-DATA [37] and REDD [38]. NREL-DATA consists of one-year power measurements from 200 randomly selected households in the 2009 RECS dataset for the midwest region of the United States. The measurements are recorded every 10 minutes, providing a versatile dataset to evaluate the calculation accuracy and resistance to filtering attacks of our ABDP and the baselines. However, the resistance against the NILM attack cannot be assessed using the NREL-DATA dataset, as it requires individual appliance power recordings. To evaluate our ABDP and the baselines in terms of the NILM attack, we introduce the REDD dataset, which includes power measurements from 6 households over a period of approximately four months. The dataset provides aggregated power signals for the households and individual appliance power measurements recorded every 1 and 3 seconds, respectively.

Performance metrics: We adopt four metrics in this paper to evaluate the experimental results.

1) Pearson's correlation coefficient ρ. ρ is computed to measure the correlation between the raw data sequence and masked data sequence:

$$
\rho\left(C, \hat{C}\right) = \frac{Cov(C, \hat{C})}{Var(C)Var(\hat{C})}, \tag{13}
$$

where, Cov represents the covariance, $Var(C)$ is the standard deviation of C, and $Var(\hat{C})$ is the standard deviation of $\hat{C}$. Generally, a smaller value of ρ indicates a greater dissimilarity and lower correlation between the sequences C and $\hat{C}$.

2) Mean absolute error (MAE). MAE is a general metric used for NILM attack to measure the power estimation error by the NILM attacker at each time point:

$$
MAE_i = \frac{1}{T} \sum_{t=1}^{T} |\hat{x}_i^t - x_i^t|, \tag{14}
$$

where $\hat{x}_i^t$ is the estimated power signal of the ith appliance at t time point and x_i^t corresponds to the real power signal.

3) Normalized signal aggregate error (SAE). SAE is another common used metric for NILM attack to compute the total estimation error of NILM attackers:

$$
SAE_i = \frac{|\hat{r}_i - r_i|}{r_i}, \tag{15}
$$

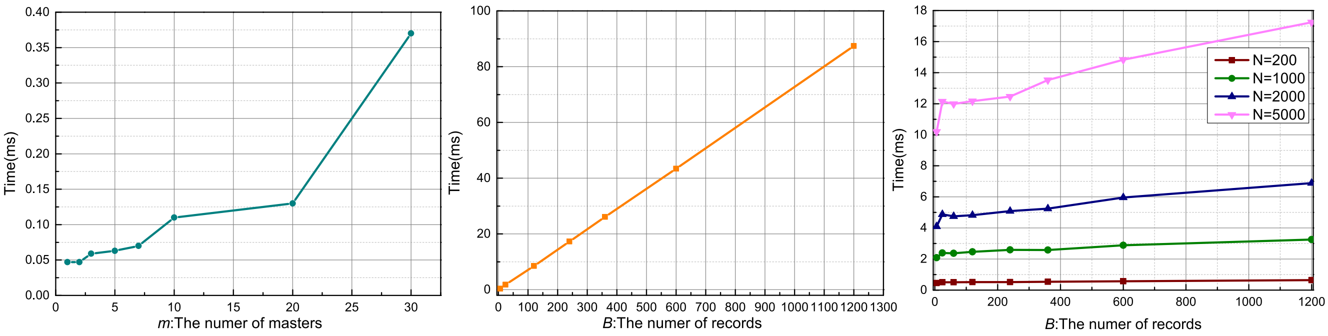


Fig. 3. Computation time (ms) for Algorithms 1, 2, and 3.

where $r_i = \sum_{t=1}^{T} x_i^t$ and $\hat{r}_i = \sum_{t=1}^{T} \hat{x}_i^t$ denote the real and estimated total power consumption of the ith appliance over T time points.

4) F1-score. F1-score is used to compute the accuracy of NILM attacks for the appliance's on-off state information:

$$F1 = \frac{2 \times Precision \times Recall}{Precison + Recall}, \tag{16}$$

where $Precison = \frac{TP}{TP+FP}$ and $Recall = \frac{TP}{TP+FN}$. TP represents the number of positive samples that are correctly predicted as positive. In this context, "positive" refers to the appliance being in the "on" state, indicated by the power signal x_i^t exceeding a specified threshold. FP corresponds to the number of negative samples that are incorrectly predicted as positive. In this case, "negative" denotes the appliance being in the "off" state, with the power signal x_i^t not exceeding the specified threshold. Lastly, FN signifies the number of positive samples that are incorrectly predicted as negative.

B. Experimental Results

We begin our discussion with an analysis of the time complexities of the three proposed algorithms. For Algorithm 1, namely the Master Selection, the time complexity is $O(m^2)$, where m denotes the number of masters in each region, set to 5 in this paper. Fig. 3(a) illustrates the variation in time with different m settings. The results show that the time for master selection is less than 1 ms, a negligible amount. In terms of Algorithm 2, the Distributed Data Generation, the time complexity is $O(NB)$, where N represents the number of users in each region, set to 200 in this paper, and B signifies the number of data records within each billing period, designated as 6 and 600 for the NERL-DATA and REDD datasets, respectively. Given that data generation is distributed and processed at the end of each user, the complexity for each user is $O(NB/N) = O(B)$. Fig. 3(b) provides a depiction of the variation in time for each user under different B settings. The results indicate that the data generation time for each user is on a millisecond scale. Similarly, for Algorithm 3, the Dynamic Pricing-Support Bill Calculation, the time complexity is also $O(NB)$. Fig. 3(c) is used to illustrate the specific computation time under various N and B settings. It is evident that even with the number of users N set to 5000, the computation time remains on the millisecond scale.

Next we discuss the implementation cost of our smart contract for master selection. Experimental results from the testnet reveal that uploading the smart contract takes approximately 15 seconds, and the contract execution consumes around 2.5 Gwei gas. This indicates that the execution time is negligible. Considering that meter data is typically reported every 10 minutes, it is feasible to employ the smart contract before each data reporting process.

Last, we present detailed experiments on two real-world datasets, focusing on privacy and accuracy. Regarding privacy, we provide visual representations of the protected data obtained through our ABDP under various privacy budget settings. Subsequently, we employ the aforementioned performance metrics to evaluate the effectiveness of our scheme in preserving privacy against filtering and NILM attacks. As for accuracy, we analyze the real-time aggregating error and the billing error under different billing periods for both our ABDP and the other baselines.

1) The Granularity of Privacy Protection: Although we have theoretically proven that the advantage for the attacker to win the *user data hiding game* $Game_{\mathcal{A},\mathcal{M}}^{user}$ is limited, the correlation between the privacy budget ε and the privacy-preserving effect is not yet intuitively understood. Therefore, in this section, we provide a specific and intuitive demonstration to illustrate the relationship between the privacy budget ε and the privacy-preserving effect. For this experiment, we utilize the data of all 200 users in the NREL-DATA dataset, and in Fig. 4, we compare the aggregated masked data with the aggregated raw (real) data across different ε settings.

Fig. 4 demonstrates that the amount of added Laplace noise in the aggregated data increases as the privacy budget ε decreases. With larger amounts of noise added, it becomes more challenging for an attacker to successfully launch filtering attacks and NILM attacks. However, existing baselines are unable to continuously adjust the privacy budget to a very small value as this would decrease the utility of power data and result in increased errors in operations such as user billing. Consequently, these schemes typically set ε to 1, offering some level of data privacy while minimizing errors in data operations. In contrast, our ABDP, through the introduction of masters and a noise adjustment strategy, ensures the accurate calculation of aggregated power consumption and accumulated power consumption for

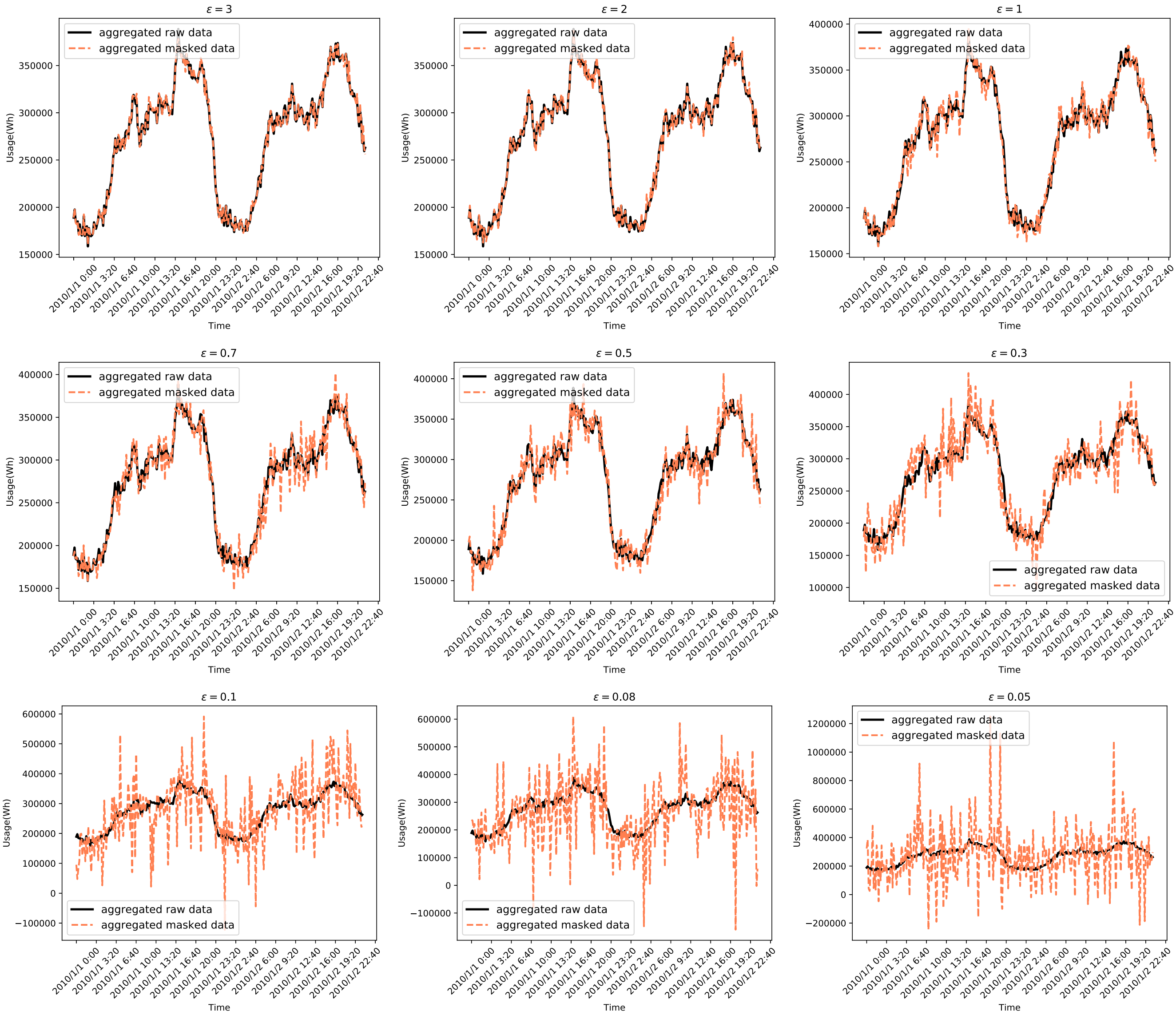


Fig. 4. Two days of signal for aggregated raw data against aggregated masked data under different ε settings.

each individual user. This enables us to enhance the granularity of privacy preservation without compromising data utility concerns.

It is worth mentioning that, to conduct a fair comparison of the privacy-preserving effectiveness, we implemented our scheme without incorporating the billing-accuracy requirement in this section.

Filtering attack: We then evaluate the privacy-preserving effectiveness of each solution through filtering attacks. Following previous approaches [9], [34], we calculate the arithmetic mean of the masked data to launch the filtering attack. Assuming an attacker has access to the masked data $A_i = A_i^1, A_i^2, \ldots, A_i^T$, they execute the filtering attack algorithm $\mathcal{F}(A_i)$ to obtain a filtered data sequence $\hat{A}_i = \hat{A}_i^1, \hat{A}_i^2, \ldots, \hat{A}_i^T$ as follows:

1) Select a positive integer w as the window size.
2) Copy the first and last window data, i.e., the first w and last w data in A_i to $\hat{A}_i$.
3) Calculate the rest of the data in $\hat{A}_i$ as follows:

$$\hat{A}_i^{w+j} = \frac{\sum_j^{2w+j} A_i^j}{2w+1} \tag{17}$$

We begin by using Fig. 5 to compare the results of the baselines and our ABDP against the filtering attack algorithm $\mathcal{F}$ under the same window size w setting. Specifically, Fig. 5 presents a comparison between the daily raw (real) aggregated profile and the filtered data. The window size w for the filtering algorithms in each scheme is set to 35. It is evident that our ABDP exhibits greater resistance to filtering attacks compared to the baselines, as the filtered power curve obtained by an adversary implementing a filtering attack is more distinguishable from the real (raw) power curve. It should be noted that we set the privacy budget ε of the power curve of our ABDP in Fig. 5 to 0.1 for better comparison with the curves of the baselines.

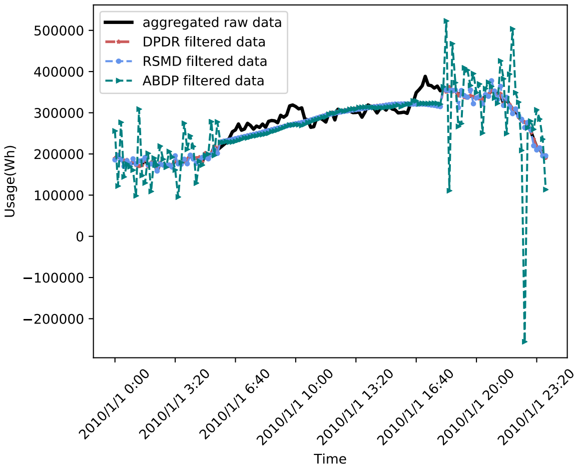


Fig. 5. A daily aggregated profile compared with our ABDP and baselines' filtered profiles with $w = 35$.

TABLE II
THE PEARSON'S CORRELATION COEFFICIENT BETWEEN THE REAL DATA AND FILTERED DATA GAINED BY THE FILTERING ATTACKER UNDER DIFFERENT w SETTINGS

	house 1	house 50	house 99	house 148	house 197
$w = 0$	-0.01	0	0.01	0.05	-0.12
$w = 5$	0.31	0.32	-0.06	-0.21	0.43
$w = 10$	0.34	-0.05	0.28	0.04	0.07
$w = 17$	-0.42	0.13	-0.13	0.36	-0.26
$w = 20$	0.08	0.06	-0.05	0.06	-0.36
$w = 25$	0.23	-0.02	-0.06	-0.23	-0.005
$w = 30$	0.07	-0.07	0.03	-0.24	0.15
$w = 40$	0.28	0.03	0.16	-0.04	0.02
$w = 60$	-0.07	-0.06	-0.07	-0.19	0.05
$w = 80$	0.14	-0.01	-0.06	-0.01	-0.1
$w = 100$	0.04	0.08	0.014	-0.015	0.025
$w = 120$	0.01	0.03	0.01	-0.06	-0.08
$w = 140$	0.06	-0.02	0.09	-0.07	-0.004

However, in reality, our ABDP can support a smaller privacy budget and provide stronger privacy protection.

In addition to this visual demonstration, we also compute the Pearson's correlation coefficient ρ (See (13)) between the filtered data $\hat{A}_i$ and the real data A_i to evaluate the effectiveness of our ABDP against the filtering attack under a smaller privacy budget of 0.01. We selected 5 houses (house 1, house 50, house 99, house 148, and house 197) with one-day power profiles (a total of 144 records) to assess the impact for different window size w settings. From the results listed in Table II, We can get following conclusions:

- The impact of filtering attacks with the same window size setting on different houses varies, as indicated by the different values in each row of Table II;
- The optimal window size settings for different houses vary. For example, the best window size (w) for house 1 is 5, while it is 10 for house 99;
- It's interesting to note that filtering attacks do not always succeed. In certain situations, as the filtered power data becomes more similar to the raw power signal, indicated by a smaller value of ρ, the effectiveness of the attack decreases. For example, in the first column, when the window size (w) is set to 17, the filtered data shows a smaller correlation with the raw data compared to the masked data without filtering (i.e., $w = 0$);
- Our ABDP effectively resists filtering attacks by ensuring a significant difference between the filtered power data and the real power data, even when the filtering attack algorithm is using the optimal window size (w) setting. This is evident from the fact that the maximum Pearson's correlation coefficients for each house are much smaller than the maximum correlation coefficient of 1.

NILM attack: We will now discuss the granularity of privacy preservation provided by our ABDP against NILM attacks. The objective of a NILM attack is to extract information about the power consumption and on-off state of individual appliances from an aggregated power signal recorded by a household smart meter. Deep learning algorithms have shown significant performance in NILM attacks on residential power datasets. For instance, the CNN-based model S2P [10], which employs a sequence-to-point output strategy, achieves an average MAE of 24.10 Watts on the REDD dataset. This represents a notable advancement in deep learning-based NILM attack algorithms. To evaluate the privacy protection of our scheme, we use the S2P model to launch NILM attacks on the privacy-protected power data and present the experimental results in Table III.

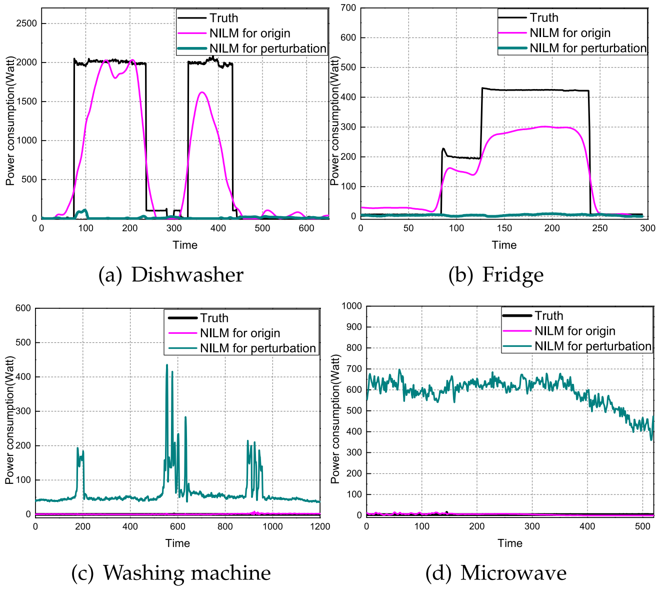
We replicate the study that introduced the S2P algorithm and use 5 common appliances from the REDD dataset to present the results of the NILM attack.

The MAE in Watts, as shown in (14), and the SAE (%), as shown in (15), are used to measure the accuracy of the NILM attack algorithm in predicting the power consumption of individual appliances compared to the actual power signal. Therefore, a smaller MAE and SAE indicate better performance of the NILM attack. Table III demonstrates that our ABDP effectively resists NILM attacks on power disaggregation. When applying DP protection to the user's power consumption data with a privacy budget ε set to 2, our scheme increases the average MAE and SAE of NILM attacks by 13.9% and 56.28%, respectively. The average MAE and SAE continue to increase as the strength of privacy protection increases, reaching an increase of 203.81% and 1081.18% when ε is set to 0.3. The third metric, F1-score (see (16)), in the table indicates the accuracy of the NILM attack algorithm in successfully inferring the on-off state information of appliances. A higher F1-score signifies better performance of the NILM attack. The F1-score reported in Table III demonstrates that our ABDP effectively reduces the capability of the NILM attack algorithm to infer the on-off state information of appliances, with an 80.09% decrease in the F1-score due to the use of the DP strategy.

Moreover, to provide an intuitive evaluation of power consumption protection, we introduce Fig. 6 to visually illustrate the differences between the original appliance power consumption data and the data after protection by our ABDP scheme. It explicitly shows a drastic reduction in the accuracy of NILM attacks in deciphering individual appliance power consumption data from the aggregated household power consumption, making it exceedingly challenging for potential adversaries to accurately ascertain the user's appliance usage and thereby effectively maintaining user privacy.

TABLE III
THE NILM ATTACK RESULTS OF MAE(WATT)/SAE(%)/F1-SCORE(%) FOR THE ORIGINAL AND PRIVACY-PRESERVING POWER CONSUMPTION DATA IN REDD

	Fridge	Dishwasher	Microwave	Washing machine	Ave	Decrease
Original	39.83/10.85/74.44	21.70/6.76/28.10	23.07/31.67/55.84	11.89/1.33/69.71	24.10/12.65/57.02	0.00%/0.00%/0.00%
$\varepsilon = 2$	42.08/29.83/74.85	29.29/40.07/17.55	24.46/7.69/50.63	14.00/1.50/62.68	27.45/19.77/51.42	13.9%/56.28%/9.82%
$\varepsilon = 1.5$	43.82/32.51/71.85	32.31/50.06/13.05	27.77/16.53/47.16	16.26/4.04/60.13	30.04/25.78/48.04	24.64%/103.79%/15.74%
$\varepsilon = 1$	46.80/35.09/65.42	33.22/61.20/7.81	35.64/49.79/37.22	23.62/27.89/40.89	34.82/43.49/37.83	44.48%/243.69%/33.65%
$\varepsilon = 0.8$	48.57/36.02/61.34	37.28/49.58/2.94	39.54/60.86/31.68	31.51/54.58/27.82	39.22/50.26/30.94	62.73%/297.31%/45.73%
$\varepsilon = 0.5$	52.93/41.52/51.00	29.27/84.92/1.12	47.66/72.95/18.46	61.40/155.74/14.57	47.81/88.78/21.28	98.38%/601.81%/62.67%
$\varepsilon = 0.3$	58.65/55.10/30.56	41.11/38.06/1.00	63.96/128.47/6.19	129.19/376.07/7.59	73.22/149.42/11.35	203.81%/1081.18%/80.09%



(a) Dishwasher

(b) Fridge

(c) Washing machine

(d) Microwave

Fig. 6. A comparative analysis of appliance power consumption in REDD: An investigation of actual consumption (Truth), NILM predictions based on original aggregated household signals (NILM for Origin), and NILM predictions utilizing perturbed/protected aggregated household signals from our ABDP mechanism (NILM for perturbation).

TABLE IV
AVERAGE USER BILLING ERRORS ($)

Period	RSMD	DDP	DPDR	E-DPNCT	ABDP (ours)
One day	0.39	0.51	0.14	3.02	0+0.0027
One week	2.75	3.64	1.00	21.11	0+0.02
One month	11.06	15.30	4.20	80.21	0+0.08
One year	142.35	186.15	51.10	1168.00	0+0.98

TABLE V
THE PEARSON'S CORRELATION COEFFICIENT BETWEEN THE REAL DATA AND FILTERED DATA GAINED BY THE FILTERING ATTACKER UNDER DIFFERENT w SETTINGS

	house 1	house 50	house 99	house 148	house 197
$w = 0$	-0.03	0.01	0.11	0.000	-0.01
$w = 5$	0.15	0.13	-0.06	-0.20	0.11
$w = 10$	0.09	-0.34	0.15	0.02	-0.01
$w = 17$	-0.23	0.09	-0.40	0.36	0.13
$w = 20$	-0.38	0.16	0.09	-0.01	0.37
$w = 25$	0.16	0.05	0.11	0.27	0.01
$w = 30$	-0.02	0.09	-0.07	0.14	0.005
$w = 40$	0.09	0.06	-0.16	0.04	0.12
$w = 80$	0.24	0.08	0.07	-0.001	-0.01
$w = 100$	-0.004	-0.08	0.02	0.11	0.02
$w = 140$	0.16	0.12	-0.11	-0.007	0.04

2) The Accuracy of Aggregating and Billing: In addition to privacy, accuracy is a critical factor for evaluating our ABDP and the baselines. Hence we implement our ABDP incorporating accuracy aims in this section. Specifically, for the power provider or power grid, accurate load monitoring and forecasting for each region are essential. Similarly, individual users are concerned about the accuracy of their billing calculations. Therefore, we evaluate the accuracy of the schemes based on real-time aggregated power and the calculation of individual customer bills.

Aggregating accuracy: We use SAE (see (15)) to measure the difference between the raw aggregated power and the output aggregated power for each scheme during a specific period. To ensure a fair comparison, we assume that the aggregator/power grid of all baselines and our ABDP successfully receive all users' power data at each time point t. We compute the SAE for each scheme using the data of all 200 users in NREL-DATA, randomly selecting one day with 144 data recordings. We conduct ten experiments for each scheme, resulting in the following average SAE values: 0.5% for RSMD, 0.3% for DDP, and 0.08% for DPDR. Although the SAE values for these three baselines appear to be low, our ABDP achieves a completely accurate aggregated power signal, resulting in an SAE of 0. This is because our ABDP introduces masters to collect the aggregated noise data from all users, as depicted in Fig. 2. Similarly, DPNCT and E-DPNCT also achieve accurate results.

Billing accuracy: The addition of noise to protect the privacy of users' data may introduce errors in billing calculations. We calculate the billing error for each scheme using different billing period settings. For the baselines DPDR and E-DPNCT, as well as our ABDP, which incorporates a dynamic pricing strategy, we set the high tariff at 2$/kWh and the low tariff at 1$/kWh. For the baselines RSMD and DDP, which do not support dynamic pricing, we set the tariff to 1.5$/kWh. consistently. Following the approach of baseline E-DPNCT, we set the maximum power consumption thresholds ($maxUnits$) for one day, one week, and one month as 785 kWh, 5500 kWh, and 22000 kWh, respectively. We randomly select ten houses/users from NREL-DATA to compute the billing error for each scheme. Each period setting corresponds to 10 experiments, and the average results are presented in Table IV. From the table, we observe that even in DPDR, which has a relatively small billing calculation error, the daily billing error for the user amounts to $0.14, resulting in a monthly error of $4.2 and a yearly error of $51.10. These errors represent costs that cannot be ignored by the user.

In contrast, our ABDP achieves accurate billing with an error of almost 0 in each billing period. This is due to the

TABLE VI
THE NILM ATTACK RESULTS OF MAE(WATT)/SAE(%)/F1-SCORE(%) FOR THE ORIGINAL AND PRIVACY-PRESERVING POWER CONSUMPTION DATA IN REDD

	Fridge	Dishwasher	Microwave	Washing machine	Ave	Decrease
Original	39.83/10.85/74.44	21.70/6.76/28.10	23.07/31.67/55.84	11.89/1.33/69.71	24.10/12.65/57.02	0.00%/0.00%/0.00%
$\varepsilon = 2$	43.01/27.18/74.15	30.19/35.07/19.55	25.12/30.23/52.23	13.87/3.58/63.18	28.04/24.01/52.27	16.78%/89.80%/8.33%
$\varepsilon = 1$	47.89/34.98/65.39	34.01/64.31/8.81	36.07/48.99/38.01	22.62/26.19/41.08	35.14/43.61/38.32	45.80%/244.74%/32.79%
$\varepsilon = 0.5$	51.98/42.12/50.53	35.00/70.92/2.12	48.13/79.99/20.06	51.42/150.72/12.89	46.63/85.93/21.40	93.48%/579.28%/62.46%
$\varepsilon = 0.3$	60.23/53.14/29.78	40.99/68.94/0.99	62.90/127.97/7.00	131.45/350.48/6.91	73.89/150.13/11.17	206.59%/1086.79%/80.41%

inclusion of Algorithm 2, which incorporates a noise cancellation operation to support accurate billing. Furthermore, the mathematical principle, specifically the additivity of the gamma distribution, ensures that our ABDP maintains its objective of protecting user privacy. While we have conducted a comprehensive evaluation of the privacy-preserving effectiveness of our scheme in Section VII-B1, the evaluated scheme did not take into account the billing-accuracy objective (hereafter referred to as the basic ABDP scheme). Nevertheless, it is essential to gauge whether our goal of ensuring accurate billing might impact the efficacy of privacy preservation (referred to henceforth as the enhanced ABDP scheme). Therefore, following the empirical investigations pertaining to our ABDP mechanism, we utilized the filtering attack and the NILM attack to assess our enhanced ABBP mechanism. The specific results are displayed in Tables V and VI of this response.

For the filtering attack, the Pearson's correlation coefficient (ρ) is utilized to measure the correlation between the filtered data and real data. w in Table I refers to the window size set by the filtering attack, with $w = 0$ representing the results in the absence of filtering attack. From the results corresponding to $w = 0$, we can find that the absolute values of the correlation coefficients are extremely small, with some even reaching 0, indicating that they are almost uncorrelated, i.e., our enhanced ABDP can effectively change the distribution characteristics of the original data. When the filtering attack applied, the results (rows 2–11 in Table I) show that our enhanced ABDP effectively resists filtering attacks by ensuring a significant difference between the filtered power data and the real power data, even when the filtering attack algorithm is using the optimal window size (w) setting. This is evident from the fact that the maximum Pearson's correlation coefficients for each house are considerably smaller than the maximum correlation coefficient of 1.

For the NILM attack, the metrics MAE and SAE are employed to measure the accuracy of the NILM attack algorithm in predicting the power consumption of individual appliances in comparison to the original power signal. Here, a lower MAE and SAE denote superior performance of the NILM attack. Table II illustrates that our enhanced ABDP effectively thwarts NILM attacks on power disaggregation. When implementing DP protection to the user's power consumption data with a privacy budget ε set to 2, our schema increases the average MAE and SAE of NILM attacks by 16.78% and 89.80%, respectively. The average MAE and SAE continue to escalate as the intensity of privacy protection augments, reaching an increase of 206.59% and 1086.79% when ε is adjusted to 0.3. The third metric, the F1-score in the table, signifies the accuracy of the NILM attack algorithm in successfully deducing the on-off state information of appliances. A higher F1-score signals enhanced performance of the NILM attack. The F1-score presented in Table II validates that our enhanced ABDP effectively diminishes the ability of the NILM attack algorithm to infer the on-off state information of appliances, with an 80.41% decrease in the F1-score as a result of the application of the DP strategy. All the results clearly suggest that the objective of ensuring billing accuracy does not compromise the privacy-preserving effectiveness of our schema.

VIII. CONCLUSION AND FUTURE WORK

In this paper, we propose ABDP, a solution that addresses the trade-off between noise intensity and data utility in existing differential privacy methods for smart grids. ABDP introduces masters to eliminate the added noise for aggregated data and utilizes the additivity of the gamma distribution to remove periodic noise for each individual user. To ensure security, ABDP incorporates a Blockchain smart contract with PRF for random selection of masters to receive noise data. Theoretical analysis and empirical experiments demonstrate that ABDP excels in providing high levels of privacy protection, data utility, and security. Our future research efforts concentrate on reducing the communication costs associated with user data collection further. Additionally, we will expand our approach to encompass scenarios such as Smart Microgrids, which integrate an array of renewable energy sources and intelligent home systems.

REFERENCES

[1] R. Mi et al., "Scalable aesthetic transparent wood for energy efficient buildings," *Nature Commun.*, vol. 11, no. 1, pp. 1–9, 2020.

[2] S. Chouikhi, M. Esseghir, and L. Merghem-Boulahia, "Energy consumption scheduling as a fog computing service in smart grid," *IEEE Trans. Serv. Comput.*, vol. 16, no. 2, pp. 1144–1157, Mar./Apr. 2023.

[3] H. K. Nguyen, J. B. Song, and Z. Han, "Demand side management to reduce peak-to-average ratio using game theory in smart grid," in *Proc. IEEE INFOCOM Workshops*, 2012, pp. 91–96.

[4] A. Jindal, G. S. Aujla, N. Kumar, and M. Villari, "GUARDIAN: Blockchain-based secure demand response management in smart grid system," *IEEE Trans. Serv. Comput.*, vol. 13, no. 4, pp. 613–624, Jul./Aug. 2020.

[5] S. Misra, S. Bera, and T. Ojha, "D2P: Distributed dynamic pricing policyin smart grid for PHEVs management," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 3, pp. 702–712, Mar. 2015.

[6] Y. Zhang and M. van der Schaar, "Structure-aware stochastic load management in smart grids," in *Proc. IEEE Conf. Comput. Commun.*, 2014, pp. 2643–2651.

[7] X. Wang, M. Zhang, and F. Ren, "Learning customer behaviors for effective load forecasting," *IEEE Trans. Knowl. Data Eng.*, vol. 31, no. 5, pp. 938–951, May 2019.

[8] S. Aminikhanghahi, T. Wang, and D. J. Cook, "Real-time change point detection with application to smart home time series data," *IEEE Trans. Knowl. Data Eng.*, vol. 31, no. 5, pp. 1010–1023, May 2019.

[9] P. Barbosa, A. Brito, and H. Almeida, "A technique to provide differential privacy for appliance usage in smart metering," *Inf. Sci.*, vol. 370, pp. 355–367, 2016.

[10] C. Zhang, M. Zhong, Z. Wang, N. Goddard, and C. Sutton, "Sequence-to-point learning with neural networks for non-intrusive load monitoring," in *Proc. AAAI Conf. Artif. Intell.*, 2018.

[11] M. D'Incecco, S. Squartini, and M. Zhong, "Transfer learning for non-intrusive load monitoring," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1419–1429, Mar. 2020.

[12] H. Çimen, N. Çetinkaya, J. C. Vasquez, and J. M. Guerrero, "A microgrid energy management system based on non-intrusive load monitoring via multitask learning," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 977–987, Mar. 2021.

[13] C. Shin, S. Joo, J. Yim, H. Lee, T. Moon, and W. Rhee, "Subtask gated networks for non-intrusive load monitoring," in *Proc. AAAI Conf. Artif. Intell.*, 2019, pp. 1150–1157.

[14] O. Tan, D. Gunduz, and H. V. Poor, "Increasing smart meter privacy through energy harvesting and storage devices," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1331–1341, Jul. 2013.

[15] F. Farokhi and H. Sandberg, "Fisher information as a measure of privacy: Preserving privacy of households with smart meters using batteries," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4726–4734, Sep. 2018.

[16] Y. Sun, L. Lampe, and V. W. Wong, "Smart meter privacy: Exploiting the potential of household energy storage units," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 69–78, Feb. 2018.

[17] G. Ács and C. Castelluccia, "I have a DREAM! (differentially private smart metering)," in *Proc. 13th Int. Conf. Inf. Hiding*, Springer, 2011, pp. 118–132.

[18] Z. Guan et al., "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 82–88, Jul. 2018.

[19] X.-D. Wang, W.-Z. Meng, and Y.-N. Liu, "Lightweight privacy-preserving data aggregation protocol against internal attacks in smart grid," *J. Inf. Secur. Appl.*, vol. 55, 2020, Art. no. 102628.

[20] 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.

[21] 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.

[22] A. Alsharif, M. Nabil, S. Tonyali, H. Mohammed, M. Mahmoud, and K. Akkaya, "EPIC: Efficient privacy-preserving scheme with EtoE data integrity and authenticity for AMI networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3309–3321, Apr. 2019.

[23] A. Mohammadali and M. S. Haghighi, "A privacy-preserving homomorphic scheme with multiple dimensions and fault tolerance for metering data aggregation in smart grid," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5212–5220, Nov. 2021.

[24] C. Dwork et al., "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, no. 3/4, pp. 211–407, 2014.

[25] Z. Zhang, Z. Qin, L. Zhu, J. Weng, and K. Ren, "Cost-friendly differential privacy for smart meters: Exploiting the dual roles of the noise," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 619–626, Mar. 2017.

[26] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differentially private dynamic pricing for efficient demand response in smart grid," in *Proc. Int. Conf. Commun.*, 2020, pp. 1–6.

[27] M. U. Hassan, M. H. Rehmani, J. T. Du, and J. Chen, "Differentially private demand side management for incentivized dynamic pricing in smart grid," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 6, pp. 5724–5737, Jun. 2023.

[28] 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.

[29] L. Lyu, K. Nandakumar, B. Rubinstein, J. Jin, J. Bedo, and M. Palaniswami, "PPFA: Privacy preserving fog-enabled aggregation in smart grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3733–3744, Aug. 2018.

[30] G. Eibl and D. Engel, "Differential privacy for real smart metering data," *Comput. Sci.-Res. Develop.*, vol. 32, no. 1, pp. 173–182, 2017.

[31] J. Won, C. Y. Ma, D. K. Yau, and N. S. Rao, "Privacy-assured aggregation protocol for smart metering: A proactive fault-tolerant approach," *IEEE/ACM Trans. Netw.*, vol. 24, no. 3, pp. 1661–1674, Jun. 2016.

[32] Z. Zheng, T. Wang, A. K. Bashir, M. Alazab, S. Mumtaz, and X. Wang, "A decentralized mechanism based on differential privacy for privacy-preserving computation in smart grid," *IEEE Trans. Comput.*, vol. 71, no. 11, pp. 2915–2926, Nov. 2022.

[33] M. B. Gough, S. F. Santos, T. AlSkaif, M. S. Javadi, R. Castro, and J. P. Catalão, "Preserving privacy of smart meter data in a smart grid environment," *IEEE Trans. Ind. Informat.*, vol. 18, no. 1, pp. 707–718, Jan. 2022.

[34] K. Hafeez, M. H. Rehmani, and D. O'Shea, "DPNCT: A differential private noise cancellation scheme for load monitoring and billing for smart meters," in *Proc. IEEE Int. Conf. Comput. Vis. Workshops*, 2021, pp. 1–6.

[35] K. Hafeez, D. OShea, and M. H. Rehmani, "E-DPNCT: An enhanced attack resilient differential privacy model for smart grids using split noise cancellation," 2021, *arXiv:2110.11091*.

[36] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," pp. 1–9, 2008. [Online]. Available: http://bitcoin.org/bitcoin.pdf

[37] M. Muratori, "Impact of uncoordinated plug-in electric vehicle charging on residential power demand," *Nature Energy*, vol. 3, no. 3, pp. 193–201, 2018.

[38] J. Z. Kolter and M. J. Johnson, "REDD: A public data set for energy disaggregation research," in *Proc. SIGKDD Workshops*, 2011, pp. 59–62.

[39] T. Zia, D. Bruckner, and A. Zaidi, "A hidden markov model based procedure for identifying household electric loads," in *Proc. 37th Annu. Conf. IEEE Ind. Electron. Soc.*, 2011, pp. 3218–3223.

[40] L. Mauch and B. Yang, "A novel DNN-HMM-based approach for extracting single loads from aggregate power signals," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, 2016, pp. 2384–2388.

[41] M. Azaza and F. Wallin, "Finite state machine household's appliances models for non-intrusive energy estimation," *Energy Procedia*, vol. 105, pp. 2157–2162, 2017.

[42] V. Piccialli and A. M. Sudoso, "Improving non-intrusive load disaggregation through an attention-based deep neural network," *Energies*, vol. 14, no. 4, 2021, Art. no. 847.

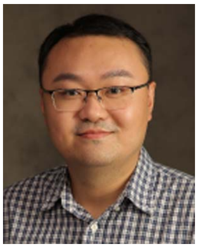
Jialing He (Member, IEEE) received the MS and PhD degrees from the Beijing Institute of Technology, Beijing, China, in 2018 and 2022, respectively. She is currently an research assistant professor with the College of Computer Science, Chongqing University, Chongqing, China. Her current research interests include differential privacy, user behavior mining, and Blockchain.

Ning Wang (Member, IEEE) received the PhD degree in information and communication engineering from the Beijing University of Posts and Telecommunication, in 2017. He was an engineer with Huaxin Post and Telecommunications Consulting Design Company Ltd. from 2012 to 2013. He was with the Department of Electrical and Computer Engineering, George Mason University, as a postdoctoral scholar from 2017 to 2020. He is currently a professor with the College of Computer Science Chongqing University. His current research interests are in physical layer security, machine learning, RF fingerprinting, and cyber-physical systems security and privacy

Tao Xiang (Senior Member, IEEE) received the BEng, MS, and PhD degrees in computer science from Chongqing University, China, in 2003, 2005, and 2008, respectively. He is currently a professor with the College of Computer Science, Chongqing University. His research interests include multimedia security, cloud security, data privacy and cryptography. He has published more than 100 papers on international journals and conferences. He also served as a referee for numerous international journals and conferences.

Yiqiao Wei received the BEng degree from Chongqing University, Chongqing, China, in 2019. He is currently working toward the MS degree with the College of Computer Science, Chongqing University, Chongqing, China. His recent research interests include differential privacy and physical layer security.

Zijian Zhang (Senior Member, IEEE) received the PhD degree from the Beijing Institute of Technology. He is a professor with the School of Cyberspace Science and Technology, Beijing Institute of Technology. His research interests include authentication and key agreement, behavior recognition, and privacy preserving.



Meng Li (Senior Member, IEEE) received the PhD degree in computer science and technology from the School of Computer Science and Technology, Beijing Institute of Technology (BIT), China, in 2019. He is an associate professor and dean assistant with the School of Computer Science and Information Engineering, Hefei University of Technology (HFUT), China. He is also a post-doc researcher with the Department of Mathematics and HIT Center, University of Padua, Italy, where he is with the Security and PRIvacy Through Zeal (SPRITZ) research group led by Prof. Mauro Conti (IEEE fellow). He was sponsored by China Scholarship Council (CSC) (from 2017.9.1 to 2018.8.31) for joint PhD study supervised by Prof. Xiaodong Lin (IEEE fellow) with the Broadband Communications Research (BBCR) Lab, University of Waterloo and Wilfrid Laurier University, Canada. His research interests include security, privacy, applied cryptography, blockchain, TEE, and Internet of Vehicles. He is an associate editor for *IEEE Transactions on Information Forensics and Security*, *IEEE Transactions on Network and Service Management*, and *IEEE Internet of Things Journal*.

Liehuang Zhu (Senior Member, IEEE) is a full professor with the School of Cyberspace Science and Technology, Beijing Institute of Technology. He is selected into the Program for New Century Excellent Talents in University from Ministry of Education, P.R. China. His research interests include Internet of Things, cloud computing security, internet and mobile security. He has published more than 100 SCI-indexed research papers in these areas, as well as a book published by Springer. He serves on the editorial boards of three international journals, including *IEEE Internet of Things Journal*, *IEEE Network*, and *IEEE Transactions on Vehicular Technology*. He won the Best Paper Award at IEEE/ACM IWQoS 2017 and IEEE TrustCom 2018.