Privacy Preservation for Time Series Data in the Electricity Sector

Haoxiang Wang, *Graduate Student Member, IEEE*, *and* Chenye Wu, *Member, IEEE*

***Abstract*—The big data era has raised public concern regarding private information leakage. Therefore, in the electricity sector, many classical privacy preserving mechanisms based on noise injection have been designed and implemented for meter data. However, injected noise of large magnitudes can affect the statistical structure of these data. Therefore, in this study, we identify the inherent randomness embedded in time series data to mitigate this issue. To this end, we study the potential of using this inherent randomness to protect the privacy for both high and low resolution time series data. We propose a privacy preserving mechanism using stochastic differential equation modeling. We theoretically prove the effectiveness of our proposed framework and design several methods to implement our mechanism to aid various data-driven consumer behavior analysis tasks in the electricity sector. The numerical results indicate that our framework can simultaneously maintain the desired level of privacy preservation and value of data in practice.**

***Index Terms*—Privacy Preserving, Stochastic Differential Equation, Consumer Behavior Analysis**

NOMENCLATURE

DP	differential privacy
MLP	multilayer perceptron
NILM	non-intrusive load monitoring
ODE	ordinary differential equation
pdf	probability density function
RDP	Rényi differential privacy
SDE	stochastic differential equation
$F(\cdot)$	bounded function to characterize V
$g(\cdot)$	ODE's governor
$R(\cdot)$	Rényi divergence
$V(\cdot)$	SDE potential function
α	order of Rényi divergence
β	SDE coefficient
Δ	sensitivity
δ	step size for SDE discretization
λ^*	strongly convex parameter of V
λ_0	inverse variance of x_0
ϕ	sensitivity assignment between time 0 and time t
θ	parameters for parametric potential function
C	bounded parameter for $F(x_t)$
D	hidden states
n_t	time independent noise of time series data
r_t	noise injected in high resolution data mechanism's implementation
$S_g(t)$	time varying sensitivity budget
$S_g^{\#}(t)$	discrete time varying sensitivity budget
t_p	shock interval length
x_t	time series data
y_t	time dependent part of time series data

Manuscript received May 7, 2022; revised September 1, 2022, and November 18, 2022; accepted November 26, 2022. Date of publication XXX, 2023; date of current version December 17, 2022. This work was supported in part by the National Natural Science Foundation of China (Grant No. 72271213), Science, Technology and Innovation Commission of Shenzhen Municipality (Grant No. JCYJ20220530143800001), and the Shenzhen Institute of Artificial Intelligence and Robotics for Society. Paper no. TSG-00659-2022. (*Corresponding author: Chenye Wu.*)

H. Wang is with the Department of Automation, Tsinghua University, Beijing, 100084, P.R. China.

C. Wu is with School of Science and Engineering, The Chinese University of Hong Kong, Shenzhen, and Shenzhen Institute of Artificial Intelligence and Robotics for Society, Guangdong, 518172, P.R. China (email: chenyewu@yeah.net).

I. INTRODUCTION

Data-driven approaches have dramatically changed our lifestyles; for example, personalized recommendations for online shopping, fraud detection in banking, and quantitative trading for investment. In the electricity sector, data-driven approaches have also enabled ambient assisted living [1], real time energy saving [2], load profiling [3], etc. Although these techniques have contributed to realizing a more efficient power grid, they have also led to significant public concern regarding private information leakage.

Thus far, several privacy protection mechanisms have been proposed; however, most of them are based on noise injection. Injected noise can clearly affect the statistical structure of time series data, which can influence the performance of various data-driven tasks that utilize these noisy data. However, the conventional privacy preserving mechanisms seldom consider these impacts. There are two major approaches to minimizing such impacts: inject as little noise as possible while maintaining the target privacy preserving level, and identify the physical meaning of injected noise in different tasks for potential error correction.

In this study, we use consumer behavior analysis as an example to design an effective privacy preserving mechanism for time series data in the electricity sector. To this end, we exploit the internal noise in the time series data to avoid injecting excessive noise. Thus, we can realize remarkable performances in various consumer behavior analysis tasks compared to those realized using classical noise injection mechanisms.

A. Related Works

We identified three major streams of close research: 1) using time series data to perform consumer analysis in the electricity sector, 2) designing various privacy preservation mechanisms

for energy data, 3) modeling time series data using stochastic differential equations (SDEs).

Time series data play an important role in consumer behavior analysis in the electricity sector. For example, high resolution time series data allow detailed appliance-level load profile analyses, termed non-intrusive load monitoring (NILM) [4]. This technique can detect switch events or track the states of appliances using high resolution meter readings. This information is highly beneficial for consumer behavior analysis. See [5] for a comprehensive survey. Further, low resolution time series data is very useful for understanding consumers' lifestyles, which can help facilitate active demand side management [6], [7]. See [8] for an excellent survey.

Next, we revisit the existing privacy mechanisms in the electricity sector. Specifically, we have now classified the privacy mechanisms into two categories: cryptographic mechanisms and statistical mechanisms [9]. Most cryptographic privacy mechanisms utilize various encryption techniques. For example, Garcia *et al.* use the homomorphic encryption method to protect privacy in smart grids [10]. Zhang *et al.* propose a multi-authority attribute-based data sharing framework for the electricity sector, and the core technique is the inner product encryption [11]. Mustafa *et al.* propose a multi-party computation based protocol to preserve privacy in smart meter data collection [12]. Romdhane *et al.* propose an encryption method for data aggregation to preserve privacy against attackers in data communication [13]. Besides encryption, blockchain techniques are also catching an increasing eye to conduct private communications for the power grid [14], and federated learning is enabling many smart meter data-driven applications [15]. However, these cryptographic methods primarily address privacy leakage issues in communication, and attackers are frequently able to deduce the truth if they have access to all keys or unlimited computational power. In our study, on the other hand, we use the statistical notion of privacy, which looks at privacy leakage from an information theory point of view.

The most representative statistical notion to characterize privacy is differential privacy (DP). The research on designing mechanisms to achieve DP in the smart grid is well researched, with the majority of them attempting to manipulate the distribution of the information (to be protected) through various methods. And the noise injection methods (e.g., injecting Gaussian or Laplacian noises [16], [17]) are among the most classical ones. Most existing works focus on investigating how to inject as little noise as possible to achieve a given privacy preserving level. Such attempts include noise amplitude adjustment [17], customizing different types of noise for different applications [18], [19], maintaining the smoothness of the perturbed data [20], and manipulating the Fourier transform coefficients [21]. Besides sanitizing the data, researchers also seek to map the data to other spaces and sanitize the mapping or algorithms to generate protected information iteratively. For example, Syed *et al.* adopt Differentially Private Stochastic Gradient Descent (DPSGD) to preserve the privacy of the data-driven model in the electricity sector [22]. Papernot *et al.* discuss the potential of applying the Private Aggregation of Teacher Ensembles (PATE) framework to protect the smart meter data [23]. In the same vein, many recent works design privacy mechanisms for clustering and other optimization tasks [24], [25], [26], [27]. These mechanisms often construct theoretical guarantees based on the composition theorem and achieve good performance in privacy preservation. However, the statistics of original data may be significantly changed after perturbation due to the mapping to another space. Other mechanisms [28], [29] utilize mutual information to achieve privacy preservation. Pal *et al.* seek to minimize the mutual information loss between the initial information and the information after privacy preservation when designing the privacy mechanism [30]. These methods often need to deal with multi-level stochastic optimizations, which are often computationally expensive to derive optimal solutions.

Clearly, noise injection methods enjoy the following two advantages: It's convenient to derive theoretically guaranteed privacy for noise injection methods, and such methods are often able to keep the statistics of the original data to support various data analyses and data-driven control applications. Therefore, we follow this research line and propose utilizing SDE modeling to achieve minimal noise injection. By doing so, our proposed mechanism can maintain many data statistics and a solid theoretical guarantee. These two characteristics are also highly desirable for the application of our interest, the problem of consumer load data protection. To enable the subsequent consumer behavior analysis, the data quality should be maintained. And the outputs of the proposed mechanism are perturbed consumers' load data. Thus, our proposed scheme can be more widely adopted in many scenarios.

Another line of closely related literature has investigated time series data modeling using SDE. To this end, many efforts have been devoted to deriving a suitable SDE for approximately modeling time series data [31], e.g., approaches based on the Einstein-Smoluchowski theory [32], and generalized stochastic Smoluchowski equation [33]. Verdejo *et al.* use SDE to model wind power generation and demand for prediction [34]. Sossan *et al.* formulate an SDE for demand side management [35]. Weron *et al.* conduct spot price predictions for the electricity market based on SDE models in [36]. However, these and other such studies focus on specific tasks based on SDE models, and they seldom discuss the physical meaning of the estimated SDE and its relationship with privacy, which forms the core of our work. This study follows our previous works [3], [37], wherein we studied the physical meaning of privacy mechanisms in clustering and NILM. We constructed criteria to evaluate the performance of the proposed privacy mechanisms.

B. Our Contributions

To the best of our knowledge, this is the first study that exploits the internal characteristics of time series data to design an effective privacy preserving mechanism for the electricity sector. The internal characteristics are distinguished through SDE modeling. Our principal contributions are summarized below:

- *Internal Privacy Characteristics Extraction:* We model both high resolution and low resolution data via SDE to extract the intrinsic noise in the original process, and

we use these models to analyze the privacy guarantee intrinsically embedded in these two types of time series data.

- *Privacy Preserving Mechanism Design:* We design a privacy preserving mechanism to achieve a certain level of privacy by utilizing the privacy characteristics of the data. We theoretically prove its privacy guarantee.
- *Enabling Pilot Implementations:* Our proposed privacy preserving mechanism has the potential to enable pilot practical implementations, such as NILM and load profiling[1]. In the numerical studies, our proposed mechanisms simultaneously protect data privacy and maintain the value of data in terms of inferring various consumer behaviors. In addition, our method can be implemented in real time, highlighting additional benefits for practical use. This is because to implement our method, the key is to determine a convex potential function, which can be learned from the historical data. And then, together with the sample collected in real time, our method could achieve the privacy preserving.

Our work is primarily motivated by the increasing need for consumer behavior analysis in the electricity sector. Such analysis could enable more customized pricing plans and more active demand response, which are essential for the future smart grid. However, directly publishing the raw data to the data analyzers is not a choice, as they can easily identify the consumers and reveal their privacy through the meter data [38]. Hence, we adopt the notion of differential privacy, which injects noise into the raw data to preserve privacy. We imagine there are at least three early adopters of our proposed mechanisms.

- The first adopters are the ISOs and utility companies. They currently have full access to the consumers' data and are required by law to protect the data. When recording the meter data collected from the consumers for analysis, the ISOs and utility companies are obliged to protect the consumers' privacy. Hence, using our mechanism, they could directly inject minimal noise into the recorded meter data. Compared with other privacy-preserving mechanisms, our mechanism better preserves the data characteristics, enabling more data analysis.
- The next adopters are third-party privacy-preserving entities. Such entities have already emerged in practice. For example, Pecan Street is actively recruiting volunteers to provide their energy consumption data. And in their agreement with the volunteers, they promise that "Data from an individual home can be viewed by the homeowner/resident. Researchers that access our database, however, cannot identify any individual participant". From an academic point of view, the most straightforward approach to enforcing such a guarantee is to employ the notion of differential privacy. And we provide an efficient way to achieve a certain level of privacy-preserving requirements while the data can also be utilized for these entities' purposes.
- Other adopters are the consumers themselves. When the number of third parties increases, the consumers who would like to sell their data may not have the capability of knowing which agent they can trust. Hence, in this case, before selling their data, they may want to adopt our method to protect their own data with the help of their local storage devices (e.g., the storage devices in electric vehicles, PV panels, etc.). Compared with existing methods, our proposed mechanism also enjoys a lower expected cost for conducting the noise injection, which benefits consumers.

[1]In our study, the potential mechanism can be regarded as a local differential privacy preserving mechanism. However, our mechanism can also be extended to multiple users.

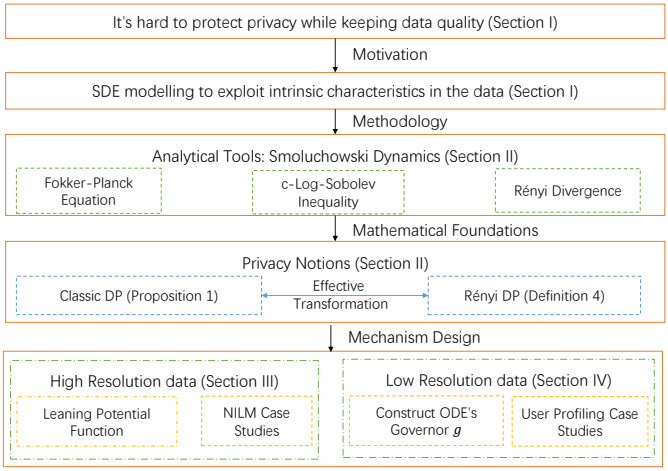

Fig. 1: The paradigm of our paper

The remainder of this paper is organized as follows: Section II revisits the preliminary definitions for the SDE analysis and privacy preserving mechanisms. Based on these definitions, we design a privacy preserving mechanism for high resolution and low resolution time series data, which are presented in Sections III and IV respectively. Section V presents numerical studies that highlight the effectiveness of the proposed mechanism. Finally, concluding remarks are delivered in Section VI. All the necessary proofs are postponed to the Appendix. Fig. 1 visualizes the structural paradigm of our proposed methodology with the notion in the preliminaries and the following discussion.

II. The Preliminaries

In this study, we investigate how to extract randomness embedded in time series data to help design a privacy preserving mechanism. Therefore, we briefly revisit useful definitions to characterize randomness through SDE and then introduce privacy notions that will be frequently used in the subsequent analysis.

A. Stochastic Differential Equation

We adopt the notion of Smoluchowski dynamics for SDE modeling and then introduce the Fokker-Planck equation to characterize such dynamics.

Definition 1. *(Smoluchowski Dynamics [39]) A stochastic process x_t satisfies the Smoluchowski dynamics if the process is governed by the SDE:*

$$dx_t = -\nabla V(x_t)dt + \sqrt{\beta^{-1}}dW_t, \tag{1}$$

where ∇, $V(x_t)$, W_t, and β represent the divergence operator, the potential function, a Wiener process (i.e., standard Brownian motion), and a fixed coefficient, respectively.

Remark: In this process, the dynamics are governed by the time invariant potential function $V(x_t)$ and independent noise. Although simple, this process is powerful for characterizing the high resolution time series data in the electricity sector. These data often have a large volume, even within a relatively short time period (e.g., 1-millisecond resolution data generated in 5 minutes). Under such a short time period, any temporal effects attributed to the physical laws can be neglected. In our work, this temporal effect refers to how the potential function varies with time. Take the high-resolution data setting as an example. We assume in a short period the potential function can be considered as a time-invariant function, denoted by $V(x_t)$. In our study, the 5-minute period is selected for NILM only. When conducting NILM, we often assume that consumers won't switch appliances frequently. This is particularly true for a short period of time, e.g., a 5-minute duration. This can also be verified by various datasets, e.g., REDD dataset [40] and UK-DALE dataset [41]. Therefore, we can safely assume that the potential function is time invariant, and the noises are independent for high resolution data. We relax these assumptions when considering low resolution data by utilizing a time varying potential function $V(x_t, t)$.

Definition 2. *(Fokker-Planck Equation [39]) If a stochastic process x_t can be described by the SDE:*

$$dx_t = \mu(x_t, t)dt + \sigma(x_t, t)dW_t, \tag{2}$$

where W_t represents a Wiener process, then the probability density function (pdf) for x_t denoted by $p(x, t)$ satisfies the Fokker-Planck equation:

$$\frac{\partial p(x,t)}{\partial t} = -\nabla \cdot (\mu(x,t)p(x,t)) + \Delta^H(\sigma(x,t)p(x,t)), \tag{3}$$

where Δ^H represents the Laplace operator.

Remark: The Fokker-Planck equation is a powerful tool for analyzing the general SDE process. It converts the SDE characterization to pdf characterization, which is easier to study.

B. Privacy Preserving Mechanism

Next, we introduce a Gaussian mechanism based on the notion of Rényi differential privacy (RDP). We first introduce Rényi divergence, which is essential for defining the RDP. Then, we introduce the connection between RDP and the classical (ϵ, δ) differential privacy ((ϵ, δ) DP), which paves the way for our subsequent privacy preserving mechanism design.

Definition 3. *(Rényi Divergence [42]) For any order $\alpha > 0$, the Rényi divergence of order α of probability distribution P from probability distribution Q is defined as:*

$$D_\alpha(P||Q) = \frac{1}{\alpha - 1} \ln \int p(\mu)^\alpha q(\mu)^{1-\alpha} d\mu, \tag{4}$$

where $p(\cdot), q(\cdot)$ are the pdfs of P, Q; and μ is a σ-finite measure.

This allows us to introduce the notion of RDP.

Definition 4. *(Rényi Differential Privacy, RDP [43]) Given dataset $D \in \mathscr{D}$, the neighborhood dataset D' of D satisfies $d(D, D') \leq 1$ for any distance metric d over $\mathscr{D}$. A randomized algorithm $\mathscr{A} : \mathscr{D} \to \mathbb{R}$ satisfies (α, ϵ) RDP if for any D and neighborhood dataset D', $R_\alpha(\mathscr{A}(D)||\mathscr{A}(D')) \leq \epsilon$.*

RDP describes the global privacy characteristics of D and can be converted to (ϵ, δ) DP as follows:

Proposition 1. *(Proposition 3 in [43]) If $\mathscr{A}$ is an (α, ϵ) RDP mechanism, it satisfies $(\epsilon + \frac{log1/\delta}{\alpha - 1}, \delta)$ DP, $\forall \delta \in (0, 1)$.*

Remark: Here, ϵ from traditional (ϵ, δ)-differential privacy is different than the ϵ in (α, ϵ)-RDP. In the traditional (ϵ, δ)-DP setting [44], we say a mechanism $\mathscr{B}$ achieves (ϵ, δ)-DP if for all neighbor datasets D_1 and D_2, and for all measurable subsets $Y \subset \mathbb{R}$, the mapping $\mathscr{B}$ satisfies,

$$\frac{Pr(\mathscr{B}(D_1) \in Y)}{Pr(\mathscr{B}(D_2) \in Y)} \leq e^\epsilon + \delta. \tag{5}$$

In contrast, (α, ϵ)-RDP requires that for all neighbor datasets D_1 and D_2, $R_\alpha(\mathscr{B}(D)||\mathscr{B}(D')) \leq \epsilon$ with α Rényi Divergence. In this work, we adopt the notion of RDP with better analytical properties in terms of designing privacy preserving mechanism.

The subsequent privacy analysis is conducted under the RDP framework and we can use Proposition 1 to convert it to the classical (ϵ, δ) DP metrics.

Definition 5. *(Gaussian Mechanism for RDP [45]) Given dataset D and its neighborhood dataset D' with metric f, if a Gaussian mechanism $\mathscr{M}$ satisfies*

$$\mathscr{M} = f(D) + \mathscr{N}(0, \sigma), \tag{6}$$

where f represents a mapping $f : \mathscr{D} \to \mathbb{R}$ and $\mathscr{N}$ represents a normal distribution, then the mechanism $\mathscr{M}$ satisfies $(\alpha, \frac{\alpha}{\sigma^2})$ RDP.

Remark: We use the classical Gaussian mechanism for RDP because parameters (ϵ, δ) in the classical DP are connected through noise variance σ in the RDP framework. Therefore, the physical meaning of the injected noise is clear. The noise of a larger variance can realize higher privacy preservation when designing a simple noise injection privacy preserving mechanism. Moreover, implementing noise of larger variance often yields a higher noise generation.[2] Therefore, we plan

[2]Since the noises are often generated by charging and discharging the storage devices, we can measure the noise generation costs in terms of the degradation costs for storage devices. Precisely, generating noises of larger variances (i.e., magnitudes) correspond to deeper charging cycles for storage, yielding higher degradation costs.

This article has been accepted for publication in IEEE Transactions on Smart Grid. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TSG.2022.3230685

to exploit the inherent noise in the time series data such that noise of smaller variance can be injected while achieving the same privacy preserving level.

III. Mechanism for High Resolution Data

The critical property of high resolution time series data in the electricity sector is sparsity in the occurrence of events (or changes) attributed to the high inertia of the power system. Thus, useful information embedded in the data can be considered as random shocks.

A. Mechanism Design

Without loss of generality, given the time series data $\mathbf{X} = (x_0, .., x_T)$ the time length T, we assume that the shock occurs at time 0. The measurement x_0 satisfies $\mathcal{N}(\tilde{x}_0, \frac{1}{\lambda_0})$, where $\tilde{x}_0$ represents the mean of shock x_0 and λ_0^{-1} is its variance, because it is a random shock. We want to make x_0 indistinguishable from $x_0' \sim \mathcal{N}(\tilde{x}_0', \frac{1}{\lambda_0})$, where x_0' has mean $\tilde{x}_0'$ and the same variance as x_0 to ensure the privacy preservation.

Remark: Random shock refers to the unpredicted significant change in the time series data. Mathematically, for time $t-1$ and t, we say a random shock occurs at time t if $|x_t - x_{t-1}| > h$, where h is the threshold to differentiate the significant change from common fluctuations. In the context of NILM for our study, the key information is embedded in the random shocks. And random shocks are also referred to as the load shocks in the NILM literature [46], [47]. In our study, we slightly changed the name from load shocks to random shocks to highlight the uncertainty embedded in the load shocks.

We denote the initial Rényi divergence between x_0 and x_0' by $R_\alpha(x_0, x_0')$, which equals $\frac{\alpha\Delta^2\lambda_0}{2}$, where $\Delta = \|\tilde{x}_0 - \tilde{x}_0'\|$ is defined as the sensitivity for noise perturbation. This value measures the indistinguishability between the two inputs. A higher sensitivity indicates that they can be identified more easily.

Thus, different initial states x_0 and x_0' lead to two SDEs. We model high resolution time series data using the Smoluchowski dynamics as:

$$dx_t = -\nabla V(x_t)dt + \sqrt{\beta^{-1}}dW_t. \tag{7}$$

Remark: We adopt the Smoluchowski dynamics because high resolution data include little information other than random shocks. The classical approach treats every sample point in $\mathbf{X}$ as the same, i.e., every point can be a random shock. Therefore, the classical approach injects noise into each sample point. Indeed, such an approach injects too much noise into $\mathbf{X}$ because the key information we want to protect is only related to x_0. To highlight these properties, we adopt simple Smoluchowski dynamics.

Next, we assume that $V(x_t)$ satisfies

$$V(x_t) = \frac{\lambda_0}{\beta}x_t^2 + F(x_t), \tag{8}$$

where $F(x_t)$ represents a C-bounded [3] function.

[3] $F(x_t)$ is C-bounded if $|F(x_t)| \leq C$ for all x_t over its domain.

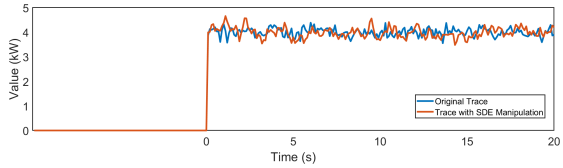

Fig. 2: High resolution sample data comparison

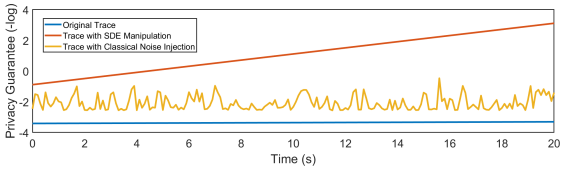

Fig. 3: Privacy guarantee comparison

This form embeds key insights of high resolution data. Fig. 2 illustrates the sample energy consumption trace corresponding to the SDE with the initial state, x_0 (blue line), and the privacy preserved trace (orange line) corresponding to the SDE with the initial state, x_0'. These two traces are from a single house load at the resolution of 1 second. After the random shock at time 0, the energy consumption roughly maintains the same level with some noise. These are exactly the insights described by the specific form of $V(x_t)$. The first term in Eq. (8) seeks to maintain a constant energy consumption level whereas the second term $F(x_t)$ describes the time independent perturbations of the system. These perturbations can cause the system to be indistinguishable from other systems, and hence, it reflects the system privacy characteristics. This form is also able to approximate all the functions with the bounded x_t and bounded changes over x_t. This flexibility is another reason for us to choose to specify the form of $V(x_t)$ as in Eq. (8) [48], [49], [50]. For practical implementation, we adopt data-driven methods to estimate $V(x_t)$.

Next, we prove the following theorem that characterizes how the privacy level evolves with time and sensitivity:

Lemma 1. *If process x_t can be characterized by the SDE process with $V(x_t)$ in the form of Eq. (8) with parameters C, λ_0 and sensitivity Δ, then x_t satisfies $(\alpha, \frac{\alpha\Delta^2\lambda_0}{2}e^{-2\frac{\lambda_0}{\beta}te^{-4C\beta}})$ RDP.*

Remark: This lemma illustrates the temporal privacy preserving effect of the time series data. The privacy level increases in the order of $O(\Delta^2 e^{-t})$ in terms of time and sensitivity. Unfortunately, the exponential term $e^{-4C\beta}$ weakens the privacy preservation. A higher C indicates a higher complexity for exploiting the characteristics of the time series and making the data more distinguishable from others, which leads to a lower privacy level.

We can obtain a stronger privacy guarantee by utilizing the strong convexity of $V(x_t)$ in Eq. (8).

Theorem 1. *If process x_t can be characterized using the SDE process in Eq. (8) with sensitivity Δ, and $V(x_t)$ is λ^*-strongly convex for $\beta\lambda^* \geq \lambda_0$, then x_t satisfies $(\alpha, \frac{\alpha\Delta^2\lambda_0}{2}e^{-2\lambda^* t})$ RDP.*

Example: In correspondence to Fig. 2, Fig. 3 shows a com-

parison between the magnitudes of privacy preservation for the three processes: the original trace, privacy preserved trace based on SDE modeling, and privacy preserved trace based on the classical noise injection method. The privacy guarantee refers to the parameter ϵ in (α, ϵ) RDP. We find that the original process has some privacy guarantee because of the embedded noise. Further, privacy preservation is improved after we adjust the potential function. Fig. 3 also shows that the privacy of our method (orange line) increases exponentially with the time duration. Finally, Fig. 3 illustrates that the proposed mechanism always achieves a higher privacy guarantee in this example compared to those of the other methods, which demonstrates the effectiveness of our proposed method with high resolution data.

B. Learning Differentiable Potential Function

A strongly convex function $V(x_t)$ needs to be constructed to maintain the strong privacy guarantee. However, the ground truth potential function may not be convex. Hence, we need to fit the original data with a parametric function V_θ, which is strongly convex.

We use polynomial and sinusoidal functions to construct one approximation of $\nabla^2 V(x_t)$, denoted by $\mathcal{H}(x_t)$, because strong convexity is related to $\nabla^2 V(x_t)$:

$$\begin{aligned}\mathcal{H}(x_t;\theta,\zeta) &= \nabla^2 V(x_t;\theta,\zeta) \\ &= \sum\nolimits_{i=1}^{n} \theta_i x_t^i + \sum\nolimits_{i=1}^{m} \zeta_i cos(ix_t),\end{aligned} \tag{9}$$

where n and m represent the number of the polynomial and sinusoidal functions respectively; and θ_i and ζ_i represent the coefficients to be estimated.

Remark: Our study focuses on the case when x_t is a scalar. In this case, for a twice continuously differentiable function $V : \mathbb{R} \to \mathbb{R}$, if V is λ^*-strongly convex, it satisfies that,

$$\nabla^2 V(x) \geq \lambda^*. \tag{10}$$

This conclusion can be extended to high-dimensional cases, and the condition becomes that the minimum eigenvalue of $\nabla^2 V(x)$ should be no smaller than λ^*.

To ensure strong convexity, we require $\mathcal{H}(x_t) \geq \lambda^*$, which yields the following optimization problem for data fitting when there are T data points:

$$\begin{aligned}&\min_{\theta,\zeta} \sum_{t=2}^{T} \left[\sum_{i=1}^{n} \frac{\theta_i x_t}{i+1} - \sum_{i=1}^{m} \frac{\zeta_i sin(ix_t)}{i} - x_t + x_{t-1} \right]^2 \\ &s.t. \quad \sum\nolimits_{i=1}^{n} \theta_i x_t + \sum\nolimits_{i=1}^{m} \zeta_i cos(ix_t) \geq \lambda^*.\end{aligned} \tag{11}$$

Further, we can construct a neural network (NN) to learn this parametric function. The general idea is to fix the output of the final layer to a value larger than λ^* to achieve the strong convexity. With the learned $\mathcal{H}_\theta(x_t)$ and the boundary conditions, we can construct the first order derivation $\nabla V_\theta(x_t)$. We illustrate this procedure in Algorithm 1.

Remark: If prior knowledge allows us to model the data with some given $F(x_t)$, then Algorithm 1 helps provide a convex approximation for the given $F(x_t)$. Clearly, such prior knowledge helps us to derive a more accurate convex approximation, yielding better performance for the subsequent data-driven tasks.

Algorithm 1: NN Construction of $\nabla V_\theta(x_t)$

Input: The time series data x_t $t = 1, ..., T$;
The privacy requirement ϵ;
The initial neural network $\mathcal{H}_\theta(x_t)$;
The Riemann summation piece number k;
The epoch number E;
The learning rate η;
Output: $\nabla V_\theta(x_t)$;

```
Derive the required convexity λ* using Theorem 2
for i ≤ E do
    ℒ = 0
    for s ∈ {1, .., T} do
        Divide [0, x_t] into k piece
        Calculate ∇V_θ = Σ_{j=1}^{k} max(H_θ(j x_t / k), λ*)
        ℒ = ℒ + (∇V_θ − (x_t − x_{t−1}))^2
    end for
    θ = θ − η ∇_θ ℒ
end for
```

If $\mathcal{H}_\theta(x_t)$ is L-Lipschitz, then the approximation error can be bounded as follows:

Corollary 1. *If the function $\mathcal{H}_\theta(x_t)$ is L-Lipschitz, the error of the Riemann summation approximation with k pieces is of the order of $\mathcal{O}(\frac{Lx_t^2}{k})$.*

Remark: Fazlyab *et al.* proposed a convex programming framework for deriving tight bounds on the global Lipschitz constant [51]. We want to emphasize that, in the SDE dynamics, we require only the knowledge of $\nabla V_\theta(x_t)$, instead of $V_\theta(x_t)$. Hence, we do not need to integrate $\nabla V_\theta(x_t)$ to derive $V_\theta(x_t)$, which incurs an additional approximation error.

After constructing a strongly convex function, our mechanism can be implemented in two ways. We can directly use the sequence sampled from the SDE induced by the constructed strongly convex V. We denote it as x_t^*. The second approach is to combine the constructed sequence x_t^* with x_t. We inject noise $x_t^* - x_0$ into the original time series x_t, which results in the process $x_t + x_t^* - x_0$. In this study, we choose the latter, and it achieves more privacy preservation. This observation can be formally stated as follows:

Proposition 2. *Process $x_t + x_t^* - x_0$ achieves more privacy preservation than process x_t^*.*

IV. Mechanism for Low Resolution Data

When dealing with high-resolution data, only the shock events expose private information, i.e., when the consumer switches on/off some specific appliance. Hence, in this case, the consumer behaviors refer to the shock events. i.e., the appliances' switch events. In contrast, the consumer behaviors embedded in the low-resolution data are more complicated. They include consumers' energy consumption habits and lifestyles, and we want to protect these critical determinants of consumer behaviors. As these determinants contain much

richer information than the information embedded in the appliance switch events in the high-resolution data case, it is more challenging to preserve the privacy of low-resolution data.

A. Mechanism Design

We utilize a time dependent potential function $V(x_t, t)$ to handle low resolution data SDE modeling. That is, we assume x_t satisfies:

$$dx_t = -\nabla V(x_t, t)dt + \sqrt{\beta^{-1}}dW_t. \tag{12}$$

We decouple $V(x_t, t)$ into two parts: a time dependent function g and a time independent function V_n. These two functions induce two processes y_t and n_t respectively. Hence, $x_t = y_t + n_t$. The time dependent process y_t is determined by the internal pattern of the time series data, such as the lifestyles of households. Thus, we assume y_t is governed by function g, which is dependent on time t and some hidden states D, i.e., $g(D, t)$. Under this assumption, y_t can be described by the ordinary differential equation (ODE):

$$dx_t = -g(D, t)dt. \tag{13}$$

Remark: We implicitly assume that process y_t is not influenced by the exact value of x_t, because y_t reflects the internal characteristics of the time series data.

The other time independent process n_t can be modeled based on the Smoluchowski dynamics as follows:

$$dn_t = -\nabla V_n(x_t)dt + \sqrt{\beta^{-1}}dW_t. \tag{14}$$

Here, we again assume that

$$V_n(x_t) = \frac{\lambda_0}{\beta}x_t^2 + F(x_t), \tag{15}$$

with C-bounded $F(x_t)$.

To ensure privacy preservation, we need to define the sensitivity between the dynamics governed by the neighbor states. For any neighbor state of D, denoted by D', and all t, we assume

$$|g(D, t) - g(D', t)| \leq \phi S_g(t), \tag{16}$$

where S_g represents the time varying sensitivity budget. This value represents the assignment of the sensitivity to each time t. To quantify the total budget of sensitivity, we require that $\|S_g(t)\|_2 \leq \phi\Delta$ (i.e., $\int_0^{+\infty} S_g(t)dt \leq \phi\Delta$), where Δ is the total budget for sensitivity and $\phi \in [0, 1]$ represents the assignment of sensitivity between time 0 and time t.

Remark: The high resolution cases correspond to the case where $\phi = 0$ and $S_g(t) = 0$, for $t > 0$ because all the information is revealed at the initial time.

The total budget Δ and the assignment constant ϕ are related to the initial states. Note that $x_0 = y_0 + n_0$. For different states D, D', $x_0 \sim \mathcal{N}(\tilde{x_0}, \frac{1}{\lambda_0})$, $x_0' \sim \mathcal{N}(\tilde{x_0'}, \frac{1}{\lambda_0})$, and parameters Δ and ϕ require that $|\tilde{x}_0 - \tilde{x}_0'| \leq (1 - \phi)\Delta$.

This allows us to derive the privacy guarantee for the process x_t as follows.

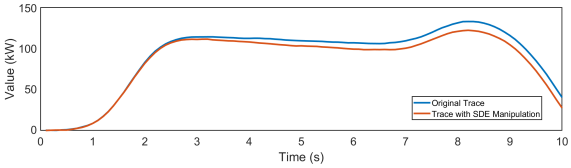

Fig. 4: Low resolution sample data comparison

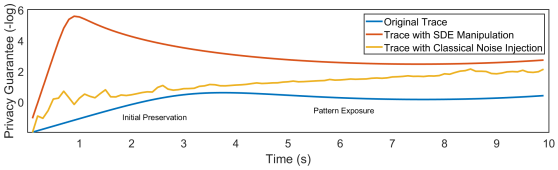

Fig. 5: Privacy guarantee comparison

Lemma 2. *For SDE process x_t specified by Eq. (12), given two states D, D', total budget Δ, assignment ϕ and sensitivity budget $S_g(t)$ with $\|S_g(t)\|_2 \leq \phi\Delta$, x_t satisfies $(\alpha, \frac{\alpha(1-\phi)^2\delta^2\lambda_0}{2}\eta_I + \frac{\alpha\phi^2\delta^2\beta^2}{2\lambda_0 e^{-4C\beta}}(1 - \eta_P))$ RDP, where η_I and η_P reflect the initial and pattern information exposure respectively, with the following closed form characterizations:*

$$\eta_I = e^{-2\frac{\lambda_0}{\beta}te^{-4C\beta}},$$
$$\eta_P = e^{-\frac{\lambda_0}{\beta}(t-1)e^{-4C\beta}} - e^{\frac{\lambda_0}{\beta}(1-2t)e^{-4C\beta}} + e^{-2\frac{\lambda_0}{\beta}te^{-4C\beta}}.$$

Remark: Note that the initial information preservation decays at the rate of order $O(\Delta^2 e^{-t})$ and the pattern information preservation decays at the rate of order $O(\Delta^2(1 - e^{-t}))$. This implies that the initial information can be protected more easily because of the noise process whereas the pattern information can only be protected by utilizing the sensitivity budget. These findings are consistent with our intuition.

If we utilize the strong convexity of $V_n(x_t)$, we can further obtain stronger privacy preservation as follows:

Theorem 2. *For the SDE process x_t specified by Eq. (12) with λ^*-strongly convex $V_n(x_t)$, that is, $\beta\lambda^* \leq \lambda_0$ as in Eq. (15), given two internal states D, D', total budget Δ, assignment ϕ and sensitivity budget $S_g(t)$ with $\|S_g(t)\|_2 \leq \phi\Delta$, x_t satisfies $(\alpha, \frac{\alpha(1-\phi)^2\delta^2\lambda_0}{2}\eta_I^* + \frac{\alpha\beta\phi^2\delta^2}{\lambda^*}(1 - \eta_P^*))$ RDP, where η_I^* and η_P^* reflect the initial and pattern information exposure respectively, with the following closed form characterizations:*

$$\eta_I^* = e^{-\lambda^* t},$$
$$\eta_P^* = e^{-\frac{\lambda^*(t-1)}{2}} - e^{\frac{\lambda^*(1-2t)}{2}} + e^{-\lambda^* t}.$$

Example: We use load profiling to explain our mechanism for low resolution data. Fig. 4 shows the sample load profiles before and after privacy preservation. However, the two profiles look considerably similar. Fig. 5 shows that both profiles share different privacy preserving levels. Owing to the inherent noise, the original profile enjoys some privacy (blue line in Fig. 5), whereas with slight noise, our mechanism achieves a higher privacy preserving level (orange line in Fig. 5). However, the privacy preserving level decreases over time. The comparison of these results with those of the classical Gaussian mechanism (yellow line in Fig. 5) with injected noise of the same magnitude indicates that our mechanism always

preserves more privacy. This demonstrates the effectiveness of our mechanism for low resolution data.

B. Mechanism Implementation

We consider a simplified setting wherein the time series data directly represent state D (e.g., the load profile of each household). We aim to protect D, where $D \in \mathbb{R}^T$ and $T < \infty$. To implement our mechanism, we need to construct $g(D,t)$.

Here, the key difficulty is that $g(D,t)$ is a continuous function and D is a discrete dataset. One approach is to require $g(D,t) = y_{t+1} - y_t$, for discrete $t = 1, ..., T-1$, and then conduct interpolation with T anchors as $g(D,t)$.

For the neighboring datasets D and D', we need to guarantee $|g(D,t) - g(D',t)| \leq S_g(t)$. Hence, the next task is to construct a continuous $S_g(t)$. We define

$$S_g^{\#}(t) := |y_{t+1} - y_t - y'_{t+1} + y'_t|, \tag{17}$$

and we require $S_g(t) = S_g^{\#}(t)$, for discrete $t = 1, ..., T$. We can follow the same routine as that for constructing $g(D,t)$. The key difference is that when constructing $S_g(t)$, we must further guarantee the first and second order smoothness. In addition, we need to guarantee sensitivity consistency by requiring $\int_t^{t+1} S_g^2(t)dt = S_g^{\#}(t)$. This can be achieved by interpolating $S_g(t)$ with the Bessel function or other functions with more than 7 parameters to satisfy the first and second order continuity at the boundary and the above integration condition. Algorithm 2 presents the process in detail.

Algorithm 2: $g(D,t)$ Construction

Input: The dataset $y_t \in D, t \in \{0, ..., T\}$;
The dataset $y'_t \in D', t \in \{0, ..., T\}$;
Output: The ODE $g(D,t), g(D',t)$ for $t \in [0, T]$;

1: Fit $g(D,t)$ with $g(D,t) = y_{t+1} - y_t$ for $t \in \{0, ..., T\}$.
2: Initialize the initial derivative and second-order derivative S_g^1, S_g^2;
3: Calculate the sensitivity budget $S_g^{\#}(t) = |y_{t+1} - y_t - y'_{t+1} + y'_t|, t \in \{0, ..., T\}$;
4: **for** $t \in \{1, .., T\}$ **do**
5: Using Bassel functions $S_g(t)$ to fit $[t, t+1)$ with $S_g(t) = S_g^{\#}(t)$; $S_g(t+1) = S_g^{\#}(t+1)$; $S'_g(t) = S_g^1$; $S''_g(t) = S_g^2$; $\int_t^{t+1} S_g^2(t)dt = S_g^{\#}(t)$
6: $S_g^1 = S'_g(t+1)$; $S_g^2 = S''_g(t+1)$
7: **end for**
8: $g(D',t) = g(D,t) + S_g(t)$
9: **return** $g(D,t); g(D',t)$

After constructing $g(D,t)$, we next construct the strongly convex function $V_n(x_t)$ following the same construction as indicated in Section III-B. With $g(D,t)$ and $V_n(x_t)$, we can complete SDE modeling for privacy preservation. Process y_t has the following property:

Corollary 2. *Induced by $g(D,t)$ constructed by Algorithm 2 and a λ^*-strong convex V_n, process y_t satisfies $(\alpha, \frac{\alpha\beta}{\lambda^*} \sum_{j=1}^{t-1} S_g^{\#}(j))$ RDP.*

Theorem 2 characterizes the privacy preserving property for each sample point. We can use the composition theorem in Proposition 3 to further obtain the privacy preserving property for time series data as follows:

Proposition 3. *For time series data $(x_1, .., x_T)$, if each x_t achieves (α, ϵ_t) RDP, then the sequence $(x_1, .., x_T)$ achieves $(\alpha, \sum_{t=1}^T \epsilon_t)$ RDP.*

V. Numerical Studies

In this section, we present the numerical studies used to highlight the effectiveness of the proposed noise injection method. We evaluate the performance of two classical consumer analysis tasks-NILM and load profiling in correspondence with high and low resolution cases.

A. Simulation Setup for High Resolution Data

We compared the identification accuracy of major NILM methods based on privacy preserved data using our mechanism, and NILM methods based on privacy preserved data using the classical noise injection method to evaluate the impact of our mechanism on NILM. We consider four major NILM methods: the sparse Viterbi algorithm for super-state HMM (Sparse-HMM) [52], recurrent neural network (RNN) [53], combinatorial optimization (CO) [54], and factorial hidden Markov model (FHMM) [55].

We used the widely adopted Redd dataset [40]. In our numerical study, we used the data for Building 1 in the dataset from 2011/04/18 21:22:13 to 2011/05/25 03:56:34 with a sampling rate of 3 Hz.

For all learning based methods, we divided the dataset for training (before 2011/04/30) and validation (after 2011/04/30). For SparseHMM algorithm, we followed the hyperparameters in the seminal Redd dataset numerical study reported in [52]. Specifically, the number of the maximal super states is set to 4; the state number choice parameter ϵ is set to 0.00021. For RNN, we followed the RNN structure reported in [53]. During training, we selected an initial learning rate of 0.01. The number of training epochs was set to 5 and the batch size was set to 128. For CO and FHMM, we adopted the classical settings in NILMTK [56].

B. Simulation Setup for Low Resolution Data

We used load profiling for residential consumers as an application example to evaluate the effectiveness of our mechanism for low resolution data. We adopted k-means clustering to conduct load profiling and studied how the injected noise may affect the clustering result. Further, we adopted clustering stability to measure these impacts. Clustering stability is defined as the probability that each consumer remains in its original cluster after privacy preservation [3]. We empirically calculated such a probability and demonstrated the effectiveness of our mechanism through comparison with the classical noise injection methods.

In this numerical study, we used the Pecan Street dataset [57], containing the load profile data of 1-minute resolution, collected from 400 users in Austin, Texas, from May 1 to October 30, 2015. We trimmed the dataset by removing all the data collected on August 9, 2015 because of missing data.

This article has been accepted for publication in IEEE Transactions on Smart Grid. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TSG.2022.3230685

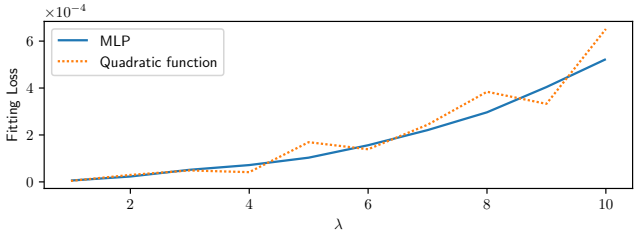

Fig. 6: Strong convex function estimation for NILM

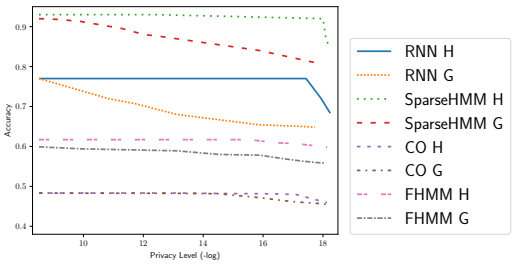

Fig. 7: Privacy preservation for high resolution data

We combined the daily load profiles of all users into a single daily load profile dataset (containing 2,048 valid load profiles in total) to better characterize the diverse user behaviors. Further, we aggregated the data to form a dataset of 30- minute resolution. Following [3], we set the number of clusters to 15, and we randomly chose 1,000 load profiles to verify cluster stability.

C. Performance Evaluation for High Resolution Data

We set sensitivity Δ to 1 and α to 2 as the benchmark for all privacy preserving mechanisms. Next, we introduce how to identify the random shock in practice for training purposes. In the simulation, when x_t is more than 3 times or less than $1/3$ of x_{t-1}, we consider time t as a shock. Further, it is important to determine the noise injection time length t_p because we do not need to inject noise during the period when no shock occurs. This time length can be determined by examining the reaction times of all appliances. In our simulation, we set t_p to 300 time slots. Furthermore, we set the step size for SDE discretization δ and proportion β to 0.001 and 0.01, respectively.

According to Theorem 1, we construct a strongly convex potential function to achieve privacy preservation.

We constructed the estimation following the routine presented in Section III-B. First, we normalized the data during the shock period. Then, we constructed a 4-layer MLP with three ReLU layers to estimate $\nabla V_\theta(x_t)$ using Algorithm 1. We constructed a simplified quadratic function corresponding to Eq. (9). We compare the estimation loss under different λ^* requirements and choose the optimal fitting, as shown in Fig. 6. Here, we use the quadratic form because it is simple and easy to calculate privacy preservation using a quadratic function. In addition, the privacy preservation level is directly reflected in the coefficient of the function.

Remark: The optimal fitting for the simplified quadratic loss function indeed outperforms the simple MLP. However, there is still room for improvement. For example, we can construct a function varying with λ and take the minimum of two forms (MLP and simplified quadratic function). The performance will be clearly better.

Based on the constructed $\nabla V_\theta(x_t)$, the results are shown in Fig. 7. We compared our privacy preserving mechanism with the classical noise injection mechanism. Further, we denote our mechanism as H and the classical mechanism as G. All the four NILM algorithms perform better when the data are protected by our mechanism. This implies that the effectiveness of NILM is less influenced by our mechanism, compared to that with conventional noise injection methods. This is true when the required privacy preserving level is not too high.

Moreover, different NILM methods have considerably diverse noise-resistance capabilities. Among the four methods, SparseHMM and RNN have higher accuracies but their performance drops rapidly with increasing privacy preserving requirements. This is large because of the utilization of temporal correlations in these two methods. Noise injection can cause cascading inference failure when utilizing temporal correlation. Further, although the performances of CO and FHMM are not as good as those of the other two methods, they exhibit higher robustness to both privacy preserving mechanisms.

The accuracy based on our mechanism decreases sharply beyond a certain privacy requirement (4×10^{-8}), which means our mechanism can no longer maintain the statistical structures of time series data when the required level of privacy preserving is too high. This is mainly attributed to our mechanism essentially being a biased noise injection mechanism. That is, it becomes increasingly impossible for the proposed mechanism to maintain the data around x_0 with an increasing privacy preserving level. In these cases, classical noise injection methods also significantly affect the accuracy of the NILM. Therefore, we can conclude that our proposed mechanism is very useful in most cases in terms of NILM because it can simultaneously guarantee the effectiveness of NILM and preserve the privacy of the original dataset. This is ideal when energy consumers seek advice from (untrusted) third parties to save energy.

D. Performance Evaluation for Low Resolution Data

We applied the proposed mechanism to the low resolution data. We followed the analytical framework in [3] and conducted the clustering for the original time series data. As mentioned in Theorem 5, we need to construct the internal dynamics ODE and noise SDE. The ODE reflects the pattern of the given time series data. After clustering, the center of the cluster reflects the characteristics of the data in its cluster. Therefore, it was used to model the ODE process. Then for the consumer data in each cluster, we constructed the noise generation SDE.

We followed the same process as in the high resolution cases. We construct a 4-layer MLP with three ReLU layers to estimate $\nabla V_\theta(x_t)$ based on Algorithm 1. Further, we

This article has been accepted for publication in IEEE Transactions on Smart Grid. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TSG.2022.3230685

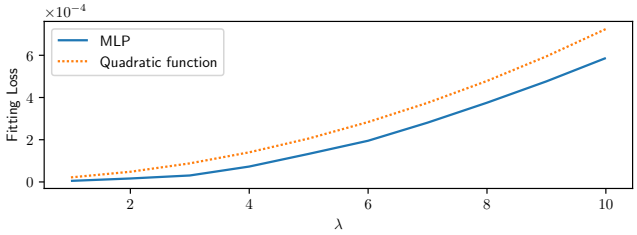

Fig. 8: Strongly convex function estimation for load profiling

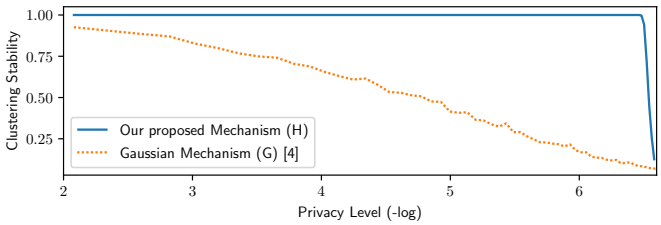

Fig. 9: Privacy preservation for low resolution data

constructed a quadratic function. The results in Fig. 8 indicate estimation loss with the increasing requirement of λ^*. We find that the improvement is not very significant because the performance for MLP is better than the quadratic function in this case. Therefore, we constructed the quadratic potential function for computational simplification.

We set the total privacy budget Δ to 1, and the assignment constant ϕ to 1. We adopted the same $S_g^{\#}$ value at each time t. The step size δ for the SDE dt discretization and parameter β were set to 0.001 and 0.009 respectively. We repeated the experiments for 1,000 times to derive a reliable estimation of clustering stability. Fig. 9 shows how clustering stability varies with the privacy level. Particularly, Fig. 9 compares the proposed mechanism and classical noise injection mechanisms. When the privacy preservation level is less than 0.0015, the clustering stability based on our mechanism is almost 1. In contrast, the classical mechanism gradually decreases clustering stability.

In addition, we observed the same phenomenon as in the high resolution data analysis. Our mechanism causes the clustering stability to drop sharply when the required privacy preserving level is beyond 0.0015. This is again attributed to the bias in our SDE modeling. Nonetheless, even in such cases, our mechanism outperforms the classical mechanism in terms of clustering stability.

VI. Conclusion

We designed a more effective privacy preserving mechanism. Specifically, we exploited the structure of time series data in the electricity sector, which consists of two parts: initial information and pattern information. Further, we identified that high resolution time series data often only consist of initial information, and hence its privacy preservation can be achieved by a time invariant SDE. In contrast, low resolution time series data often consist of both types of information, and therefore a time varying SDE is required to protect privacy. We designed the specific algorithms for both cases, proved their privacy preserving guarantee and then used a numerical study to verify our theoretical insights.

Our study can be extended in several ways. For example, time series data can be modeled as Lévy motion [58], which focuses on exploiting the non-Gaussian uncertainty in the time series data. It would be interesting to see if we can customize the privacy preserving mechanism based on this more general model. It is also essential to include more prior knowledge into our SDE modelling. To this end, (deep) probabilistic models and Bayesian graph frameworks can be employed to characterize the potential functions more accurately, hence offering better privacy preservation

Appendix

We first introduce the c-Log-Sobolev Inequality (c-LSI), which will be used frequently in the subsequent proofs.

Definition 6. *(c-Log-Sobolev Inequality) For random variable $\chi \in \mathbb{R}^d$, it satisfies logarithmic Sobolev inequality with parameter c, denoted by c-LSI, if for any function $f : \mathbb{R}^d \to \mathbb{R}$ with continuous ∇f and bounded $\mathbf{E}(f(\chi)^2)$, it holds that*

$$\begin{aligned}&\mathbf{E}[f(\chi)^2 \log f(\chi)^2] - \mathbf{E}[f(\chi)^2] \log \mathbf{E}[f(\chi)^2] \\ &\leq \frac{2}{c} E[\|\nabla f(\chi)\|]\end{aligned} \tag{18}$$

A. Proof for Lemma 1

First, we denote the SDE processes induced by the same $V(x_t)$ yet different initial random shocks x_0 and x_0' by x_t and x_t' respectively. The proof relies on the following lemma:

Lemma 3. *If the SDE process induced by $V(x_t)$ has an initial λ_0 and sensitivity Δ, and x_t' satisfies c-LSI, then x_t satisfies $(\alpha, \frac{\alpha\Delta\lambda_0}{2} e^{-2\frac{c}{\beta}t})$ RDP.*

Proof for Lemma 3: Consider the same V for two SDE processes with different initial points as those specified in Lemma 2 and 3 in [50]. Specifically, if c-LSI is satisfied, it holds that:

$$\frac{\partial R(\alpha,t)}{\partial t} \leq -2\frac{c}{\beta}\left[\frac{R(\alpha,t)}{\alpha} + (\alpha-1)\frac{\partial R(\alpha,t)}{\partial \alpha}\right], \tag{19}$$

where $R(\alpha,t)$ denotes $R_\alpha(p_t||p_t')$, with p_t and p_t' denoting pdfs for x_t and x_t'.

Next, based on Eq. (19), we know that

$$R(\alpha,t) \leq R(\alpha,0)e^{-2\frac{c}{\beta}t}. \tag{20}$$

By the definition of sensitivity Δ, we have,

$$R(\alpha,0) = \frac{\Delta\lambda_0}{2}. \tag{21}$$

This completes the proof for Lemma 3.

With Lemma 3, the remaining hurdle is proving that our process satisfies c-LSI. Without loss of generality, we assume the mean of x_0' to be 0.

This allows us to directly show $c = \lambda_0 e^{-4\beta C}$ in our theorem from Lemma 34 in [49], because the potential function V in SDE modeling satisfies all conditions in Lemma 34.

B. Proof for Theorem 1

The key is to study the case when $V(x_t')$ is λ^*-strongly convex. Since we require $\beta\lambda^* \geq \lambda_0$, then $V(x_t')$ is $\frac{\lambda_0}{\beta}$-strongly convex. Thus, x_t' satisfies $\frac{\lambda_0}{2}$-LSI according to Lemma 7 in [50]. Furthermore, it must satisfy $\frac{\beta\lambda^*}{2}$-LSI by definition of c-LSI. Finally, setting $c = \frac{\beta\lambda^*}{2}$ completes our proof.

C. Proof for Corollary 1

We need to divide the $\mathcal{H}(x)$ into k pieces to conduct the integration. Then for piece $[\frac{i}{k}x_t, \frac{i+1}{k}x_t)$, it holds that for any $x \in [\frac{i}{k}x_t, \frac{i+1}{k}x_t)$,

$$\left|\mathcal{H}(x) - \mathcal{H}\left(\frac{i}{k}x_t\right)\right| \leq L\left|x - \frac{i}{k}x_t\right| \leq L\frac{x_t}{k}. \tag{22}$$

Thus, we have

$$\begin{aligned}&\left|\int_{\frac{i}{k}x_t}^{\frac{i+1}{k}x_t} \mathcal{H}(x)dx - \frac{x_t}{k}\mathcal{H}\left(\frac{i}{k}x_t\right)\right| \\ &\leq \int_{\frac{i}{k}x_t}^{\frac{i+1}{k}x_t}\left|\mathcal{H}(x) - \mathcal{H}\left(\frac{i}{k}x_t\right)\right|dx = L\left(\frac{x_t}{k}\right)^2,\end{aligned} \tag{23}$$

Therefore we can conclude that the approximation error is at the order of $O(\frac{Lx_t^2}{k})$.

D. Proof for Proposition 2

Assume that the time series data can be represented as $x_t = x_0 + n(x_t, t)$, where x_0 denotes the shock and $n(x_t, t)$ represents the internal random noise. This inspires us to consider the process $r_t = x_t^* - x_0$, where x_t^* represents the time series with a constructed strongly convex V. Our proof relies on the following lemma:

Lemma 4. *(Theorem 9 in [42]) If we fix the transition probabilities $P(Y|X)$ in a Markov chain $X \to Y$, then $R_\alpha(P_Y||Q_Y) \leq R_\alpha(P_X||Q_X)$ for any $\alpha \in [0, \infty]$, where P_Y, Q_Y denote two probability measures for Y and P_X, Q_X denote those for X.*

In our problem, we can construct the Markov chain: $x_0 \to x_t^0 \to x_t^1$ where $x_t^0 = x_0 + r_t$ and $x_t^1 = x_t^0 + n(x_t, t)$. Further, we denote neighbor shock x_0', which yields $x_t^{0'}$ and $x_t^{1'}$. Subsequently, based on Lemma 4 we show that

$$R_\alpha(x_t^1||x_t^{1'}) \leq R_\alpha(x_t^0||x_t^{0'}). \tag{24}$$

E. Proof for Lemma 2

First, we denote the SDE processes induced by different internal states D and D' and different initial random shocks x_0 and x_0' by x_t and x_t' respectively.

Lemma 5. *For $\alpha > 1$, if the probability density ratio for x_t and x_t' is continuous and bounded, then the following inequality holds*

$$\begin{aligned}&R(\alpha, t) + \alpha(\alpha-1)\frac{\partial R(\alpha,t)}{\partial\alpha} \\ &\leq \frac{\alpha\beta}{c}\left(\frac{\alpha\beta S_g^2}{2} - \frac{\partial R_\alpha(p_t||p_t')}{\partial t}\right)\end{aligned} \tag{25}$$

if and only if x_t' satisfies c-LSI.

Lemmas can be proved by following the proofs of Lemma 2 and 3 in [50]. Specifically, we can directly replace $V(t, x_t)$ with $V_t(\theta)$ and replace $V'(t, x_t)$ with $V_t'(\theta)$ in [50].

Lemma 6. *If the SDE process x_t has a potential function $V(x_t, t)$, λ_0, sensitivity Δ, and neighbor process x_t' satisfies c-LSI, then x_t satisfies $(\alpha, \frac{\alpha(1-\phi)^2\delta^2\lambda_0}{2}\eta_I + \frac{\alpha\beta^2\phi^2\Delta^2}{2c}(1-\eta_P))$ RDP, where η_I and η_P reflect the initial and pattern information exposure respectively, with the following closed form characterizations:*

$$\begin{aligned}\eta_I &= e^{-2\frac{c}{\beta}t}, \\ \eta_P &= e^{-\frac{c}{\beta}(t-1)} - e^{\frac{c}{\beta}(1-2t)} + e^{-2\frac{c}{\beta}t}.\end{aligned}$$

Proof for Lemma 6: According to Lemma 5, if c-LSI is satisfied, we know that the following PDE holds

$$\begin{aligned}&\frac{\partial R(\alpha,t)}{\partial t} \\ &\leq \frac{\alpha\beta S_g^2(t)}{2} - \frac{c}{\beta}\left[\frac{R(\alpha,t)}{\alpha} + (\alpha-1)\frac{\partial R(\alpha,t)}{\partial\alpha}\right]\end{aligned} \tag{26}$$

Solving this PDE with the initial condition yields:

$$R(\alpha, 0) = \frac{\Delta\lambda_0}{2}, \tag{27}$$

which completes the proof.

Based on Lemma 6, we need to show that x_t' satisfies c-LSI by induction to prove Lemma 2.

To this end, we decouple x_t' into two processes, the noise process in Eq. (14) and the dynamics of Eq. (13). We know $dx_t = dy_t + dn_t$ and $dx_t' = dy_t' + dn_t'$ for the neighbor process. First, we assume the distribution at time t by p_t^0. Then the noise dn_t' changes the distribution, which yields the distribution p_t^1. Note that the potential function of dn_t' is temporally independent.

We assume p_t^0 satisfies c-LSI, and set c to be $\lambda_0 e^{-4\beta C}$.

Note that the process for n_t is a standard Smoluchowski dynamics. Lemma 33 in [49] implies with our V_n''s form, the steady distribution for SDE when $t \to \infty$ satisfies c-LSI. Then using Lemma 34 in [49] and the induction assumption, we know that p_t^1 also satisfies c-LSI.

Next, we examine dy_t' to derive $p_{t+\delta}^0$. We know dy_t' is a 1-Lipschitz transformation because $g(D', t)$ is deterministic at time t. Thus, Lemma 8 in [50] implies that for time $t+\delta$ $p_{t+\delta}^0$ also satisfies c-LSI.

Finally, we have already guaranteed that our distribution satisfies c-LSI. Therefore, the whole mathematical induction holds. By substituting $c = \lambda_0 e^{-4\beta C}$ in Lemma 6, we complete the proof.

F. Proof for Theorem 2

The proof follows the same routine as that for Lemma 2. The only difference is that the parameter c is now $\frac{\beta\lambda^*}{2}$, instead of $\lambda_0 e^{-4\beta C}$. For more details of the proof, please see Lemma 5, 8 and 9 in [50].

G. Proof for Corollary 2

First, in this case $\phi = 1$ since no information leakage will occur when $t = 0$. Then, for period $[j, j+1)$,

$$\frac{\alpha\beta}{2}\int_{j}^{j+1} e^{\frac{\lambda^*(\xi-t)}{2}} S_g^2(\xi)d\xi \leq \frac{\alpha\beta}{2}\int_{j}^{j+1} S_g^2(j)d\xi = \frac{\alpha\beta}{\lambda^*}S_g^{\#}(j). \tag{28}$$

The inequality holds since $e^{\lambda^*(\xi-t)} \leq 1$, $\forall \lambda^* > 0$, $t > \xi$.

H. Hyperparameters and Network Settings

In this section, we state the choice of our hyperparameters and provide the network structures. The choice of α will not influence any result of our privacy, it is just provided for calculation and representation convenience. The choice of sensitivity Δ is also because we scale all the data to $[0, 1]$ by dividing the maximal for calculation convenience and the sensitivity will not be larger than 1. The SDE discretization δ and proportion β is chosen from the list $[0.001, 0.01, 0.1, 1]$ and we choose the ones with the best accuracy/stability and the highest privacy guarantee. In practice, it can be chosen by the hyperparameter search with historical data. Then as for the network structure of our MLP, it has a width of 4,8,4,1 with standard RELU activation functions. At the final layer, we clamp the output lower than λ^* to guarantee the strong convexity.

I. More Comparison with Other Mechanisms

To highlight the efficiency of our proposed mechanism, we compare it with three state-of-the-art mechanisms, including the smooth Gaussian mechanism [20], directly injecting noise at the outputs of data analytic tasks ('inject at output' in short), and differentially privacy generative adversarial network (PPGAN) [59]. We also implement the classical Gaussian mechanism as the basic benchmark. Hence, altogether we generate five datasets for the data analytic tasks, i.e., NILM for high-resolution data (specifically, we implement the SparseMM method to conduct NILM) and user profiling for low-resolution data. Specifically, to examine the privacy-performance trade-off, we compare NILM accuracy and clustering stability with the privacy guarantee on the five kinds of generated datasets. We also compare the norm of injected noise to show the energy efficiency for the five mechanisms, as injected noise is often generated by storage systems. In addition, we compare the running time for the five mechanisms to generate the data.

Next, we explain the hyperparameter settings. For the smooth Gaussian mechanisms, we use the Savitzky–Golay filter [60] with a window size of 9 and order of 3. For PPGAN, we choose 100 as the dimension for the noise input to GAN, which is consistent with other GAN implementations. Specifically, we adopt 3 layers MLP with leaky ReLUs' activation for the generator network in GAN. We choose 4 layers MLP with leaky ReLUs and dropouts for the discriminator network in GAN. We employ the Adam optimizer with privacy-preserving noise injected. The learning rate is set to 0.002, and the batch size is set to 128.

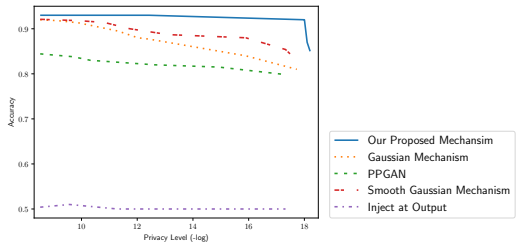

Fig. 10: The privacy-performance comparison for different privacy mechanisms for high resolution data

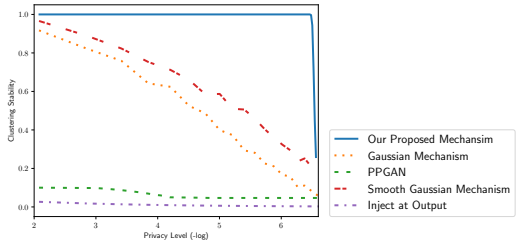

Fig. 11: The privacy-performance comparison for different privacy mechanisms for low resolution data

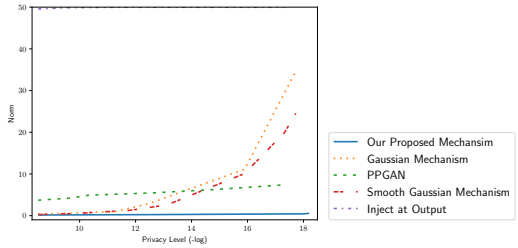

Fig. 12: The energy consumption comparison for different privacy mechanisms for high resolution data

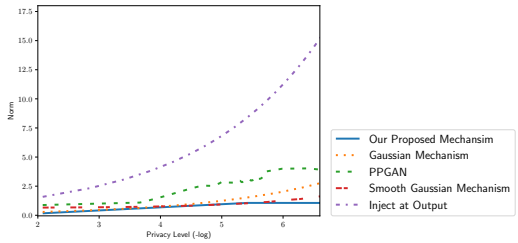

Fig. 13: The energy consumption comparison for different privacy mechanisms for low resolution data

Fig. 10 compares the privacy-performance trade-off for NILM based on high-resolution data. We can conclude that our proposed mechanism achieves the best performance in terms of NILM accuracy. The 'inject at output' method has the worst performance because it directly manipulates the final results. We also observe that the smooth Gaussian indeed outperforms the classic Gaussian mechanism. The synthetic data generated by PPGAN fail to catch the original data's inherent features, yielding non-favorable performance. Fig. 11 compares the privacy-performance trade-off for user profiling based on low-resolution data analysis. We observe similar patterns. Specifically, PPGAN again fails to generate useful

data. This implies that manipulating the model parameters may seriously deteriorate the performance of subsequent data analytic tasks. Our mechanism again achieves the best stability.

Furthermore, we study the noise injection's norm to show our proposed mechanism's energy efficiency. For the case study based on high-resolution data, Fig. 12 shows that the noise injected by our mechanism achieves the minimal norm. The advantage of our mechanism is particularly clear when the privacy requirement is high. For the case study based on low-resolution data, Fig. 13 shows that our mechanism achieves the smallest cost, though the two Gaussian mechanisms also achieve similar costs. As for the running time comparison, besides PPGAN, all the other mechanisms perform rather well, taking less than 1 ms. In contrast, the training process of PPGAN already costs more than 15s. In summary, compared with state-of-the-art mechanisms, our proposed mechanism achieves the best performance in terms of privacy-performance trade-off, energy consumption, and running time.

REFERENCES

[1] M. Fell, H. Kennard, G. Huebner, M. Nicolson, S. Elam, and D. Shipworth, "Energising health: A review of the health and care applications of smart meter data," *London, UK: SMART Energy GB*, 2017.

[2] J. R. Herrero, Á. L. Murciego, A. L. Barriuso, D. H. de La Iglesia, G. V. González, J. M. C. Rodríguez, and R. Carreira, "Non intrusive load monitoring (nilm): A state of the art," in *International Conference on Practical Applications of Agents and Multi-Agent Systems*, pp. 125–138, Springer, 2017.

[3] H. Wang, X. Luo, and C. Wu, "Differential privacy in consumer behavior analysis," in *2021 IEEE Power & Energy Society General Meeting (PESGM), Washington, DC, USA*, pp. 1–5, 2021.

[4] G. W. Hart, "Residential energy monitoring and computerized surveillance via utility power flows," *IEEE Technology and Society Magazine*, vol. 8, no. 2, pp. 12–16, 1989.

[5] A. Ruano, A. Hernandez, J. Ureña, M. Ruano, and J. Garcia, "Nilm techniques for intelligent home energy management and ambient assisted living: A review," *Energies*, vol. 12, no. 11, p. 2203, 2019.

[6] A. Capozzoli, M. S. Piscitelli, and S. Brandi, "Mining typical load profiles in buildings to support energy management in the smart city context," *Energy Procedia*, vol. 134, pp. 865–874, 2017.

[7] S. Lin, F. Li, E. Tian, Y. Fu, and D. Li, "Clustering load profiles for demand response applications," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 1599–1607, 2017.

[8] Y. Wang, Q. Chen, T. Hong, and C. Kang, "Review of smart meter data analytics: Applications, methodologies, and challenges," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3125–3148, 2018.

[9] Y. Duan and J. Canny, "Practical distributed privacy-preserving data analysis at large scale," *Large-Scale Data Analytics*, pp. 219–252, 2014.

[10] F. D. Garcia and B. Jacobs, "Privacy-friendly energy-metering via homomorphic encryption," in *The 6th International Workshop on Security and Trust Management, Copenhagen, Denmark*, pp. 226–238, 2010.

[11] L. Zhang, J. Ren, Y. Mu, and B. Wang, "Privacy-preserving multi-authority attribute-based data sharing framework for smart grid," *IEEE Access*, vol. 8, pp. 23294–23307, 2020.

[12] M. A. Mustafa, S. Cleemput, A. Aly, and A. Abidin, "A secure and privacy-preserving protocol for smart metering operational data collection," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6481–6490, 2019.

[13] Z. Guan, Y. Zhang, L. Zhu, L. Wu, and S. Yu, "Effect: An efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid," *Science China Information Sciences*, vol. 62, no. 3, pp. 1–14, 2019.

[14] D. Gabay, K. Akkaya, and M. Cebe, "Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5760–5772, 2020.

[15] A. Taïk and S. Cherkaoui, "Electrical load forecasting using edge computing and federated learning," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland*, pp. 1–6, 2020.

[16] M. Savi, C. Rottondi, and G. Verticale, "Evaluation of the precision-privacy tradeoff of data perturbation for smart metering," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2409–2416, 2015.

[17] Z. Zhang, W. Cao, Z. Qin, L. Zhu, Z. Yu, and K. Ren, "When privacy meets economics: Enabling differentially-private battery-supported meter reporting in smart grid," in *2017 IEEE/ACM 25th International Symposium on Quality of Service (IWQoS), Vilanova i la Geltrú, Spain*, pp. 1–9, 2017.

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

[19] 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 Transactions on Smart Grid*, vol. 8, no. 2, pp. 619–626, 2016.

[20] G. Eibl and D. Engel, "Differential privacy for real smart metering data," *Computer Science-Research and Development*, vol. 32, no. 1, pp. 173–182, 2017.

[21] F. Leukam Lako, P. Lajoie-Mazenc, M. Laurent, and C. Vorakulpipat, "Privacy-preserving publication of time-series data in smart grid," *Security and Communication Networks*, vol. 2021, p. 21, 2021.

[22] D. Syed, S. S. Refaat, and O. Bouhali, "Privacy preservation of data-driven models in smart grids using homomorphic encryption," *Information*, vol. 11, no. 7, p. 357, 2020.

[23] N. Papernot, S. Song, I. Mironov, A. Raghunathan, K. Talwar, and Ú. Erlingsson, "Scalable private learning with PATE," in *6th International Conference on Learning Representations, ICLR 2018, Vancouver, BC, Canada*, 2018.

[24] Z. Lv, L. Wang, Z. Guan, J. Wu, X. Du, H. Zhao, and M. Guizani, "An optimizing and differentially private clustering algorithm for mixed data in sdn-based smart grid," *IEEE Access*, vol. 7, pp. 45773–45782, 2019.

[25] L. Mitridati, E. Romei, G. Hug, and F. Fioretto, "Differentially-private heat and electricity markets coordination," *arXiv preprint arXiv:2201.10634*, 2022.

[26] K. Khan, A. Kasis, M. M. Polycarpou, and S. Timotheou, "Privacy of distributed optimality schemes in power networks," *arXiv preprint arXiv:2201.10221*, 2022.

[27] F. Fioretto, T. W. Mak, and P. Van Hentenryck, "Differential privacy for power grid obfuscation," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 1356–1366, 2019.

[28] R. R. Avula, T. J. Oechtering, and D. Månsson, "Privacy-preserving smart meter control strategy including energy storage losses," in *2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Sarajevo, Bosnia and Herzegovina*, pp. 1–6, 2018.

[29] M. Shateri, F. Messina, P. Piantanida, and F. Labeau, "Privacy-cost management in smart meters with mutual-information-based reinforcement learning," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22389–22398, 2022.

[30] R. Pal, P. Hui, and V. Prasanna, "Privacy engineering for the smart micro-grid," *IEEE Transactions on Knowledge and Data Engineering*, vol. 31, no. 5, pp. 965–980, 2018.

[31] J. P. Bishwal, *Parameter estimation in stochastic differential equations*. Springer, 2007.

[32] N. H. Bingham and B. Dunham, "Estimating diffusion coefficients from count data: Einstein-smoluchowski theory revisited," *Annals of the Institute of Statistical Mathematics*, vol. 49, no. 4, pp. 667–679, 1997.

[33] P.-H. Chavanis, "The generalized stochastic smoluchowski equation," *Entropy*, vol. 21, no. 10, p. 1006, 2019.

[34] H. Verdejo, A. Awerkin, E. Saavedra, W. Kliemann, and L. Vargas, "Stochastic modeling to represent wind power generation and demand in electric power system based on real data," *Applied Energy*, vol. 173, pp. 283–295, 2016.

[35] F. Sossan, V. Lakshmanan, G. T. Costanzo, M. Marinelli, P. J. Douglass, and H. Bindner, "Grey-box modelling of a household refrigeration unit using time series data in application to demand side management," *Sustainable Energy, Grids and Networks*, vol. 5, pp. 1–12, 2016.

[36] R. Weron and A. Misiorek, "Forecasting spot electricity prices: A comparison of parametric and semiparametric time series models," *International journal of forecasting*, vol. 24, no. 4, pp. 744–763, 2008.

[37] H. Wang, J. Zhang, C. Lu, and C. Wu, "Privacy preserving in non-intrusive load monitoring: A differential privacy perspective," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2529–2543, 2020.

[38] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE security & privacy*, vol. 7, no. 3, pp. 75–77, 2009.

[39] G. A. Pavliotis, *Stochastic processes and applications: diffusion processes, the Fokker-Planck and Langevin equations*, vol. 60. Springer, 2014.

[40] J. Z. Kolter and M. J. Johnson, "Redd: A public data set for energy disaggregation research," in *Workshop on data mining applications in sustainability (SIGKDD), San Diego, CA, USA*, vol. 25, pp. 59–62, 2011.

[41] J. Kelly and W. Knottenbelt, "The UK-DALE dataset, domestic appliance-level electricity demand and whole-house demand from five UK homes," *Scientific Data*, vol. 2, no. 150007, 2015.

[42] T. Van Erven and P. Harremos, "Rényi divergence and kullback-leibler divergence," *IEEE Transactions on Information Theory*, vol. 60, no. 7, pp. 3797–3820, 2014.

[43] I. Mironov, "Rényi differential privacy," in *2017 IEEE 30th Computer Security Foundations Symposium (CSF), Santa Barbara, CA, USA*, pp. 263–275, 2017.

[44] C. Dwork, "Differential privacy: A survey of results," in *Theory and Applications of Models of Computation*, pp. 1–19, Springer Berlin Heidelberg, 2008.

[45] C. Dwork, A. Roth, *et al.*, "The algorithmic foundations of differential privacy," *Foundations and Trends® in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2014.

[46] R. Gopinath, M. Kumar, C. P. C. Joshua, and K. Srinivas, "Energy management using non-intrusive load monitoring techniques–state-of-the-art and future research directions," *Sustainable Cities and Society*, vol. 62, p. 102411, 2020.

[47] F. Zhang, L. Qu, W. Dong, H. Zou, Q. Guo, and Y. Kong, "A novel nilm event detection algorithm based on different frequency scales," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–11, 2022.

[48] D. Bakry, I. Gentil, M. Ledoux, *et al.*, *Analysis and geometry of Markov diffusion operators*, vol. 103. Springer, 2014.

[49] J. Li, X. Luo, and M. Qiao, "On generalization error bounds of noisy gradient methods for non-convex learning," in *8th International Conference on Learning Representations, ICLR 2020, Addis Ababa, Ethiopia*, 2020.

[50] R. Chourasia, J. Ye, and R. Shokri, "Differential privacy dynamics of langevin diffusion and noisy gradient descent," in *Advances in Neural Information Processing Systems 34: Annual Conference on Neural Information Processing Systems 2021, NeurIPS 2021, virtual*, pp. 14771–14781, 2021.

[51] M. Fazlyab, A. Robey, H. Hassani, M. Morari, and G. J. Pappas, "Efficient and accurate estimation of lipschitz constants for deep neural networks," in *Advances in Neural Information Processing Systems 32: Annual Conference on Neural Information Processing Systems 2019, NeurIPS 2019, Vancouver, BC, Canada*, pp. 11423–11434, 2019.

[52] S. Makonin, F. Popowich, I. V. Bajic, B. Gill, and L. Bartram, "Exploiting hmm sparsity to perform online real-time nonintrusive load monitoring," *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2575–2585, 2016.

[53] J. Kelly and W. Knottenbelt, "Neural nilm: Deep neural networks applied to energy disaggregation," in *the 2nd ACM International Conference on Embedded Systems for Energy-Efficient Built Environments, Seoul, South Korea*, p. 55–64, 2015.

[54] M. Z. A. Bhotto, S. Makonin, and I. V. Bajic, "Load disaggregation based on aided linear integer programming," *IEEE Transactions on Circuits and Systems Ii-express Briefs*, vol. 64, no. 7, pp. 792–796, 2017.

[55] H. Kim, M. Marwah, M. Arlitt, G. Lyon, and J. Han, "Unsupervised disaggregation of low frequency power measurements," in *the 2011 SIAM International Conference on Data Mining, Mesa, Arizona, USA*, pp. 747–758, 2011.

[56] N. Batra, J. Kelly, O. Parson, H. Dutta, W. Knottenbelt, A. Rogers, A. Singh, and M. Srivastava, "Nilmtk: an open source toolkit for non-intrusive load monitoring," in *the 5th international conference on Future energy systems, Cambridge, United Kingdom*, pp. 265–276, 2014.

[57] Pecan Street INC., "Pecan street data." http://www.pecanstreet.org, accessed in Dec. 2022.

[58] G. Samorodnitsky, M. S. Taqqu, and R. Linde, "Stable non-gaussian random processes: stochastic models with infinite variance," *Bulletin of the London Mathematical Society*, vol. 28, no. 134, pp. 554–555, 1996.

[59] L. Xie, K. Lin, S. Wang, F. Wang, and J. Zhou, "Differentially private generative adversarial network," *arXiv preprint arXiv:1802.06739*, 2018.

[60] P. G. Guest and P. G. Guest, *Numerical methods of curve fitting*. Cambridge University Press, 2012.

Haoxiang Wang (Graduate Student Member, IEEE) is a Ph.D student at the department of Automation, Tsinghua University, advised by Professor Hui Qiao. Mr. Wang received his master's degree in Computer Science from the Institute for Interdisciplinary Information Sciences (IIIS), Tsinghua University, advised by Professor. Chenye Wu, in 2022. Mr. Wang received his bachelor's degree from the Department of Energy and Power Engineering, Tsinghua University, in 2019. He has been awarded Excellent Comprehensive Scholarship of Tsinghua University in 2018.

Currently, he is working on privacy preservation and algorithm robustness in power systems.

Chenye Wu (Member, IEEE) is an Assistant Professor and the Presidential Young Fellow at the School of Science and Engineering, The Chinese University of Hong Kong, Shenzhen. Before joining CUHK Shenzhen, he was an Assistant Professor at IIIS, Tsinghua University. He worked at ETH Zurich as a Research Scientist, working with Professor Gabriela Hug, in 2016. Before that, Professor Kameshwar Poolla and Professor Pravin Varaiya hosted Dr. Wu as a postdoctoral researcher at UC Berkeley for two years. In 2013-2014, He spent one year at Carnegie Mellon University as a postdoc fellow, hosted by Professor Gabriela Hug and Professor Soummya Kar.

Dr. Wu received his Ph.D. in Computer Science from IIIS, Tsinghua University, in July 2013. His Ph.D. advisor is Professor Andrew Yao, the laureate of the A.M. Turing Award in the year of 2000. Dr. Wu was the best paper award co-recipients of IEEE SmartGridComm 2012, IEEE PES General Meeting 2013, IEEE PES General Meeting 2020. Currently, he is working on economic analysis, optimal control and operation of power systems.