Privacy-Preserving and Approximately Truthful Local Electricity Markets: A Differentially Private VCG Mechanism

Milad Hoseinpour, *Student Member, IEEE*, Mohammad Hoseinpour, Mahdi Haghifam, *Member, IEEE*, Mahmoud-Reza Haghifam, *Senior Member, IEEE*

***Abstract*—Privacy-aware market participants care about the leakage of their private information via statistical releases of local electricity markets outputs. This kind of privacy breach would have major implications on the future transactions of the market participants and unauthorized observers' beliefs about them. To address this challenge, we introduce the notion of noisy electricity markets in the framework of Differential Privacy (DP) for preserving the privacy of individuals and maintaining the utility of their data for social good. In this regard, this paper proposes a novel differentially private mechanism for local electricity markets that releases a near-optimal solution while guarantying the outputs of the market would reveal almost nothing about any individual's input data. To do so, we implement the exponential mechanism for privatizing the baseline Vickrey–Clarke–Groves (VCG) mechanism in the proposed local electricity market. Moreover, we provide an upper-bound on the social welfare loss incurred by the privacy constraint and analyze the inherent trade-off between the privacy and suboptimality. In the end, numerical case studies for reflecting the theoretical properties of the proposed mechanism are provided.**

***Index Terms*—Differential privacy, local electricity market, privacy-aware agent, mechanism design.**

I. Introduction

THE recent decarbonization, decentralization, and digitalization of power systems have paved the way for the advent of local electricity markets [1], [2]. The emerging electricity markets are an abundant source of individuals' data, such as financial data and electricity transactions [3]. Publicly releasing these data and giving access to researchers, business owners, policymakers, etc., brings a multitude of economic as well as technical and societal benefits. However, these rich and fine-grained datasets could expose individuals to a privacy breach and reveal sensitive information about them that may result in noticeably undesired outcomes, which are not likely otherwise [4]. For instance, electricity transactions in the market could reveal the consumption patterns of the market participants that can be used for behavioral surveillance and hyper-personalization by marketing agencies [5]. Therefore, the privacy concern can motivate the market participants to behave strategically by misreporting their data or even opt out of the market. Moreover, data privacy laws, e.g., the General Data Protection Regulation (GDPR) passed by the European Union, impose legal obligations on local electricity markets to safeguard the private information of individuals participating in the market [6].

As a result, the privacy challenge in local electricity markets is to balance the value of sharing the data and the risk of compromising the privacy of individuals. In this regard, the central question motivating this paper is how to give trusted market operators unrestricted access to individuals' data and permit them to safely publish the market-clearing outputs. To address this challenge, this paper aims to design a local electricity market that simultaneously guarantees a rigorous privacy constraint, maintains data utility for statistical inference, and achieves near-optimal social welfare. The proposed privacy-preserving local electricity market is in a centralized setting, where privacy-aware market participants report their private information to a trustworthy market operator who runs the market. In addition, the VCG mechanism is adopted as the pricing rule of the market.

To achieve our privacy goal, we implement the notion of DP, which gives us a framework to quantitatively reason about privacy. DP is a rigorous privacy notion used to bound the disclosure risk of the private information associated with an individual's participation in a computation [7]. By embedding carefully calibrated random noise in a computation, DP guarantees that the noisy outputs do not disclose the private information of individuals in the input data. Differentially private computations typically offer a trade-off between the level of individuals' privacy in a dataset and the accuracy of the computation on that dataset [8]. DP has several important properties, including immunity to post-processing and composition [9]. Furthermore, DP is the de-facto standard for privacy protection. In fact, other privacy-preserving approaches, e.g., data anonymization and k-anonymity, are fragile under appropriate side information, while DP makes no assumptions about an adversary's computational power or side information [10].

A. Related Work

The cryptographic literature addresses the privacy concerns in electricity markets. For instance, in [11], a decentralized privacy-preserving protocol based on secure Multi-Party Computation (MPC) is proposed for local electricity markets. The proposed model performs the bid selection and calculation of the market-clearing price in a data oblivious and secure manner. For addressing the security issues in transactive energy

Milad Hoseinpour and Mahmoud-Reza Haghifam are with Tarbiat Modares University, Tehran, Iran. Mohammad Hoseinpour is with Babol Noshirvani University of Technology, Babol, Iran. Mahdi Haghifam is with University of Toronto, Toronto, Canada.

systems, a cryptography-based implementation framework is proposed in [12]. Under the proposed framework, the market participants' bidding information is kept private throughout the market-based interactions by an enhanced Paillier encryption scheme. In addition, the proposed model is robust to any extraneous data injection attack. In [13], a secure double auction mechanism is proposed for smart grids. To protect the market participants anonymity and privacy, a pseudo-identity is assigned to each participant, and their bids are encrypted using a cryptosystem. A privacy-preserving Peer-to-Peer (P2P) energy trading platform is proposed in [14]. The private information of market participants, including sellers' price and buyers' demand, are encrypted based on homomorphic encryption cryptosystem. However, our paper fundamentally differs from these papers. Indeed, the overarching goal of our paper is to safely promote public access to electricity markets outputs, whereas the goal of cryptographic realization of privacy-preserving electricity markets is to hide all information except for running the market-clearing mechanism. More precisely, cryptography solves the data security problem by using encryption algorithms and preventing unauthorized access to individuals' sensitive data [15].

In another line of research, data anonymization techniques are used for protecting the privacy of market participants. In [16], an anonymization method based on k-anonymity is proposed for preserving the privacy of households in local energy markets. In particular, this paper focuses on the cost of privacy, including environmental consequences and costs of market participants, under data anonymization. A privacy-preserving economic dispatch approach is proposed in [17] for preventing strategic market participants from identifying their rivals' financial information in competitive electricity markets. In this paper, the generation companies and load serving entities obfuscate their actual data by multiplying with random numbers before submitting to the market operator. The privacy guarantee in these research papers is not provable. In addition, these approaches are vulnerable to side information and reconstruction attacks.

As we mentioned, we implement the notion of DP to achieve our privacy goal, which provides rigorous, provable, and quantifiable guarantees against privacy risks.There is a rich literature on the theoretical foundations of DP, and it is also widely deployed as a leading technology for preserving individuals' privacy by Apple, Google, Uber, Microsoft, United States Census Bureau, etc. [18]. Nevertheless, the application of DP in power systems is in its initial stages, and it is getting more attention in recent years. Authors in [19] propose a differentially private mechanism for releasing the sensitive data of power grids, e.g., parameters of transmission lines and transformers. The proposed mechanism guarantees that the released data leads to a feasible Optimal Power Flow (OPF) problem, and the utility loss is a constant factor away from optimality. In [20], a privacy-preserving OPF mechanism via DP is introduced that prevents an adversary with access to OPF solutions, e.g., voltage and current measurements, to learn about customers' private information. To ensure the feasibility of the OPF solutions, the proposed mechanism implements chance constraints enforced on the grid limits. In [21], authors provide a mechanism for privately releasing aggregate network statistics obtained from a DC-OPF. Moreover, the paper demonstrates that the privacy-aware mechanism depends on the topology of network. A privacy-preserving mechanism for OPF in distributed power systems is proposed in [22]. The local differentially private mechanism relies on Alternating Direction Method of Multipliers (ADMM) for a distributed individuals' load obfuscation while ensuring AC-OPF feasibility. The trade-off between individuals' privacy and the utility of the released data is investigated in a DP framework in [23]. Moreover, the authors in [23] analyze the contribution of the injected noise on the locational marginal prices and generators dispatch.

DP is also applied to protect the privacy of consumers connected to smart meters. In [24] and [25], differentially private algorithms are provided for protecting the data of consumers while the effects of the algorithm on the operation of the grid are investigated. Moreover, to allocate the extra cost incurred by the privacy constraint, several cost allocation mechanisms based on cooperative game theory are used. Authors in [26] exploit an extended version of DP for designing a mechanism that perturbs electricity rates before publishing them and protects the occupancy state of the houses connected to the smart meters. To hide the actual electricity consumption from outsiders, a battery-based load hiding technique with a differentially private mechanism is combined in [27].

B. Summary of Contributions

For incentivizing the privacy-aware customers to participate in local electricity markets and behave truthfully, we should address their privacy concerns. In this regard, this paper aims to introduce a privacy-preserving local electricity market in the framework of DP. The main contributions of this paper can be summarized as follows:

- Conjunction of privacy protection and data utility: We propose a differentially private mechanism for local electricity markets that guarantees the outputs of the market would reveal almost nothing about any individual's input data. At the same time, the proposed mechanism maintains the benefits of the data that local electricity markets can offer for social good.
- Fidelity of the market under the privacy constraint: We ensure the feasibility of the market-clearing solution and its quality with respect to the social welfare of the market. In this regard, unlike the additive noise approaches for achieving DP, e.g., Laplace mechanism and Gaussian mechanism, which may result in infeasible and low-quality solutions, we implement the exponential mechanism that makes it possible to explicitly include the social welfare in the privacy mechanism and privately select from a range of arbitrary solutions. Moreover, we provide an upper-bound on the social welfare loss incurred by the privacy constraint in the market, which reflects the inherent trade-off between privacy and suboptimality in DP.
- Computational efficiency: We propose a computationally-efficient implementation of the exponential mechanism.

Due to the infinite continuous solution space of a market-clearing problem, the output of the exponential mechanism has an intractable distribution, making it difficult to sample from in practice. Therefore, by using the techniques for sampling from polytopes, we discretize the solution space of the market-clearing problem for specifying a finite set of solutions as the range of the exponential mechanism.

C. Paper Organization

The problem setup is presented in section II. Section III belongs to the methodology overview including DP and the baseline mechanism in our local electricity market. In section IV, we propose our privacy-preserving mechanism for local electricity markets. Then, in section V, approximate truthfulness of the mechanism is demonstrated. In section VI, we provide numerical case studies for reflecting the theoretical properties of the mechanism. Following that, the conclusion is presented in section VII.

II. Problem Setup

We consider a centralized market-clearing problem in a local energy community with a finite set of market participants denoted by Ω, consisting of producers Ω^p and consumers Ω^c. Moreover, we assume that there is a trust-worthy market operator who should centrally collect the private information of the market participants and run the market. For notational brevity, the following notations are based on a general agent without distinguishing producers and consumers. There is a set of potential social decisions $S = \prod_{i=1}^{n} S_i$, where $S_i \subset \mathbb{R}^{|S_i|}$ is the domain of agent i's potential local decisions. Then, the local decisions $s_i \in S_i$ of consumer i and producer i are characterized by demand $d_i \in [\underline{d_i}, \overline{d_i}]$ and active power $g_i \in [\underline{g_i}, \overline{g_i}]$, respectively.

Each agent $i \in \Omega$ is endowed with a private information $\theta_i \in \Theta_i$, called type, that represents its preferences over the set of potential decisions S. Given a type, agent i's preferences can be evaluated by a valuation function $v_i : S \times \theta_i \to \mathbb{R}$, where $v_i(s, \theta_i)$ denotes the value of alternative $s \in S$ for agent i with type θ_i. Moreover, since we assume that agent i's valuation depends only on its local decisions, we can say $v_i(s, \theta_i) = v_i(s_i, \theta_i)$. The valuation function of consumer i reflects the utility of using demand d_i, denoted by $v_i(d_i, \theta_i) = U_{i,\theta_i}(d_i)$. Also, for producer i, the valuation function reflects the negation of the generation cost of active power g_i, denoted as $v_i(g_i, \theta_i) = -C_{i,\theta_i}(g_i)$. Note that $U_{i,\theta_i}(\cdot)$ and $C_{i,\theta_i}(\cdot)$ are the utility and cost functions of consumer i and producer i respectively, parameterized by type θ_i. Furthermore, for mathematical convenience, we normalize the valuation functions so that their range is [0,1].

Fig.1 depicts a high-level view of the problem setup. As can be seen, customer i, $\forall i \in \Omega$, reports the valuation v_i to the market. Given the valuation profile $v = (v_i)_{i\in\Omega}$, a trusted market operator defines an allocation rule $\mathcal{M}(v)$ for determining the market-clearing quantities, $d^* = (d_i^*)_{i\in\Omega^c}$ and $g^* = (g_i^*)_{i\in\Omega^p}$, and a payment rule $\mathcal{P}(v)$ for determining customers' payments $p = (p_i)_{i\in\Omega}$. In electricity markets, the

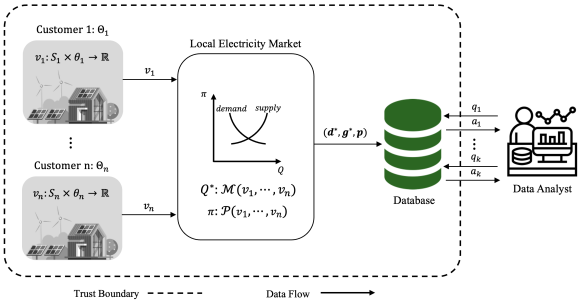

Fig. 1. A high-level view of the problem setup.

allocation rule is determined by maximizing the social welfare function $\mathrm{sw}(v, s) = \sum_{i\in\Omega} v_i(s_i)$ subject to the technical constraints of the market participants and the market-clearing equation. By substituting the valuation functions of consumers and producers in $\mathrm{sw}(v, s)$, the allocation rule $\mathcal{M}(v)$ is based on:

$$(d^*, g^*) \in \arg\max_{d,g} \sum_{i\in\Omega^c} U_{i,\theta_i}(d_i) - \sum_{i\in\Omega^p} C_{i,\theta_i}(g_i) \tag{1a}$$

$$\text{s.t.} \quad \underline{d_i} \le d_i \le \overline{d_i}, \quad \forall i \in \Omega^c \tag{1b}$$

$$\underline{g_i} \le g_i \le \overline{g_i}, \quad \forall i \in \Omega^p \tag{1c}$$

$$\sum_{i\in\Omega^p} g_i - \sum_{i\in\Omega^c} d_i = 0, \tag{1d}$$

where constraints (1b) and (1c) reflect the demand and supply limits of the consumers and producers, respectively. Also, constraint (1d) relates to the market-clearing equation.

Hence, the output of the market-clearing problem is the tuple (d^*, g^*, p), which is stored in a database. The data analyst represents all the third parties, e.g., energy efficiency service providers, policymakers, and insurance companies, requesting access to the market-clearing outputs for purposes that are not expected by the market participants. The goal of a well-intentioned data analyst of having access to the database is to learn useful information about the market participants, as a statistical population, by making queries $\{q_j\}_{j=1}^{k}$ and receiving answers $\{a_j\}_{j=1}^{k}$. That is, they have no intention to learn anything about the market participants at the individual level. However, by publicly releasing the market-clearing outputs, we also give access to malicious third-parties that exposes the market participants to the risk of a privacy breach. Thus, to unlock the benefits of the data that local electricity markets can offer for social good, the privacy-preserving market-clearing mechanism should ensure that whoever outside of the trust boundary is not able to learn anything at the individual level.

III. Methodology Overview

A. Differential Privacy

DP is a formal mathematical standard for protecting individuals' privacy [15]. DP ensures that the output of a computation will be roughly unchanged whether or not an individual's data is used, thus limiting an adversary's power to infer about individuals' data points [28], [29]. The main idea for satisfying this condition is to perturb the computation by injecting a calibrated amount of noise to mask the contribution of each

individual in the dataset. In the following, we present the formal definition of DP and a couple of remarks about this notion.

Definition 1 (Differential Privacy)**.** For $\epsilon > 0$, a randomized algorithm $\mathcal{M} : \mathcal{X}^n \to \mathcal{R}$ is $\epsilon-$differentially private if for every pair of neighboring datasets $x \sim x' \in \mathcal{X}^n$ (i.e., x and x' differ in one element) and for any subset of the output space $S \subseteq \mathcal{R}$, the following holds:

$$\Pr\left[\mathcal{M}\left(x\right) \in S\right] \leq e^{\epsilon}.\Pr\left[\mathcal{M}\left(x'\right) \in S\right], \tag{2}$$

where the probability is over the internal randomness of $\mathcal{M}$ [7].

The aforementioned definition is about the behavior of $\mathcal{M}$ and promises that no individual's data has a large impact on the output. More formally, when an $\epsilon-$differentially private algorithm runs on two neighboring datasets, the resulting distributions over the output space will be very similar, and this similarity is captured by a multiplicative factor e^{ϵ}. The required noise for satisfying DP is calibrated based on the global sensitivity of the computation. We formalize the mathematical definition of the global sensitivity in the following.

Definition 2 (Global Sensitivity)**.** For a function $f : \mathcal{X}^n \to \mathbb{R}^k$, the global sensitivity over all pairs of neighboring datasets $x \sim x' \in \mathcal{X}^n$ is

$$GS\left(f\right) = \max_{x \sim x' \in \mathcal{X}^n} \|f(x) - f(x')\|_1, \tag{3}$$

where $\|\cdot\|_1$ is the ℓ_1-norm [30].

For achieving differential privacy in a computation, we need to bound the contribution of any individual data point on that computation. Hence, we should implement an appropriate privacy mechanism for perturbing the computation, e.g., Laplace mechanism and Gaussian mechanism, known as the additive noise approaches. Moreover, perturbation techniques for satisfying DP in a computation are mainly classified into two basic categories: (1) adding calibrated random noise to the input data, (2) adding calibrated random noise to the outputs [7].

Nevertheless, leveraging these additive noise techniques in a market-clearing problem has major drawbacks. In the input perturbation technique, when market participants perturb their data before reporting to the market, the fidelity of the market with respect to the original problem is severely compromised. In fact, the input perturbation technique fits the Local Differential Privacy (LDP) framework, where there is no trustworthy centralized data curator. LDP is a strictly more stringent notion of privacy, but its accuracy is typically less than the central DP [31], [32]. In the output perturbation technique, simply adding noise to the output of the market-clearing problem may lead to an infeasible solution, which entails corrective mechanisms by the market operator. Besides, in this technique, we have no measure to guarantee a near-optimal solution, and the social welfare may suffer drastically. That is, the social welfare of the market is directly related to the noise values generated.

In this paper, we implement the exponential mechanism which overcomes the aforementioned challenges in market-clearing problems. The exponential mechanism is designed for settings in which we aim to choose the best solution, but adding noise directly to the computed quantity degrades its quality [33]. The exponential mechanism gives us the capability to choose randomly from an arbitrary range with respect to an arbitrary score function specified by the central planner. Indeed, the output of this mechanism is always a member of that arbitrary range, which is an important desideratum for privatizing constrained computations. The exponential mechanism takes in a dataset $x \in \mathcal{X}^n$, a set $\mathcal{R}$ of possible outputs, and a score function $q : \mathcal{R} \times \mathcal{X}^n \to \mathbb{R}$ that measures the quality of each output for a dataset. Given these inputs, the exponential mechanism assigns a probability proportional to $\exp\left(\frac{\epsilon q(x,r)}{2\Delta}\right)$ to each $r \in \mathcal{R}$, where Δ is the global sensitivity of the score function and ϵ is the privacy parameter. The idea is that we sample from the possible outputs $\mathcal{R}$ with probability that grows exponentially with their score $q(x, r)$. We formalize the exponential mechanism in the following definition. Moreover, it is straightforward to show that the exponential mechanism satisfies DP, and for theoretical proof, we refer readers to [30].

Definition 3 (Exponential Mechanism)**.** Given a dataset $x \in \mathcal{X}^n$, a set of possible outputs $\mathcal{R}$, a score function $q : \mathcal{R} \times \mathcal{X}^n \to \mathbb{R}$, and a privacy parameter ϵ, the exponential mechanism samples an outcome $r \in \mathcal{R}$ with probability proportional to $\exp\left(\frac{\epsilon q(x,r)}{2\Delta}\right)$, where Δ is the global sensitivity of the score function [34].

B. The Non-Private Market-Clearing Mechanism

Before presenting the privacy-preserving market-clearing mechanism, it is helpful to demonstrate the non-private market-clearing mechanism we try to build upon. Due to the desirable theoretical properties of the VCG mechanism, e.g., individual rationality, incentive compatibility, and efficiency, we apply it in our local electricity market [35]. Based on Algorithm 1, agents report their valuation functions $v = (v_i)_{i \in \Omega}$ into the market, and the VCG mechanism selects an outcome s^* that maximizes the social welfare function. Then, the mechanism charges each agent i with its social cost, which is the difference between the social welfare of others in the absence and presence of agent i.

Since the VCG mechanism is incentive compatible [35], truthful behavior is the dominant strategy for agents. Nevertheless, privacy-aware agents are concerned about the plausible harms on their future transactions in the market, caused by revealing their personal information, and wish to minimize potential losses in their utility. In addition, some agents may simply care about the intrinsic value of privacy and beliefs of unauthorized observers about them. Yet incorporating all the scenarios in which the disclosed information might affect the agents' utility in the future is a complicated task. DP avoids the need for such intricate modeling by providing a worst-case bound on agents' exposure to privacy loss [36].

We should mention that the Uniform-Price Double Auction (UPDA) is a more common market-clearing mechanism. But, in this paper, we adopt the VCG mechanism. The reason we choose the VCG mechanism over the UPDA is mainly rooted

Algorithm 1 VCG Mechanism for Local Electricity Markets

Inputs: Set of valuation functions $v = (v_i)_{i\in\Omega}$.
Outputs: Market participants' set points $s^* = (d^*, g^*) \in S$ and payments $p = (p_i)_{i\in\Omega}$.

1: Solve the social welfare $\mathrm{sw}(v, s)$ maximization problem:

$$s^* \in \arg\max_{s\in S} \sum_{i\in\Omega} v_i(s_i)$$

2: **for all** $i \in \Omega$ **do**
3: Charge market participant i:

$$p_i\left(v_i, v_{-i}\right) = \max_{s\in S} \sum_{j\neq i\in\Omega} v_j(s_j) - \sum_{j\neq i\in\Omega} v_j(s^*)$$

4: **end for**
5: **return** s^* and p.

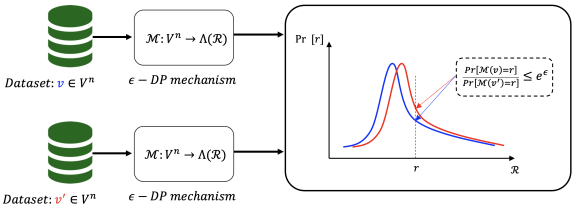

Fig. 2. Illustration of a differentially private market-clearing mechanism.

in computing the market-clearing price. That is, privately mapping the market-clearing quantities resulted by the exponential mechanism onto a market-clearing price is a challenging task in the UPDA. For computing the market-clearing price under this mechanism, we need to compute the gradient of market participants' valuation functions, which are not priori bounded. Therefore, the sensitivity of computing the market-clearing price under the UPDA is high, which requires adding more noise. As a consequence, the coupling between market-clearing quantities and the corresponding price would be loose, which puts the revenue adequacy and cost recovery of the market at stake.

IV. The Model

A. Differentially Private Market-Clearing Mechanism

An illustration of a differentially private market-clearing mechanism is shown in Fig. 2. The ϵ-differentially private mechanism $\mathcal{M}$ with domain V^n and discrete range $\mathcal{R}$ is associated with a mapping $\mathcal{M} : V^n \to \Lambda(\mathcal{R})$, where $\Lambda(\cdot)$ is the probability simplex over $\mathcal{R}$. On the input $v \in V^n$, the mechanism $\mathcal{M}$ outputs $\mathcal{M}(v) = r$ with probability $\Pr[\mathcal{M}(v) = r]$ for each $r \in \mathcal{R}$. So, DP guarantees that for any neighboring vector of valuations $v \sim v' \in V^n$, the output distributions under $\mathcal{M}(v)$ and $\mathcal{M}(v')$ are almost the same, up to a small multiplicative factor e^{ϵ}. Also, $\ln\frac{\Pr[\mathcal{M}(v)=r]}{\Pr[\mathcal{M}(v')=r]}$ is the privacy loss and is bounded by ϵ.

We implement the exponential mechanism for privatizing the underlying VCG mechanism in our local electricity market. For doing so, we should determine the inputs of the exponential mechanism, including x, $q(\cdot)$, and $\mathcal{R}$. In our setting, the valuation profile, $v \in V^n$, of the market participants characterizes dataset x, and the social welfare function $\mathrm{sw}(\cdot)$ is applied as the score function $q(\cdot)$. Moreover, due to constraints (1b)-(1d), the feasibility set $\mathcal{O}$ of the market-clearing problem, in the following, represents the set of outputs $\mathcal{R}$ that the exponential mechanism takes as an input for defining the probability distribution:

$$\mathcal{O} = \Big\{ d \in \mathbb{R}^{|\Omega^c|}, g \in \mathbb{R}^{|\Omega^p|} \mid \underline{d} \leq d \leq \overline{d}, \underline{g} \leq g \leq \overline{g}, \sum_{i\in\Omega^c} d_i = \sum_{i\in\Omega^p} g_i \Big\} \quad (4)$$

Then, we calculate the global sensitivity of the social welfare function $\mathrm{sw}(\cdot)$, which we designate as the score function, in the following:

$$\begin{aligned} \Delta(\mathrm{sw}) &= \max_{v\sim v'\in V^n} \|\mathrm{sw}(v) - \mathrm{sw}(v')\|_1 \\ &= \max_{v\sim v'\in V^n} \|\sum_{j\neq i}^{n} v_j + v_i - \sum_{j\neq i}^{n} v_j - v_i'\|_1 \\ &= \max_{v\sim v'\in V^n} \|v_i - v_i'\|_1 = 1, \end{aligned} \quad (5)$$

where $v_i \in [0, 1]$, $\forall i \in \Omega$. That is, the maximum possible change to the social welfare between any neighboring valuation profile $v \sim v'$, differing in v_i, arises from a situation when v_i is equal to 1 and v'_i is equal to 0, or vice versa.

In the next step, we need to define the output distribution of the mechanism by assigning a probability proportional to $\exp\left(\epsilon\frac{\sum_{i=1}^{n} v_i(r)}{2}\right)$ to each $r \in \mathcal{R}$. Furthermore, those probabilities should be normalized via the normalizing factor $\phi(\mathcal{R}) = \sum_{r\in\mathcal{R}} \exp\left(\epsilon\frac{\sum_{i=1}^{n} v_i(r)}{2}\right)$. While the exponential mechanism helps us to approximately select the optimal solution amongst the feasibility set $\mathcal{O}$ of the market-clearing problem, it can be computationally intractable. Indeed, the exponential mechanism requires enumerating over the all points $r \in \mathcal{R}$ of the output space, which is, in our setting, a convex set constrained by the physical limits of the market participants and the market-clearing equation. Since $\mathcal{R}$ is an infinite set, the resulting distribution of the mechanism is intractable, making it difficult to sample from in practice.

For addressing this challenge, we discretize the output space $\mathcal{R}$ in such a way that the accuracy does not suffer too much, but coarse enough that computing the score function for candidate outputs is tractable. In this regard, we use a Markov Chain Monte Carlo (MCMC) sampling algorithm from [37] for sampling from convex bodies in n-dimentional spaces. By implementing this algorithm, we uniformly take n_s samples from the feasibility set $\mathcal{O}$ for making a finite discretized set $\mathcal{R}$ for the exponential mechanism. The basic idea is to construct an ergodic Markov chain whose set of states is the output space of the market-clearing problem and whose stationary distribution is the required sampling distribution, which is the uniform distribution in our case. Then, for drawing samples, we should simulate the chain for a certain number of steps. For more detail, we refer readers to [37]. Algorithm 2 summarizes the proposed differentially private market-clearing mechanism for local electricity markets.

Algorithm 2 Differentially Private Market-Clearing Mechanism

Inputs: Set of valuation functions $v = (v_i)_{i\in\Omega}$, privacy loss parameter ϵ, sample size n_s.

Outputs: Probability distribution over the discretized version of the output space $\mathcal{O}$.

1: Draw n_s sample r uniformly from the output space $\mathcal{O} \subset \mathbb{R}^n$

2: **for all** $r \in \mathcal{R}$ **do**

3: Compute the social welfare $\mathrm{sw}\,(v, r) = \sum_{i=1}^{n} v_i(r)$

4: **end for**

5: Compute the normalizing factor:

$$\phi\,(\mathcal{R}) = \sum_{r\in\mathcal{R}} \exp\left(\epsilon \frac{\sum_{i=1}^{n} v_i\,(r)}{2}\right)$$

6: Construct the probability distribution $\mathcal{D}$ such that

$$\Pr_{\mathcal{D}}[r] = \frac{\exp\left(\epsilon \frac{\sum_{i=1}^{n} v_i(r)}{2}\right)}{\phi(\mathcal{R})}$$

7: **return** $r \sim \mathcal{D}$.

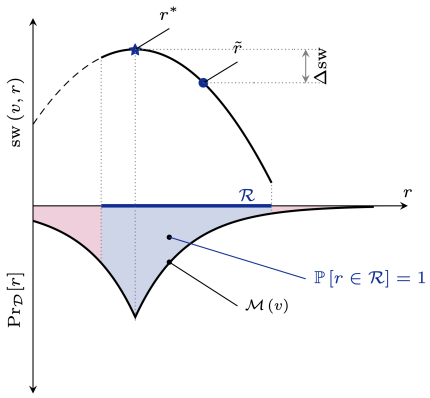

Fig. 3. A high-level view of the proposed market-clearing mechanism.

Fig. 3 represents a high-level view of how the exponential mechanism selects a privatized solution for the market-clearing problem. Suppose that the social welfare function of the market, $\mathrm{sw}\,(v, r)$, is depicted on the top plane in Fig. 3. The exponential mechanism $\mathcal{M}\,(v)$ constructs a probability distribution, due to Algorithm 2, over the feasible market-clearing solutions $r \in \mathcal{R}$, highlighted in blue. Also, the normalizing factor $\phi\,(\mathcal{R})$ is computed with respect to $\mathbb{P}\,[r \in \mathcal{R}] = 1$. As you can see on the bottom plane in Fig. 3, the maximum of the social welfare function at $r^* \in \mathcal{R}$ has the highest probability density in the output probability distribution $\Pr_{\mathcal{D}}[r]$ of the exponential mechanism. In addition, we can see as the social welfare decreases for a solution $r \in \mathcal{R}$, the corresponding likelihood $\Pr_{\mathcal{D}}[r]$ is also decreased in compare to the optimal solution. If $\widetilde{r} \in \mathcal{R}$ is the solution that the exponential mechanism selects for the market-clearing problem, then $\Delta\mathrm{sw}$ is the social welfare loss with respect to the optimal solution $r^* \in \mathcal{R}$. In the following section, we provide an upper-bound on $\Delta\mathrm{sw}$, which can be interpreted as the cost of privacy.

B. Performance Gap

We constructed a privacy-preserving market-clearing mechanism, which approximately maximizes the social welfare in a differentially private manner. Drawing on a theorem in [38], we discuss the accuracy of this computation and investigate the performance gap of running the proposed market-clearing mechanism in the following.

Theorem 1. For any $\mathcal{R}$, v, ϵ, δ, Δ where $\mathcal{R}$ is a finite set of feasible market-clearing allocations, with probability at least $1-\delta$, the exponential mechanism outputs an allocation r such that

$$\mathrm{sw}(v, r) \geq \max_{r\in\mathcal{R}} \mathrm{sw}\,(v, r) - \frac{2\Delta}{\epsilon} \ln\left(\frac{|\mathcal{R}|}{\delta}\right). \tag{6}$$

Proof. Let $r^* = \arg\max_{r\in\mathcal{R}} \mathrm{sw}(v, r)$. For any value of x, we have the following for the probability distribution of the social welfare over the outcomes $r \in \mathcal{R}$:

$$\Pr[\mathrm{sw}(v, r) \leq x] \leq \frac{\Pr[\mathrm{sw}(v, r) \leq x]}{\Pr[\mathrm{sw}(v, r) = \mathrm{sw}(v, r^*)]}. \tag{7}$$

Because the denominator $\Pr[\mathrm{sw}\,(v, r) = \mathrm{sw}\,(v, r^*)]$, which is the probability that the exponential mechanism outputs the optimal allocation, is at most 1. In the next step, we should find an upper bound for the right hand-side of this inequality. The nominator $\Pr[\mathrm{sw}(v, r) \leq x]$ in (7) is the probability that the mechanism gives us an allocation that does not hit the social welfare target x. Thus, in the worst case, all the feasible allocations $r \in \mathcal{R}$ of the market-clearing are unsatisfactory for the target social welfare. Since, the exponential mechanism chooses each allocation $r \in \mathcal{R}$ with a probability proportional to its social welfare, we have

$$(7) \leq \frac{|\mathcal{R}|\,.\exp\left(\epsilon \frac{x}{2\Delta}\right)}{\exp\left(\epsilon \frac{\mathrm{sw}(v, r^*)}{2\Delta}\right)}. \tag{8}$$

After simplifying the right-hand side of (8), we have

$$\Pr\left[\mathrm{sw}\,(v, r) \leq x\right] \leq |\mathcal{R}|\,.\exp\left(\frac{\epsilon\,(x - \mathrm{sw}\,(v, r^*))}{2\Delta}\right). \tag{9}$$

By artfully choosing $x = \mathrm{sw}\,(v, r^*) - \frac{2\Delta}{\epsilon} \ln\left(\frac{|\mathcal{R}|}{\delta}\right)$, we get the maximum cancellation. After plugging this x, we have

$$\begin{aligned} \Pr\left[\mathrm{sw}\,(v, r) \leq x\right] &\leq |\mathcal{R}|\,.\exp\left(-\ln\left(\frac{|\mathcal{R}|}{\delta}\right)\right) \\ &= |\mathcal{R}|\,.\frac{\delta}{|\mathcal{R}|} = \delta. \end{aligned} \tag{10}$$

Therefore, with probability at least $1-\delta$, the upper-bound (6) for the gap between the output of the exponential mechanism and the optimal output holds. □

C. Differentially Private Computation of Payments

Besides the market-clearing quantities, the payments of the market participants will be published publicly. Hence, an adversary who tries to learn about the private valuations of the market participants has access to all the payments. Thus, we should make the payment profile $p = (p_1\,(v)\,, \cdots\,,\ p_n\,(v))$ of the market indistinguishable via DP. In this regard, for every pair of the neighboring valuation profiles $v \sim v' \in V^n$ and

any possible payment $p \in \mathcal{P}$, the following privacy constraint should hold:

$$\Pr\left[\, p_1\left(v\right), \cdots,\ p_n\left(v\right) \in \mathcal{P}\right] \leq e^{\epsilon}.\Pr\left[\, p_1\left(v'\right), \cdots,\ p_n\left(v'\right) \in \mathcal{P}\right]. \quad (11)$$

As mentioned previously, for computing the VCG payments, we need to compute the social welfare. Consequently, for privatizing the VCG payments, there is no need for an additional privacy-aware mechanism, and it suffices to embed Algorithm 2 in the non-private computation of the VCG payments, which results in Algorithm 3.

In the first step, Algorithm 3 calls Algorithm 2 with the valuation profile $v = (v_i)_{i\in\Omega}$ as its input and stores the probability distribution $\mathcal{D}$, which will be used later for computing the expected social welfare of others in the presence of agent $i \in \Omega$, $\mathrm{sw}_{-i}\left(\mathcal{D}\right)$. Then, for each agent i, Algorithm 3 removes agent i and passes $v = (v_j)_{j\in\Omega, j\neq i}$ into Algorithm 2 for getting the probability distribution $\mathcal{D}_{-i}$ and computing the expected social welfare of others in the absence of agent i, $\mathrm{sw}_{-i}\left(\mathcal{D}_{-i}\right)$. Finally, by subtracting $\mathrm{sw}_{-i}\left(\mathcal{D}\right)$ from $\mathrm{sw}_{-i}\left(\mathcal{D}_{-i}\right)$ for each agent, Algorithm 3 returns the payment profile p.

Algorithm 3 Private Computation of the VCG Payments

Inputs: Set of valuation functions $v = (v_i)_{i\in\Omega}$, privacy loss parameter ϵ, sample size n_s.
Outputs: Expected payments p of the market participants.

1: **call** Algorithm 2:
   Inputs: $v = (v_i)_{i\in\Omega}$, ϵ, n_s
   Outputs: $r \sim \mathcal{D}$
2: **for all** agent $i \in \Omega$ **do**
3: **call** Algorithm 2:
    Inputs: $v = (v_j)_{j\in\Omega, j\neq i}$, ϵ, n_s
    Outputs: $r \sim \mathcal{D}_{-i}$
4: $\mathrm{sw}_{-i}\left(\mathcal{D}_{-i}\right) = \mathbb{E}_{r\sim\mathcal{D}_{-i}}\left[\sum_{j\neq i} v_j\left(r\right)\right]$
5: $\mathrm{sw}_{-i}\left(\mathcal{D}\right) = \mathbb{E}_{r\sim\mathcal{D}}\left[\sum_{j\neq i} v_j\left(r\right)\right]$
6: $p_i = \mathrm{sw}_{-i}\left(\mathcal{D}_{-i}\right) - \mathrm{sw}_{-i}\left(\mathcal{D}\right)$
7: **end for**
8: **return** p.

For measuring the privacy loss in computing the VCG payments, we implement the composition property of DP. That is, the privacy loss of running multiple differentially private computation on the same input data is equivalent to the sum of their individual privacy losses. More formally, if there are k independent mechanisms $\mathcal{M}_1$, $\mathcal{M}_2$,..., $\mathcal{M}_k$, which are ϵ_i-differentially private for $i = 1,\ 2, \ldots,\ k$, respectively, then $\mathcal{M} = (\mathcal{M}_1,\ \mathcal{M}_2,\ \ldots,\ \mathcal{M}_k)$, which is any combination of the individual mechanisms, is $\sum_{i=1}^{k}\epsilon_i-$differentially private [15]. As we can see in Fig. 4, computing the VCG payment of each individual requires querying the input data v for computing a realization of $\mathrm{sw}_{-i}\left(\mathcal{D}_{-i}\right)$ and $\mathrm{sw}_{-i}\left(\mathcal{D}\right)$. We know that the proposed mechanism for maximizing the social welfare and computing the market-clearing quantities is $\epsilon-$differentially private. Therefore, due to the sequential composition of the proposed mechanism, computation of the VCG payment for each individual is $2\epsilon-$differentially private. Since we have n market participants, the total computation of the VCG payments is $2n\epsilon-$differentially private. Moreover, by adding the privacy leakage of the market-clearing quantities, the total outputs of the proposed market-clearing mechanism is $(2n+1)\epsilon-$differentially private.

D. Beyond the Centralized Setting

In this paper, we developed a centralized differentially private mechanism for local electricity markets, where there is a trustworthy market operator who centrally collects the private information of the market participants and runs the market. But, in P2P electricity markets, where there is no central entity, each market participant performs local computations on its private data and exchanges the output with its neighbors in an iterative fashion. Thus, in addition to the market outputs, the communications between market participants in this iterative process leak private information about them and can lead to their privacy breach. Therefore, the adversary can be either a market participant who observes the information exchanged with its neighbors or an outsider who observes the market outputs. In this regard, the trust boundary in P2P electricity markets is pushed towards each individual. For addressing the privacy concern in this setting, we can implement a differentially private variant of ADMM, via additive noise mechanisms, e.g., Laplace mechanism and Gaussian mechanism. There are two main approaches for achieving differentially private ADMM. The first approach is dual variable perturbation, where each market participant perturbs the dual variables in its local computation at every ADMM iteration. The second approach is the primal variable perturbation, where each market participant adds noise to the updated primal variables before information exchange with its neighbors. We refer readers to [39]–[41] for more detail about the implementation of differentially private ADMM and improving the privacy and accuracy of the algorithm.

V. Differential Privacy as a Solution Concept

Truthfulness is the most desired property for mechanism design, where the central planner designs the mechanism in such a way that truthful reporting of the valuation function is the dominant strategy for agents. The realization of this property in local electricity markets eliminates the complexities of strategic behavior for customers, facilitates their participation, and ensures the efficiency of the market. In this section, we focus on the utility-theoretic interpretation of DP and its connection with truthfulness in mechanism design. Before that, we introduce the notion of approximate truthfulness.

Definition 4 (Approximate Truthfulness)**.** A mechanism $\mathcal{M} : [0,1]^n \to \mathcal{O}$ is $\epsilon-$approximately dominant strategy truthful if for every agent i, every utility function $u_i : [0,1]\times\mathcal{O} \to [0,1]$, every vector of valuations $v \in [0,1]^n$, and every deviation $v_i' \in [0,1]$, if we write $v' = (v_{-i}, v_i')$, then [38]:

$$\mathbb{E}_{o\sim M(v)}\left[u_i\left(v_i, o\right)\right] \geq \mathbb{E}_{o\sim M(v')}\left[u_i\left(v_i, o\right)\right] - \epsilon. \quad (12)$$

This definition implies that in an $\epsilon-$approximately dominant strategy truthful mechanism, no agent has more than ϵ additive

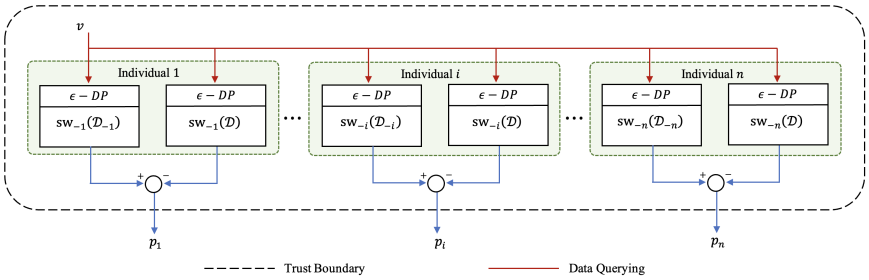

Fig. 4. Measuring the privacy loss in computing the VCG payments of n individuals.

incentive for misreporting its valuation. This notion gives almost immediately a formal connection with DP due to the following theorem.

Theorem 2. If a mechanism $\mathcal{M} : [0,1]^n \to \mathcal{O}$ is $\epsilon-$differentially private, then $\mathcal{M}$ is also $\epsilon-$approximately dominant strategy truthful [42].

Proof. Fix any agent i, valuation profile v, and utility function $u_i : [0,1] \times \mathcal{O} \to [0,1]$. The expectation of agent i's utility over the randomness of the outcome chosen by $\mathcal{M}$ can be obtained as

$$\mathbb{E}_{o\sim M(v)}\left[u_i\left(v_i,o\right)\right] = \sum_{o\in\mathcal{O}} u_i\left(v_i,o\right)\Pr\left[\mathcal{M}(v)=o\right]. \quad (13)$$

Since $\mathcal{M}$ is $\epsilon-$differentially private, the following inequality holds for any neighboring valuation profile v':

$$\begin{aligned}(13) &\geq \sum_{o\in\mathcal{O}} u_i\left(v_i,o\right)\exp(-\epsilon)\Pr\left[\mathcal{M}(v')=o\right] \\ &= \exp(-\epsilon)\mathbb{E}_{o\sim M(v')}\left[u_i\left(v_i,o\right)\right].\end{aligned} \quad (14)$$

For $\epsilon \leq 1$, we have $\exp(-\epsilon) \geq 1-\epsilon$. Besides, as we mentioned earlier, the utility $u_i\left(v_i,o\right)$ is bounded in [0,1]. Then, we obtain

$$(14) \geq \mathbb{E}_{o\sim M(v')}\left[u_i\left(v_i,o\right)\right] - \epsilon. \quad (15)$$

□

Our proposed differentially private market-clearing mechanism guarantees that market participants have limited incentive to behave strategically. This guarantee of approximate truthfulness is rooted in the fact that the output of a differentially private computation has minimal sensitivity to each individual data point.

Furthermore, truthfulness in mechanisms is normally proved in a setting under strong assumptions, which are prohibiting of collusion among agents, constraining the utility functions of agents to quasilinear class, and banning multiple execution. These assumptions can limit the domains in which the truthful mechanisms can be implemented. Specifically, in electricity markets, collusion of market participants is likely, and the market-clearing problem is solved sequentially with a predefined time frame. Thus, the benefits of truthfulness cannot be fully realized. However, none of the aforementioned assumptions are considered in Theorem 2. Therefore, differentially private market-clearing mechanisms are approximately dominant strategy truthful under arbitrary agent utility functions, are automatically resilient to collusion, and easily allow repeatability [33]. For more information about the connection between differential privacy and truthfulness in mechanism design, we refer readers to [8] and [43].

TABLE I
CHARACTERISTICS OF PRODUCERS

Producers	a_i^g ($/kWh^2)	b_i^g ($/kWh)	c_i^g ($)	$\underline{g_i}$ (kW)	$\overline{g_i}$ (kW)
1	0.0022	0.0056	0	0	20
2	0.0013	0.0076	0	0	25
3	0.001	0.003	0	0	30

VI. Numerical Results

This section presents numerical case studies to reflect the theoretical properties of the proposed differentially private mechanism for local electricity markets. Towards that, we provide a local energy community consisting of three producers and three consumers by modifying a test system from [44]. We assume that the market participants in the present local energy community are privacy-aware and sensitive to the leakage of their private information due to the publicly releasing of the market data for social good. The market operator has obligation to protect the privacy of individuals under the data privacy laws, e.g., GDPR. In addition, the privacy concern can motivate the market participants to behave strategically and misreport their data to the market, which leads to the market inefficiency. Our goal in the following case studies is to investigate the impacts of our proposed differentially private market-clearing mechanism on the performance of the market. The cost function of producer i and utility function of consumer i are in the quadratic format $C_{i,\theta_i}(\cdot) := a_i^g g_i^2 + b_i^g g_i + c_i^g$ and $U_{i,\theta_i}(\cdot) := a_i^u d_i^2 + b_i^u d_i + c_i^u$, respectively. The parameters for producers and consumers are given in Table I and Table II. All the simulations are conducted in Python using a computer with 16 GB RAM and a 3.2 GHz 8-core Apple M1 processor. Moreover, the package in [37] is used for sampling from polytopes.

A. Market-Clearing Quantities

In this section, we demonstrate the feasibility and quality of the market-clearing quantities under the proposed mechanism. In addition, we focus on the inherent trade-off between the

TABLE II
CHARACTERISTICS OF CONSUMERS

Consumers	a_i^u ($/kWh^2)	b_i^u ($/kWh)	c_i^u ($)	$\underline{d_i}$ (kW)	$\overline{d_i}$ (kW)
1	− 0.00125	0.125	− 0.5937	5	15
2	− 0.006	0.216	− 0.93	5	18
3	− 0.0067	0.2975	− 2.305	10	25

privacy protection and social welfare of the market. We investigate the probability distribution over the discretized output space of the market-clearing problem based on the exponential mechanism. The sample size for discretizing the output space in our case studies is 10, and the samples are fixed during our studies. These samples comprised of producers' generation (kW) and consumers' demand (kW), uniformly drawn from the feasibility set of the market-clearing problem, are represented in Table III. Moreover, the optimal solution (opt) of the non-private market-clearing problem in (1a)-(1d) is added to these samples, which has the highest value for the score function. Then, the social welfare of each sample is calculated, and based on that a probability is assigned to it via the exponential mechanism for different values of the privacy parameter ϵ. Fig. 5 shows the probability distribution of the social welfare for different values of ϵ. As we know, small quantities of privacy loss parameter, e.g., $\epsilon = 0.1$, reflect higher level of privacy, and we can see, in Fig. 5, that the probability distribution over the possible outputs is almost uniform for $\epsilon = 0.1$. It means that the market-clearing mechanism does not take into account the quality of the solutions and just randomly chooses a solution from the output space given a uniform probability distribution. Albeit the provided solution is highly privatized, but the utility of the solution may fall drastically. When ϵ increases, and there is less concern about the privacy of the market participants, the market-clearing mechanism imposes more discrimination between the samples in the output space based on their social welfare. In this regard, the solutions with higher social welfare are more likely to be chosen by the mechanism. In an extreme scenario, when $\epsilon = 100$, our privacy-preserving market-clearing mechanism turns to a non-private mechanism with the optimal solution. Thus, choosing a value for ϵ requires balancing the level of privacy protection and the accuracy of the market-clearing outputs. However, there is no rigorous method for determining the optimal value of ϵ. For more information about the practical implementation of DP and choosing ϵ, we refer readers to [18].

B. Privacy Guarantee

This section provides a sanity check for the privacy guarantee of our proposed mechanism. DP guarantees that the output of our market-clearing mechanism is not sensitive to each individual's reported valuation function. Based on this guarantee, the unilateral change of an individual's reported valuation to the market can have at most a small e^{ϵ} multiplicative effect on the output distribution of the market. For

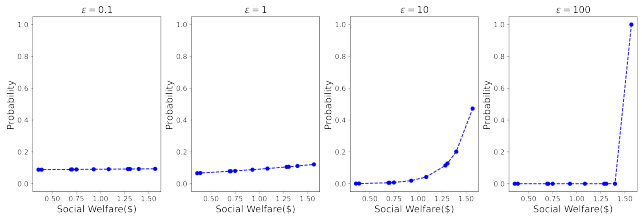

Fig. 5. Probability distribution of the social welfare under different privacy regimes.

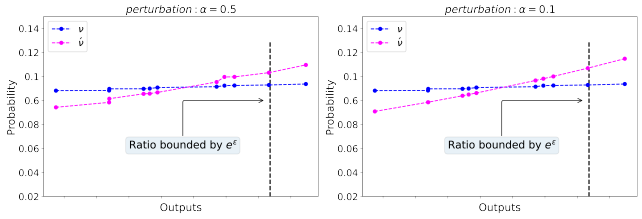

Fig. 6. Multiplicative closeness of probability distributions over the outputs given two neighbouring sets of valuation functions.

examining this property, we create two pairs of neighboring valuation profiles via perturbing the valuation function of producer 3. In both pairs, the perturbation is in the form of $v_3' = \alpha v_3$, where α is equal to 0.5 and 0.1. Moreover, the privacy loss parameter in this section is $\epsilon = 0.5$. Fig. 6 shows that the ratio of probabilities in the output distributions of the mechanism under the two neighboring valuation profiles $v \sim v'$ is bounded by $e^{0.5}$. Indeed, if we go point by point through the corresponding social welfare of the samples drawn from the output space of the market-clearing mechanism, the probability ratio of the two distributions is at most $e^{0.5}$.

C. Privatized Payments

This section focuses on the privatized VCG payments of the market participants. The payment of each market participant i entails computing the social welfare via the exponential mechanism in two scenarios: (1) the welfare of other participants when the individual i is in the market, $\mathrm{sw}_{-i}(\mathcal{D})$, (2) the welfare of other participants when the individual i is not in the market, $\mathrm{sw}_{-i}(\mathcal{D}_{-i})$. After subtracting $\mathrm{sw}_{-i}(\mathcal{D})$ from $\mathrm{sw}_{-i}(\mathcal{D}_{-i})$, Fig. 7 shows the expected VCG payment of each individual. We can see in the plots that there is a swing in each payment. These swings are rooted in the different degradation speed of $\mathrm{sw}_{-i}(\mathcal{D})$ and $\mathrm{sw}_{-i}(\mathcal{D}_{-i})$ when ϵ decreases. In addition, by increasing the privacy loss parameter ϵ, the payments reach to their optimal values: $p_1^g = -0.57$, $p_2^g = -0.9$, $p_3^g = -1.45$, $p_1^c = 0.59$, $p_2^c = 0.53$, $p_3^c = 0.7$. Note that the negative sign of the producers' payments reflects their earning. In Table IV, the expected values of the payments are shown for non-trivial values of ϵ. For these quantities of ϵ, the privatized payments of consumers and revenues of producers (except for producer 1) are less than their non-private values.

D. Payoffs Under Privacy Constraints

This section belongs to the utility-theoretic interpretation of DP. Fig. 8 depicts the payoffs of the market participants

TABLE III
SOCIAL WELFARE AND PROBABILITY COMPUTATION OF EACH SAMPLE

	Consumers			Producers				Probability			
No.	d_1	d_2	d_3	g_1	g_2	g_3	sw ($)	$\epsilon = 0.1$	$\epsilon = 1$	$\epsilon = 10$	$\epsilon = 100$
1	12.38	13.4	19.43	1.91	15.04	28.27	1.28	0.0924	0.105	0.114	≈ 0
2	7.48	9.6	10.71	3.5	2.35	21.9	0.356	0.0882	0.0662	0.0011	≈ 0
3	11.31	7.52	12.66	2.7	6.08	22.73	0.7	0.0897	0.0784	0.0059	≈ 0
4	14.5	16.87	24	19.14	12.05	24.18	1.08	0.0915	0.0953	0.0422	≈ 0
5	5.95	6.12	15.78	10.2	11.7	5.96	0.388	0.0883	0.0673	0.0012	≈ 0
6	8.73	14.86	14.8	16.25	9.3	12.85	0.93	0.0907	0.0882	0.0193	≈ 0
7	13.06	16.4	19.13	10.08	20.51	18	1.4	0.0929	0.115	0.201	≈ 0
8	13.56	12.55	15.18	2.56	16.43	22.31	1.3	0.0925	0.106	0.127	≈ 0
9	8.11	14.32	14.53	19	6.76	11.2	0.7	0.0897	0.0788	0.0062	≈ 0
10	10.23	7.23	18.97	15.02	1.51	19.9	0.75	0.0899	0.0806	0.0079	≈ 0
opt	15	14	18.62	9.62	15.52	22.47	1.56	0.0937	0.121	0.472	≈ 1

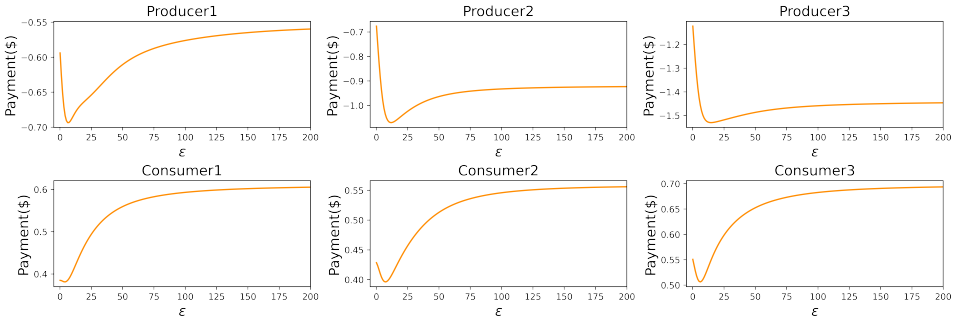

Fig. 7. Asymptotic convergence of the privatized VCG payments to their optimal value versus privacy loss parameter ϵ.

TABLE IV
THE EXPECTED VCG PAYMENTS OF THE MARKET PARTICIPANTS

	Consumers' Payments ($)			Producers' Payments ($)		
ϵ	p_1^c	p_2^c	p_3^c	p_1^g	p_2^g	p_3^g
0.01	0.375	0.413	0.637	− 0.613	− 0.722	− 1.121
0.5	0.374	0.412	0.634	− 0.627	− 0.756	− 1.15
1	0.372	0.41	0.63	− 0.64	− 0.791	− 1.19

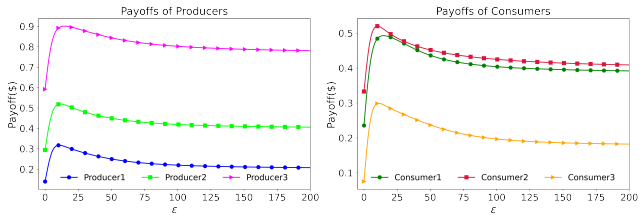

Fig. 8. Payoffs of the market participants versus privacy loss parameter ϵ.

versus ϵ. At the first sight, we notice that all the payoffs are non-negative, which is a significant desideratum that we have for granted by implementing the VCG mechanism. Based on this property, known as individual rationality, individuals have incentive to participate in the market, and at the worst case, their payoff would be zero. Due to Fig. 8, even providing high level of privacy does not incur negative payoffs to the market participants. Also, by increasing ϵ, payoffs converge towards their non-private values.

In the following case study, we demonstrate that our proposed differentially private market-clearing mechanism is also approximately truthful. Based on the utility-theoretic interpretation of DP, no agent can gain more than ϵ utility by misreporting its valuation to an ϵ-differentially private mechanism. For investigating this property, we leverage the same class of perturbation as in section VI-B, where individual i deviates from the real valuation function in a multiplicative form $v_i' = \alpha v_i$. The results are shown in Table V for six scenarios based on α and ϵ, where $\Delta\mathcal{U}_i^p$ and $\Delta\mathcal{U}_i^c$ denote the changes in the payoff of producer i and consumer i, respectively.

TABLE V
CHANGE OF THE MARKET PARTICIPANTS' PAYOFFS CAUSED BY MISREPORTING THEIR VALUATION FUNCTIONS

	Perturbation $\alpha = 0.9$			Perturbation $\alpha = 0.5$		
No.	$\epsilon = 0.1$	$\epsilon = 0.5$	$\epsilon = 1$	$\epsilon = 0.1$	$\epsilon = 0.5$	$\epsilon = 1$
$\Delta\mathcal{U}_1^p$	− 0.026	− 0.024	− 0.022	− 0.042	− 0.043	− 0.044
$\Delta\mathcal{U}_2^p$	0.0051	0.0054	0.0058	− 0.009	− 0.005	≈ 0
$\Delta\mathcal{U}_3^p$	0.005	0.007	0.01	− 0.001	0.004	0.01
$\Delta\mathcal{U}_1^c$	0.004	0.001	− 0.002	− 0.006	− 0.01	− 0.03
$\Delta\mathcal{U}_2^c$	0.02	0.016	0.012	0.01	0.006	− 0.01
$\Delta\mathcal{U}_3^c$	0.011	0.01	0.008	0.0048	− 0.002	− 0.01

Due to Table V, despite producer 1 with a negative $\Delta\mathcal{U}_1^p$ in all scenarios, the other market participants can be slightly better off in some scenarios by deviating from their real valuation. However, as we mentioned, their gain is bounded by ϵ. For example, unilateral deviation of consumer 2 from its

TABLE VI
QUANTITATIVE COMPARISON BETWEEN THE EXPONENTIAL MECHANISM AND INPUT PERTURBATION VIA THE LAPLACE MECHANISM

ϵ	Mech.	Consumers						Producers						sw($)	
		d_1		d_2		d_3		g_1		g_2		g_3			
		mean	std	mean	std	mean	std	mean	std	mean	std	mean	std	mean	std
0.1	Exp	10.98	2.9	12.12	3.62	16.74	3.54	9.98	6.35	10.74	5.77	19.12	6.21	**0.95**	**0.38**
	InLap	9.51	4.86	10.65	6.26	16.26	7.21	10.22	8.48	12.53	10.12	13.67	11.51	0.08	0.47
1	Exp	11.45	2.82	12.58	3.48	17.13	3.44	9.89	6.28	11.6	5.67	19.68	5.93	**1.02**	**0.36**
	InLap	9.93	4.85	11.73	6.1	17.54	7.02	9.56	7.37	13.12	9.4	16.52	10.75	0.32	0.45
10	Exp	13.83	1.41	14.23	1.57	18.42	1.87	8.5	2.04	16.04	2.97	21.94	3.27	**1.40**	**0.19**
	InLap	13.5	3.23	13.81	3.53	19	3.95	9.26	2.58	15.27	4.52	21.76	5.12	1.24	0.24
	opt.	15		14		18.62		9.62		15.52		22.47		1.56	

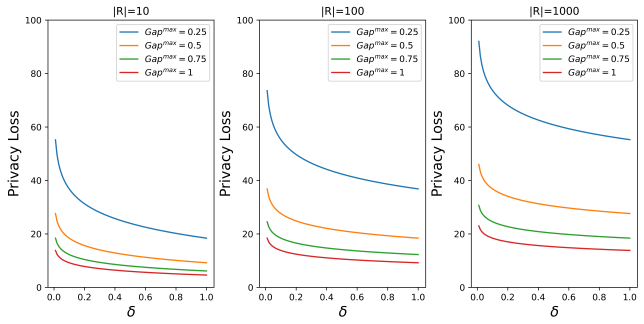

Fig. 9. Privacy loss ϵ versus confidence level $1-\delta$ for different values of Gap^{max}.

real valuation function, given $\alpha = 0.9$ and $\epsilon = 0.1$, leads to $\Delta\mathcal{U}_2^c = 0.02$ that is less than ϵ.

E. Tuning Privacy and Optimality Parameters

As we saw in section IV-B , the upper-bound for the performance gap is parametrized by ϵ, $|\mathcal{R}|$, and $\delta \in [0,1]$. In this section, we investigate how these parameters are related, and how the market operator should tune them. By some simple manipulations on the provided performance gap in (6), we obtain

$$\epsilon = \frac{2}{Gap^{max}} \ln\left(\frac{|\mathcal{R}|}{\delta}\right), \tag{16}$$

where Gap^{max} is the upper-bound of the gap between the optimal solution and the private solution. Based on this equation, Fig. 9 illustrates that, given a specific Gap^{max}, how much the market incurs privacy loss for different values of confidence level $1-\delta$. As we expected, for decreasing the Gap^{max}, the market operator should blatantly increase the privacy loss parameter, which means higher risk of privacy breach for the market participants. Indeed, for having a non-trivial privacy loss with a reasonable guarantee, the market operator has to scarify the social welfare. Due to (16), the dependence of ϵ on $|\mathcal{R}|$ is logarithmic, and it is clearly shown in Fig. 9 that larger set of samples for the output space imposes higher privacy loss. Therefore, choosing the sample size of the output space comes to a trade-off between the Gap^{max} and the sampling error for discretizing the output space.

F. Comparison with the input perturbation approach

In this section, we provide a quantitative comparison between our proposed mechanism and the input perturbation approach. Specifically, we implement the Laplace mechanism to obfuscate the input data and achieve DP in a market-clearing problem. The input perturbation is a straightforward approach for achieving DP in a computation, where the input data is privatized. Then, based on the post-processing property of DP, every computation on this privatized input data is differentially private [15].

The Laplace mechanism adds a calibrated zero-mean Laplace noise for privatizing the desired quantity x in the following sense:

$$\tilde{x} = x + \mathrm{Lap}\left(\frac{\Delta}{\epsilon}\right), \tag{17}$$

where $\tilde{x}$ is the privatized quantity, Δ is the sensitivity of the quantity x, ϵ is the privacy parameter, and $\mathrm{Lap}(\cdot)$ is the Laplace noise with parameter $b = \Delta/\epsilon$ and the probability density function $p(y) = \frac{1}{2b}\exp\left(-\frac{|y|}{b}\right)$ [30]. For implementing the input perturbation via the Laplace mechanism in our setting, we need to privatize each market participant i's valuation function v_i. In this regard, we add calibrated Laplace noise to the coefficients of each producer i's cost function, $C_{i,\theta_i}(\cdot) := a_i^g g_i^2 + b_i^g g_i + c_i^g$, and each consumer i's utility function, $U_{i,\theta_i}(\cdot) := a_i^u d_i^2 + b_i^u d_i + c_i^u$. Moreover, the sensitivity of each coefficient is equal to its range, e.g., $\Delta(a^u) = a^u_{\max} - a^u_{\min}$.

Table VI summarizes the quantitative comparison between the two mechanisms, where we use the shorthand Exp for the exponential mechanism and the shorthand InLap for the input perturbation via the Laplace mechanism. We provide the mean and standard deviation (std) of the market-clearing quantities and social welfare for three values of ϵ. For a given ϵ, the std of the market-clearing quantities and social welfare are higher under the input perturbation in compare to the exponential mechanism. Indeed, the input perturbation approach introduces more noise into the market-clearing problem for the same privacy level. As we expected, the exponential mechanism results in a solution with higher social welfare. In particular, in a high privacy regime, the superiority of the exponential mechanism is more considerable. For instance, when $\epsilon = 0.1$, the mean of

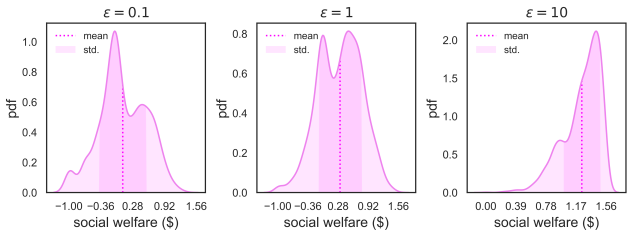

Fig. 10. Probability distribution of the social welfare under InLap.

the social welfare under the exponential mechanism and input perturbation are 0.95 and 0.08, respectively.

Fig. 10 shows the probability distribution of the social welfare under the InLap mechanism. Unlike the exponential mechanism, the randomness of the InLap mechanism does not consider the quality of the market-clearing outputs for a given privacy parameter. That is, the output of the market-clearing problem based on the InLap mechanism is not biased towards the high quality solutions. Thus, as we can see in Fig. 10, the InLap mechanism does not assign higher probability density to solutions with higher social welfare. However, as ϵ increases, the probability distribution of the social welfare leans towards the optimal value, $\mathrm{sw}^* = 1.56$, which reflects the inherent trade-off between the privacy and utility of the computation in DP. Due to Fig. 10, in a high privacy regime, it is likely to experience negative social welfare under the InLap mechanism. In contrast, the exponential mechanism suppresses the likelihood of the solutions with the negative social welfare.

VII. Conclusion

This paper presented a differentially private mechanism for local electricity markets. The proposed mechanism provides a provable bound on the disclosure risk of individuals' private data and the corresponding informational harms caused by releasing the market outputs. We applied the VCG mechanism as our underlying non-private mechanism in the market and implemented the exponential mechanism for privatizing the allocation and payment rules of the market. We saw that providing privacy for the market participants comes with a social welfare reduction, and we provided an upper-bound for this optimality gap. Furthermore, the proposed mechanism is approximately truthful and the market participants have almost no incentive to behave strategically by misreporting their data to the market.

There are several future directions to explore. One interesting direction is to consider heterogeneous privacy preferences for the market participants in a differentially private market-clearing mechanism. Indeed, by specifying the privacy requirements at the individual level, rather than a uniform privacy parameter selected by the market operator, we do not provide excess privacy protection for the market participants with lower privacy requirement. As a result, we can achieve a higher level of social welfare. In another avenue for future research, one can focus on allocating the cost of privacy, which is the optimality gap in the market, to the market participants based on their privacy preferences.

Acknowledgments

We would like to thank the anonymous reviewers for their thoughtful comments and constructive suggestions. We are also grateful to Matin Nassabian for helpful and inspiring discussions in the process of preparing this paper.

References

[1] S. Bjarghov, M. Löschenbrand, A. I. Saif, R. A. Pedrero, C. Pfeiffer, S. K. Khadem, M. Rabelhofer, F. Revheim, and H. Farahmand, "Developments and challenges in local electricity markets: A comprehensive review," *IEEE Access*, vol. 9, pp. 58 910–58 943, 2021.

[2] G. Tsaousoglou, J. S. Giraldo, and N. G. Paterakis, "Market mechanisms for local electricity markets: A review of models, solution concepts and algorithmic techniques," *Renewable and Sustainable Energy Reviews*, vol. 156, p. 111890, 2022.

[3] M. Kezunovic, P. Pinson, Z. Obradovic, S. Grijalva, T. Hong, and R. Bessa, "Big data analytics for future electricity grids," *Electric Power Systems Research*, vol. 189, p. 106788, 2020.

[4] A. Samy, H. Yu, H. Zhang, and G. Zhang, "Spets: Secure and privacy-preserving energy trading system in microgrid," *Sensors*, vol. 21, no. 23, p. 8121, 2021.

[5] S. Xie, H. Wang, Y. Hong, and M. Thai, "Privacy preserving distributed energy trading," in *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2020, pp. 322–332.

[6] D. Lee and D. J. Hess, "Data privacy and residential smart meters: Comparative analysis and harmonization potential," *Utilities Policy*, vol. 70, p. 101188, 2021.

[7] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," *Journal of Privacy and Confidentiality*, vol. 7, no. 3, pp. 17–51, 2016.

[8] Y. Chen, S. Chong, I. A. Kash, T. Moran, and S. Vadhan, "Truthful mechanisms for agents that value privacy," *ACM Transactions on Economics and Computation (TEAC)*, vol. 4, no. 3, pp. 1–30, 2016.

[9] K. Nissim, "Privacy: From database reconstruction to legal theorems," in *Proceedings of the 40th ACM SIGMOD-SIGACT-SIGAI Symposium on Principles of Database Systems*, 2021, pp. 33–41.

[10] C. Domingo-Enrich and Y. Mroueh, "Auditing differential privacy in high dimensions with the kernel quantum r\'enyi divergence," *arXiv preprint arXiv:2205.13941*, 2022.

[11] A. Abidin, A. Aly, S. Cleemput, and M. A. Mustafa, "An mpc-based privacy-preserving protocol for a local electricity trading market," in *International Conference on Cryptology and Network Security*. Springer, 2016, pp. 615–625.

[12] Y. Lu, J. Lian, M. Zhu, and K. Ma, "Transactive energy system deployment over insecure communication links," *arXiv preprint arXiv:2008.00152*, 2020.

[13] R. Sarenche, M. Salmasizadeh, M. H. Ameri, and M. R. Aref, "A secure and privacy-preserving protocol for holding double auctions in smart grid," *Information Sciences*, vol. 557, pp. 108–129, 2021.

[14] K. Erdayandi, A. Paudel, L. Cordeiro, and M. A. Mustafa, "Privacy-friendly peer-to-peer energy trading: A game theoretical approach," *arXiv preprint arXiv:2201.01810*, 2022.

[15] S. Vadhan, "The complexity of differential privacy," in *Tutorials on the Foundations of Cryptography*. Springer, 2017, pp. 347–450.

[16] E. Buchmann, S. Kessler, P. Jochem, and K. Böhm, "The costs of privacy in local energy markets," in *2013 IEEE 15th Conference on Business Informatics*. IEEE, 2013, pp. 198–207.

[17] L. Wu and J. Li, "Privacy-preserving economic dispatch in competitive electricity market," in *2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*. IEEE, 2018, pp. 1–5.

[18] C. Dwork, N. Kohli, and D. Mulligan, "Differential privacy in practice: Expose your epsilons!" *Journal of Privacy and Confidentiality*, vol. 9, no. 2, 2019.

[19] 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.

[20] V. Dvorkin, F. Fioretto, P. Van Hentenryck, P. Pinson, and J. Kazempour, "Differentially private optimal power flow for distribution grids," *IEEE Transactions on Power Systems*, vol. 36, no. 3, pp. 2186–2196, 2020.

[21] F. Zhou, J. Anderson, and S. H. Low, "Differential privacy of aggregated dc optimal power flow data," in *2019 American Control Conference (ACC)*. IEEE, 2019, pp. 1307–1314.

[22] T. W. Mak, F. Fioretto, and P. Van Hentenryck, "Privacy-preserving obfuscation for distributed power systems," *Electric Power Systems Research*, vol. 189, p. 106718, 2020.
[23] Z. Yang, P. Cheng, and J. Chen, "Differential-privacy preserving optimal power flow in smart grid," *IET Generation, Transmission & Distribution*, vol. 11, no. 15, pp. 3853–3861, 2017.
[24] 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 Transactions on Industrial Informatics*, vol. 18, no. 1, pp. 707–718, 2021.
[25] X. Lou, D. K. Yau, R. Tan, and P. Cheng, "Cost and pricing of differential privacy in demand reporting for smart grids," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 3, pp. 2037–2051, 2020.
[26] M. G. Boroujeni, D. Fay, C. Dimitrakakis, and M. Kamgarpour, "Privacy of real-time pricing in smart grid," in *2019 IEEE 58th Conference on Decision and Control (CDC)*. IEEE, 2019, pp. 5162–5167.
[27] J. Zhao, T. Jung, Y. Wang, and X. Li, "Achieving differential privacy of data disclosure in the smart grid," in *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*. IEEE, 2014, pp. 504–512.
[28] A. Wood, M. Altman, A. Bembenek, M. Bun, M. Gaboardi, J. Honaker, K. Nissim, D. R. O'Brien, T. Steinke, and S. Vadhan, "Differential privacy: A primer for a non-technical audience," *Vand. J. Ent. & Tech. L.*, vol. 21, p. 209, 2018.
[29] S. Truex, N. Baracaldo, A. Anwar, T. Steinke, H. Ludwig, R. Zhang, and Y. Zhou, "A hybrid approach to privacy-preserving federated learning," in *Proceedings of the 12th ACM workshop on artificial intelligence and security*, 2019, pp. 1–11.
[30] C. Dwork, A. Roth *et al.*, "The algorithmic foundations of differential privacy." *Found. Trends Theor. Comput. Sci.*, vol. 9, no. 3-4, pp. 211–407, 2014.
[31] A. Cheu, A. Smith, J. Ullman, D. Zeber, and M. Zhilyaev, "Distributed differential privacy via shuffling," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2019, pp. 375–403.
[32] M. Joseph, A. Roth, J. Ullman, and B. Waggoner, "Local differential privacy for evolving data," *Advances in Neural Information Processing Systems*, vol. 31, 2018.
[33] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*. IEEE, 2007, pp. 94–103.
[34] J. Dong, D. Durfee, and R. Rogers, "Optimal differential privacy composition for exponential mechanisms," in *International Conference on Machine Learning*. PMLR, 2020, pp. 2597–2606.
[35] G. Tsaousoglou, J. S. Giraldo, P. Pinson, and N. G. Paterakis, "Mechanism design for fair and efficient dso flexibility markets," *IEEE transactions on smart grid*, vol. 12, no. 3, pp. 2249–2260, 2021.
[36] Y. Chen, O. Sheffet, and S. Vadhan, "Privacy games," *ACM Transactions on Economics and Computation (TEAC)*, vol. 8, no. 2, pp. 1–37, 2020.
[37] Y. Chen, R. Dwivedi, M. J. Wainwright, and B. Yu, "Fast mcmc sampling algorithms on polytopes," *The Journal of Machine Learning Research*, vol. 19, no. 1, pp. 2146–2231, 2018.
[38] M. M. Pai and A. Roth, "Privacy and mechanism design," *ACM SIGecom Exchanges*, vol. 12, no. 1, pp. 8–29, 2013.
[39] T. Zhang and Q. Zhu, "Dynamic differential privacy for admm-based distributed classification learning," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 172–187, 2016.
[40] X. Zhang, M. M. Khalili, and M. Liu, "Improving the privacy and accuracy of admm-based distributed algorithms," in *International Conference on Machine Learning*. PMLR, 2018, pp. 5796–5805.
[41] X. Cao, J. Zhang, H. V. Poor, and Z. Tian, "Differentially private admm for regularized consensus optimization," *IEEE Transactions on Automatic Control*, vol. 66, no. 8, pp. 3718–3725, 2020.
[42] K. Nissim, R. Smorodinsky, and M. Tennenholtz, "Approximately optimal mechanism design via differential privacy," in *Proceedings of the 3rd innovations in theoretical computer science conference*, 2012, pp. 203–213.
[43] A. Ghosh and A. Roth, "Selling privacy at auction," in *Proceedings of the 12th ACM conference on Electronic commerce*, 2011, pp. 199–208.
[44] Y. Chen, C. Zhao, S. H. Low, and S. Mei, "Approaching prosumer social optimum via energy sharing with proof of convergence," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2484–2495, 2020.