A Differentially Private Mechanism for Local Electricity Markets

Milad Hoseinpour, Mohammad Hoseinpour, *Student Member, IEEE*, 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 the market outputs. This kind of privacy breach would have major implications on the future transactions of the market participants or an unauthorized observer's belief 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. For doing 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 for the social welfare loss incurred by the privacy constraint and analyze the inherent trade-off between privacy and suboptimality. At 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 ongoing decarbonization, decentralization, and digitalization of power systems have paved the way for the advent of local electricity markets [1], [2]. These 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 technical, economic, 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 in the market, which are not likely otherwise [4], [5]. Therefore, the privacy concern can urge market participants to behave strategically by misreporting their data or even opt out of the market.

As a result, the privacy challenge 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 an unrestricted access to individuals' data and permit them to safely publish the market-clearing outcomes. To address this question, this paper aims to design a local electricity market that simultaneously guarantees rigorous privacy constraints, maintains data utility for statistical inference, and achieves near-optimal social welfare. To do so, we implement the notion of DP, which gives us a framework to quantitatively reason about privacy and bounds the disclosure risk of the private information associated with an individual's participation in the market [6]. Differentially private mechanisms typically offer a trade-off between the level of individuals' privacy in a dataset and the accuracy of the computation on that dataset [7]. Furthermore, unlike other privacy-preserving approaches, e.g., k-anonymity, DP gives a privacy guarantee which is robust to subsequent post-processing and makes no assumptions about an adversary's computational powers or side information [8].

A. Related Work

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. [9]. Nevertheless, the application of DP in power systems is in its initial stages, and it is getting more attention in recent years. Authors in [10] 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 OPF problem, and the utility loss is a constant factor away from optimality. In [11], 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 [12], authors provide a mechanism for privately releasing aggregate network statistics obtained from a DC-OPF. Moreover, the paper demonstrates that the noise distribution parameters injected by the proposed differentially private mechanism are linked to the topology of the network. A privacy-preserving mechanism for OPF in distributed power systems is proposed in [13]. The local differentially private mechanism relies on 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 [14]. And authors analyze the contribution of the injected noise on the locational marginal prices and generators dispatches.

In another line of works, the privacy of consumers connected to smart meters is studied. In [15], [16], differentially

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.

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 privacy constraints several cost allocation mechanisms based on cooperative game theory are used. Authors in [17] 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 [18].

The aforementioned research works are leaned toward two main categories including privacy-preserving OPF problems and statistical release of smart meters data. There is a significant research gap in addressing the privacy concerns in local electricity markets, which motivates this paper. It is worth mentioning that the cryptographic literature also addresses privacy concern in electricity markets, e.g., [19]–[21]. But our paper fundamentally differs from these works as in our setting the market participants are worried about what the public outcome of a market-clearing problem may leak about their sensitive information, 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.

B. Summary of Contributions

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

- We propose a differentially private mechanism for local electricity markets that releases a nearly-optimal solution while guarantying the outputs of the market would reveal virtually nothing about any individual's input data.
- Unlike additive noise approaches for achieving DP, e.g., Laplace mechanism and Gaussian mechanism, which may result in unfeasible and low-quality solutions, we implement the exponential mechanism which ensures the feasibility of the market outputs and selects high-quality solutions due to its embedded score function.
- We provide an upper-bound for the social welfare loss incurred by the privacy constraint in the market, which reflects the inherent trade-off between privacy and sub-optimality in DP.
- To reduce the computational complexity of the exponential mechanism, we discretize the feasibility space of the market-clearing problem via a sampling method for polytopes.

C. Paper Organization

The rest of the paper is organized as follows. The problem setup is presented in section II. Section III belongs to the methodology overview including the baseline mechanism in our local electricity market and DP. 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.

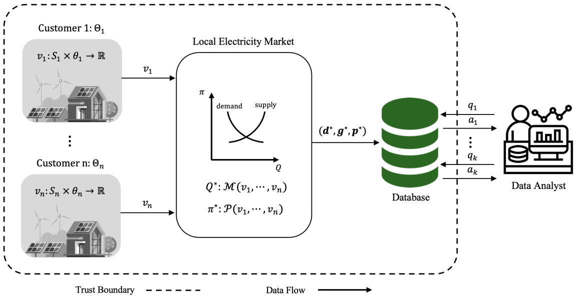
Customer 1: Θ_1
$v_1 : S_1 \times \theta_1 \to \mathbb{R}$
v_1
Customer n: Θ_n
$v_n : S_n \times \theta_n \to \mathbb{R}$
v_n
Local Electricity Market
π
demand
supply
Q
$Q^* : \mathcal{M}(v_1, \cdots, v_n)$
$\pi^* : \mathcal{P}(v_1, \cdots, v_n)$
$(\boldsymbol{d}^*, \boldsymbol{g}^*, \boldsymbol{p}^*)$
Database
q_1
a_1
q_k
a_k
Data Analyst
Trust Boundary
Data Flow

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

II. Problem Setup

We consider a pool-based market-clearing problem in a local energy community with a finite set of market participants Ω, comprising of producers Ω^p and consumers Ω^c. 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. In this regard, the local decisions $s_i \in S_i$ of consumer i and producer i are characterized by demand d_i and active power 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 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 as $v_i(d_i, \theta_i) = U_{i,\theta_i}(d_i)$. Also, for producer i, the valuation function reflects the negative of the cost of generating 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 i^{th} consumer and producer respectively, parameterized by type θ_i. Furthermore, for mathematical convenience, we rescale all the valuation functions by min-max normalization to the range of [0,1].

Fig.1 depicts a high-level view of the problem setup. As we can see, 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' payment, $p^* = (p_i^*)_{i \in \Omega}$. In electricity markets, the allocation rule is determined by maximizing the social welfare function $\text{sw}(v, s) = \sum_{i \in \Omega} v_i(s_i)$ subject to technical constraints of 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 the following:

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

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

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

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

where the constraint (1b) and (1c) reflect the demand and supply limits of the consumers and producers respectively. Also, the 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 goal of the data analyst is to learn about the population of the market participants by asking queries $\{q_j\}_{j=1}^k$ and taking answers $\{a_j\}_{j=1}^k$ from the database. But, the statistical release of the market-clearing outputs exposes the market participants to the risk of a privacy breach. Indeed, whoever outside of the trust boundary should not be able to learn anything at the individual level and violate the privacy of individuals.

III. Methodology Overview

A. The Non-Private Market-Clearing Mechanism

Before presenting the privacy-aware market-clearing mechanism, it is helpful to demonstrate the non-private market-clearing mechanism we try to build upon. Due to the nice theoretical properties of the VCG mechanism, e.g., individual rationality, incentive compatibility, and efficiency, we apply it in our local electricity market [22]. Based on Algorithm 1, agents report their valuation functions $\{v_i\}_{i=1}^n$ 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.

Algorithm 1 VCG Mechanism for Local Electricity Markets

Inputs: Set of valuation functions $\{v_i\}_{i=1}^n$.
Outputs: Market participants' set points $s^* = (d^*, g^*) \in S$ and payments $p = \{p_i\}_{i=1}^n$.

```
Solve the social welfare sw(v, s) maximization problem:
    $s^* \in \arg\max_{s\in S} \sum_{i\in\Omega} v_i(s_i)$
for all $i \in \Omega$ do
    Charge market participant $i$:
        $p_i(v_i, v_{-i}) = \max_{s\in S} \sum_{j\neq i\in\Omega} v_j(s_j) - \sum_{j\neq i\in\Omega} v_j(s^*)$
end for
return $s^*$ and $p$.
```

Since the VCG mechanism is incentive compatible, truthful behavior is the dominant strategy for the agents. Nevertheless, privacy-aware agents are concerned about the plausible harms of disclosure of their personal information, in the current market outcomes, on future transactions 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 an unauthorized observer about them. Yet incorporating all the scenarios in which information might affect the agents' future utility is a complicated task. DP avoids the need for such intricate modelling by providing a worst-case bound on agents' exposure to privacy loss [23].

B. Differential Privacy

DP is a formal mathematical standard for protecting individuals' privacy [24]. 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 ability to infer about individuals' data points [25], [26]. 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 $\epsilon \ge 0$, 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:

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

where the probability is over the internal randomness of $\mathcal{M}$ [6].

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

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

where $\|\cdot\|_1$ is the ℓ_1-norm [27].

Perturbation techniques for satisfying DP in a computation are classified into two basic categories: 1) adding calibrated random noise to the input data, and 2) adding calibrated random noise to the outputs [6]. Nevertheless, leveraging these additive noise techniques in a market-clearing problem has two major drawbacks. First, simply adding noise to the output of a market-clearing problem may lead to unfeasible solutions,

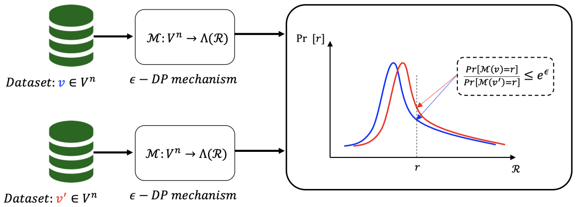
$\mathcal{M}: V^n \to \Lambda(\mathcal{R})$
Dataset: $v \in V^n$
$\epsilon - DP$ mechanism
$\mathcal{M}: V^n \to \Lambda(\mathcal{R})$
Dataset: $v' \in V^n$
$\epsilon - DP$ mechanism
Pr [r]
$\frac{Pr[\mathcal{M}(v)=r]}{Pr[\mathcal{M}(v')=r]} \leq e^{\epsilon}$
r
$\mathcal{R}$

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

which entails corrective mechanisms by the market operator. Second, by perturbing the answer of a market-clearing problem the social welfare may suffer drastically.

Unlike additive noise approaches, we implement the exponential mechanism which overcomes the aforementioned challenges in market-clearing problems. 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 [28]. Indeed, the output of this mechanism is always a member of that arbitrary range, and it is a 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 $q : \mathcal{R} \times \mathcal{X}^n \to \mathbb{R}$ which 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 [27].

Definition 3 (The 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 $\mathrm{ExpMech}\,(x, q, \mathcal{R}, \epsilon)$ 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 [29].

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 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 in for defining the probability distribution:

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

Then, we determine the sensitivity of the social welfare function $\mathrm{sw}(\cdot)$, which we designate as the score function, that is

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

where $v_i \in [0, 1]$, $\forall i \in \Omega$.

In the next step, we need to define the output distribution of the mechanism by assigning a probability proportional to $\exp\left(\epsilon \frac{\sum_{i=1}^{n} v_i(r)}{2}\right)$ for each $r \in \mathcal{R}$. Furthermore, those probabilities should be normalized via the normalizing factor $\phi(\mathcal{R}) = \sum_{r \in \mathcal{R}} \exp\left(\epsilon \frac{\sum_{i=1}^{n} v_i(r)}{2}\right)$. Thus, the exponential mechanism gives a greater weight to outputs with higher social welfare and makes their selection as the market-clearing outcome exponentially more likely.

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 [30] 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. Algorithm 2 summarizes the proposed privacy-aware market-clearing mechanism for local electricity markets.

B. Performance Gap

We constructed a privacy-aware market-clearing mechanism, which approximately maximizes the social welfare in a differentially private manner. Drawing on a theorem in [31],

Algorithm 2 Differentially Private Market-Clearing Mechanism

Inputs: Set of valuation functions $\{v_i\}_{i=1}^n$, privacy loss parameter ϵ, sample size n_s.

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

```
Draw $n_s$ sample $r$ uniformly from the output space $\mathcal{O} \subset \mathbb{R}^n$
for all $r \in \mathcal{R}$ do
    Compute the social welfare $sw(v, r) = \sum_{i=1}^n v_i(r)$
end for
Compute the normalizing factor:
    $\phi(\mathcal{R}) = \sum_{r \in \mathcal{R}} \exp\left(\epsilon \frac{\sum_{i=1}^n v_i(r)}{2}\right)$
Construct the probability distribution $\mathcal{D}^*$ such that
    $\Pr_{\mathcal{D}^*}(r \in \mathcal{R}) = \frac{\exp\left(\epsilon \frac{\sum_{i=1}^n v_i(r)}{2}\right)}{\phi(\mathcal{R})}$
return $r \sim \mathcal{D}^*$.
```

we discuss the accuracy of this computation and investigate the performance gap by running the proposed market-clearing mechanism in the following.

Theorem 1. *For any $\mathcal{R}$, v, ϵ, 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*

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

Proof. Let $r^* = \max_{r \in \mathcal{R}} \mathrm{sw}(v, r)$. For any value 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 allocation $r \in \mathcal{R}$ 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

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

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

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

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

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

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

C. Differentially Private Computation of Payments

Besides the market-clearing outcomes, the payments of the market participants will be available 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 functions $v \sim v' \in V^n$ and any possible payment $p \in \mathcal{P}$, the following privacy constraint should hold:

$$\begin{aligned} &\Pr[\, p_1(v), \cdots, \, p_n(v) \in \mathcal{P}] \leq \\ &\qquad e^{\epsilon} . \Pr[\, p_1(v'), \cdots, \, p_n(v') \in \mathcal{P}]. \end{aligned} \tag{11}$$

As mentioned previously, for computing the VCG payments, we need to compute the social welfare. In addition, arbitrary computation on the output of an ϵ-differentially private mechanism does not undermine its privacy guarantee, and the resulting computation would also be ϵ-differentially private, known as post-processing property [24]. Consequently, for privatizing the VCG payments, there is no need for 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 $\{v_i\}_{i=1}^n$ 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 $i \in \Omega$, $\mathrm{sw}_{-i}(\mathcal{D}^*)$. Then, for each agent $i \in \Omega$, Algorithm 3 removes agent i and passes $\{v_j\}_{j=1 \& j \neq i}^n$ 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 $\mathrm{sw}_{-i}(\mathcal{D}^*)$ from $\mathrm{sw}_{-i}\left(\mathcal{D}_{-i}^*\right)$ for each agent, Algorithm 3 returns the payment profile p.

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 each agent. 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.

Algorithm 3 Private Computation of the VCG Payments

Inputs: Set of valuation functions $\{v_i\}_{i=1}^n$, privacy loss parameter ϵ, sample size n_s.

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

```
call Algorithm 2:
    Inputs: $\{v_i\}_{i=1}^n$, $\epsilon$, $n_s$
    Outputs: $r \sim \mathcal{D}^*$
for all agent $i \in \Omega$ do
    call Algorithm 2:
        Inputs: $\{v_j\}_{j=1\&j\neq i}^n$, $\epsilon$, $n_s$
        Outputs: $r \sim \mathcal{D}_{-i}^*$
    $\mathrm{sw}_{-i}\left(\mathcal{D}_{-i}^*\right) = \mathbb{E}_{r\sim\mathcal{D}_{-i}^*}\left[\sum_{j\neq i} v_j\left(r\right)\right]$
    $\mathrm{sw}_{-i}\left(\mathcal{D}^*\right) = \mathbb{E}_{r\sim\mathcal{D}^*}\left[\sum_{j\neq i} v_j\left(r\right)\right]$
    $p_i = \mathrm{sw}_{-i}\left(\mathcal{D}_{-i}^*\right) - \mathrm{sw}_{-i}\left(\mathcal{D}^*\right)$
end for
return $p$.
```

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 [31]:

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

This definition implies that in an $\epsilon-$approximately dominant strategy truthful mechanism, no agent has more than ϵ additive incentive for mis-reporting 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 [32].

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

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

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

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

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

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

□

In this regard, our proposed privacy-preserving market-clearing mechanism is approximately truthful, and market participants have almost no incentive for strategic behavior. Nonetheless, we give up on the exact truthfulness of the VCG mechanism for satisfying privacy constraints.

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

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

VI. Numerical Results

This section presents numerical case studies to reflect the theoretical properties of the proposed differentially private mechanism for local electricity markets. Toward that, a testbed comprised of three producers and three consumers in a local energy community is provided by modifying a testbed from [33]. The cost function of producer i and utility function of consumer i are in the quadratic format $C_i\left(\cdot\right) := a_i^g g_i^2 + b_i^g g_i + c_i^g$ and $U_i\left(\cdot\right) := a_i^u d_i^2 + b_i^u d_i + c_i^u$ respectively. The parameters for producers and consumers are given in Table I and Table II. Our model is implemented in Python using CPLEX Python package and the package in [30] for sampling from polytopes.

A. Market-Clearing Outcomes

In this section, we examine 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), which are drawn uniformly from the feasibility set of the market-clearing problem, are represented in Table III. Moreover, the optimal solution (opt) of the market-clearing problem in a non-private setting is added to these samples. 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. 3 shows the probability distribution of the social welfare for different values of ϵ. As we know, small quantities of privacy loss parameter, like $\epsilon = 0.1$, reflect higher level of privacy, and, we can see, in Fig. 3, that the probability distribution over

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

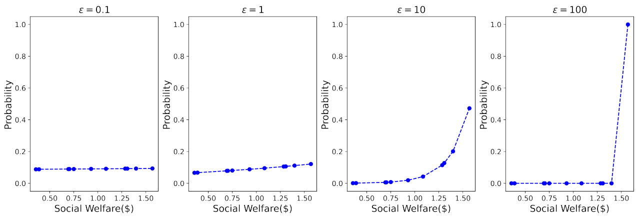

Fig. 3. Probability distribution over the possible social welfares.

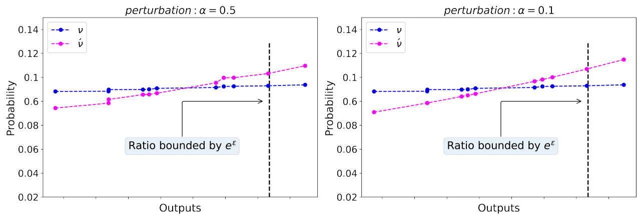

Fig. 4. Multiplicative closeness of probability distributions over the outputs given two neighbouring sets of valuation functions.

the outcomes is almost uniform for $\epsilon = 0.1$. It means that the market-clearing mechanism does not care about the quality of the outcomes 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-aware market-clearing mechanism turn to a non-private mechanism with the optimal solution.

B. Privacy Guarantee

DP guarantees that the output of our privacy-preserving 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 examining this property, we created two pair of neighboring valuation functions via perturbing the valuation function of the 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. 4 shows that the ratio of probabilities in the output distributions of the mechanism under the two neighboring sets of valuation profile $v \sim v'$ is bounded by $e^{0.5}$. Indeed, if we go point by point through the social welfares corresponding to 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, $\mathrm{sw}_{-i}(\mathcal{O}^*)$, 2) the welfare of other participants when the individual i is not in the market, $\mathrm{sw}_{-i}\left(\mathcal{O}^*_{-i}\right)$. After subtracting $\mathrm{sw}_{-i}(\mathcal{O}^*)$ from $\mathrm{sw}_{-i}\left(\mathcal{O}^*_{-i}\right)$, Fig. 5 shows the expected VCG payment of each individual i. We can see in the plots that there is a swing in each payment. These swings are rooted in the different degradation speed of $\mathrm{sw}_{-i}(\mathcal{O}^*)$ and $\mathrm{sw}_{-i}\left(\mathcal{O}^*_{-i}\right)$ when ϵ decreases. In addition, by increasing the privacy loss parameter ϵ, payments reach to their optimal values: $p^g_1 = -0.57$, $p^g_2 = -0.9$, $p^g_3 = -1.45$, $p^c_1 = 0.59$, $p^c_2 = 0.53$, $p^c_3 = 0.7$. 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 privacy loss parameter 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. 6 depicts the payoffs of the market participants 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

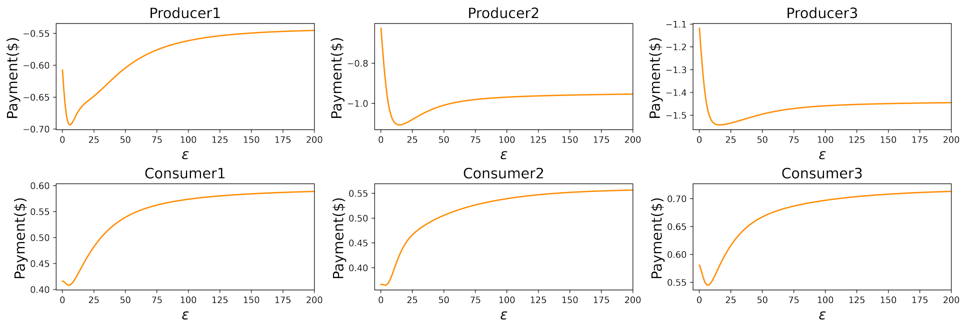

Fig. 5. Asymptotic convergence of the privatized VCG payments to their optimal value versus privacy loss parameter ϵ.

TABLE IV
THE EXPECTED VCG PAYMENTS OF 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

TABLE V
CHANGE OF MARKET PARTICIPANTS' PAYOFF CAUSED BY MIS-REPORTING 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

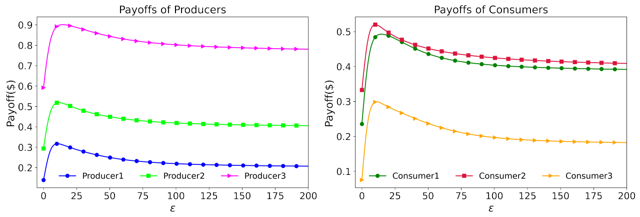

Fig. 6. Payoffs of market participants versus privacy loss parameter ϵ.

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. 6, even providing high level of privacy does not incur negative payoffs to the market participants. Furthermore, by increasing ϵ, payoffs converge towards their non-private values.

As mentioned before, based on the utility-theoretic interpretation of DP, no individual can gain more than ϵ utility by mis-reporting their 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 change in the payoff of i^{th} producer and consumer, respectively. Due to Table V, despite producer 1 with a negative $\Delta\mathcal{U}_1^p$ in all scenarios, 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, 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 upper-bound 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. 7 illustrates that, given a specific Gap^{max}, how much the market incurs privacy loss for different values of the confidence level $1-\delta$. As we expected, for decreasing the Gap^{max}, the market operator should blatantly rise 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 the (16), the dependence of the privacy loss on $|\mathcal{R}|$ is logarithmic, and it is clearly shown in Fig. 7 that larger set of samples for the output space imposes

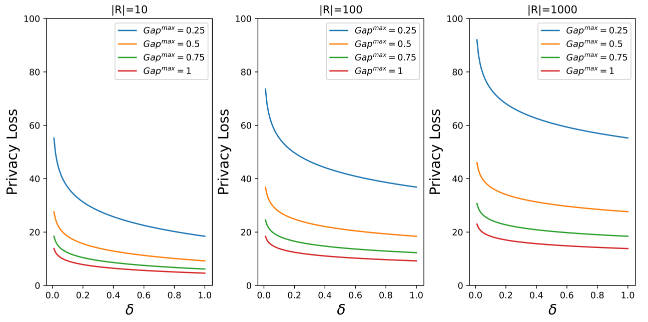

Fig. 7. Privacy loss ϵ versus confidence level $1 - \delta$ for different values of Gap^{max}.

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.

VII. Conclusion

This paper presented a differentially private mechanism for local electricity markets, which entails privacy-preserving guarantees. 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 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 market participants have nearly no incentive to behave strategically by misreporting their data to the market.

There are several future directions to explore. One interesting direction is to address the privacy concern in Peer-to-Peer (P2P) electricity markets, where there is no centralized market operator, and the trust boundary is pushed toward each individual. Roughly speaking, in such settings, market participants individually randomize their own data and send it to the negotiation process with other peers. In another avenue for future research, one can focus on allocating the cost of privacy, which is the optimality gap in the market, to customers with heterogenous value for privacy.

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] Z. Erkin, J. R. Troncoso-Pastoriza, R. L. Lagendijk, and F. Pérez-González, "Privacy-preserving data aggregation in smart metering systems: An overview," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 75–86, 2013.

[6] 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.

[7] 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.

[8] 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.

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

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

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

[20] J. M. Junior, J. P. C. da Costa, C. C. Garcez, R. de Oliveira Albuquerque, A. Arancibia, L. Weichenberger, F. L. L. de Mendonça, G. d. Galdo, and R. T. de Sousa Jr, "Data security and trading framework for smart grids in neighborhood area networks," *Sensors*, vol. 20, no. 5, p. 1337, 2020.

[21] 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.

[22] Y. Xu and S. H. Low, "An efficient and incentive compatible mechanism for wholesale electricity markets," *IEEE Transactions on Smart Grid*, vol. 8, no. 1, pp. 128–138, 2015.

[23] Y. Chen, O. Sheffet, and S. Vadhan, "Privacy games," *ACM Transactions on Economics and Computation (TEAC)*, vol. 8, no. 2, pp. 1–37, 2020.

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

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] M. M. Pai and A. Roth, "Privacy and mechanism design," *ACM SIGecom Exchanges*, vol. 12, no. 1, pp. 8–29, 2013.

[32] 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.

[33] 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.