The Cost of Privacy for Energy Sectors Coordination

Lesia Mitridati[1,3],Emma Romei[1],Ferdinando Fioretto[2],Gabriela Hug[1]
[1] Institute for Power Systems & High Voltage Technology, ETH Zurich, Zürich, Switzerland,
[2] Dept. of Electrical Engineering and Computer Science, Syracuse University, Syracuse, USA,
[3] corresponding author: mitridati@eeh.ee.ethz.ch

***Abstract*—The coordination between interdependent energy systems has been identified has a cornerstone in the path towards a sustainable future. The coordination between the sequential markets that operate these systems can be achieved through a Stackelberg game framework. However, this coordination framework relies on the exchange of sensitive information between the market operators, namely data streams representing the supply and demand curves of market participants. To address these privacy concerns and facilitate the exchange of information between the agents in a Stackelberg game, this paper introduces the so-called *w*-privacy-preserving Stackelberg mechanism (*w*-PPSM). The proposed *w*-PPSM ensures (i) *privacy* of the information exchanged, using a differential-privacy framework; and (ii) *fidelity* of the Stackelberg game coordination framework w.r.t. its original solutions, using an optimization-based post-processing phase. In addition, multiple numerical simulations in a realistic integrated heat and electricity system demonstrate that the *w*-PPSM increases the fidelity of the Stackelberg game solutions by up to two orders of magnitude compared to a traditional Laplace mechanism.**

***Index Terms*—multi-energy systems, hierarchical optimization, differential privacy, time series, Laplace noise**

I. Introduction

The coordination between energy sectors, such as natural gas, district heating, electricity, as well as industries, such as transportation, has been identified as a crucial step towards an energy-efficient, cost-effective, and sustainable future [1]–[3]. Indeed, the underlying techno-economic interactions between different energy carriers create potential synergies that can be harnessed.

However, the coordination between the *sequential* and *interdependent* markets that operate these energy sectors is challenging. This coordination issue has traditionally been modelled using *Stackelberg game* frameworks, in which one market operator (leader) anticipates the impact of its decisions on another market operator (follower), which, in turn, impact the objective cost of the leader [4]. This framework has been used extensively in the literature to coordinate district heating [5], [6], natural gas [3], [7], transportation [8], and electricity markets. In particular, the electricity-aware heat market (EAHM) developed in [6] provides a market-based mechanism for the coordination of heat and electricity systems. This market framework allows the heat market operator (leader) to optimize the dispatch of combined heat and power plants (CHPs) and heat pumps (HPs), while anticipating their impact on the electricity market (follower) prices, which in turn impact heat production costs of CHPs and HPs. Another relevant application of this coordination framework is the gas-aware electricity market framework proposed in [7]. In this application, the electricity market (leader) must anticipate gas prices in the natural gas market (follower) to minimize the production cost of gas-fired power plants. Similarly, the coordination of the transportation and power systems has been modelled using Stackelberg game frameworks [8]. Indeed, the optimal placement and control of electric vehicles charging stations (leader) must anticipate electricity prices (follower) to minimize charging and investment costs.

These coordination frameworks can achieve an optimal coordination between the energy systems while maintaining independence of the market operators. However, they rely on the exchange of high-fidelity information, such as supply and demand curves, between the leader and the follower in order to model and harness the bi-direction interactions between them. Indeed, [6] shows that the uncertainty resulting from the lack of information exchange between the agents in a Stackelberg game may result in a sub-optimal operation of the overall system, and financial losses for both agents. Despite recent regulatory changes encouraging information exchange between market and system operators [9], individual users may be reluctant to exchange some information with other system and market operators due to privacy concerns. Revealing this sensitive data may provide a competitive advantage over other strategic agents, reveal identifying personal information, induce financial losses and security risks for the users, and even benefit external attackers [10], [11]. In particular, in the EAHM developed in [6], the hourly electricity loads of individual consumers are considered as sensitive data. These privacy concerns are a major barrier to the social acceptance and wide-spread development of market-based coordination between energy sectors. In this context, this paper focuses on developing a privacy-preserving mechanism for the exchange of high-fidelity data between agents in a Stackelberg game to facilitate the market-based coordination of energy systems.

This work is partially funded by the NCCR Automation.

To address the aforementioned privacy concerns, *Differential Privacy* (DP) has emerged as a robust privacy framework for various cyber-physical systems [12]. In particular, it has found multiple applications in energy systems [13], the healthcare and transportation sectors [14], and demographics [15]. DP mechanisms inject carefully calibrated noise to protect the disclosure of the individuals' data, while enabling meaningful calculations and analysis on the population's data. This framework is therefore relevant to protect the sensitive data exchanged between the leader and the follower in a Stackelberg game, while facilitating their coordination. However, the obfuscation of highly correlated and high-dimensional streams of data is particularly challenging due to the high level of noise required to maintain privacy goals [16]. When highly-perturbed data is used as input to optimization problems with strong techno-economic constraints, such as market clearing, control, and dispatch problems in energy systems, it may lead to severe fidelity and feasibility issues. To address this issue the authors in [17] developed an optimization-based approach to restore fidelity of the perturbed data in classic DP mechanisms. The authors in [18] adapted this approach to the exchange of information between the leader and the follower in a Stackelberg game. However, these recent advances in the literature are not suited to the release of highly correlated data streams, such as supply and demand curves in energy markets. Furthermore, the aforementioned papers provided only limited theoretical properties on the fidelity of these DP mechanisms. In this context, the w-privacy framework, which obfuscates *data streams* over a predefined time window, is of particular interest [19]. Our preliminary work [20] introduced the w-PPSM algorithm, which protects the exchange of hourly electricity loads over a 24-hour window for the coordination between heat and electricity markets. However, this preliminary work did not provide theoretical guarantees on the fidelity of this privacy-preserving coordination framework, or extensive numerical validations of the proposed mechanism under realistic operating conditions.

The work in this paper aims at addressing the aforementioned research gaps, and providing a general privacy-preserving framework for the coordination of energy and industry sectors. The contributions of this paper are fourfold:

1) We introduce and formulate a general class of Stackelberg game frameworks for the coordination of interdependent energy and industry sectors. While this work is motivated and illustrated by the coordination between heat and electricity markets, a broader range of applications in energy systems is discussed.
2) We generalize the w-PPSM algorithm developed in our preliminary work [20] to facilitate the sharing of differentially-private data streams with high fidelity for this class of Stackelberg games.
3) We show that the w-PPSM satisfies interesting theoretical properties. In particular, it achieves strong privacy properties for data streams, while providing a bound on the error introduced on the sensitive data and energy prices. Furthermore, major novelty of this work is to quantify and provide provide theoretical bounds on the fidelity of the w-PPSM using the so-called *cost of privacy*.
4) Through multiple realistic numerical simulations, we show the efficiency of the w-PPSM under varying privacy parameters and operating conditions. The numerical results show that the w-PPSM can reduce the cost of privacy by up to two orders of magnitude compared to a standard DP mechanism, and achieves a close-to-optimal coordination between the energy sectors.

The remainder of this paper is organized as follows. Section II introduces the standard Stackelberg game framework for the coordination of energy sectors through the motivating example of heat and electricity systems. Section III summarizes the background on DP and introduces the privacy and fidelity goals of the DP algorithm considered. Section IV presents the generalized w-PPSM algorithm. Section V introduces the theoretical properties of the w-PPSM. Section VI presents the numerical evaluations of the mechanism in the case of the coordination between heat and electricity markets. Section VII concludes this paper. Detailed mathematical formulations of the market-clearing problems and proofs of the theoretical properties of the w-PPSM are provided in the online Appendix.

II. Coordination between Energy Sectors: The Case of Heat and Electricity

For the sake of clarity, this section introduces a Stackelberg game framework for the coordination between energy sectors using the case of heat and electricity systems as a motivating example. We will then discuss how the case of heat and electricity systems represents a typical class of Stackelberg games that have applications to multiple coordination problems in energy systems.

A. Motivating Example: Status Quo in Heat and Electricity Markets

In Nordic countries, including in Denmark, heat and electricity systems are operated by *sequential* and *decoupled* competitive markets; where the heat market is cleared *before* the electricity market. Due to their techno-economic characteristics, CHPs and HPs implicitly create interdependencies between the heat and electricity markets. We introduce below these interdependencies, as well as the mathematical formulation of these sequential and decoupled heat and electricity markets.

1) Challenges in Heat Market: Prior to the electricity market clearing, all heat market participants $s \in \mathcal{S}^{\mathrm{H}}$, including CHPs and HPs, place independent price-quantity bids in the heat market for each hour of the

following day $t \in \mathcal{T}$. Their heat production $\boldsymbol{h_{st}}$ is dispatched based on a merit-order and least-cost principle.

The quantity bids of all heat market participants at each hour represent their minimum and maximum production ($H_{st}^{\min}, H_{st}^{\max}$), and their price bids represent their variable heat production costs. The price bids of heat-only producers $s \in \mathcal{S}^{\text{HO}}$ is defined by their constant marginal heat production cost at each hour, such that their heat production cost $\boldsymbol{\Gamma_{st}^{H}}(\boldsymbol{h_{st}}) = C_{st}^{\text{H}}\boldsymbol{h_{st}}$. However, the heat production cost of CHPs and HPs is a function of electricity prices. Indeed, HPs $s \in \mathcal{S}^{\text{HP}}$ purchase electricity $\boldsymbol{e_{st}}$ to produce heat $\boldsymbol{h_{st}}$ at a fixed ratio, such that:

$$\boldsymbol{e_{st}} = -\frac{\boldsymbol{h_{st}}}{\text{COP}_s},\ \forall s \in \mathcal{S}_z^{\text{HP}}, t \in \mathcal{T}. \tag{1}$$

Therefore, their heat production cost is defined as:

$$\boldsymbol{\Gamma_{st}^{H}}(\boldsymbol{h_{st}}, \boldsymbol{\lambda_{zt}^{E}}) = \boldsymbol{\lambda_{zt}^{E}}\frac{\boldsymbol{h_{st}}}{\text{COP}_s},\ \forall s \in \mathcal{S}_z^{\text{HP}}, t \in \mathcal{T}, \tag{2}$$

where $\boldsymbol{\lambda_{zt}^{E}}$ represents the electricity market price in zone $z \in \mathcal{Z}^{\text{E}}$. Furthermore, CHPs can produce heat $\boldsymbol{h_{st}}$ and electricity $\boldsymbol{e_{st}}$ at varying ratios, within the joint feasible space:

$$\boldsymbol{e_{st}} \geq R_s \boldsymbol{h_{st}}, \forall s \in \mathcal{S}^{\text{CHP}}, t \in \mathcal{T} \tag{3a}$$

$$\rho_s^{\text{H}}\boldsymbol{h_{st}} + \rho_s^{\text{E}}\boldsymbol{e_{st}} \leq F_s^{\max}, \forall s \in \mathcal{S}^{\text{CHP}}, t \in \mathcal{T}, \tag{3b}$$

where R_s represents the minimum power-to-heat ratio, $F_s^{\max}$ the maximum fuel intake, and ρ_s^{E} and ρ_s^{H} the electricity and heat efficiency (respectively). The heat production cost of CHPs is defined as their total production cost, minus revenues from electricity sales, such that, for a given value of the heat dispatch $\boldsymbol{h_{st}}$ and electricity price $\boldsymbol{\lambda_{zt}^{E}}$:

$$\begin{aligned}\boldsymbol{\Gamma_{st}^{H}}(\boldsymbol{h_{st}}, \boldsymbol{\lambda_{zt}^{E}}) = \quad & \min_{\boldsymbol{e_{st}}} \{C_{st}(\rho_s^{\text{H}}\boldsymbol{h_{st}} + \rho_s^{\text{E}}\boldsymbol{e_{st}}) - \boldsymbol{\lambda_{zt}^{E}}\boldsymbol{e_{st}}\} \\ & \text{s.t. Eqs. (3a)} - \text{(3b)} \\ , \forall s \in \mathcal{S}_z^{\text{CHP}}, t \in \mathcal{T}.\end{aligned} \tag{4}$$

For low electricity prices, it represents the cost of producing heat at the minimum electricity ratio (3a), and, for high electricity prices, it represents the opportunity loss of producing heat at the maximum electricity ratio (3b). For each value of the heat dispatch, this heat production cost is a concave piece-wise linear function of the electricity prices, and, can be expressed as:

$$\begin{aligned}\boldsymbol{\Gamma_{st}^{H}}(\boldsymbol{h_{st}}, \boldsymbol{\lambda_{zt}^{E}}) = \min\left\{\boldsymbol{\Gamma_{st1}^{H}}(\boldsymbol{h_{st}}, \boldsymbol{\lambda_{zt}^{E}}), \boldsymbol{\Gamma_{st2}^{H}}(\boldsymbol{h_{st}}, \boldsymbol{\lambda_{zt}^{E}})\right\} \\ , \forall s \in \mathcal{S}_z^{\text{CHP}}, t \in \mathcal{T}\end{aligned} \tag{5}$$

where

$$\begin{aligned}\boldsymbol{\Gamma_{st1}^{H}}(\boldsymbol{h_{st}}, \boldsymbol{\lambda_{zt}^{E}}) &= \left[C_{st}(\rho_s^{\text{E}}R_s + \rho_s^{\text{H}}) - R_s\boldsymbol{\lambda_{zt}^{E}}\right]\boldsymbol{h_{st}}, \forall s \in \mathcal{S}_z^{\text{CHP}}, t \in \mathcal{T} \\ \boldsymbol{\Gamma_{st2}^{H}}(\boldsymbol{h_{st}}, \boldsymbol{\lambda_{zt}^{E}}) &= \frac{\rho_s^{\text{H}}}{\rho_s^{\text{E}}}\boldsymbol{\lambda_{zt}^{E}}\boldsymbol{h_{st}} + F_s^{\max}(C_{st} - \frac{\boldsymbol{\lambda_{zt}^{E}}}{\rho_s^{\text{E}}}), \forall s \in \mathcal{S}_z^{\text{CHP}}, t \in \mathcal{T}\end{aligned} \tag{6}$$

Since the day-ahead heat market is cleared prior to the day-ahead electricity market, CHPs and HPs use a deterministic forecast of the electricity prices for each hour of the following day when bidding in the heat market. This approach allows the heat market operator to minimize the heat production cost of all market participants based on the expected electricity prices. However, as these electricity prices are considered as exogenous parameters, the heat market operator cannot model how the heat production of CHPs and HPs may impact the electricity market outcomes (i.e. prices), which in turn, impact the heat production costs of CHPs and HPs and the merit order in the heat market. This electricity-myopic heat dispatch may lead to a sub-optimal heat dispatch and financial losses for CHPs and HPs in the heat market.

2) Challenges in Electricity Market: Once the day-ahead heat market has been cleared, all electricity market participants, including CHPs and HPs, place independent price-quantity bids in the electricity market for each hour of the following day and are dispatched based on a merit-order and least-cost principle.

The price bids of all electricity market participants at each hour are defined by their constant marginal electricity production costs. The quantity bids of electricity-only market participants at each hour are defined by their minimum and maximum electricity production. However, as the heat and electricity outputs of CHPs and HPs are strongly linked, their quantity bids are dependent on their day-ahead heat dispatch. The quantity bids of HPs represent their inflexible electricity consumption to supply their day-ahead heat dispatch. The quantity bids of CHPs represents their minimum and maximum electricity ratio based on their day-ahead heat dispatch, as defined in (3).

As the day-ahead heat dispatch of CHPs and HPs is treated as an exogenous parameter in this optimization problem, in systems with high penetration of renewable energy sources, CHPs, and HPs, an electricity-myopic heat dispatch may limit the operational flexibility in the electricity market, and lead to increased electricity prices and renewable energy curtailment.

B. A Stackelberg Game Coordination Framework

To address the aforementioned challenges, the authors in [6] proposed an EAHM model which coordinates the decisions of the sequential and interdependent heat and electricity market operators. As previously highlighted, the decisions of the heat market operator (leader), specifically the heat dispatch of CHPs and HPs, impact the feasible space of the electricity market operator (follower) through the quantity bids of CHPs and HPs. These bidirectional interactions are illustrated in the upper-part of Fig. 1. As a result, in the EAHM, the leader must anticipate the impact of its decisions on the follower in order to minimize its own cost. This EAHM is modelled as a bilevel optimization problem, in which the upper-level problem, representing the heat market clearing, is

constrained by the lower-level problem, representing the electricity market clearing for a given value of the heat market outcomes.

For the sake of concision we introduce the matrix $\boldsymbol{x}^{\mathbf{L}} = (\boldsymbol{x}^{\mathbf{L}}_{it}) \in \mathbb{R}^{X^{\mathrm{L}} \times T}$ and $\boldsymbol{x}^{\mathbf{L}}_{\boldsymbol{i}} = (\boldsymbol{x}^{\mathbf{L}}_{\boldsymbol{it}}) \in \mathbb{R}^{T \times 1}$ of leader's continuous variables, representing the heat dispatch of all market participants, and the set $D^{\mathrm{L}} = \{C^{\mathrm{L},0}_{ik}, C^{\mathrm{L},1}_{ik}, C^{\mathrm{L},2}_{ik}, C^{\mathrm{L},3}_{ik}, A^{\mathrm{L}}, b^{\mathrm{L}}\}$ of matrices of leader's input parameters, including price-quantity bids and loads. As a result, the upper-level problem $\mathcal{P}^{\mathrm{L}}\left(D^{\mathrm{L}}, D^{\mathrm{F}}\right)$ of this EAHM is formulated in a compact manner as:

$$\Theta^{\mathrm{L}^*} = \min_{\boldsymbol{x}^{\mathbf{L}}, \boldsymbol{y}^{\mathbf{F}}} \sum_{i \in \mathcal{X}^{\mathrm{L}}} \min_{k \in \{1,\dots,K\}} \left\{ \Gamma^{\mathrm{L}}_{ik}(\boldsymbol{x}^{\mathbf{L}}, \boldsymbol{y}^{\mathbf{F}}) \right\} \tag{7a}$$

$$\text{s.t.} \quad A^{\mathrm{L}} \boldsymbol{x}^{\mathbf{L}} \leq b^{\mathrm{L}} \tag{7b}$$

$$\boldsymbol{y}^{\mathbf{F}} \in \text{dual sol. of } \mathcal{P}^{\mathrm{F}}\left(\boldsymbol{x}^{\mathbf{L}}, D^{\mathrm{F}}\right). \tag{7c}$$

This market-clearing problem minimizes the objective function in (7a), which represents the heat production costs of all market participants, with $\Gamma^{\mathrm{L}}_{ik}(\boldsymbol{x}^{\mathbf{L}}, \boldsymbol{y}^{\mathbf{F}}) = (C^{\mathrm{L},0}_{ik} + C^{\mathrm{L},1}_{ik}\boldsymbol{y}^{\mathbf{F}})\boldsymbol{x}^{\mathbf{L}}_{\boldsymbol{s}} + (C^{\mathrm{L},2}_{ik}\boldsymbol{y}^{\mathbf{F}} + C^{\mathrm{L},3}_{ik})\mathbb{1}$, subject to linear constraints representing the heat balance equations, and quantity bids of all market participants (7b). Note that the bilinear terms in (7a) can be exactly linearized using and this objective function can be formulated as a concave piece-wise linear function, as detailed in [6]. Furthermore, the electricity prices and outputs of CHPs and HPs, are defined as the optimal solutions to the lower-level problem $\mathcal{P}^{\mathrm{F}}\left(\boldsymbol{x}^{\mathbf{L}}, D^{\mathrm{F}}\right)$ in (7c), which represents the electricity market clearing.

We introduce $\boldsymbol{x}^{\mathbf{F}} = (\boldsymbol{x}^{\mathbf{F}}_{\boldsymbol{it}}) \in \mathbb{R}^{X^{\mathrm{F}} \times T}$, and $\boldsymbol{x}^{\mathbf{F}}_{\boldsymbol{i}} = (\boldsymbol{x}^{\mathbf{F}}_{\boldsymbol{it}}) \in \mathbb{R}^{T \times 1}$ the matrix of follower's primal variables, representing the electricity dispatch of all market participants and flows between market zones for each hour of the following day, and the set $D^{\mathrm{L}} = \{A^{\mathrm{F}}, B^{\mathrm{F}}, C^{\mathrm{F}}, b^{\mathrm{F}}\}$ of matrices of leader's input parameters, including price-quantity bids and loads. As a result, the day-ahead electricity market clearing can be formulated as a compact linear optimization problem $\mathcal{P}^{\mathrm{F}}(\boldsymbol{x}^{\mathbf{L}}, D^{\mathrm{F}})$, such that:

$$\Theta^{\mathrm{F}^*} = \min_{\boldsymbol{x}^{\mathbf{F}}} \sum_{i \in \mathcal{X}^{\mathrm{F}}} C^{\mathrm{F}}_i \boldsymbol{x}^{\mathbf{F}}_{\boldsymbol{i}} \tag{8a}$$

$$\text{s.t.} \quad A^{\mathrm{F}} \boldsymbol{x}^{\mathbf{F}} + B^{\mathrm{F}} \boldsymbol{x}^{\mathbf{L}} \leq b^{\mathrm{F}} \ : \ \boldsymbol{y}^{\mathbf{F}}, \tag{8b}$$

This market clearing minimizes the objective function in (8a), representing the electricity production costs of all electricity market participants, subject to linear constraints representing the electricity balance equations in each electricity market zone, the available transmission capacity between market zones, and the quantity bids of electricity market participants (8b). Furthermore, we introduce the matrix $\boldsymbol{y}^{\mathbf{L}} = (\boldsymbol{y}_{\boldsymbol{jt}}) \in \mathbb{R}^{Y^{\mathrm{F}} \times T}$ of follower's dual variables associated with the electricity balance equations, representing the electricity prices in each market zone and for each hour of the following day.

A detailed formulation of these optimization problems and of the matrices introduced above is provided in the online Appendix. We denote as x^{L^*}, x^{F^*}, and $y^{\mathrm{F}^*}\}$ the *original* primal and dual solutions to the leader and the follower's problems in this Stackelberg game problem. And, Θ^{L^*} and Θ^{F^*} represent the *original* follower and leader's optimal costs, respectively.

The EAHM described above represents a specific class of Stackelberg games, in which the (primal) decisions of the leader impact the linear *feasible space* of the follower, and in turn, the (dual) decisions of the follower impact the *objective function* of the leader, represented as a sum of concave piece-wise linear functions of the follower's dual variables for each given value of the leader's primal variables. As previously discussed, this class of Stackelberg games can model a wide range of coordination problems between interdependent energy and industry sectors. Therefore, in the remainder of this paper, the *w*-PPSM algorithm and its theoretical properties are discussed in the context of this general class of Stackelberg games represented by the bilevel optimization problem in (7)-(8).

III. DP Framework for Stackelberg Games

A. Privacy Goal

As highlighted above, the leader takes the follower's data D^{F} as input to its own optimization problem $\mathcal{P}^{\mathrm{L}}(D^{\mathrm{L}}, D^{\mathrm{F}})$. Some of this data can be considered as available information that can be shared with the leader without privacy concerns ($D^{\mathrm{F,a}}$), while some of it is sensitive ($D^{\mathrm{F,p}}$). In the target application, this data includes i) price-quantity bids of electricity suppliers and ii) electricity loads of individual consumers for each hour of the following day. This exchange of information by the follower to the leader is fundamental to achieve an optimal coordination between the two energy sectors [6], and has been encouraged by recent regulatory changes [9]. In line with these changes, the price-quantity bids of electricity suppliers can be considered as available information ($D^{\mathrm{F,a}}$) that is freely shared with the leader. However, the loads of individual consumers are still considered as sensitive information ($D^{\mathrm{F,p}}$) that needs to be protected before being shared with the leader. Indeed, sharing this information before the clearing of the electricity market may lead to competitive advantages for other market participants, or the leakage of identifying information [10]. As the leader problem is solely impacted by changes to the aggregate electricity load in each market zone, the follower can share this aggregate load with the leader without jeopardizing the coordination of the two sectors. However, aggregation has been showed to be insufficient to protect the individuals' data and their identifying information [21]. Therefore, in this target application, the sensitive data represents the hourly aggregate electricity loads in each market zone.

As discussed above, the sensitive data in energy systems includes highly correlated times series. Therefore, the *privacy goal* addressed in this work is to protect the follower's sensitive data over a predefined time window,

before sharing it with the leader. For this purpose, the infinite sequence of sensitive data is represented as a *data stream* $D_{zt}^{\mathrm{F,p}}$, with the tuples (z,t) in the universe $\mathcal{U} = \mathcal{Z}x\mathcal{T}^{\infty}$, where $\mathcal{Z}$ is the set of users and $\mathcal{T}^{\infty}$ is an unbounded set of time steps [16]. In this data stream, an *event* $D_t^{\mathrm{F,p}} = \left[D_{1t}^{\mathrm{F,p}}, ..., D_{Zt}^{\mathrm{F,p}}\right]$ is defined as all the data points reported by all the users that occurred at time t. The privacy goal is therefore to protect this data stream over a predefined time window. In particular, in the target application, the privacy goal is to protect the hourly aggregate electricity loads in each market zone over a 24-hour time window.

B. Differential Privacy for Data Streams

The aforementioned privacy goal is addressed using the framework of DP applied to data streams. DP is a rigorous privacy notion which relies on the injection of carefully calibrated noise to protect disclosures of the users' data, while allowing to extract information about the population [12]. This framework enjoys several important properties, including *composability* and *immunity to post-processing*.

This paper adopts the *w-privacy* framework [19], which extends the standard definition of DP to protect data streams within a time window of w time steps. This framework operates on *stream prefixes*, i.e., the sequence $D^{\mathrm{F,p}}[t] = \left[D_1^{\mathrm{F,p}}, ..., D_t^{\mathrm{F,p}}\right]$ of all events that occurred at or before time t. It relies on the notion of *w-adjacency* [16] to capture the differential information to be protected, as defined below:

Definition 1 *Two data streams prefixes $D^{F,p}[t]$ and $D^{F,p'}[t]$ are w-neighbors, denoted by $D^{F,p}[t] \sim_w D^{F,p'}[t]$, if*

1) *their elements (events) are pairwise neighbors, i.e. they differ at most by one element. This is formally defined for a given pair of events $D_i^{F,p}$ and $D_i^{F,p'}$, where $i \in [t]$, as: $\exists z$ s.t. $|D_{zi}^{F,p} - D_{zi}^{F,p'}| \leq \alpha$ and $\forall z' \neq z$, $D_{z'i}^{F,p} = D_{z'i}^{F,p'}$ with $\alpha \in \mathbb{R}^+$ the indistinguishability parameter representing how much data variation has to be protected; and*
2) *all the differing elements are within a time window of up to w time steps. This is formally defined as: for any given $i < j \in [t]$, if $D_i^{F,p} \neq D_i^{F,p'}$ and $D_s^{F,p} \neq D_s^{F,p'}$, then it holds that $j - i + 1 \leq w$.*

In the context of data exchanged between the leader and follower in a Stackelberg game, a mechanism is said to satisfy w-event ε-differential privacy (w-privacy for short) if it satisfies the following privacy goal:

Definition 2 *Let $\mathcal{M}$ be a randomized algorithm that takes as input a stream prefix of arbitrary size and outputs an element from a set of possible output sequences $\mathcal{S}$. Algorithm $\mathcal{M}$ satisfies w-privacy if, for all w-neighboring stream prefixes $D^{F,p}[t] \sim_w D^{F,p'}[t]$, with $t \in \mathcal{T}^{\infty}$, and all sets $S \subseteq \mathcal{S}$, it satisfies:*

$$\frac{\mathbb{P}\Big(\mathcal{M}(D^{F,p}[t]) \in S\Big)}{\mathbb{P}\Big(\mathcal{M}(D^{F,p'}[t]) \in S\Big)} \leq exp(\varepsilon), \tag{9}$$

where $\varepsilon \in \mathbb{R}^+$ is the privacy budget.

It is a well-known result that the *Laplace mechanism*, $\mathcal{M}^{\mathrm{Lap}}$ which takes as input a stream prefix $D^{\mathrm{F,p}}[t]$ and outputs the perturbed sequence $\tilde{D}^{\mathrm{F,p}}[t] = \left[\tilde{D}_1^{\mathrm{F,p}}, ..., \tilde{D}_t^{\mathrm{F,p}}\right]$, such that $\tilde{D}_i^{\mathrm{F,p}} = D_i^{\mathrm{F,p}} + \xi_i$ where $\xi_i \in \mathbb{R}^Z$ is drawn from the i.i.d. Laplace distribution $Lap(\frac{w\alpha}{\varepsilon})^Z$ for $i \in [t]$, achieves w-privacy [16].

C. Fidelity Goal

The main limitation of traditional DP mechanisms, such as the Laplace mechanism, is that the original data is highly perturbed and the outcome of the algorithm is a data stream that, used as input to an optimization problem, may lead to severe fidelity and feasibility issues [18]. In the context of a Stackelberg game, the Leader's problem taking as input this Laplace-obfuscated data $\mathcal{P}^{\mathrm{L}}(D^{\mathrm{L}}, D^{\mathrm{F,a}}, \tilde{D}^{\mathrm{F,p}})$ may result in sub-optimal solutions for the leader (upper-level) and follower (lower-level), due to their strong techno-economic interactions [20].

The w-PPSM introduced in this work specifically aims at mitigating these issues in order to achieve a close-to-optimal coordination between the leader and the follower in a Stackelberg game. The goal of this mechanism is to generate privacy-preserving data $\hat{D}^{\mathrm{F,p}^*}$ that ensures *fidelity* of the solutions to the leader and follower's problems, w.r.t. to the original Stackelberg game solutions. In particular, we propose to quantify this goal using the so-called *cost of privacy*, which represents the impact of the mechanism on the objective costs of the leader and the follower. We define formally the leader and follower's costs of privacy below.

Definition 3 (Cost of privacy) *The cost of privacy of a DP mechanism for each agent a (leader or follower) in a Stackelberg game is defined as the following quantity:*

$$\Delta\Theta^a := |\hat{\Theta}^{a^*} - \Theta^{a^*}|, \tag{10}$$

where Θ^{a^*} represents the original objective cost of agent a before the DP mechanism, and $\hat{\Theta}^{a^*}$ represents the objective cost of agent a after the DP mechanism.

Theoretical guarantees on the privacy and fidelity goals achieved by the proposed w-PPSM will be provided in Section V.

IV. w-Privacy-Preserving Stackelberg Mechanism

This section presents a generalization of the w-PPSM introduced in our preliminary work [20] to a broad class of Stackelberg games.

A. Assumptions

This paper assumes that the follower and the leader each have access to prediction models that can privately forecast the original values of their relevant coordination variables ($\bar{x}^{\mathrm{L}}$ and $\bar{y}^{\mathrm{F}}$) and costs ($\bar{\Theta}^{\mathrm{F}}$) in the Stackelberg game. We formally define the accuracy of these prediction models below.

Assumption 1 *We assume that there exists small-enough constants $\eta_x > 0$, $\eta_\Theta > 0$, $\eta_y > 0$, and $p > 0$, such that, for any values of the original solutions Θ^{F^*}, x^{L^*}, and y^{F^*}:*

$$\mathbb{P}\left(\{\Delta_{\bar{\Theta}^F} \leq \eta_\Theta\} \cap \{\Delta_{\bar{x}^L} \leq \eta_x \mathbb{1}\} \cap \{\Delta_{\bar{y}^F} \leq \eta_y \mathbb{1}\}\right) \geq 1 - p, \tag{11a}$$

where $\Delta_{\bar{\Theta}^F} = |\bar{\Theta}^F - \Theta^{F^*}|$, $\Delta_{\bar{x}^L} = (|\bar{x}^L_{it} - x^{L^*}_{it}|) \in \mathbb{R}^{X^L \times T}$, and $\Delta_{\bar{y}^F} = (|\bar{y}^F_{jt} - y^{F^*}_{jt}|) \in \mathbb{R}^{Y^F \times T}$.

As discussed in [18], [20], this assumption is realistic in energy systems, since prediction models are commonly used to efficiently bid in the markets and the market operators themselves have access to historical bids and market outcomes data.

B. Steps

The proposed w-PPSM algorithm ($\mathcal{M}^{\mathrm{PPSM}}$) is performed before each instance of the Stackelberg game (e.g. each day prior to the market clearings), to protect the sensitive data of the follower $D^{\mathrm{F,p}}$ over a time horizon of w time steps (e.g. 24 hours of the following day). The outcome of this mechanism is the privacy-preserving data $\hat{D}^{\mathrm{F,p}^*}$ to be shared with the leader. The steps of this mechanism are schematically represented in Fig. 1 and summarized below.

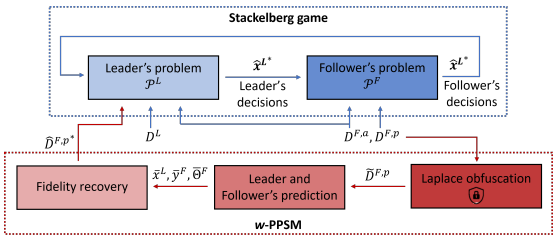


Figure 1. Stackelberg game and w-PPSM flowchart

*1) **Laplace-obfuscation**:* Firstly, the follower obfuscates the sensitive data $D^{\mathrm{F,p}}$ using the w-private Laplace mechanism $\mathcal{M}^{\mathrm{Lap}}$ introduced in Section III, before releasing it to the leader. We denote as $\tilde{D}^{\mathrm{F,p}}$ the Laplace-obfuscated data of the follower.

*2) **Original solutions prediction**:* Using their respective available data, D^{L} and $D^{\mathrm{F,a}}$, and the Laplace-obfuscated data $\tilde{D}^{\mathrm{F,p}}$ obtained in step (1), the leader and the follower privately estimate their original decisions and costs for the following day using the prediction models, as defined in Section IV-A. This prediction step is not the main focus on this paper and has been discussed in more details in our preliminary work [20].

*3) **Fidelity recovery**:* The follower optimally redistributes the noise on the sensitive data introduced in step (1) while recovering fidelity w.r.t to the solutions to the original Stackelberg game, as estimated in step (2). This is achieved by solving a bilevel optimization problem, inspired by [18], [20], which is formulated as:

$$\min_{\hat{\boldsymbol{D}}^{\mathbf{F,p}}, \hat{\boldsymbol{y}}^{\mathbf{F}}, \hat{\boldsymbol{\Theta}}^{\mathbf{F}}} \|\hat{\boldsymbol{D}}^{\mathbf{F,p}} - \tilde{D}^{\mathrm{F,p}}\|_2^2 \tag{12a}$$

$$\text{s.t.} \quad |\hat{\boldsymbol{\Theta}}^{\mathbf{F}} - \bar{\Theta}^F| \leq \beta_\Theta \tag{12b}$$

$$|\hat{\boldsymbol{y}}^{\mathbf{F}}_{jt} - \bar{y}^{\mathrm{F}}_{jt}| \leq \beta_y, \forall j \in \mathcal{Y}^{\mathrm{F}}, t \in \mathcal{T} \tag{12c}$$

$$\{\hat{\boldsymbol{y}}^{\mathbf{F}}, \hat{\boldsymbol{\Theta}}^{\mathbf{F}}\} = \text{dual sol. and obj. of } \mathcal{P}^{\mathrm{F}}\left(\bar{x}^{\mathrm{F}}, D^{\mathrm{F,a}}, \hat{\boldsymbol{D}}^{\mathbf{F,p}}\right), \tag{12d}$$

where the objective (12a) is to find a vector of privacy-preserving data $\hat{\boldsymbol{D}}^{\mathbf{F,p}}$ that minimizes the distance w.r.t. the Laplace-obfuscated data $\tilde{D}^{\mathrm{F,p}}$, subject to *fidelity constraints* on the leader and follower's objective costs (12b)-(12c). Eq. (12b) directly enforces fidelity of the follower's objective cost w.r.t. its (estimated) original value $\bar{\Theta}^{\mathrm{F}}$. Meanwhile (12c) indirectly enforces fidelity of the leader's objective cost w.r.t its original (estimated) value by enforcing fidelity of the follower's dual decision variables, w.r.t. to their (estimated) original value $\bar{y}^{\mathrm{F}}$, which directly impact the leader's objective cost. Furthermore, the upper-level variables $\hat{\boldsymbol{\Theta}}^{\mathbf{F}}$ and $\hat{\boldsymbol{y}}^{\mathrm{F}}$ are defined objective cost and dual variables of the lower-level problem (12d), which represents the follower's problem taking as inputs the privacy-preserving data $\boldsymbol{D}^{\mathbf{F,p}}$. The optimal solutions to this optimization problem include the follower's privacy-preserving data $\hat{D}^{\mathrm{F,p}^*}$, which is then shared with the leader, its objective cost $\hat{\Theta}^{\mathrm{F}^*}$, primal $\hat{x}^{\mathrm{F}^*}$ and dual $\hat{y}^{\mathrm{F}^*}$ variables. Furthermore, we denote as $\hat{x}^{\mathrm{L}^*}$ and $\hat{\Theta}^{\mathrm{L}^*}$ the the leader's variables and objective cost associated with these values of the follower's decisions and privacy-preserving data.

The fidelity goal of the w-PPSM is to ensure fidelity of the leader's and follower's objective costs after the fidelity-recovery phase, i.e. $\hat{\Theta}^{\mathrm{L}^*}$, and $\hat{\Theta}^{\mathrm{F}^*}$, w.r.t. their original values, i.e., Θ^{L^*}, and Θ^{F^*}. This goal is studied theoretically in Section V, and empirically in Section VI.

V. Theoretical properties of w-PPSM

This section introduces strong theoretical properties on the error introduced by the w-PPSM, as well as the privacy and coordination it achieves. Proofs of these properties are provided in the online Appendix.

A. Error Analysis

After the fidelity-recovery phase, theoretical bounds on the error introduced on the sensitive data can be derived.

Theorem 1 (Error on Sensitive Data) *After the fidelity recovery phase, the expected error induced by the w-PPSM on the original sensitive data is bounded by the inequality:*

$$\mathbb{E}\left[\|\hat{D}^{F,p^*} - D^{F,p}\|\right] \leq 4(w\alpha)^2, \tag{13}$$

where $\hat{D}^{F,p^*}$ is the solution to fidelity-recovery Problem (12).

B. Privacy Goal

Theorem 2 (Privacy) *For given positive real values of the parameters α, ε, β_Θ and β_y, the proposed w-PPSM satisfies w-privacy.*

This theorem states that the proposed w-PPSM ensures high levels of privacy on the sensitive data.

C. Fidelity Goal

We use the so-called *cost of privacy*, which represents the impact of the w-PPSM on the objective costs of the leader and the follower, to quantify the fidelity of the w-PPSM w.r.t to the original solutions of the Stackelberg game. One major contribution of this paper compared to the literature is to provide theoretical bounds on these costs.

Firstly, we derive the following bounds on the follower's cost of privacy after the fidelity-recovery phase:

Theorem 3 (Follower's Cost of Privacy) *After the fidelity recovery phase, the follower's cost of privacy induced by the w-PPSM is bounded by the inequality:*

$$\mathbb{P}(\Delta\Theta^F \leq \beta_\Theta + \eta_\Theta) \geq 1 - p. \tag{14}$$

This theorem shows that the follower can control its cost of privacy and find a trade-off between privacy risks and fidelity through the selection of adequate parameters ε, α, and β_Θ.

Additionally, the objective cost of the leader is directly impacted by the dual variables of the follower. Therefore, we derive theoretical bounds on the leader's cost of privacy as follows:

Theorem 4 (Leader's Cost of Privacy) *After the fidelity recovery phase, the leader's cost of privacy induced by the w-PPSM is bounded by the inequality:*

$$\mathbb{P}\left(\Delta\Theta^L \leq \max\left\{f(\hat{x}^{L^*}, \hat{y}^{F^*}), f(x^{L^*}, y^{F^*})\right\}\right) \geq 1 - p. \tag{15}$$

where

$$\begin{aligned} f : (\boldsymbol{x^L}, \boldsymbol{y^F}) \rightarrow \sum_{i \in \mathcal{X}^L} \{&\Gamma^L_{i\hat{k}^*}(\boldsymbol{x^L}, \boldsymbol{y^F}) - \Gamma^{\boldsymbol{L}}_{i\hat{k}^*}(\boldsymbol{x^L}, \boldsymbol{y^F}) \\ &+ (\eta_y + \beta_y)(\|C^{L,1}_{ik}\|_1 \mathbb{1} \|\boldsymbol{x^L}\|_1 + \|C^{L,2}_{ik}\|_1 \mathbb{1})\}, \end{aligned} \tag{16}$$

and $\hat{k}^*$ and k^* are defined such that:

$$\begin{aligned} \Gamma^L_{i\hat{k}^*}(\hat{x}^{L^*}, \hat{y}^{F^*}) &= \min_{k \in \{1,\dots,K\}} \Gamma^L_{ik}(\hat{x}^{L^*}, \hat{y}^{F^*}) \\ \Gamma^L_{ik^*}(x^{L^*}, y^{F^*}) &= \min_{k \in \{1,\dots,K\}} \Gamma^L_{ik}(x^{L^*}, y^{F^*}). \end{aligned} \tag{17}$$

This theorem provides actionable bounds on the leader's cost of privacy, which can be used to implement a compensation mechanism for each market participant impacted by the w-PPSM mechanism.

VI. Numerical Results

A. Case Study Setup

The case study considered is a modified version of the IEEE 24-bus system coupled with two 3-node district heating networks, in which network constraints are neglected.

The 24-bus IEEE Reliability Test System consists of twelve thermal power plants, six wind farms, two extraction CHPs, and two HPs. Data for power generation, costs, loads and transmission for the 24-bus IEEE Reliability Test System is derived from [22]. Additionally, six wind farms of 250MW each are installed.

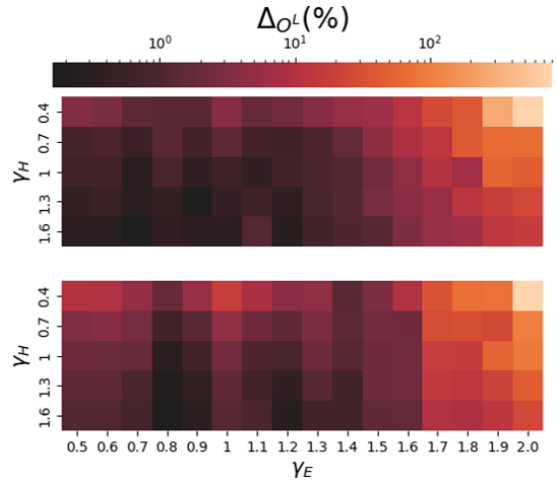
Each isolated DHN comprises one CHP, one waste incinerator heat-only unit, one heat-only peak boiler, and one large-scale HP. The techno-economic characteristics of these units and DHNs are derived from [23]–[25] and available in the online Appendix. Furthermore, realistic time series of heat and electricity loads and wind power generation are derived from [5], [26], [27] and available in the online Appendix.

This numerical analysis evaluates the performance of the w-PPSM in comparison to the traditional Laplace mechanism. And all the values displayed are average results over several instances. In all simulations, the privacy budget ε is fixed to 1, and the fidelity parameters β_Θ and β_y are fixed to 0.1% of the follower's objective and 10.0% of the electricity prices, respectively. The preliminary work [20] focused on tuning and studying the impact of these parameters. Therefore, the following results provide an in-depth analysis of the cost of privacy introduced by the proposed w-PPSM under varying privacy risks (i.e. values of the indistinguishability parameter) and operational conditions (i.e. loads and renewable energy production) in the heat and electricity systems.

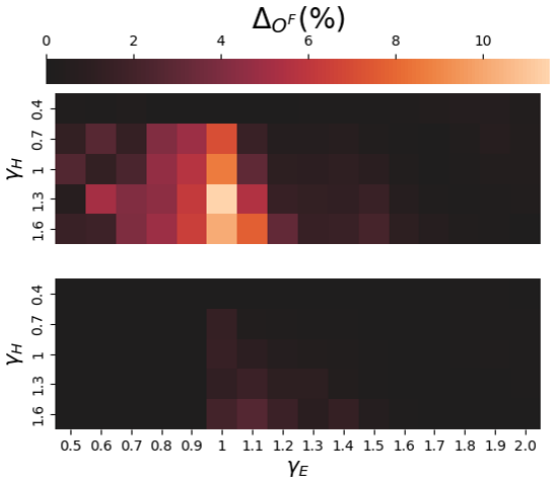
B. Results

1) Limitations of Laplace Mechanism: Trade-off Between Cost and Privacy Risk: Figs. 2 and 3 illustrate the leader and follower's costs of privacy introduced by the Laplace mechanism and the w-PPSM for two different values of the indistinguishability parameter $\alpha = \{10, 100\}$, and under different operating conditions. These operating conditions are simulated by varying stress factors γ_{H} (γ_{E}) representing the multiplying factors applied to the heat (electricity) loads of a reference day. Note that, for the sake of legibility, the scale is logarithmic for the leader's cost and linear for the follower cost, and adapted for each value of the indistinguishability parameter.

We first analyse the impact of the indistinguishability parameter α on the error introduced by the Laplace mechanism. Fig. 2 shows that both mechanisms perform relatively well for a low value of $\alpha = 10$. However, this value of α represents a moderate privacy risk, especially for higher values of electricity loads and larger consumers, as the aggregate electricity demand ranges between 644.47MWh and 2498.54MWh.

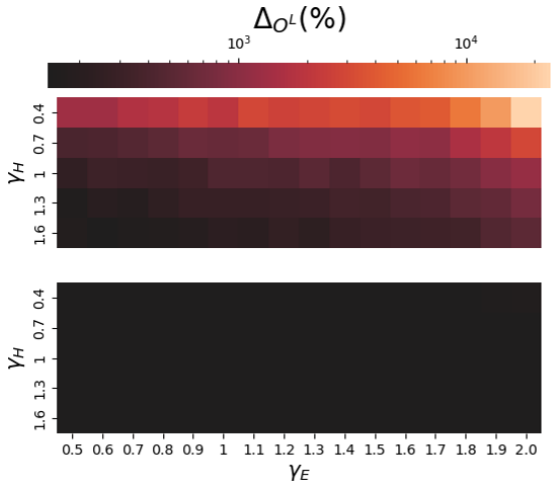


(a) Leader's cost of privacy ($\Delta\Theta^{\mathrm{L}}$).

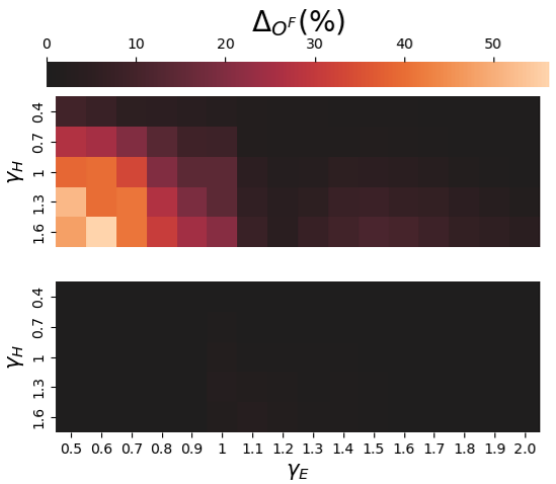


(b) Follower's cost of privacy ($\Delta\Theta^{\mathrm{F}}$).

Figure 2. Costs of privacy (in % of original cost) at varying heat (γ_{H}) and electricity (γ_{E}) stress levels, obtained via the Laplace mechanism (top) and w-PPSM (bottom), for indistinguishability parameter α = 10(MWh), averaged over 20 instances.



(a) Leader's cost of privacy ($\Delta\Theta^{\mathrm{L}}$).



(b) Follower's cost of privacy ($\Delta\Theta^{\mathrm{F}}$).

Figure 3. Costs of privacy (in % of original cost) at varying heat (γ_{H}) and electricity (γ_{E}) stress levels, obtained via the Laplace mechanism (top) and w-PPSM (bottom), for indistinguishability parameter α = 100(MWh), averaged over 20 instances.

As α represents how much variation of load is protected, it directly impacts the level of noise added to the original data, and the leader's cost of privacy in the Laplace mechanism. This can be observed in Fig. 3, where the cost of privacy induced by the Laplace mechanism drastically increases for $\alpha = 100$. This shows that there is a necessary trade-off in the Laplace mechanism between privacy risks for the follower, and costs of privacy for the leader. This constitutes a major limitation for the social acceptance and deployment of this mechanism. On the contrary, the fidelity-recovery phase allows the w-PPSM to bound these errors when the value of α increases. As a result, the w-PPSM achieves substantially better performances for higher values of α, and up to two orders of magnitude reduction in the leader's cost of privacy, and, up to one order of magnitude reduction in the follower's cost of privacy.

We also observe that the follower's cost of privacy, for both mechanisms, remains stable with higher values of α. Intuitively, this can be explained by the strategic advantage of the leader on the follower in the Stackelberg game. As both mechanisms add noise to the sensitive data of the follower, the leader is less capable of anticipating the follower's reactions to optimize its own objective. This interesting finding suggests that a privacy-aware coordination mechanism is favorable to the follower, and would facilitate the social acceptance of information exchange for a broad range of applications in energy systems. As the w-PPSM is also able to limit the impact on the leader's cost of privacy, it has the potential to be beneficial for both agents. Besides, the impact of DP on reducing strategic behaviors and encouraging truthfulness in mechanism design has been studied in the literature [28].

2) Impact of Operating Conditions: We now analyse the impact of varying operating conditions in both heat and electricity systems on the costs of privacy achieved by the Laplace mechanism and the w-PPSM. In Figs.

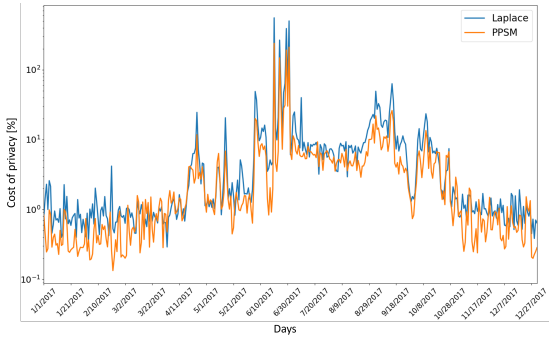
2 and 3, the reference heat load is uniformly varied between $\pm 60\%$, and the electricity load between -50% and $+100\%$. For a given value of the indistinguishability parameter, we notice that the highest costs of privacy for each mechanism are achieved under different combinations of stress factors. However, some similar patterns can be observed.

In Fig. 2, i.e. for $\alpha = 10$ and Fig 3, i.e. for $\alpha = 100$, we notice that both mechanisms achieve the highest leader's cost of privacy for high values of the electricity stress factor. Intuitively, this can be explained by the fact that the elasticity of electricity prices increases for higher electricity loads, due to peak-load generators being turned on. In turn, these electricity prices perturbations impact the CHPs and HPs heat costs and their merit order in the heat market. As a result, even small electricity load variations may lead to significant changes in the heat dispatch and operating costs. However, this cost of privacy is somehow reduced for corresponding higher values of the heat stress factor. Indeed, with higher heat loads, HPs and CHPs are not the marginal producers anymore in the heat market. Therefore, small errors in their heat costs calculation and merit order does not impact greatly the heat dispatch. Furthermore, as more expensive peak-load generators are turned-on in the heat system, the relative operating costs of CHPs and HPs in the heat system is decreased.

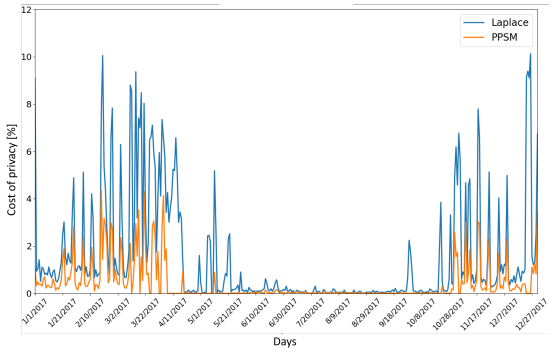
Furthermore, both mechanisms achieve the highest follower's cost of privacy for the highest heat stress factor and electricity stress factors lower than 1. Intuitively, this can be explained by the fact that, with higher heat loads, the heat dispatch of HPs and CHPs increases, which reduces their operational flexibility in the electricity market. In the meantime, the reduce electricity loads lead to these CHPs and HPs being marginal producers. Therefore, small variations in their production may lead to significant changes in the electricity dispatch and prices.

Overall tightened interactions between heat and electricity markets at given operating conditions result in higher costs of privacy for the respective systems. This analysis identifies the operating conditions that are the most vulnerable to perturbations on the sensitive data, and the ones resulting in a negligible cost of privacy when applying DP. This information can be leveraged to design an adaptive mechanism that applies DP solely when the privacy risks are the highest, and therefore, to reduce the privacy budget over multiple days [16].

3) Yearly analysis: The heat maps provided above are derived synthetically, by multiplying once specific day's loads profiles uniformly by various stress factors. In order to analyse the impact of peak loads as well as load profiles' shapes, and renewable energy production, we now evaluate the leader and follower's costs of privacy daily over an entire year using real load data, as shown in Fig. 4. For this analysis, in order to provide a fair comparison between the w-PPSM and the Laplace mechanism, and for the sake of legibility, the indistinguishability parameter is fixed to $\alpha = 10$.



(a) Leader's cost of privacy ($\Delta\Theta^{\mathrm{L}}$). Logarithmic scale.



(b) Follower's cost of privacy ($\Delta\Theta^{\mathrm{F}}$). Linear scale.

Figure 4. Costs of privacy (in % of original cost) computed for each day of the year ($\alpha = 10$).

We observe that the follower's cost of privacy is higher in the winter period and, in general, which corresponds to high heat and electricity loads. This can be explained by the fact that, in periods of high consumption, the CHP plants represent a higher share of the electricity mix. The resulting tight interactions and low flexibility of CHPs in the electricity market, result in higher errors when noise is introduced to the original data. Additionally, in the winter period, the follower's costs of privacy achieved by the Laplace mechanism and the w-PPSM strongly fluctuate, and appear correlated, since the w-PPSM largely depends on the noise introduced by the Laplace mechanism. However, the cost related to the w-PPSM always remains more restrained.

In contrast, with both mechanisms, larger leader's costs of privacy occur during the summer season, i.e., when the heat demand is very low. To improve the graph readability, the y-axis in the bottom figure has been limited to a value of 100%. When the error exceeds this limit, the one related to the Laplace mechanism reaches almost 560%, while the PPSM has a maximum value of 240%. This extreme behavior is associated with the lowest values of heat consumption of the year. Therefore, any amount of noise on the sensitive data causes, as expected, a relatively large change in heat system cost. The leader's cost of privacy remains limited in winter, since the indistinguishability parameter selected for this analysis is the lowest: $\alpha = 10$. Yet, the PPSM consistently

performs better during the whole year.

VII. Conclusion

The w-PPSM developed in this paper generates differentially-private data streams in the context of the exchange of information between the leader and the follower in a Stackelberg game. The w-PPSM was shown to enjoy strong privacy and fidelity properties. In particular, we derived theoretical bounds on the cost of privacy for both the leader and the follower in the Stackelberg game. Furthermore, numerical simulations, based on a realistic integrated heat and electricity system, show that the w-PPSM achieves up to two orders of magnitude reduction in the leader and follower's cost of privacy compared to the traditional Laplace mechanism. This theoretical and empirical validation of the w-PPSM shows that the w-PPSM provides an efficient framework to facilitate the exchange of information between agents in energy systems, and facilitate their coordination.

Future work will aim at extending the w-PPSM framework, to (i) account for potential correlations between the users' data; (ii) further reduce the cost of privacy using advanced obfuscation methods, such as Gaussian noise; and (iii) mitigate the privacy budget, using the sparse vector technique (SVT), which can privately identify thresholds in the operating conditions resulting in high privacy risks, and dynamically adapt the noise added under these conditions [16]. Furthermore, the remaining cost of privacy, and its potentially disproportionate impact on certain market participants should be addressed by developing privacy-aware market mechanisms that (i) incentivize agents to share accurate information, and (ii) compensate users that incur financial losses due to privacy-preserving information exchange [28].

References

[1] P. Pinson, L. Mitridati, C. Ordoudis, and J. Ostergaard, "Towards fully renewable energy systems: Experience and trends in denmark," *CSEE journal of power and energy systems*, vol. 3, no. 1, pp. 26–35, 2017.

[2] L. M.-J. M. Mitridati, "Market-based coordination of heat and electricity systems," Ph.D. dissertation, Department of Electrical Engineering, Technical University of Denmark (DTU), 2019.

[3] C. Ordoudis, "Market-based approaches for the coordinated operation of electricity and natural gas systems," Ph.D. dissertation, Technical University of Denmark (DTU), 2018.

[4] M. Simaan and J. B. Cruz, "On the Stackelberg strategy in nonzero-sum games," *J. Optim. Theory Appl.*, vol. 11, no. 5, pp. 533–555, 1973.

[5] L. Mitridati, P. Van Hentenryck *et al.*, "A bid-validity mechanism for sequential heat and electricity market clearing," *arXiv preprint arXiv:1910.08617*, 2019.

[6] L. Mitridati, J. Kazempour, and P. Pinson, "Heat and electricity market coordination: A scalable complementarity approach," *European Journal of Operational Research*, vol. 283, no. 3, pp. 1107–1123, 2020.

[7] G. Byeon and P. Van Hentenryck, "Unit commitment with gas network awareness," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1327–1339, 2020.

[8] B. Zeng, H. Dong, R. Sioshansi, F. Xu, and M. Zeng, "Bilevel robust optimization of electric vehicle charging stations with distributed energy resources," *IEEE Transactions on Industry Applications*, vol. 56, no. 5, pp. 5836–5847, 2020.

[9] FERC and NERC, "Staff report on outages and curtailments during the southwest cold weather event of february 1-5, 2011: Causes and recommendations," Aug. 2011. [Online]. Available: https://www.nerc.com/pa/rrm/ea/Pages/September-2011-Southwest-Blackout-Event.aspx

[10] M. Lisovich and S. Wicker, "Privacy concerns in upcoming residential and commercial demand-response systems," *IEEE Proceedings on Power Systems*, vol. 1, no. 1, pp. 1–10, 2008.

[11] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Basar, "Dependable demand response management in the smart grid: A stackelberg game approach," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 120–132, 2013.

[12] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Theoretical Computer Science*, vol. 9, no. 3-4, pp. 211–407, 2013.

[13] 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.

[14] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: a survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 746–789, 2019.

[15] F. Fioretto, P. Van Hentenryck, and K. Zhu, "Differential privacy of hierarchical census data: An optimization approach," *Artificial Intelligence*, vol. 296, p. 103475, 2021.

[16] F. Fioretto and P. Van Hentenryck, "Optstream: Releasing time series privately," 2019.

[17] T. W. Mak, F. Fioretto, L. Shi, and P. Van Hentenryck, "Privacy-preserving power system obfuscation: A bilevel optimization approach," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1627–1637, 2019.

[18] F. Fioretto, L. Mitridati, and P. Van Hentenryck, "Differential privacy for Stackelberg games," in *Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence (IJCAI-2020)*, Jan 2021.

[19] G. Kellaris, S. Papadopoulos, X. Xiao, and D. Papadias, "Differentially private event sequences over infinite streams," 2014.

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

[21] N. Buescher, S. Boukoros, S. Bauregger, and S. Katzenbeisser, "Two is not enough: Privacy assessment of aggregation schemes in smart metering," 2017.

[22] C. Ordoudis, P. Pinson, J. M. Morales, and M. Zugno, "An updated version of the IEEE RTS 24-bus system for electricity market and power system operation studies - DTU working paper (available online)," 2016. [Online]. Available: http://orbit.dtu.dk/files/120568114/An

[23] M. Zugno, J. M. Morales, and H. Madsen, "Commitment and dispatch of heat and power units via affinely adjustable robust optimization," *Computers & Operations Research*, vol. 75, pp. 191–201, 2016.

[24] Z. Li, W. Wu, M. Shahidehpour, J. Wang, and B. Zhang, "Combined heat and power dispatch considering pipeline energy storage of district heating network," *IEEE Transactions on Sustainable Energy*, vol. 7, no. 1, pp. 12–22, 2016.

[25] L. Mitridati and J. A. Taylor, "Power systems flexibility from district heating networks," in *Power Systems Computation Conference (PSCC)*, Dublin, Ireland, 2018.

[26] H. Madsen, "Time series analysis. course notes," 2015. [Online]. Available: http://www.imm.dtu.dk/~hmad/time.series.analysis/assignments/index.html

[27] Energinet.dk. (2020) Danish system operator. [Online]. Available: https://en.energinet.dk/

[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.