The Cost of Privacy for Heat and Electricity Markets 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*—Sector coordination between heat and electricity systems has been identified has an energy-efficient and cost-effective way to transition towards a more sustainable energy system. However, the coordination of sequential markets relies on the exchange of sensitive information between the market operators, namely time series of consumers' loads. To address the privacy concerns arising from this exchange, this paper introduces a novel privacy-preserving Stackelberg mechanism (w-PPSM) which generates differentially-private data streams with high fidelity. The proposed w-PPSM enforces the *feasibility* and *fidelity* of the privacy-preserving data with respect to the original problem through a post-processing phase in order to achieve a close-to-optimal coordination between the markets. Multiple numerical simulations in a realistic energy system demonstrate the effectiveness of the w-PPSM, which achieves up to two orders of magnitude reduction in the cost of privacy compared to a traditional differentially-private mechanism.**

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

I. Introduction

In the context of the liberalization of energy markets, the development of market-based coordination mechanisms for heat and electricity systems has been identified as a crucial step towards an energy-efficient, cost-effective, and sustainable energy system [1], [2].

Due to the underlying techno-economic interactions between different energy carriers, the coordination between *sequential* and *interdependent* energy markets them has traditionally been modelled as a *Stackelberg game* [3]. This framework has been used extensively in the literature to coordinate district heating [4], [5], natural gas [6], [7], and electricity systems. In particular, the electricity-aware heat market (EAHM) developed in [5] provides a market-based mechanism for the coordination of heat and electricity systems. This market framework allows the heat market operator to optimize the dispatch of combined heat and power plants (CHPs) and heat pumps (HPs), while anticipating their impact on electricity market dispatch and prices. An optimal coordination is achieved through the sharing of information between the electricity and heat market operators. In particular, the electricity market operator must communicate information on its supply and demand curves so that the heat market operator can model its reactions to the dispatch of CHPs and HPs.

Despite recent regulatory changes encouraging information exchange between system operators [8], users in the electricity market may be reluctant to exchange some information with the heat market operator 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 [9], [10]. In particular, in the EAHM developed in [5] and used in this paper as a target application, we consider that the hourly electricity loads of individual consumers represent a sensitive data stream to be obfuscated before releasing to the heat market operator.

To address this privacy issue, *Differential Privacy* (DP) has emerged as a robust privacy framework for multiple applications [11]. DP relies on the injection of carefully calibrated noise to protect the disclosure of the individuals' data, while allowing to extract information about the population. This framework can thus be used to *obfuscate* the sensitive data exchanged between the electricity and heat market operators in the EAHM. In particular, the w-privacy framework introduced in [12] provides an interesting framework to obfuscate time series of hourly data, such as electricity loads, within a predefined time window. 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 [13]. When obfuscated data is used as input to optimization problems with strong techno-economic constraints, such as market clearing problems in energy systems, it may lead to severe fidelity and feasibility issues. To address this issue the authors in [14] developed an optimization-based fidelity-recovery phase to classic DP mechanisms. This approach has been adapted to the exchange of information in Stackelberg games, and applied to the coordination of electricity and natural gas markets in [15]. However, these recent advances in the literature are limited to classic definitions of DP. To the best of our knowledge, there is no existing mechanism to share differentially-private data streams which guarantee high fidelity of the solutions in a Stackelberg games.

This work is partially funded by the NCCR Automation.

Given the described research gaps, the contributions of this paper are threefold:

1) We introduce the novel w-PPSM which allows for the sharing of differentially-private data streams in Stackelberg games with high fidelity. This mechanism uses an optimization-based approach to recover the fidelity and feasibility of the obfuscated data w.r.t. the original Stackelberg game. This mechanism is developed for the target application of the coordination between heat and electricity markets and the exchange of hourly electricity loads over a 24-hour window.
2) We show that the w-PPSM satisfies interesting theoretical properties. In particular, it achieves strong privacy goals for data streams, while providing a bound on the error introduced on the sensitive data and energy prices. Furthermore, we focus on the notion of *cost of privacy*, which represents the difference in objective costs for the Leader and follower, before and after the obfuscation. We provide theoretical bounds for the cost of privacy introduced by the proposed w-PPSM. Proofs of these theoretical properties are provided.
3) Through multiple numerical simulations, we show the efficiency and robustness of the w-PPSM under varying privacy parameters and operating conditions. The numerical results show that the w-PPSM can achieve up to two orders of magnitude cost reduction compared to a standard differentially-private mechanism.

The remainder of this paper is organized as follows. Section II introduces the target application, Section III summarizes the background on DP, Section IV defines the proposed w-PPSM, Section **??** introduces and prooves the theoretical properties of the w-PPSM, Section VI presents the numerical evaluations of the mechanism, and Section VII concludes this paper.

Nomenclature

A. Sets and Indexes

$\mathcal{J}^x$	Set of units of type x: heat market participant (H), combine dheat and power plant (CHP), heat pump (HP), and electricity market participant (E)
$\mathcal{J}_z^x$	Set of units of type x, connected to market zone z
$\mathcal{T}$	Set of 24 hours
$\mathcal{Z}^{\mathrm{E}}$	Electricity market zones
$\mathcal{Z}^{\mathrm{H}}$	Heat market zones

B. Leader's data ($D^{\mathbf{L}}$)

ρ_j^{E}	Electricity efficiency ratio of CHP j (-)
ρ_j^{H}	Heat efficiency ratio of CHP j (-)
COP_j	Coefficient of performance of HP j (-)
$\mathrm{C}_{jt}^{\mathrm{H}}$	Variable heat cost of supplier j at time t (€/Wh)
$\mathrm{F}_j^{\max}$	Maximum fuel consumption of CHP j (Wh)
$\mathrm{H}_{jt}^{\max}$	Maximum heat output of supplier j at time t (Wh)
$\mathrm{H}_{jt}^{\min}$	Minimum heat output of supplier j at time t (Wh)
$\mathrm{L}_{lt}^{\mathrm{H}}$	Heat load l at time t (Wh)
R_j	Minimum power-to-heat ratio of CHP j (-)

C. Follower's data ($D^{\mathbf{F}}$)

$\mathrm{ATC}_{zz't}^{\max}$	Maximum transmission capacity from zone z to z' at time t (Wh)
$\mathrm{ATC}_{zz't}^{\min}$	Minimum transmission capacity from zone z to z' at time t (Wh)
$\mathrm{C}_{jt}^{\mathrm{E}}$	Variable electricity cost of supplier j at time t (€/Wh)
$\mathrm{E}_{jt}^{\max}$	Maximum electricity output of supplier j at time t (Wh)
$\mathrm{E}_{jt}^{\min}$	Minimum electricity output of supplier j at time t (Wh)
$\mathrm{L}_{lt}^{\mathrm{E}}$	Electricity load l at time t (Wh)

D. Leader's variables)

$e_{jt}^{\max}$	Maximum electricity output of CHP or HP j at time t (Wh)
$e_{jt}^{\min}$	Minimum electricity output of CHP or HP j at time t (Wh)
h_{jt}	Heat production of supplier j at time t (Wh)

E. Follower's variables)

$\lambda_{zt}^{\mathrm{E}}$	Electricity market price in zone z at time t (Wh)
e_{jt}	Electricity production of supplier j at time t (Wh)
$f_{zz't}$	Electricity flow from zone z to z' at time t (Wh)

II. Heat and Electricity Market Coordination

A. Interactions between Heat and Electricity Sectors

In Nordic countries, heat and electricity systems are operated by sequential and independent competitive markets. The day-ahead heat market is traditionally cleared *before* the day-ahead electricity market. In each day-ahead energy market, suppliers place price-quantity bids for each hour of the following day that are dispatched based on a merit-order and least-cost principle. In particular, CHPs and HPs must place their bids in the heat market before the electricity market. And, once the heat market has been cleared, they place their bids in the electricity market. The sequential participation of combined heat and power plants (CHPs) and heat pumps (HPs) in both heat and electricity markets creates implicit interactions between the systems.

Firstly, the physical characteristics of CHPs and HPs induce a strong linkage between heat and electricity production. As a result, in the current day-ahead electricity market, the minimum and maximum electricity outputs of CHPs and HPs are defined by their day-ahead heat dispatch. This heat-driven approach limits the operational flexibility of these units in the electricity market, which may limit the penetration of renewable energy sources and increase electricity prices.

Additionally, the production costs of CHPs and HPs are intrinsically linked to their heat and electricity outputs. Indeed, the heat production cost Γ_j^{H} of HPs represents the cost of purchasing electricity in the day-ahead market. Similarly, the heat production cost of CHPs represents their total production cost minus revenues from electricity sales. However, the current market framework does not account for the impact of the heat production of CHPs and HPs on the electricity market prices, which in turn, impact the production costs in the heat market and may result in an inefficient dispatch.

B. Decoupled Heat and Electricity Market Framework

Based the aforementioned heat and electricity market framework, the *decoupled* heat market problem $\mathcal{P}^{\mathrm{L,Dec}}(D^{\mathrm{L}}, \bar{\lambda}^{\mathrm{E}}_{zt})$ can be expressed as:

$$\min_{\substack{\boldsymbol{e}_{jt},\boldsymbol{h}_{jt},\\ \boldsymbol{e}^{\min}_{jt},\boldsymbol{e}^{\max}_{jt}}} \theta^{\mathrm{L}}(\boldsymbol{e}_{jt},\boldsymbol{h}_{jt},\bar{\lambda}^{\mathrm{E}}_{jt}) = \sum_{z\in\mathcal{Z}^{\mathrm{E}},t\in\mathcal{T}} \Big[\sum_{j\in\mathcal{J}^{\mathrm{HP}}_z} \frac{\boldsymbol{\lambda}^{\mathbf{E}}_{zt}}{\mathrm{COP}_j}\boldsymbol{h}_{jt} + \sum_{j\in\mathcal{J}^{\mathrm{H}}_z} \mathrm{C}^{\mathrm{H}}_{jt}\boldsymbol{h}_{jt} - \sum_{j\in\mathcal{J}^{\mathrm{CHP}}_z} (\bar{\lambda}^{\mathbf{E}^{\mathrm{L}}}_{zt} - \mathrm{C}^{\mathrm{E}}_{jt})\boldsymbol{e}_{jt} \Big] \tag{1a}$$

$$\text{s.t.} \quad \sum_{l\in\mathcal{L}^{\mathrm{H}}_z} L_{lt} = \sum_{j\in\mathcal{J}^{\mathrm{H}}_z} \boldsymbol{h}_{jt},\ \forall z\in\mathcal{Z}^{\mathrm{H}}, t\in\mathcal{T} \tag{1b}$$

$$\mathrm{H}^{\min}_{jt} \le \boldsymbol{h}_{jt} \le \mathrm{H}^{\max}_{jt},\ \forall j\in\mathcal{J}^{\mathrm{H}}, t\in\mathcal{T} \tag{1c}$$

$$\boldsymbol{e}^{\min}_{jt} = \boldsymbol{e}^{\max}_{jt} = -\frac{\boldsymbol{h}_{jt}}{\mathrm{COP}_j},\ \forall j\in\mathcal{J}^{\mathrm{HP}}, t\in\mathcal{T} \tag{1d}$$

$$\boldsymbol{e}^{\min}_{jt} = \frac{\boldsymbol{h}_{jt}}{\mathrm{R}_j},\ \forall j\in\mathcal{J}^{\mathrm{CHP}}, t\in\mathcal{T} \tag{1e}$$

$$\boldsymbol{e}^{\max}_{jt} = \frac{\mathrm{F}^{\max}_j - \rho^{\mathrm{H}}_j\boldsymbol{h}_{jt}}{\rho^{\mathrm{E}}_j},\ \forall j\in\mathcal{J}^{\mathrm{CHP}}, t\in\mathcal{T} \tag{1f}$$

$$\boldsymbol{e}^{\max}_{jt} \le \boldsymbol{e}_{jt} \le \boldsymbol{e}^{\min}_{jt},\ \forall j\in\mathcal{J}^{\mathrm{CHP}\cup\mathrm{HP}}, t\in\mathcal{T} \tag{1g}$$

where $\theta^{\mathrm{L}}(\boldsymbol{e}_{jt},\boldsymbol{h}_{jt},\bar{\lambda}^{\mathrm{E}}_{jt})$ in (1a) represents the heat production cost as a function of the expected electricity prices $\bar{\lambda}^{\mathbf{E}^{\mathrm{L}}}_{zt}$, the heat production $\boldsymbol{h}_{jt}$ of heat-only producers, and the *expected* electricity outputs $\boldsymbol{e}_{jt}$ of CHPs and HPs. Note that $\bar{\lambda}^{\mathbf{E}^{\mathrm{L}}}_{zt}$ is considered as a fixed parameters, whereas $\boldsymbol{h}_{jt}$ and $\boldsymbol{e}_{jt}$ are considered as decision variables. While, in practice $\boldsymbol{e}_{jt}$ is not controlled by the heat market operators, this formulation allows them to compute the CHPs and HPs' expected heat costs, defined as $\mathrm{C}^{\mathrm{H}}_{jt}\boldsymbol{h}_{jt} - (\bar{\lambda}^{\mathbf{E}}_{zt} - \mathrm{C}^{\mathrm{E}}_{jt})\boldsymbol{e}_{jt}$ for $j\in\mathcal{J}^{\mathrm{CHP}}$ and$\bar{\lambda}^{\mathbf{E}^{\mathrm{L}}}_{zt}\boldsymbol{e}_{jt}$ for $j\in\mathcal{J}^{\mathrm{HP}}$, and to clear the heat market based on the least cost principle.

The feasible region $\mathcal{F}^{\mathrm{L,Dec}}$ represents the set of decision variables $\{\boldsymbol{e}_{jt},\boldsymbol{h}_{jt},\boldsymbol{e}^{\min}_{jt},\boldsymbol{e}^{\max}_{jt}\}$ that satisfy constraints (1b)-(1g). Constraint (1b) is the heat balance equation in each market zone[1], (1c) represents the heat production bounds for all heat suppliers, (1d)-(1f) define the minimum and maximum electricity production (or consumption) of CHPs and HPs as function of their heat dispatch, and (1g) enforces constraints on their *expected* electricity outputs in the electricity market.

Once the heat market has been cleared, CHPs and HPs participate in the day-ahead electricity market $\mathcal{P}^{\mathrm{F}}\left(\boldsymbol{e}^{\min}_{jt},\boldsymbol{e}^{\max}_{jt},D^{\mathrm{F}}\right)$, is formulated as:

$$\min_{\substack{\boldsymbol{e}_{jt},\\ f_{zz't}}} \sum_{t\in\mathcal{T}}\sum_{j\in\mathcal{J}^{\mathrm{E}}} \mathrm{C}^{\mathrm{E}}_{jt}\boldsymbol{e}_{jt} \tag{2a}$$

$$\text{s.t.} \quad \sum_{l\in\mathcal{L}^{\mathrm{E}}_z} L^{\mathrm{E}}_{lt} = \sum_{j\in\mathcal{J}^{\mathrm{E}}_z} \boldsymbol{e}_{jt} + \sum_{z'\in\mathcal{Z}^{\mathrm{E}}} \boldsymbol{f}_{zz't} : \boldsymbol{\lambda}^{\mathbf{E}}_{zt},\ \forall z\in\mathcal{Z}^{\mathrm{E}}, t\in\mathcal{T} \tag{2b}$$

$$\mathrm{TC}^{\min}_{zz't} \le \boldsymbol{f}_{zz't} = -\boldsymbol{f}_{z'zt} \le \mathrm{TC}^{\max}_{zz't},\ \forall z,z'\in\mathcal{Z}^{\mathrm{E}}, t\in\mathcal{T} \tag{2c}$$

$$\mathrm{E}^{\min}_{jt} \le \boldsymbol{e}_{jt} \le \mathrm{E}^{\max}_{jt},\ \forall j\in\mathcal{J}^{\mathrm{E}\setminus\{\mathrm{CHP}\cup\mathrm{HP}\}}, t\in\mathcal{T} \tag{2d}$$

$$\boldsymbol{e}^{\min}_{jt} \le \boldsymbol{e}_{jt} \le \boldsymbol{e}^{\max}_{jt},\ \forall j\in\mathcal{J}^{\mathrm{CHP}\cup\mathrm{HP}}, t\in\mathcal{T} \tag{2e}$$

where (2a) represents the electricity production cost, (2b) is the electricity balance equation in each market zone, (2d) and (2e) represent the electricity production (or consumption) bounds of electricity-only producers, as well as CHPs and HPs, respectively. Note that the upper- and lower-bounds on the electricity outputs of CHPs and HPs in (2e) are defined with respect to their heat dispatch in (1d)-(1f), and treated as parameters in $\mathcal{P}^{\mathrm{F}}\left(\boldsymbol{e}^{\min}_{jt},\boldsymbol{e}^{\max}_{jt},D^{\mathrm{F}}\right)$.

C. Electricity-Aware Heat Market Framework

This paper provides an extension of the EAHM developed in [5]. This market framework aims at improving the coordination between heat and electricity sectors by better accounting for the interactions between them, while maintaining the sequential order of their decisions. This coordination framework is a classic Stackelberg game, in which the decisions of the first player (leader) impact the decisions of the second player (follower), which, in turn turn, impact the objective of the leader. As illustrated in the upper-part of Fig. 1, in the EAHM, the heat market operator (leader) tries to minimize heat production costs while anticipating the impact of the heat dispatch of CHPs and HPs on the electricity market outcomes, specifically on electricity prices, which in turn impact heat production costs. This EAHM can be modelled as a bilevel optimization problem, in which the the upper-level problem, representing the heat market clearing, is constrained by the lower-level problem $\mathcal{P}^{\mathrm{F}}\left(\boldsymbol{e}^{\min}_{jt},\boldsymbol{e}^{\max}_{jt},D^{\mathrm{F}}\right)$, representing the electricity market clearing for a given value of the heat market outcomes (namely the minimum and maximum electricity outputs of CHPs and HPs). The upper-level problem $\mathcal{P}^{\mathrm{L}}\left(D^{\mathrm{L}},D^{\mathrm{F}}\right)$ of this EAHM is formulated as:

$$\min_{\substack{\boldsymbol{e}_{jt},\boldsymbol{h}_{jt},\boldsymbol{\lambda}^{\mathbf{E}}_{zt},\\ \boldsymbol{e}^{\min}_{jt},\boldsymbol{e}^{\max}_{jt}}} \theta^{\mathrm{L}}(\boldsymbol{e}_{jt},\boldsymbol{h}_{jt},\boldsymbol{\lambda}^{\mathbf{E}}_{jt}) \tag{3a}$$

$$\text{s.t.} \quad \text{constraints (1b)} - \text{(1f)} \tag{3b}$$

$$\{\boldsymbol{e}_{jt},\boldsymbol{\lambda}^{\mathbf{E}}_{zt}\} \in \text{sol. of } \mathcal{P}^{\mathrm{F}}\left(\boldsymbol{e}^{\min}_{jt},\boldsymbol{e}^{\max}_{jt},D^{\mathrm{F}}\right), \tag{3c}$$

where $\theta^{\mathrm{L}}(\boldsymbol{e}_{jt},\boldsymbol{h}_{jt},\boldsymbol{\lambda}^{\mathbf{E}}_{jt})$ in (3a) represents the heat production cost defined in (1a) as a function of the electricity prices $\boldsymbol{\lambda}^{\mathbf{E}}_{zt}$, the heat production $\boldsymbol{h}_{jt}$ of heat-only producers, and the electricity outputs $\boldsymbol{e}_{jt}$ of CHPs and HPs. The feasible set $\mathcal{F}^{\mathrm{L}}$ of this problem represents the decision

[1]Each heat market zone represents a geographically isolated district heating network.

variables $\{\boldsymbol{h_{jt}}, \boldsymbol{e_{jt}}, \boldsymbol{\lambda^{E}_{zt}}, \boldsymbol{e^{min}_{jt}}, \boldsymbol{e^{max}_{jt}}\}$ that satisfy constraints (3b) and (3c). Constraint (3b) enforces the same operating constraints (1b) - (1f) as the decoupled heat market-clearing problem for the upper-level decision variables $\{\boldsymbol{h_{jt}}, \boldsymbol{e^{min}_{jt}}, \boldsymbol{e^{max}_{jt}}\}$. And, the lower-level decision variables $\{\boldsymbol{e_{jt}}, \boldsymbol{\lambda^{E}_{zt}}\}$ are defined as the solutions to the electricity market-clearing problem in Constraint (3c). A detailed formulation of this bilevel optimization problem and its solution method is provided in [5].

We denote with $\{e^*_{jt}, h^*_{jt}, \lambda^{E^*}_{zt}, e^{min^*}_{jt}, e^{max^*}_{jt}\}$ the optimal solutions to this *original* Stackelberg problem $\mathcal{P}^{L}(D^{L}, D^{F})$. And, Θ^{L^*} and Θ^{F^*} represent the *original* follower and leader's optimal costs, respectively.

III. Differential Privacy Framework

A. Privacy Goals

To achieve coordination, the leader problem takes the follower's data D^{F} as input. This data includes price-quantity bids of suppliers and electricity loads of consumers for each hour of the following day. In line with recent regulatory changes, encouraging information exchange for sector coordination [8], the electricity suppliers' bids are considered as available information ($D^{F,a}$) shared with the leader. However, the loads of individual consumers is sensitive information ($D^{F,p}$) that needs to be protected to avoid the leakage of identifying or competitive information [9]. Although the leader solely requires the aggregate electricity load in each market zone as input data, aggregation has been showed to be insufficient to protect individuals' data [16]. Therefore, in this target application, the framework of DP is applied to obfuscate the aggregate electricity loads in each market zone $z \in \mathcal{Z}$ over a 24-hour period, before sharing it with the leader.

For this purpose, the infinite sequence of hourly aggregate electricity loads is represented as so-called *data stream* $L^{E}_{zt} = \sum_{j \in \mathcal{L}^{E}_{z}} L^{E}_{jt}$, with the tuples (z, t) in the universe $\mathcal{U} = \mathcal{Z}x\mathcal{T}^{\infty}$, where $\mathcal{Z} = \{1, ..., Z\}$ is the set of users (market zones) and $\mathcal{T}^{\infty} = \{1, 2, ...\}$ is an unbounded set of time steps (hours) [13]. In this data stream, an *event* $L^{E}_{t} = \left[L^{E}_{1t}, ..., L^{E}_{Zt}\right]$ is defined as all the data points reported by the users that occurred at time t. The goal is therefore to apply DP to this data stream.

B. Differential Privacy for 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 [11]. This framework enjoys several important properties, including *composability* and *immunity to post-processing*. This paper adopts the *w-privacy* framework [12], 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 $L^{E}[t] = \left[L^{E}_{1}, ..., L^{E}_{t}\right]$ of all events that occurred at or before time t. It relies on the notion of *w-adjacency* [13] to capture the differential information to be protected, as defined below:

Definition 1 *Two data streams prefixes $L^{E}[t]$ and $L'^{E}[t]$ are w-neighbors, denoted by $L^{E}[t] \sim_{w} L'^{E}[t]$, 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 L^{E}_{i} and L'^{E}_{i}, where $i \in [t]$, as: $\exists z$ s.t. $|L^{E}_{zi} - L'^{E}_{zi}| \leq \alpha$ and $\forall z' \neq z$, $L^{E}_{z'i} = L'^{E}_{z'i}$ 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 $L^{E}_{i} \neq L'^{E}_{i}$ and $L^{E}_{j} \neq L'^{E}_{j}$, then it holds that $j - i + 1 \leq w$.*

In the context of the target application, a mechanism is said to satisfy w-event ε-differential privacy (w-privacy for short) if it satisfies the following definition:

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 $L^{E}[t] \sim_{w} L'^{E}[t]$, with $t \in \mathcal{T}^{\infty}$, and all sets $S \subseteq \mathcal{S}$, it satisfies:*

$$\frac{\mathbb{P}\left(\mathcal{M}(L^{E}[t]) \in S\right)}{\mathbb{P}\left(\mathcal{M}(L'^{E}[t]) \in S\right)} \leq exp(\varepsilon), \tag{4}$$

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

C. Laplace Mechanism

A commonly used method to achieve w-privacy for data streams is the so-called *Laplace mechanism*. In the target application of this work, the privacy goal is to protect a data stream of aggregate loads within a 24-hour window. Therefore, we consider the Laplace mechanism $\mathcal{M}^{Lap}$ which takes as input a stream prefix $L^{E}[t]$ and outputs the sequence $\tilde{L}^{E}[t] = \left[\tilde{L}^{E}_{1}, ..., \tilde{L}^{E}_{t}\right]$, such that $\tilde{L}^{E}_{i} = L^{E}_{i} + \xi_i$ where $\xi_i \in \mathbb{R}^{Z}$ is drawn from the i.i.d. Laplace distribution $Lap(\frac{w\alpha}{\varepsilon})^{Z}$ for $i \in [t]$, with the time window parameter $w = 24$. It is a well-known result that this Laplace mechanism achieves w-privacy with $w = 24$ [13].

The main limitation of this 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 [15]. The w-PPSM introduced in this paper specifically aims at mitigating this issue.

IV. w-Privacy-Preserving Stackelberg Mechanism

the w-PPSM developed in [15] allows the exchange of differentially private data of high fidelity between the agents of a Stackelberg game. This section describes an extension of the w-PPSM that achieves w-privacy for a data stream.

A. Assumptions

Similarly to [15], this paper assumes that the leader and the follower each have access to the prediction model $\mathcal{M}$ that can privately forecast the electricity market cost $\bar{\Theta}^{\mathrm{F}}$ and prices $\bar{\lambda}^{\mathrm{E}}_{zt}$. This assumption is realistic in energy systems, since prediction models are commonly used to efficiently bid in the markets. The theoretical results introduced in this Section hold under the assumption that these prediction models are *accurate*.

Assumption 1 *We assume that there exists small-enough constants $\eta_\Theta > 0$, $\eta_\lambda > 0$ and $p > 0$, such that:*

$$\mathbb{P}\left(\left|\bar{\Theta}^{F} - \Theta^{F^*}\right| \leq \eta_\Theta\right) \geq 1 - p \tag{5a}$$

$$\mathbb{P}\left(\left|\bar{\lambda}^{E}_{zt} - \lambda^{E^*}_{zt}\right| \leq \eta_\lambda,\ \forall z \in \mathcal{Z}^E, t \in \mathcal{T}\right) \geq 1 - p, \tag{5b}$$

where $\bar{\Theta}^F$ and $\bar{\lambda}^E_{zt}$ represent the electricity market cost and prices privately predicted by the model model $\mathcal{M}$, and Θ^{F^*} and $\lambda^{E^*}_{zt}$ represent the original electricity market cost and prices from the Stackelberg problem in (3).

B. Steps

The proposed w-PPSM ($\mathcal{M}^{\mathrm{PPSM}}$) is performed each day, before the heat and electricity markets are cleared, to protect the sensitive data of the follower $D^{\mathrm{F,p}}$ for each hour 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 Figure 1 and summarized below.

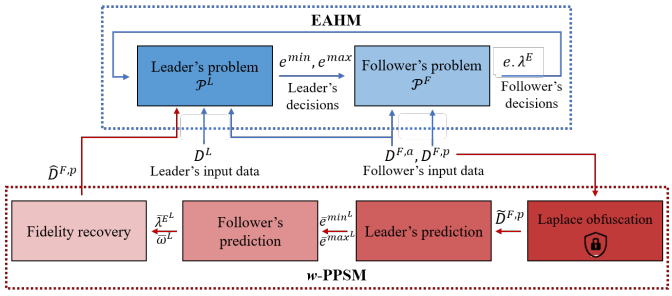

Figure 1. EAHM and w-PPSM flowchart

*1) **Laplace-obfuscation**:* Firstly, the follower obfuscates the sensitive data $D^{\mathrm{F,p}}$ according to the w-private Laplace mechanism $\mathcal{M}^{\mathrm{Lap}}$ described in Section III-C, before releasing it to the leader.

*2) **Leader's prediction**:* Using publicly available data and the Laplace-obfuscated data $\tilde{D}^{\mathrm{F,p}}$ obtained in step (1), the leader estimates the values of the minimum and maximum electricity outputs of CHPs and HPs ($\bar{e}^{\min}_{jt}$ and $\bar{e}^{\max}_{jt}$) for the following day. To do so, it uses its prediction model $\mathcal{M}$ to predict the electricity prices $\bar{\lambda}^{\mathrm{E}}_{zt}$. The leader then uses this estimate to solve the decoupled heat market $\mathcal{P}^{Dec}(D^{\mathrm{L}}, \bar{\lambda}^{\mathrm{E}}_{zt})$. Note that this optimization problem does not take the follower's data D^{F} as input. The solutions of this optimization problem ($\bar{e}^{\max}_{jt}$ and $\bar{e}^{\min}_{jt}$) are shared with the follower.

*3) **Follower's prediction**:* With publicly available information, the Laplace-obfuscated data obtained in step (1), and the predicted values obtained in step (2), the follower predicts the electricity market costs $\bar{\Theta}^{\mathrm{F}}$ and prices $\bar{\lambda}^{\mathrm{E}}_{zt}$ using the prediction model $\mathcal{M}$.

*4) **Fidelity recovery**:* Given its own available data, the obfuscated data obtained in step (1) and the predicted values computed in steps (2) and (3), the follower derives the new privacy-preserving data $\hat{\boldsymbol{D}}^{\mathrm{F,p}}$. To do so, it uses an optimization-based approach to optimally redistribute the noise on the sensitive data introduced in step (1) while recovering feasibility and fidelity w.r.t to the solutions of the original Stackelberg game. This bilevel optimization problem, inspired by [15], is formulated as:

$$\min_{\hat{\boldsymbol{D}}^{\mathbf{F,p}}, \hat{\boldsymbol{\lambda}}^{\mathbf{E}}_{\boldsymbol{zt}}, \hat{\boldsymbol{\Theta}}^{\mathbf{F}}} \|\hat{\boldsymbol{D}}^{\mathbf{F,p}} - \tilde{D}^{\mathrm{F,p}}\|_2^2 \tag{6a}$$

$$\text{s.t.} \quad |\hat{\boldsymbol{\Theta}}^{\mathbf{F}} - \bar{\Theta}^{F}| \leq \beta_\Theta \tag{6b}$$

$$|\hat{\boldsymbol{\lambda}}^{\mathbf{E}}_{\boldsymbol{zt}} - \bar{\lambda}^{\mathrm{E}}_{zt}| \leq \beta_\lambda, \forall z \in \mathcal{Z}, t \in \mathcal{T} \tag{6c}$$

$$\hat{\boldsymbol{\lambda}}^{\mathbf{E}}_{\boldsymbol{zt}} = \text{sol. of } \mathcal{P}^{\mathrm{F}}\left(\bar{e}^{\min}_{jt}, \bar{e}^{\max}_{jt}, D^{\mathrm{F,a}}, \hat{\boldsymbol{D}}^{\mathbf{F,p}}\right), \tag{6d}$$

where the objective (6a) 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 w.r.t. the predicted objective value $\bar{\Theta}^{\mathrm{F}}$ (6b) and electricity prices $\bar{\lambda}^{\mathrm{E}}_{zt}$ (6b), and feasibility constraints w.r.t. the follower's problem $\mathcal{P}^{\mathrm{F}}\left(\bar{e}^{\min}_{jt}, \bar{e}^{\max}_{jt}, D^{\mathrm{F,a}}, \hat{\boldsymbol{D}}^{\mathbf{F,p}}\right)$ in (6d). β_Θ and β_λ are parameters specifying the desired fidelity levels. Note that since the dual variables of the follower directly impact the leader's problem, (6c) indirectly enforces fidelity w.r.t. the leader's objective value. Furthermore, the follower's objective function $\hat{\Theta}^{\mathrm{F}}$ and dual variables $\hat{\lambda}^{\mathrm{E}}_{zt}$ are defined as the solutions to the lower-level problem (6d). The solutions to this optimization problem $\hat{D}^{\mathrm{F,p}}$ are shared with the leader.

After the w-PPSM has been performed, the leader uses the privacy-preserving data $\hat{D}^{\mathrm{F,p}}$ as input to solve its bilevel optimization problem $\mathcal{P}^{\mathrm{L}}(D^{\mathrm{L}}, D^{\mathrm{F,a}}, \hat{D}^{\mathrm{F,p}})$ described by (3). The optimal objective value of this privacy-preserving problem is denoted $\hat{\Theta}^{\mathrm{L}}$ and represents the optimal objective cost of the Leader after the w-PPSM.

V. Theoretical properties of w-PPSM

This section introduces strong theoretical properties on the privacy and error introduced by the w-PPSM. Proofs of these properties are detailed in the Appendix.

A. Privacy

Theorem 1 (Privacy) *For given positive real values of the parameters α, ε, β_Θ and β_λ, the proposed w-PPSM satisfies w-privacy.*

Proof Sketch. The proof relies on the observation that step (1) satisfies w-privacy, and that Therefore, the immunity to post-processing of DP, guarantees the w-privacy of the proposed w-PPSM. □

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

B. Error Analysis

After the post-processing phase, theoretical bounds on the error introduced on the sensitive data and on the electricity prices can be derived.

Theorem 2 (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:*

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

where $\hat{D}^{F,p}$ is the solution to post-processing Problem (6)*.*

Proof Sketch. The proof relates the distance between $\hat{D}^{\mathrm{F,P}}$ and $D^{\mathrm{F,P}}$ to that between the Laplace-obfuscated $\tilde{D}^{\mathrm{F,P}}$ and $D^{\mathrm{F,P}}$, and relies on the triangular inequality on norms, optimality of $\hat{D}^{\mathrm{F,P}}$, and the fact that the Laplace mechanism is an unbiased estimator. □

Theorem 3 (Error on Prices) *After the fidelity recovery phase, the error induced by the w-PPSM on the original electricity prices $\lambda_{zt}^{E^*}$ is bounded by the inequality:*

$$\mathbb{P}\left(\left|\hat{\lambda}_{zt}^{E} - \lambda_{zt}^{E^*}\right| \leq \beta_\lambda + \eta_\lambda^F,\ \forall z \in \mathcal{Z}^E, t \in \mathcal{T}\right) \geq 1 - p, \quad (7)$$

where $\hat{\lambda}_{jt}^{E}$ is the solution to post-processing Problem (6a)-(6d)*.*

Proof Sketch. The proof relates the distance between the privacy-preserving prices $\hat{\lambda}_{zt}^{\mathrm{E}}$ and the original prices $\lambda_{zt}^{\mathrm{E}^*}$ to that between the estimated prices $\bar{\lambda}_{zt}^{\mathrm{E}}$ in Step (3) and $\lambda_{zt}^{\mathrm{E}^*}$, and relies on the triangular inequality on norms, optimality of $\hat{\lambda}_{zt}^{\mathrm{E}}$, Assumption 1, and the fidelity constraint (6c). □

This theorem allows us to measure the impact of the w-PPSM on the leader's objective cost, as discussed below.

C. Cost of Privacy

The so-called *cost of privacy* represents the impact of the w-PPSM on the objective costs of the leader and the follower. In particular, we define formally the follower the leader and follower's costs of privacy below.

Definition 3 (Cost of privacy) *The cost of privacy of the w-PPSM for each agent a (leader or follower) is defined as the following quantity:*

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

where Θ^{a^*} represents the original objective cost of agent a before the w-PPSM, and $\hat{\Theta}^a$ represents the objective cost of agent a after the fidelity recovery phase.

One major contribution of the proposed w-PPSM is to provide theoretical bounds on these costs.

Theorem 4 (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:*

$$\mathbb{P}(\Delta\Theta^F \leq \beta_\Theta + \eta_\Theta) \geq 1 - p. \quad (8)$$

Proof Sketch. The proof relates the distance between the privacy-preserving cost $\hat{\Theta}^{\mathrm{F}}$ and the original cost Θ^{F^*} to that between the estimated cost $\bar{\Theta}^{\mathrm{F}}$ in Step (3) and Θ^{F^*}; and relies on the triangular inequality on norms, optimality of $\hat{\Theta}^{\mathrm{F}}$, Assumption 1, and the fidelity constraint (6b). □

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

Additionally, the objective of the leader is directly impacted by the error on the coordination variables $\boldsymbol{\lambda}_{\boldsymbol{zt}}^{\mathbf{E}}$. As result, we can derive theoretical bounds on the leader's cost of privacy as follows:

Theorem 5 (Leader's Cost of Privacy) *After the fidelity recovery phase, the error induced by the w-PPSM on the original electricity prices $\lambda_{zt}^{E^*}$ is bounded by the inequality:*

$$\mathbb{P}\left(\Delta\Theta^L \leq (\beta_\lambda + \eta_\lambda^F)\left[\sum_{j\in\mathcal{J}^{HP}} \frac{H_j^{max}}{COP_j} + \sum_{j\in\mathcal{J}^{CHP}} \frac{F_j^{max}}{\rho_j^E}\right]\right) \geq 1 - p. \quad (9)$$

Proof Sketch. The proof relies on the triangular inequality on norms, optimality of $\hat{\lambda}_{zt}^{\mathrm{E}}$, and Theorem 3. □

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

As illustrated in Figure 2, 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 [17]. 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 [18]–[20] and available online at [21].

Furthermore, realistic time series of heat and electricity loads and wind power generation for an entire year (2017) are derived from [4], [22], [23] and depicted in Figures 3 and 4.

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.

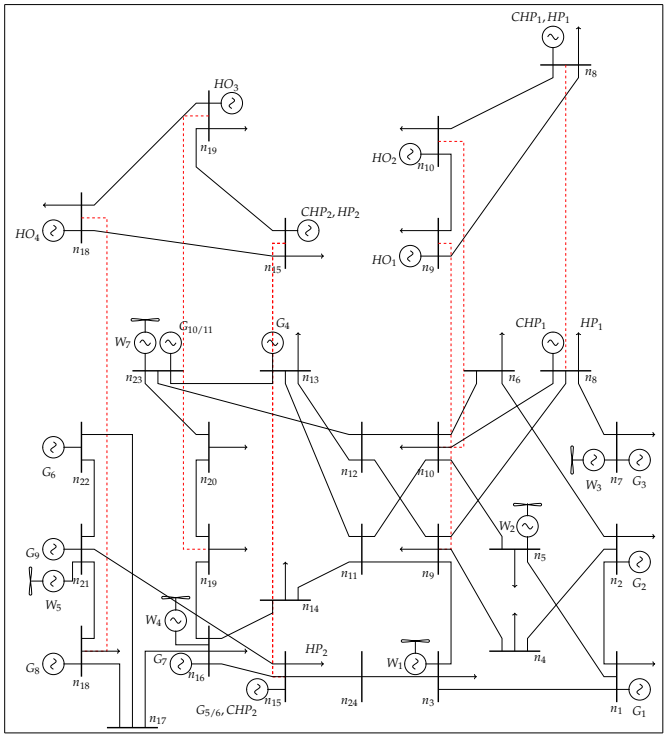

Figure 2. Case study 1: Modified IEEE 24-node electricity system with 6 wind farms (the bottom system) connected to two isolated 3-node district heating systems (the two systems on the top of the figure)

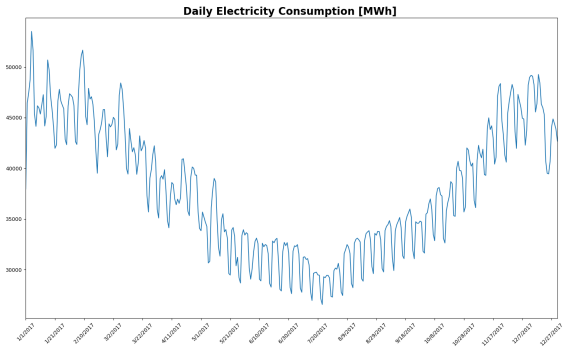

Figure 3. Daily electricity consumption over one year [MWh].

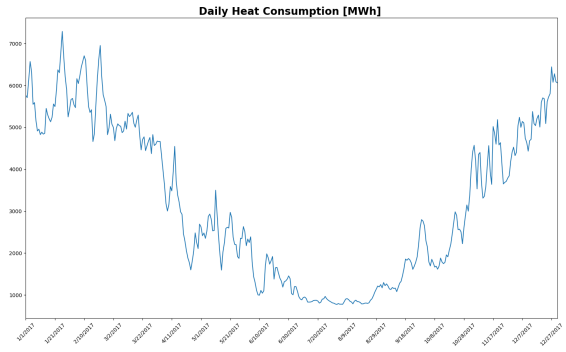

Figure 4. Daily heat consumption over one year [MWh].

B. Results

1) Limitations of Laplace Mechanism: In this first analysis, the privacy budget ε is fixed to 1, and the fidelity parameters β_Θ and β_λ are fixed to 0.1% of the follower's objective and 10.0% of the electricity prices, respectively. We analyse the impact of the indistinguishability parameter α on the error introduced by the different mechanisms. As α represents how much variation of load is protected, it directly impacts the level of noise added to the original data.

Table I reports the error on the original sensitive data, and the leader and follower's *costs of privacy*, defined as the relative errors on the objective values of the leader and the follower, achieved by the Laplace mechanism and the w-PPSM for different values of the indistinguishability parameter α[2]. As expected, the errors on the sensitive data and the leader's cost of privacy induced by the Laplace mechanism drastically increase as α grows. On the contrary, the w-PPSM shows substantially better performances, and these errors remain stable with the increase of the parameter α. For larger values of α (≥ 50), the w-PPSM achieves up to one order of magnitude reduction in the error on the sensitive data, and two orders of magnitude reduction in the leader's cost of privacy.

We also observe that the follower's cost of privacy, for both mechanisms, slightly decreases with higher values of α. Intuitively, this can be explained by the interactions between the leader and the follower in the Stackelberg game. As the noise added to the electricity demand increases, the leader is less capable of anticipating the reaction of the follower, and of optimizing its own objective at the expense of the follower. Similar observations have been made related to the impact of DP on truthfulness in mechanism design [24]. Furthermore, the w-PPSM consistently achieves better performances compared to the Laplace mechanism, and up to two orders of magnitude reduction in the follower's cost of privacy.

Table I
ERRORS ON THE ELECTRICITY DEMAND VECTOR ($\Delta D^{\mathrm{F,p}}$), OBJECTIVE VALUES OF THE LEADER ($\Delta\Theta^{\mathrm{L}}$) AND THE FOLLOWER ($\Delta\Theta^{\mathrm{F}}$) FOR VARYING INDISTINGUISHABILITY PARAMETERS α, AVERAGED OVER 100 INSTANCES.

$\mathcal{M}$	α	$\Delta D^{\mathrm{F,p}}$ (L1)	$\Delta\Theta^{\mathrm{L}}$ (%)	$\Delta\Theta^{\mathrm{F}}$ (%)
Laplace	10.0	6139.88	0.764773	8.751309
	50.0	34131.08	47.556005	6.352331
	100.0	39131.19	58.455686	5.430761
PPSM	10.0	3723.66	0.842956	1.067518
	50.0	3843.56	0.606088	0.483239
	100.0	3296.58	0.302367	0.058785

2) Impact of Fidelity Recovery Phase: For this analysis, the privacy budget ε is fixed to 1, the fidelity parameter on the dual variables is fixed to β_λ is fixed to 10.0% of the electricity prices, and the indistinguishability parameter is fixed to $\alpha = 100$. We analyze the impact of the fidelity

[2]The chosen values of α guarantee a low privacy risk since the aggregate electricity demand ranges between 644.47MWh and 2498.54MWh.

parameter β_Θ, which enforces fidelity on the leader's objective cost, on the follower's cost of privacy. Table II summarizes the difference in the leader and follower's costs of privacy achieved by the w-PPSM for varying values of the fidelity parameter η_Θ. As expected, for growing values of η_Θ, the follower's cost of privacy increases. However, this change is slight. Furthermore, we observe that this parameter does not impact the leader's cost of privacy, which remains stable for all values of η_Θ. Furthermore, we note that the w-PPSM reduces the costs of privacy for both the leader and the follower by up to two orders of magnitude compared to the Laplace mechanism.

Table II
LEADER AND FOLLOWER'S COSTS OF PRIVACY (IN % OF ORIGINAL COSTS) AT VARYING FIDELITY PARAMETERS η_λ (WITH $\eta_\Theta = 10\%$).

$\mathcal{M}$	η	$\Delta\Theta^{\mathbf{L}}$ (%)	$\Delta\Theta^{\mathbf{F}}$ (%)
Laplace	NA	58.455686	5.430761
PPSM	0.1%	0.302367	0.058785
	1.0%	0.313176	0.176356
	10.0%	0.234731	0.205749

3) Impact of Operating Conditions: In this analysis, the privacy budget ε is fixed to 1, and the fidelity parameters β_Θ and β_λ are fixed to 0.1% of the follower's objective and 10.0% of the electricity prices, respectively. We 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. Figure 5 presents heat maps of the leader and follower's costs of privacy under varying stress factors η_H (η_E) representing the multiplying factors applied to the heat (electricity) loads of the reference day previously considered. In this analysis, the heat load is uniformly increased by 30% to 60%, and the electricity load by 10% to 100%. This analysis is conducted for three different values of the indistinguishability parameter α.

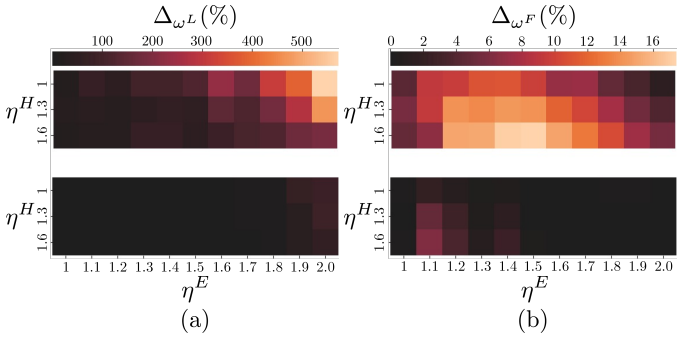

Figure 5. (a) Leader's cost of privacy ($\Delta\Theta^{\mathrm{L}} in\%$) at varying heat ($\eta_\mathrm{H}$) and electricity ($\eta_\mathrm{E}$) stress levels, obtained via the Laplace mechanism (top) and w-PPSM (bottom). (a) Follower's cost of privacy ($\Delta\Theta^{\mathrm{F}} in\%$) at varying heat ($\eta_\mathrm{H}$) and electricity ($\eta_\mathrm{E}$) stress levels, obtained via the Laplace mechanism (top) and w-PPSM (bottom) for $\alpha = 100.0$(MWh), averaged over 20 instances.

Overall, this stress analysis underlines once more the robustness of the w-PPSM under various operating conditions. Indeed, the w-PPSM succeeds in keeping the leader and follower's cost of privacy very low compared to the Laplace mechanism, for all the stress factor levels. Under certain operating conditions, the w-PPSM achieves up to two orders of magnitude reduction in the leader and follower's costs of privacy.

We also notice that the highest costs of privacy for each mechanism are achieved under different combinations of stress factors. The Laplace mechanism performs especially poorly for the leader's cost of privacy for high values of the electricity stress factor. Intuitively, this can be explained by the fact that, for higher electricity loads, the volatility of the electricity prices is increased, which in turn, impacts the merit order in the heat market and leads to a sub-optimal dispatch. However, this error is somehow reduced for corresponding higher values of the heat stress factor. Indeed, with higher heat loads, the relative share of HPs and CHPs in the heat dispatch, and therefore their impact on the leader's objective value, decreases. Furthermore, the Laplace mechanism achieves the highest follower's cost of privacy for the highest heat stress factor. 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. These tightened interactions between heat and electricity markets result in higher errors on the electricity costs. This analysis identifies the system's operating conditions that are the most vulnerable to perturbations and the ones resulting in a negligible cost of privacy when applying DP. This information can be leveraged to reduce the privacy budget [13].

4) Yearly analysis: The heat maps provided above are derived synthetically, by multiplying once specific day's loads profiles by stress factors. In order to analyse the impact of peak loads as well as load profiles' shapes, the leader and follower's costs of privacy has been evaluated daily over an entire year using real load data, as shown in Figure 6. For this analysis, the privacy budget ε is fixed to 1, the fidelity parameter on the dual variables is fixed to β_λ is fixed to 10.0% of the electricity prices, and the indistinguishability parameter is fixed to $\alpha = 10$.

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

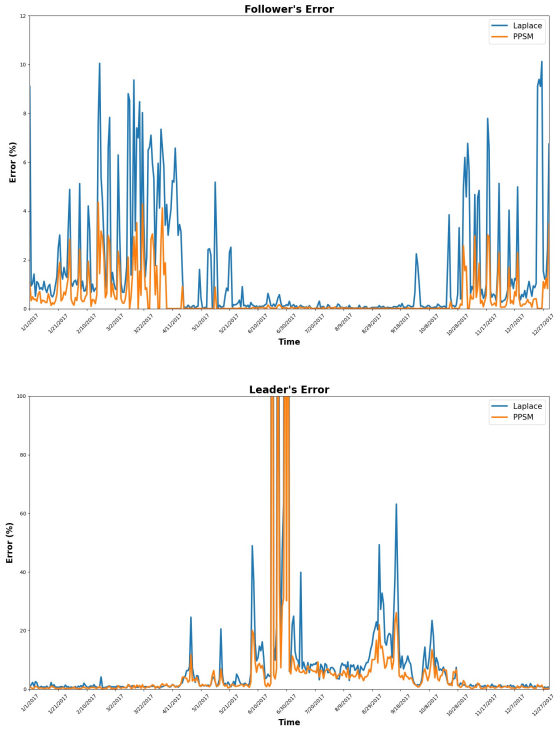

Figure 6. Follower's (top) and leader's (bottom) cost of privacy (in % of original cost) computed for each day of the year ($\alpha = 10$, $\eta_\lambda = 0.1\%$ and $\eta_\Theta = 10\%$).

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

This paper introduces the w-PPSM which generates differentially-private data streams with high fidelity that can be used as input to the EAHM to coordinate the operation of heat and electricity systems. The w-PPSM was shown to enjoy strong theoretical properties compared to the traditional Laplace mechanism. In particular, the error introduced on the sensitive data, the prices and follower's costs can be bounded. Furthermore, the numerical results show that the w-PPSM achieves up to two orders of magnitude reduction in the costs of privacy in both heat and electricity systems compared to the traditional Laplace mechanism.

Future work will aim at developing tight theoretical bounds on the costs of privacy for the Leader, and accounting for potential correlations between the users' data streams. Furthermore, focus will be placed on reducing the costs of privacy. Firstly, advanced obfuscation methods, such as Gaussian noise, can be used to reduce the initial noise added to the data. Secondly, the sparse vector technique (SVT) will be investigated and adapted to privately identify the operating conditions resulting in negligible costs of privacy, and adapt the noise added under these conditions to reduce the privacy budget [13].

References

[1] Heat Road Map Europe, "A low-carbon heating and cooling strategy for Europe," 2018. [Online]. Available: http://www.heatroadmap.eu/

[2] 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.

[3] 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.

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

[5] 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.

[6] C. Ordoudis, "Market-based approaches for the coordinated operation of electricity and natural gas systems," 2018.

[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] 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

[9] 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.

[10] 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.

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

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

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

[14] 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.

[15] 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.

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

[17] 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

[18] 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.

[19] 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.
[20] L. Mitridati and J. A. Taylor, "Power systems flexibility from district heating networks," in *Power Systems Computation Conference (PSCC)*, Dublin, Ireland, 2018.
[21] L. Mitridati, P. Van Hentenryck, and J. Kazempour, "Supplementary material - case study 1," Nov. 2021. [Online]. Available: https://doi.org/10.5281/zenodo.5717239
[22] H. Madsen, "Time series analysis. course notes," 2015. [Online]. Available: http://www.imm.dtu.dk/~hmad/time.series.analysis/assignments/index.html
[23] Energinet.dk. (2020) Danish system operator. [Online]. Available: https://en.energinet.dk/
[24] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *Foundations of Computer Science, 2007. FOCS'07. 48th Annual IEEE Symposium on*. IEEE, 2007, pp. 94–103.

Appendix

A. Proof of Theorem 1

Proof. The privacy phase (step 1) of the w-PPSM produces an obfuscated data $\tilde{D}^{\mathrm{F,p}}$ using the Laplace mechanism with parameter $w\alpha/\varepsilon$ (with $w = 24$). It is know that this mechanism satisfies w-privacy.

Steps (2) and (3) can be seen as a post-processing transformations of the obfuscated data $\tilde{D}^{\mathrm{F,p}}$. Indeed, these steps use exclusively public information and data-independent models.

As DP is immune to post-processing, this ensures that the w-PPSM protocol (steps 1-3) satisfied w-privacy. □

B. Proof of Theorem 2

Proof. Denote with $\tilde{D}^{\mathrm{F,p}} = D^{\mathrm{F,p}} + Lap(\alpha)$ the Laplace-obfuscated data obtained in step (1) of the w-PPSM. We have that:

$$\begin{aligned}\|\hat{D}^{\mathrm{F,p}} - D^{\mathrm{F,p}}\|_2 &\leq \|\hat{D}^{\mathrm{F,p}} - \tilde{D}^{\mathrm{F,p}}\|_2 + \|\tilde{D}^{\mathrm{F,p}} - D^{\mathrm{F,p}}\|_2 \\ &\leq 2\|\tilde{D}^{\mathrm{F,p}} - D^{\mathrm{F,p}}\|_2 \leq 4(w\alpha)^2.\end{aligned}$$

The first inequality follows from the triangular inequality on norms. The second inequality follows from:

$$\|\hat{D}^{\mathrm{F,p}} - \tilde{D}^{\mathrm{F,p}}\|_2 \leq \|\tilde{D}^{\mathrm{F,p}} - D^{\mathrm{F,p}}\|_2$$

by optimality of $\langle \hat{D}^{\mathrm{F,p}}, \hat{e_{jt}}, \hat{\lambda}^{\mathrm{E}} \rangle$ and the fact that $\langle \hat{D}^{\mathrm{F,p}}, \hat{e_{jt}}, \hat{\lambda}^{\mathrm{E}} \rangle$ is a feasible solution to the lower-level problem of the post-processing problem (6). The third inequality follows directly from the variance of the Laplace distribution. □

C. Proof of Theorem 3

Proof. We denote with $\hat{\lambda}^{\mathrm{E}}_{jt}$ the solution to the post-processing problem (6). We have that:

$$\begin{aligned}\|\hat{\lambda}^{\mathrm{E}}_{jt} - \lambda^{\mathrm{E}^*}_{jt}\| &\leq \|\hat{\lambda}^{\mathrm{E}}_{jt} - \bar{\lambda}^{\mathrm{E}}_{jt}\| + \|\bar{\lambda}^{\mathrm{E}}_{jt} - \lambda^{\mathrm{E}^*}_{jt}\| \\ &\leq \beta_\lambda + \|\bar{\lambda}^{\mathrm{E}}_{jt} - \lambda^{\mathrm{E}^*}_{jt}\|\end{aligned}$$

The first inequality follows from the triangular inequality on norms. The second inequality results from the fidelity constraint (6c). As a result, (7) derives from Assumption 1. □

D. Proof of Theorem 4

Proof. Denote with $\hat{\Theta}^{\mathrm{F}}$ the optimal objective value of the lower-level in the post-processing problem (6). We have the following inequalities:

$$\begin{aligned}\|\hat{\Theta}^{\mathrm{F}} - \Theta^{\mathrm{F}^*}\| &\leq \|\hat{\Theta}^{\mathrm{F}} - \bar{\Theta}^{\mathrm{F}}\| + \|\bar{\Theta}^{\mathrm{F}} - \Theta^{\mathrm{F}^*}\| \\ &\leq \beta_\Theta + \|\bar{\Theta}^{\mathrm{F}} - \Theta^{\mathrm{F}^*}\|.\end{aligned}$$

The first inequality follows from the triangular inequality on norms. The second inequality results from the fidelity constraint (6c). We derive (8) from Assumption 1. □

E. Proof of Theorem 5

Proof. We denote with $\hat{\lambda}^{\mathrm{E}}_{zt}$ and $\hat{e}_{jt}$ the solutions to the post-processing problem (6), and with $\hat{\Theta}^{\mathrm{L}}$ and $\hat{h}_{jt}$ the optimal objective value and solutions of the leader's problem $\mathcal{P}^{\mathrm{L}}(D^{\mathrm{L}}, D^{\mathrm{F,a}}, \hat{D}^{\mathrm{F,p}})$ after the post-processing step. Furthermore, we notice that

$$\begin{aligned}\hat{\Theta}^{\mathrm{L}} &= \hat{\Theta}^{\mathrm{L,Dec}} = \theta^{\mathrm{L}}(\hat{e}_{jt}, \hat{h}_{jt}, \hat{\lambda}^{\mathrm{E}}_{zt}), \\ \Theta^{\mathrm{L}^*} &= \Theta^{\mathrm{L,Dec}^*} = \theta^{\mathrm{L}}(e^*_{jt}, h^*_{jt}, \lambda^{\mathrm{E}^*}_{zt}),\end{aligned}$$

where $\hat{\Theta}^{\mathrm{L,Dec}}$ (resp. $\Theta^{\mathrm{L,Dec}^*}$) is the optimal objective value of the decoupled leader's problem $\mathcal{P}^{\mathrm{L,Dec}}(D^{\mathrm{L}}, \hat{\lambda}^{\mathrm{E}}_{zt})$ (resp. $\mathcal{P}^{\mathrm{L,Dec}}(D^{\mathrm{L}}, \lambda^{\mathrm{E}^*}_{zt})$) introduced in Section II-B with the input data fixed to D^{L} and $\hat{\lambda}^{\mathrm{E}}_{zt}$ (resp. $\lambda^{\mathrm{E}^*}_{zt}$). Therefore, we derive:

$$\begin{aligned}\hat{\Theta}^{\mathrm{L}} &\leq \theta^{\mathrm{L}}(\hat{\lambda}^{\mathrm{E}}_{zt}, \boldsymbol{e_{jt}}, \boldsymbol{h_{jt}}),\ \forall \{\boldsymbol{e_{jt}}, \boldsymbol{h_{jt}}\} \in \mathcal{F}^{\mathrm{L,Dec}}, \\ \Theta^{\mathrm{L}^*} &\leq \theta^{\mathrm{L}}(\lambda^{\mathrm{E}^*}_{zt}, \boldsymbol{e_{jt}}, \boldsymbol{h_{jt}}),\ \forall \{\boldsymbol{e_{jt}}, \boldsymbol{h_{jt}}\} \in \mathcal{F}^{\mathrm{L,Dec}}.\end{aligned}$$

As $\{e^*_{jt}, h^*_{jt}\} \in \mathcal{F}^{\mathrm{L,Dec}}$ and $\{\hat{e}_{jt}, \hat{h}_{jt}\} \in \mathcal{F}^{\mathrm{L,Dec}}$, it results that

$$\hat{\Theta}^{\mathrm{L}} - \Theta^{\mathrm{L}^*} \leq \sum_{\substack{t \in \mathcal{T} \\ z \in \mathcal{Z}^{\mathrm{E}},}} \left[\sum_{j \in \mathcal{J}^{\mathrm{HP}}_z} \frac{\hat{\lambda}^{\mathrm{E}}_{zt} - \lambda^{\mathrm{E}^*}_{zt}}{\mathrm{COP}_j} h^*_{jt} - \sum_{j \in \mathcal{J}^{\mathrm{CHP}}_z} (\hat{\lambda}^{\mathrm{E}}_{zt} - \lambda^{\mathrm{E}^*}_{zt}) e^*_{jt} \right],$$

$$\hat{\Theta}^{\mathrm{L}} - \Theta^{\mathrm{L}^*} \geq \sum_{\substack{t \in \mathcal{T} \\ z \in \mathcal{Z}^{\mathrm{E}},}} \left[- \sum_{j \in \mathcal{J}^{\mathrm{HP}}_z} \frac{\hat{\lambda}^{\mathrm{E}}_{zt} - \lambda^{\mathrm{E}^*}_{zt}}{\mathrm{COP}_j} \hat{h}_{jt} + \sum_{j \in \mathcal{J}^{\mathrm{CHP}}_z} (\hat{\lambda}^{\mathrm{E}}_{zt} - \lambda^{\mathrm{E}^*}_{zt}) \hat{e}_{jt} \right].$$

As a result, we derive (9) using the triangular inequalities on the norms, the bounds on the error on the dual variables (7), and the upper-bounds on the variables $\{e^*_{jt}, h^*_{jt}, \hat{e}_{jt}, \hat{h}_{jt}\}$. □