Differential Privacy for Power Grid Obfuscation

Ferdinando Fioretto, Terrence W.K. Mak, *Member, IEEE,* and Pascal Van Hentenryck, *Member, IEEE*

***Abstract*—The availability of high-fidelity energy networks brings significant value to academic and commercial research. However, such releases also raise fundamental concerns related to privacy and security as they can reveal sensitive commercial information and expose system vulnerabilities. This paper investigates how to release power networks where *the parameters of transmission lines and transformers are obfuscated*. It does so by using the framework of Differential Privacy (DP), that provides strong privacy guarantees and has attracted significant attention in recent years. Unfortunately, simple DP mechanisms often result in AC-infeasible networks. To address these concerns, this paper presents a novel differential privacy mechanism that guarantees AC-feasibility and largely preserves the fidelity of the obfuscated network. Experimental results also show that the obfuscation significantly reduces the potential damage of an attacker exploiting the release of the dataset.**

I. Introduction

The availability of test cases representing high-fidelity power system networks is fundamental to foster research in optimal power flow, unit commitment, and transmission planning, to name only a few challenging problems. This need was recognized by ARPA-E when it initiated the *Grid Data Program* in 2015. However, the release of such rich datasets is challenging due to legal issues related to privacy and national security. For instance, the electrical load of an industrial customer indirectly reveals sensitive information on its production levels and strategic investments, and the value parameters of lines and generators may reveal how transmission operators operate their networks. Furthermore, this data could be exploited by an attacker to inflict targeted damages on the network infrastructure.

This paper explores whether differential privacy can help to mitigate these concerns. Differential Privacy (DP) [1] is an algorithmic property that measures and bounds the privacy risks associated with answering sensitive queries or releasing a privacy-preserving dataset. It introduces carefully calibrated noise to the data to prevent the disclosure of sensitive information. An algorithm satisfying DP offers privacy protection regardless of the external knowledge of an attacker. In particular, the definition of DP adopted in this paper ensures that an attacker obtaining access to a differentially private output, cannot detect (w.h.p.) how close is the privacy-preserving value to its original one.

However, DP faces significant challenges when the resulting privacy-preserving datasets are used as inputs to complex optimization algorithms, e.g., *Optimal Power Flow* (OPF) problems. Indeed, the privacy-preserving dataset may have lost the fidelity and realism of the original data and may even not admit feasible solutions for the optimization problems of interest [2].

This paper studies how to address this challenge when the goal is to preserve the privacy of line parameters and transformers. It presents a DP mechanism ensuring that the resulting dataset is realistic and limits the power of an attacker. More precisely, the contribution of this paper is fourfold. *(1)* It proposes the *Power Line Obfuscation* (PLO) mechanism to obfuscate the line parameters in a power system network. *(2)* It shows that PLO has strong theoretical properties: It achieves ϵ-differential privacy, ensures that the released data can produce feasible solutions for OPF problems, and its objective value is a constant factor away from optimality. *(3)* It extends the PLO mechanism to handle time-series network data. *(4)* It demonstrates experimentally that the PLO mechanism improves the accuracy of existing approaches on the largest collection of OPF test cases available, results in solutions with similar costs and optimality gaps to those obtained on the original problems, and it protects well against an attacker that has access to the released network data and uses it to damage the real network. Interestingly, *on the test cases, the damage inflicted on the real network when the attacker exploits the PLO-obfuscated data converges to that of a random, uniformed attack as the indistinguishibilty level increases.*

II. Preliminaries

This section reviews the AC Optimal Power Flow (AC-OPF) problem and key concepts from differential privacy. A summary of the notation adopted is tabulated in Table I. Bold-faced symbols are used to denote constant values.

A. AC Optimal Power Flow

Optimal Power Flow (OPF) is the problem of determining the most economical generator dispatch to serve demands while satisfying operating and feasibility constraints. *AC-OPF* refers to modeling the full AC power equations when computing an OPF. This paper views the grid as a graph (N, E) where N is the set of buses and E is the set of transmission lines and transformers, called *lines* for simplicity. We use E to represent the set of directed arcs and E^R to refer to the arcs in E with the reverse direction. The AC power flow equations use complex quantities for current I, voltage V, admittance Y, and power S. The quantities are linked by constraints expressing Kirchhoff's Current Law (KCL) and Ohm's Law, resulting in the AC Power Flow equations:

$$S_i^g - \boldsymbol{S}_i^d = \sum_{(i,j)\in E \cup E^R} S_{ij} \quad \forall i \in N$$

$$S_{ij} = \boldsymbol{Y}_{ij}^* |V_i|^2 - \boldsymbol{Y}_{ij}^* V_i V_j^* \quad (i,j) \in E \cup E^R$$

The authors are affiliated with H. Milton Stewart School of Industrial and Systems Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA e-mail: fioretto@gatech.edu, wmak@gatech.edu, pvh@isye.gatech.edu.

TABLE I
POWER NETWORK NOMENCLATURE.

N	The set of nodes in the network	θ^{Δ}	Phase angle difference limits
E	The set of *from* edges in the network	$S^d = p^d + \boldsymbol{i}q^d$	AC power demand
E^R	The set of *to* edges in the network	$S^g = p^g + \boldsymbol{i}q^g$	AC power generation
$\boldsymbol{i}$	Imaginary number constant	c_0, c_1, c_2	Generation cost coefficients
n, m	$\|E\|$ and $\|N\|$, respectively	$\Re(\cdot)$	Real component of a complex number
$S = p + \boldsymbol{i}q$	AC power	$\Im(\cdot)$	Imaginary component of a complex number
$V = v\angle\theta$	AC voltage	$Y = g + \boldsymbol{i}b$	Line admittance
$\|\cdot\|$	Magnitude of a complex number	$\angle$	Angle of a complex number
s^u	Line apparent power thermal limit	x^l, x^u	Lower and upper bounds of x
θ_{ij}	Phase angle difference (i.e., $\theta_i - \theta_j$)	$\boldsymbol{x}$	A constant value
$\mathcal{N}$	A network description	$\mathbf{g}$	Network's line conductances
$\mathbf{b}$	Network's line susceptances	Δ_Q	Query sensitivity
ϵ	Privacy budget	α	Indistinguishability value
β	Faithfulness parameter	$\tilde{\mathbf{x}}$	Privacy-preserving version of $\mathbf{x}$
$\dot{\mathbf{x}}$	Post-processed version of $\tilde{\mathbf{x}}$	$\mathbf{x}^*$	Complex conjugate of $\mathbf{x}$

Model 1 The AC Optimal Power Flow Problem (AC-OPF)

variables: $S_i^g, V_i \ \ \forall i \in N, \quad S_{ij} \ \ \forall (i,j) \in E \cup E^R$

minimize:
$$\sum_{i \in N} \boldsymbol{c}_{2i}(\Re(S_i^g))^2 + \boldsymbol{c}_{1i}\Re(S_i^g) + \boldsymbol{c}_{0i} \tag{1}$$

subject to:
$$\angle V_s = 0, \tag{2}$$
$$\boldsymbol{v}_i^{\boldsymbol{l}} \leqslant |V_i| \leqslant \boldsymbol{v}_i^{\boldsymbol{u}} \ \ \forall i \in N \tag{3}$$
$$-\boldsymbol{\theta}_{ij}^{\boldsymbol{\Delta}} \leqslant \angle(V_i V_j^*) \leqslant \boldsymbol{\theta}_{ij}^{\boldsymbol{\Delta}} \ \ \forall (i,j) \in E \tag{4}$$
$$\boldsymbol{S}_i^{\boldsymbol{gl}} \leqslant S_i^g \leqslant \boldsymbol{S}_i^{\boldsymbol{gu}} \ \ \forall i \in N \tag{5}$$
$$|S_{ij}| \leqslant \boldsymbol{s}_{ij}^{\boldsymbol{u}} \ \ \forall (i,j) \in E \cup E^R \tag{6}$$
$$S_i^g - \boldsymbol{S}_i^d = \textstyle\sum_{(i,j) \in E \cup E^R} S_{ij} \ \ \forall i \in N \tag{7}$$
$$S_{ij} = \mathbf{Y}_{ij}^* |V_i|^2 - \mathbf{Y}_{ij}^* V_i V_j^* \ \ \forall (i,j) \in E \cup E^R \tag{8}$$

These non-convex nonlinear equations are the core building block in many power system applications and Model 1 depicts the AC-OPF formulation. The objective function (1) minimizes the cost of the generator dispatch. Constraint (2) sets the reference angle for a slack bus $s \in N$ to be zero to eliminate numerical symmetries. Constraints (3) and (4) capture the voltage bounds and phase angle difference constraints. Constraints (5) and (6) enforce the generator output and line flow limits. Finally, Constraints (7) and (8) capture the AC Power Flow equations. We use $\mathcal{N} = \langle N, E, \mathbf{S}, \mathbf{Y}, \boldsymbol{\theta}^{\boldsymbol{\Delta}}, \mathbf{s}, \mathbf{v} \rangle$ for a succinct *network description* and define $m = |N|$ and $n = |E|$.

B. Differential Privacy

Differential privacy [1] is a privacy framework that protects the disclosure of the participation of an individual to a dataset. In the context of this paper, differential privacy is used to protect the disclosure of conductance and susceptance values of transmission lines. The paper considers datasets $D = \{g_1, \ldots, g_n\} \in \mathbb{R}^n$ as n-dimensional real-valued vector describing conductance values and aims at protecting the value of each conductance g_i up to some quantity $\alpha > 0$. This requirement allows to *obfuscate* the parameters of lines whose values are close to one another while keeping the distinction between line parameters that are far apart from each other. This privacy notion is characterized by the *adjacency relation* between datasets that captures the *indistinguishability* of individual line values and defined as:

$$D \sim_\alpha D' \ \Leftrightarrow \ \exists i \text{ s.t. } |g_i - g_i'| \leqslant \alpha \text{ and } g_j = g_j', \forall j \neq i. \tag{9}$$

where D and D' are two datasets and $\alpha > 0$ is a real value [3]. Informally speaking, a DP mechanism needs to ensure that queries on two indistinguishable datasets (i.e., datasets differing on a single value by at most α) give similar results. The following definition formalizes this intuition [1], [3].

Definition *1:* A randomized algorithm $\mathcal{A} : \mathcal{D} \to \mathcal{R}$ with domain $\mathcal{D}$ and range $\mathcal{R}$ is ϵ-differential private if, for any output response $O \subseteq \mathcal{R}$ and any two *adjacent* inputs $D \sim_\alpha D' \in \mathbb{R}^n$, fixed a value $\alpha > 0$,

$$\frac{Pr[\mathcal{A}(D) \in O]}{Pr[\mathcal{A}(D') \in O]} \leqslant \exp(\epsilon). \tag{10}$$

The level of *privacy* is controlled by the parameter $\epsilon \geqslant 0$, called the *privacy budget*, with small values denoting strong privacy. The level of *indistinguishability* is controlled by the parameter $\alpha > 0$. Differential privacy satisfies several important properties, including *composability* and *immunity to post-processing* [4].

Theorem *1 (Sequential Composition):* The composition $(\mathcal{A}_1(D), \ldots, \mathcal{A}_k(D))$ of a collection $\{\mathcal{A}_i\}_{i=1}^k$ of ϵ_i-differential private algorithms satisfies $(\sum_{i=1}^k \epsilon_i)$-differential privacy.

Theorem *2 (Parallel Composition):* Let D_1 and D_2 be disjoint subsets of D and $\mathcal{A}$ be an ϵ-differential private algorithm. Computing $\mathcal{A}(D \cap D_1)$ and $\mathcal{A}(D \cap D_2)$ satisfies ϵ-differential privacy.

Theorem *3 (Post-Processing Immunity):* Let $\mathcal{A}$ be an ϵ-differential private algorithm and g be an arbitrary mapping from the set of possible output sequences to an arbitrary set. Then, $g \circ \mathcal{A}$ is ϵ-differential private.

A function (also called *query*) $Q : \mathbb{R}^n \to \mathbb{R}$ can be made differential private by injecting random noise to its output. The amount of noise to inject depends on the *sensitivity* of the query, denoted by Δ_Q and defined as

$$\Delta_Q = \max_{D \sim_\alpha D'} \left\| Q(D) - Q(D') \right\|_1.$$

For instance, querying the conductance values of a line from a dataset D is achieved through an identity query Q, whose

Model 2 Maximum Load Restoration

$$\textbf{variables:} \quad S^g_i, V_i, l_i \;\; \forall i \in N, \quad S_{ij} \;\; \forall (i,j) \in E \cup E^R$$

$$\textbf{maximize:} \quad \sum_{i \in N} l_i \Re(S^d_i) \tag{11}$$

$$\textbf{subject to:} \quad (2) - (8) \tag{12}$$

$$0 \leqslant l_i \leqslant 1 \;\; \forall i \in N \tag{13}$$

$$S^g_i - l_i \boldsymbol{S}^d_i = \textstyle\sum_{(i,j) \in E \cup E^R} S_{ij} \;\; \forall i \in N \tag{14}$$

sensitivity $\Delta_Q = \alpha$. The Laplace distribution with 0 mean and scale b, denoted by $\text{Lap}(\lambda)$, has a probability density function $\text{Lap}(x|\lambda) = \frac{1}{2\lambda} e^{-\frac{|x|}{\lambda}}$. It can be used to obtain an ϵ-differential private algorithm to answer numeric queries [1]. In the following, $\text{Lap}(\lambda)^n$ denotes the i.i.d. Laplace distribution over n dimensions with parameter λ.

Theorem *4 (Laplace Mechanism):* Let Q be a numeric query that maps datasets to $\mathbb{R}^n$. The Laplace mechanism that outputs $Q(D) + z$, where $z \in \mathbb{R}^n$ is drawn from the Laplace distribution $\text{Lap}\left(\frac{\Delta_Q}{\epsilon}\right)^n$, achieves ϵ-differential privacy.

III. The Obfuscation Mechanism for Power Lines

A. Problem Setting and Attack Model

A power grid operator desires to release a network description $\tilde{\mathcal{N}} = \langle N, E, \mathbf{S}, \tilde{\mathbf{Y}}, \boldsymbol{\theta}^{\boldsymbol{\Delta}}, \mathbf{s}, \mathbf{v}\rangle$ of a network $\mathcal{N} = \langle N, E, \mathbf{S}, \mathbf{Y}, \boldsymbol{\theta}^{\boldsymbol{\Delta}}, \mathbf{s}, \mathbf{v}\rangle$, that *obfuscates* the lines admittance values $\mathbf{Y}$ within a given indistinguishability parameter α. In addition, the released data must preserve the realism of the original network. Lines parameters are considered to be extremely sensitive as they can reveal important operational information and can be exploited by an attacker to inflict targeted damages on the network infrastructure. The paper assumes that the optimal dispatch cost $\mathcal{O}(\mathcal{N})$ and typical conductance-susceptance line ratios are publicly available and thus accessible by an attacker. This is not restrictive since the optimal dispatch cost can be inferred from market clearing prices which are publicly accessible, and the ratios between conductance and susceptance of a line can be retrieved from the manufacture informational material.

This paper also considers an attack model in which a malicious user can disrupt k power lines (called *attack budget*) to inflict maximal network damage. It further assumes that the attacker has full knowledge of a network description $\mathcal{N}$ and can use it to estimate the damages inflicted by its actions. To measure the impact of an attack on the power network, this paper measures the total load affected and the amount of the affected loads that can be restored via Model 2. The latter aims at maximizing the active load $l_i \Re(S^d_i)$ served by the damaged network while preserving the active/reactive factor.

B. The PLO Problem

The *Power Lines Obfuscation* (PLO) problem establishes the fundamental desiderata to be delivered by the obfuscation mechanism. It operates on the line conductances and suceptances, which are denoted by by $\mathbf{g} = \{g_{ij}\}_{(i,j) \in E}$ and $\mathbf{b} = \{b_{ij}\}_{(i,j) \in E}$, respectively.

Definition *2 (PLO problem):* Given a network description $\mathcal{N}$ and positive real values α, β, and ϵ, the PLO problem produces a network description $\tilde{\mathcal{N}}$ that satisfies

1) *Lines obfuscation*: The lines conductances $\tilde{\mathbf{g}}$ of $\tilde{\mathcal{N}}$ satisfy ϵ-differential privacy under α-indistinguishability.
2) *Consistency*: $\mathcal{N}$ must have feasible solutions to OPF Constraints (2)–(8).
3) *Objective faithfulness*: $\mathcal{N}$ must be faithful to the value of the objective function up to a factor β, i.e., $\frac{|\mathcal{O}(\mathcal{N}) - \mathcal{O}(\tilde{\mathcal{N}})|}{\mathcal{O}(\mathcal{N})} \leqslant \beta$.

Finding values $\tilde{\mathbf{g}}$ satisfying α-indistinguishability is readily achieved through the Laplace mechanism. However, finding values $\tilde{\mathbf{Y}}$ that satisfy conditions (2) and (3) is well more challenging. Indeed, these conditions require that the new network $\tilde{\mathcal{N}}$ satisfies the AC power flow equations, the operational constraints, and closely preserves the objective value. In other words, these conditions ensure the realism and fidelity of $\tilde{\mathcal{N}}$.

C. The PLO Mechanism

The *PLO* mechanism, described in Algorithm 1, addresses these challenges. It takes as input a power network description $\mathcal{N}$ as well as three positive real numbers: ϵ which determines the *privacy value* of the private data, α, which determines the *indistinguishability value*, and β, which determines the required *faithfulness* of the objective function.

The PLO mechanism first injects Laplace noise with parameter $\lambda = 3\alpha/\epsilon$ to each query on each dimension of the conductance vector $\mathbf{g}$ of $\mathcal{N}$ to produce new noisy conductance and susceptance vectors:

$$\tilde{\mathbf{g}} = \mathbf{g} + Lap\left(\frac{3\alpha}{\epsilon}\right)^n, \qquad \tilde{\mathbf{b}} = \mathbf{r} \cdot \tilde{\mathbf{g}}, \tag{15}$$

as shown in lines (1) and (2), where $\tilde{\mathbf{g}} = \{\tilde{g}_{ij}\}_{(ij) \in E}$ and $\tilde{\mathbf{b}} = \{\tilde{b}_{ij}\}_{(ij) \in E}$ are the vectors of noisy conductances and suceptances, $\mathbf{r}$ is the vector of ratios $\{\frac{g_{ij}}{b_{ij}}\}_{(ij) \in E}$ between $\mathbf{g}$ and $\mathbf{b}$, and $\cdot$ denotes the dot-product. Note that the mechanism retains the conductance-susceptance ratio.

It is also important to ensure that line values within different voltage levels preserve their differences. Denote by $VL(\mathcal{N})$ as the set of voltage levels in $\mathcal{N}$. For each voltage level v, the PLO mechanism computes the noisy mean value of the conductance vector $\mathbf{g}$ (lines 3–4):

$$\tilde{\mu}^v_{\mathbf{g}} = \left(\frac{1}{n_v} \sum_{(ij) \in E(v)} g_{ij}\right) + \text{Lap}\left(\frac{3\alpha}{n_v \epsilon}\right), \tag{16}$$

and suceptance $\mathbf{b}$:

$$\tilde{\mu}^v_{\mathbf{b}} = \left(\frac{1}{n_v} \sum_{(ij) \in E(v)} b_{ij}\right) + \text{Lap}\left(\frac{3\alpha}{n_v \epsilon}\right), \tag{17}$$

where $E(v)$ denotes the subset of lines at voltage level v, and $n_v = |E(v)|$. These estimates are used to guarantee that the lines' parameters do not deviate too much from their original values within each voltage level.

While the application of the Laplace noise to produce new conductance and susceptance vectors satisfies condition (1)

Algorithm 1: *The PLO mechanism for the AC-OPF*

input : $\langle \mathcal{N}, \mathcal{O}^*, \epsilon, \alpha, \beta \rangle$

1 $\tilde{\mathbf{g}} \leftarrow \mathbf{g} + \text{Lap}(\frac{3\alpha}{\epsilon})^n$

2 $\tilde{\mathbf{b}} \leftarrow \mathbf{r} \cdot \tilde{\mathbf{g}}$

3 **foreach** $v \in VL(\mathcal{N})$ **do**

4 $\quad \tilde{\mu}^v_{\mathbf{x}} \leftarrow \frac{1}{n}\sum_{(ij)\in E(v)} x_{ij} + \text{Lap}(\frac{3\alpha}{n_v \epsilon})$ (for $x = \mathbf{g}, \mathbf{b}$)

5 Solve the following model:

$$
\begin{aligned}
&\textbf{variables: } S^g_i, V_i && \forall i \in N \\
&\qquad\qquad\quad \dot{Y}_{ij}, S_{ij} && \forall (i,j) \in E_k \cup E^R_k \\
&\textbf{minimize: } \|\dot{\mathbf{g}} - \tilde{\mathbf{g}}\|_2^2 + \|\dot{\mathbf{b}} - \tilde{\mathbf{b}}\|_2^2 && (s_1) \\
&\textbf{subject to:} \\
&\quad (2) - (7) \\
&\quad \frac{\left|\sum_{i\in N} \boldsymbol{cost}(S^g_i) - \mathcal{O}^*\right|}{\mathcal{O}^*} \leqslant \beta && (s_2) \\
&\quad S_{ij} = \dot{Y}^*_{ij}|V_i|^2 - \dot{Y}^*_{ij} V_i V^*_j \quad \forall (i,j) \in E \cup E^R && (s_3) \\
&\quad \forall (i,j) \in E(v) \cup E^R(v),\ \forall v \in VL(\mathcal{N}): \\
&\qquad \frac{1}{\lambda}\mu^v_{\mathbf{g}} \leqslant \dot{g}_{ij} \leqslant \lambda\, \mu^v_{\mathbf{g}} && (s_4) \\
&\qquad \frac{1}{\lambda}\mu^v_{\mathbf{b}} \leqslant \dot{b}_{ij} \leqslant \lambda\, \mu^v_{\mathbf{b}} && (s_5)
\end{aligned}
$$

output : $\dot{\mathcal{N}} = \langle N, E, \mathbf{S}, \dot{\mathbf{Y}}, \boldsymbol{\theta}^{\boldsymbol{\Delta}}, \mathbf{s}, \mathbf{v} \rangle$

of Definition 2, it may not satisfy conditions (2) and (3). In fact, Section V shows that the Laplace noise induced on the lines' parameters often result in a new network description that induces no feasible flow. To overcome this limitation, the PLO mechanism *post-processes* the noisy values $\tilde{\mathbf{b}}$ and $\tilde{\mathbf{g}}$ by exploiting an optimization model specified in line (5) of Algorithm 1. The result of such an optimization-based post-processing step is a new network $\dot{\mathcal{N}} = \langle N, E, \mathbf{S}, \dot{\mathbf{Y}}, \boldsymbol{\theta}^{\boldsymbol{\Delta}}, \mathbf{s}, \mathbf{v} \rangle$ that satisfies the objective faithfulness and consistency requirements of Definition 2.

The optimization model minimizes the sum of the L_2-distances between the variables $\dot{\mathbf{g}} \in \mathbb{R}^n$ and the noisy conductances $\tilde{\mathbf{g}} \in \mathbb{R}^n$, and the variables $\dot{\mathbf{b}} \in \mathbb{R}^n$ and the noisy susceptances $\tilde{\mathbf{b}} \in \mathbb{R}^n$. The model is subject to Constraints (2)–(7) of Model 1 with the addition of the β-faithfulness constraint (s_2) that guarantees to satisfy condition (3) of the PLO problem (Definition 2). Notation $\boldsymbol{cost}(S^g_i)$ is a shorthand for $c_{2i}(\Re(S^g_i))^2 + \boldsymbol{c}_{1i}\Re(S^g_i) + \boldsymbol{c}_{0i}$. Constraint ($s_3$) enforces the power-flow based on the Ohm's Law on the post-processed conductance and suceptance values. Finally, Constraints (s_4) and (s_5) bound the values for the post-processed conductance and suceptance to be close to their *privacy-preserving* means, parameterized by $\lambda > 0$. These constraints are used to avoid that the post-processed values deviate arbitrarily from the original ones. The optimization also works on a pre-processed network to ensure the realism and feasibility. This pre-processing ensures that parallel lines have the same resistance and reactance parameters and that negative resistance values are not part of the obfuscation. Moreover, the optimization guarantees that all remaining resistances are positive.

The PLO mechanism can be thought as redistributing the noise of the Laplace mechanism applied to the admittance values of the lines in $\mathcal{N}$ to obtain a new network $\dot{\mathcal{N}}$ that is consistent with the problem constraints and objective. It searches for a feasible solution that satisfies the AC-OPF constraints and the β-faithfulness constraint. The following results, whose proofs are reported in the appendix, show that PLO has desirable properties.

Theorem *5:* For a given α-indistinguishability level, the PLO mechanism is ϵ-differential private.

The following result is a consequence of [2](Theorem 5).

Corollary *1:* The optimal solution $\langle \mathbf{g}^*, \mathbf{b}^* \rangle$ to the optimization model in line (4) of Algorithm 2 satisfies $\|\mathbf{g}^* - \mathbf{g}\|_2 + \|\mathbf{b}^* - \mathbf{b}\|_2 \leqslant 2\|\tilde{\mathbf{g}} - \mathbf{g}\|_2 + 2\|\tilde{\mathbf{b}} - \mathbf{b}\|_2$.

This last result implies the PLO mechanism is at most a factor 2 away from optimality. Such a result, in turn, follows from the optimality of the Laplace mechanism [5]. Note that a solution to the PLO always exists: Indeed, the original network's values $\boldsymbol{Y}$ represent a feasible solution satisfying all requirements of Definition 2.

IV. Extension: Multi-step PLO

The PLO mechanism obfuscates the line parameters based on a single snapshot of the steady state of the network. To improve the fidelity and realism of the network, the mechanism can be generalized by reasoning about multiple snapshots. Consider a set of network descriptions $\{\mathcal{N}_t\}_{t=1}^h$ over a finite time horizon h where loads and optimal generator dispatches are varying over time. Each $\mathcal{N}_t = (N, E, \mathbf{S}_t, \mathbf{Y}, \boldsymbol{\theta}^{\boldsymbol{\Delta}}, \mathbf{s}, \mathbf{v})$ represents the steady state of the power grid at time step $0 < t \leqslant h$, and therefore $\{\mathcal{N}_t\}_{t=1}^h$ represents a network of *time-series* data.

The *Multi-step Power Lines Obfuscation* (MPLO) problem extends the PLO by enforcing the *objective faithfulness* condition (Definition 2) for every $\mathcal{N}_t$ ($t \in [h]$). The derived MPLO mechanism is outlined in the appendix (Algorithm 2). It extends the PLO mechanism in taking as input the collection of networks $\{\mathcal{N}_t\}_{t=1}^h$ and it returns the admittance values $\dot{\mathbf{Y}}$ for the lines in the power grid that satisfy the conditions of Definition 2. We use $x(t)$ to represent variable x at time step t. The MPLO mechanism differs from the PLO mechanism exclusively in the post-processing optimization step of line (4). Its objective (m_1) is equivalent to the objective (s_1) of the post-processing step in the PLO mechanism. The model constraints extend those of the PLO mechanism by considering multiple time steps. The MPLO mechanism outputs a new time-series network $\{\tilde{\mathcal{N}}_t\}_{t=1}^h$ whose line parameters $\dot{\mathbf{Y}}$ are *obfuscated* and that satisfies the AC-OPF problem constraints, the β consistency constraint, and that do not deviate too much from their privacy-preserving mean values.

Theorem *6:* For a given α-indistinguishability level, the MPLO mechanism is ϵ-differential private.

V. Experimental Evaluations

This section examines the proposed mechanisms on a variety of networks from the NESTA library [6]. It analyzes the line values produces by the obfuscation procedures, studies the mechanism ability to preserve dispatch costs and optimality gaps, determines how well the resulting network can sustain

TABLE II
LAPLACE MECHANISM FEASIBILITY (%)

	α		
Network instance	0.001	0.01	$\geqslant$0.1
nesta_case30_ieee	100	80	0
nesta_case39_epri	100	0	0
nesta_case57_ieee	100	61	0
nesta_case118_ieee	100	47	0

an attack, and analyzes the mechanism computational runtime. It also extends this analysis to time-series networks using a multiple-step approach.

For presentation simplicity, the analysis focus primarily on the IEEE 39-bus network. However, our results are consistent across the entire NESTA benchmark set. All experiments use a privacy budget $\epsilon = 1.0$ and vary the *indistinguishability level* $\alpha \in \{10^{-3}, 10^{-2}, 10^{-1}, 1.0\}$ and the *faithfulness level* $\beta \in \{10^{-2}, 10^{-1}\}$. The model was implemented using the Julia package PowerModels.jl [7] with the nonlinear solver IPOPT [8] for solving the various power flow models, including the nonlinear AC model and the QC [9], [10] and SOCP [11] relaxations.

A. Analysis of the Line Parameters

This section studies the realism of the Laplace mechanism. Table II reports the percentage of feasible instances (over 100 runs) for obfuscated networks obtained using (exclusively(the Laplace mechanism on the IEEE-30 bus, IEEE-39 bus, IEEE-57 bus, and the IEEE-118 bus networks. When the indistinguishability values α exceed 0.1, the Laplace-obfuscated networks are rarely AC-feasible. In contrast, the PLO mechanism is *always* AC-feasible (except for one IEEE-118 instance). These results justify the need of studying mechanisms that are more sophisticated than the Laplace mechanism, and hence the PLO mechanism. Figure 1 illustrates the line resistances of an IEEE 39-bus network obtained by the Laplace and the PLO mechanisms and compare them with the associated values in the original network. The figure reports the results at varying of the indistinguishability level α and fixing $\beta = 0.01$. *The results indicate that the OPF obfuscated values differ by at most 1% from their original ones.* Not surprisingly, the differences are more pronounced as the indistinguishability level increases: For larger indistinguishability levels, the PLO mechanism introduces more noise and hence more diverse lines values are generated.

B. Dispatch Costs and Optimality Gaps

The next results evaluate the ability of the PLO-obfuscated networks to preserve the dispatch costs and optimality gaps. Figure 2(top) shows the difference, in percentage, of the dispatch costs obtained via the Laplace and the PLO mechanisms w.r.t. the original costs at varying of the indistinguishability level α and the faithfulness parameter β. The figure illustrates the mean and standard deviation (shown with black, solid, lines) obtained on 100 runs, for each combination of the α and β parameters. The percentage differences are measured as: $100 \times \frac{\mathcal{O}(\mathcal{N}) - \mathcal{O}(\tilde{\mathcal{N}})}{\mathcal{O}(\mathcal{N})}$, where $\mathcal{N}$ is the original network, $\tilde{\mathcal{N}}$ is the obfuscated network (using the Laplace or the PLO mechanisms), and $\mathcal{O}$ is the cost of a (local) optimal solution to the AC-OPF problem. Parameter α controls the amount of noise being added to the line parameters, therefore, the OPF costs are close to their original values when α is small (e.g., $\leqslant 10^{-3}$). The PLO mechanism often produces obfuscated network inducing OPFs with lower costs than the original ones. This is because PLO returns an AC-feasible solution whose cost is close to the original network's cost, ignoring whether a lower dispatch cost may exists.

Figure 2(bottom) compares the optimality gaps on the QC and the SOCP relaxations of the AC-OPF obtained using the original and the PLO-obfuscated networks. The percentage measures are defined as: $100 \times \frac{\mathcal{O}(\mathcal{N}) - \hat{\mathcal{O}}(\mathcal{N})}{\mathcal{O}(\mathcal{N})}$, where $\mathcal{N}$ is either the original or the obfuscated network, and $\hat{\mathcal{O}}$ is the function returning the costs of the QC or the SOCP AC-OPF relaxation on $\mathcal{N}$. The results are averaged over 100 runs and show that the optimality gaps attained with the obfuscated networks are close to those attained with the original networks for small ($\leqslant 10^{-2}$) α values. *This is important for capturing the fidelity of the obfuscated network and the difficulty of the associated OPF.* In general, the PLO mechanism increases the optimality gaps slightly, and these results are consistent across the NESTA networks.

C. Power Grid Attack Simulation

The next experiments evaluate the damages that an attacker may inflict on a real power network $\mathcal{N}$, if the obfuscated network $\tilde{\mathcal{N}}$ is released. The attack setting is as follows: An attacker is given a budget denoting the percentage k of lines he can damage. The attacker chooses the lines to damage based on the obfuscated network, but the attack impact is evaluated on the real network. To assess the benefits of the proposed obfuscation scheme in response to such an attack, we compare three attack strategies:

1) *Random Attack*: k lines are randomly selected. This represents a scenario in which an attacker carries an *uninformed* attack.
2) *Obfuscated Flow Attack*: The attacker solves an OPF problem on the *obfuscated network* $\tilde{\mathcal{N}}$ and chooses the top-k lines carrying the largest active flows. This case represents a scenario in which an attacker carries an informed attack based on the obfuscated network data.
3) *Real Flow Attack*: The attacker solves an OPF problem on the *real network* $\mathcal{N}$ and chooses the top-k lines carrying the largest active flows. This case represents a scenario in which the *real data* is released and exploited by an attacker.

To compare the damages inflicted by the attacks, the experiments report the amount of load that can be restored after an attack, by solving the maximum load restoration problem described in Model 2. Figure 3 shows the percentage of the load being restored for each attack strategies, at varying of the attack budget $k \in \{5, 10, 15\}$ and the indistinguishability value $\alpha \in \{0.01, 0.1, 1.0\}$ on the IEEE-39 bus (top) and the IEEE-118 bus (bottom) benchmarks, with faithfulness value

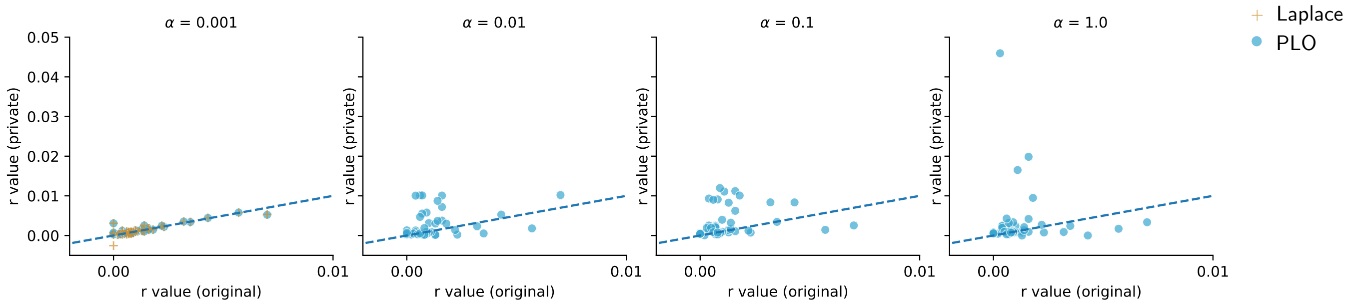

Fig. 1. IEEE-39 bus line resistances (p.u.) at varying of the indistinguishability level $\alpha \in \{0.001, 0.01, 0.1, 1.0\}$ and for $\beta = 0.01$. The x-axis shows values for the original network and the y-axis shows values for the PLO/Laplace obfuscated network.

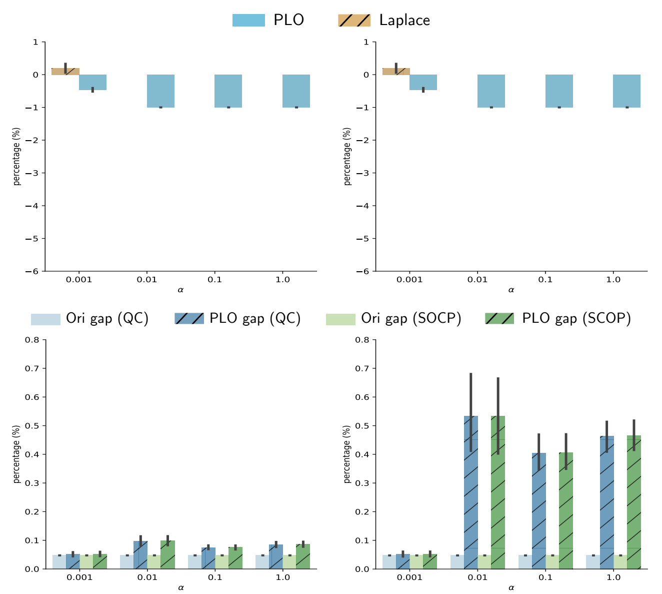

Fig. 2. The IEEE-39 bus AC Optimal Dispatch Costs (top) and Optimality Gap (bottom) Differences in Percentage Between Original and Obfuscated Networks with Faithfulness Parameters $\beta = 0.01$ (left) and 0.1 (right).

TABLE III
PLO COMPUTATIONAL RUNTIME

Network instance	α 0.01	0.1	1.0
nesta_case3_lmbd	0.04	0.05	0.07
nesta_case4_gs	0.09	0.14	0.16
nesta_case5_pjm	0.10	0.09	0.15
nesta_case6_c	0.05	0.12	0.19
nesta_case6_ww	0.05	0.26	0.39
nesta_case9_wscc	0.08	0.21	0.29
nesta_case14_ieee	0.10	0.44	0.74
nesta_case24_ieee_rts	0.63	1.04	1.88
nesta_case29_edin	4.23	3.26	4.59
nesta_case30_as	0.38	1.31	1.77
nesta_case30_fsr	0.39	1.43	1.70
nesta_case30_ieee	0.43	1.41	1.63
nesta_case39_epri	1.67	2.00	2.25
nesta_case57_ieee	1.11	3.43	4.81
nesta_case73_ieee_rts	2.86	8.03	13.90
nesta_case89_pegase	33.67	44.96	48.12
nesta_case118_ieee	8.79	8.64	17.73
nesta_case162_ieee_dtc	17.48	38.83	50.43

$\beta = 0.01$. The results show the average values of 100 simulations for each combination of parameters.

The *random attacks* are used as a baseline to assess the damage that may be caused by an uninformed attacker. Not surprisingly, they result in the largest load restoration for each setting and the restored load decreases as the attack budget increases. In contrast, the *real flow attacks* produce the largest damage on the networks. In all cases tested, the load restoration after these attacks were close to 0%, meaning that *these attacks are highly effective and extremely harmful*.

On the other hand, the results for the *Obfuscated Flow Attacks* show a different pattern. Even though the attacker selects the lines with the highest flows (in the obfuscated network), the network ability to restore loads is substantially higher when compared to those of the real flow attacks. *Remarkably, as the indistinguishability values increase, the strength of the obfuscated flow attack to inflict damages decreases and its success rate are close to those of random attacks*. This is because larger indistinguishability implies more noise and thus higher chance for an attacker to damage less harmful lines.

D. Computational Runtime

Having shown the effective of the PLO mechanism in generating obfuscated networks, we now analyze its computational efficiency. Table III tabulates the average computational runtime in seconds for 100 experiments on several NESTA instances [6] at varying of the indistinguishability values (α in $\{0.01, 0.1, 1.0\}$) and setting the faithfulness value β to 0.01. *In all cases, producing an obfuscated network requires less than* 60 *seconds.* The results illustrate that, in general, the runtime increases when α increases. Larger α values may result in obfuscated line parameters that are farther from the original values, thus affecting the power losses and the feasible power flows. Therefore, minimizing the PLO optimization model (line (5) of Algorithm 1) may increase the runtime.

E. MPLO for Time-Series Data

This subsection evaluates the effect of obfuscating a network with the Multistep PLO mechanism. The experiments use time-series data $\{\mathcal{N}_t\}_{t=1}^{h}$, with $h = 31$, obtained by varying the load profile in the range of $[80\%, 110\%]$ of their original values. Each time step is associated with a load profile and the MPLO mechanism finds line parameters that meet the constraints imposed by a fixed number r of the h time steps. These r time steps are equally spaced in the time horizon $[h]$.

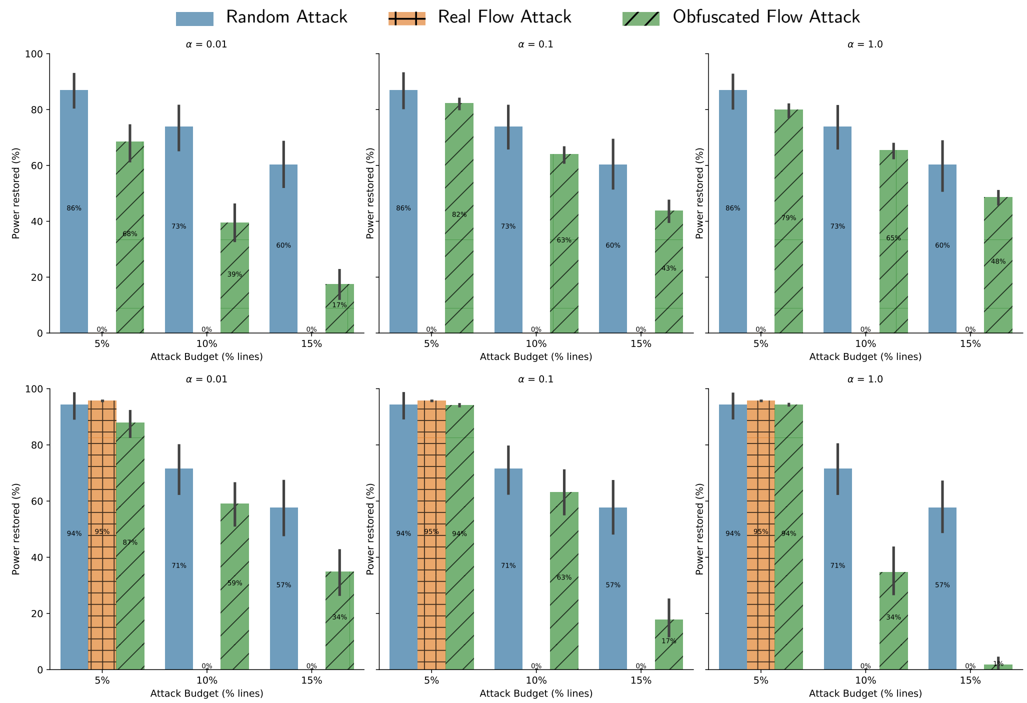

Fig. 3. Percentage of the active load restored after different attacks on the IEEE-39 bus network (top) and the IEEE-118 bus network (bottom) with $\alpha = 0.01$ (left), 0.1 (center), and 1.0 (right). $\beta = 0.01$.

The results on OPF and optimality gap are very similar to those obtained by the (single-step) PLO mechanism. Therefore, the presentationfocuses on the power network attacks. Figure 4 illustrates the percentage of the load restored on the IEEE-39 bus network for the attack strategies and settings discussed earlier, using $r = 4$ (left) and $r = h = 31$ (right). The results for $r = 4$ are similar to those obtained by the PLO mechanism on stady state networks. In contrast, when the whole time horizon is considered, the effectiveness of the Obfuscated Flow attacks increases. This is because constraining the MPLO optimization problem to consider each single time step in the time horizon reduces the degrees of freedom for generating obfuscated networks that differ substantially from the original networks.

Figure 5 further explains these results. It quantifies the similarity of the attacks on the real and obfuscated networks using the following metric: $100 \times \frac{|E^o \cap E^d|}{|E^o|}$ where E^o and E^d are the set of lines selected by the real and obfuscated flow attack, respectively. We fix the attack budget $k = 10\%$ and vary the number of time steps r considered within the MPLO mechanism. The figure clearly illustrates that the number of lines chosen by both attacks grows as r increases. When $r \geqslant 7$ the two attacks select, on average, up to 90% of common lines. The experiment highlights the tradeoffs between obfuscation and network fidelity: Larger values for r result in higher network fidelity but reduce the effects of the obfuscation process, making the networks more vulnerable to attacks.

VI. Related Work

There is a rich literature on theoretical results of DP (e.g., [4], [12]). The literature on DP applied to energy systems includes considerably fewer efforts. Ács and Castelluccia [13] exploited a direct application of the Laplace mechanism to hide user participation in smart meter data sets, achieving ϵ-DP. Zhao et al. [14] studied a DP schema that exploits the ability of households to charge/discharge a battery to hide the real energy consumption of their appliances. Liao et al. [15] introduce Di-PriDA, a privacy-preserving mechanism for appliance-level peak-time load balancing control in the smart grid, aimed at masking the consumption of the top-k appliances of a household.

Karapetyan et al. [16] empirically quantify the trade-off between privacy and utility in demand response systems. The authors analyze the effects of a simple Laplace mechanism on the objective value of the demand response optimization problem. Their experiments on a 4-bus micro-grid show drastic results: the optimality gap approaches nearly 90% in some cases. Zhou et al. [17] have recently studied the problem of releasing differential private network statistics obtained from solving a DC optimal power flow problem.

A differential private schema that uses constrained post-processing was recently introduced by Fioretto et al. [2] and adopted to protect load consumption in power networks. In contrast, the proposed PLO mechanism releases the obfuscated network data protecting the line parameters imposing constraints to ensure that the problem solution cost is close to the solution cost of the original problem, and that the underlying optimal power flow constraints are satisfiable.

VII. Conclusions

This paper presented a privacy-preserving scheme for the release of power grid benchmarks that obfuscate the parameters of transmission lines and transformers. The proposed

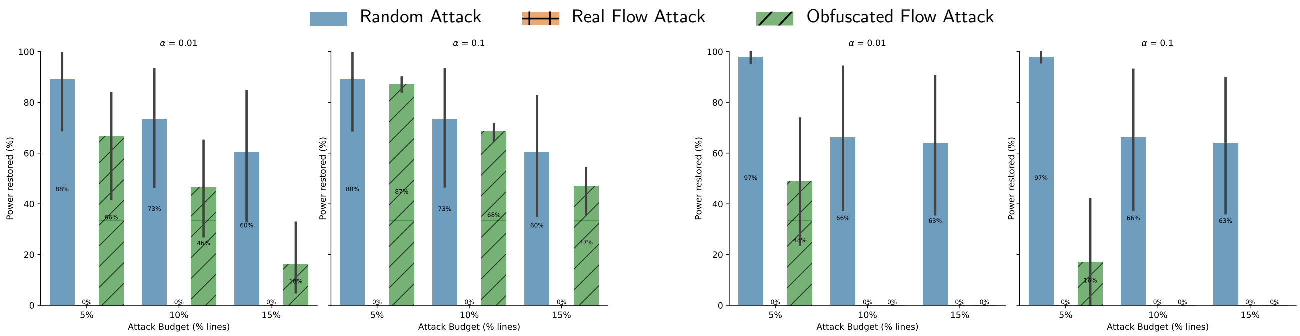

Fig. 4. Percentage of the active load restored after different attacks on the IEEE-39 bus network with $\alpha \in \{0.01, 0.1\}$ and number r of time step evaluated 4 (left), and 31 (right).

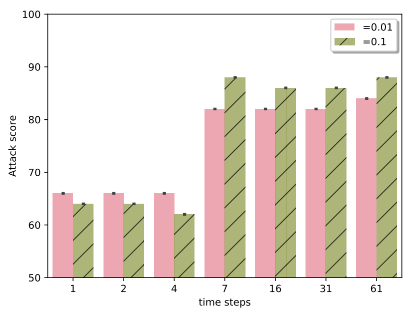

Fig. 5. IEEE-39 bus' Attack score over an increasing number of time steps, with $\alpha \in \{0.01, 0.1\}$, $\beta = 0.01$, and $k = 10\%$.

Power Line Obfuscation (PLO) mechanism hides the network sensitive values using differential privacy, while also ensuring that the released obfuscated network preserves fundamental properties useful in optimal power flow. Specifically, the released networks have dispatch costs similar to those of the original networks and satisfy the power flow operational constraints. The PLO mechanism was tested on a large collection of test cases: It was shown to be efficient and to produce obfuscated networks that preserve dispatch costs and optimality gaps values. Finally, the networks released by the PLO mechanism are shown to be effective in deceiving an attacker attempting to damage the network components for disrupting the power grid load. Future work will focus on jointly obfuscating other sensitive aspects of the network, such as loads and generators. Another avenue of future research is to study more complex attack models, including those in which the attacker evaluates the (near)-optimal subset of lines to disrupt so to minimize the total load restoration.

Acknowledgment

The authors would like to thank Kory Hedman for extensive discussions about obfuscation techniques and effective attack strategies. This research is partly funded by the ARPA-E Grid Data Program under Grant 1357-1530.

References

[1] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *TCC*, vol. 3876. Springer, 2006, pp. 265–284.

[2] F. Fioretto and P. V. Hentenryck, "Constrained-based differential privacy: Releasing optimal power flow benchmarks privately," in *Proceedings of the International Conference on the Integration of Constraint Programming, Artificial Intelligence, and Operations Research (CPAIOR)*, 2018, pp. 215–231. [Online]. Available: https://doi.org/10.1007/978-3-319-93031-2_15

[3] K. Chatzikokolakis, M. E. Andrés, N. E. Bordenabe, and C. Palamidessi, "Broadening the scope of differential privacy using metrics," in *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 2013, pp. 82–102.

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

[5] F. Koufogiannis, S. Han, and G. J. Pappas, "Optimality of the laplace mechanism in differential privacy," *arXiv preprint arXiv:1504.00065*, 2015.

[6] C. Coffrin, D. Gordon, and P. Scott, "Nesta, the NICTA energy system test case archive," *CoRR*, vol. abs/1411.0359, 2014. [Online]. Available: http://arxiv.org/abs/1411.0359

[7] C. Coffrin, R. Bent, K. Sundar, Y. Ng, and M. Lubin, "Powermodels.jl: An open-source framework for exploring power flow formulations," in *2018 Power Systems Computation Conference (PSCC)*, June 2018, pp. 1–8.

[8] A. Wächter and L. T. Biegler, "On the implementation of an interior-point filter line-search algorithm for large-scale nonlinear programming," *Mathematical Programming*, vol. 106, no. 1, pp. 25–57, 2006.

[9] C. Coffrin, H. Hijazi, and P. Van Hentenryck, "The QC relaxation: A theoretical and computational study on optimal power flow," *IEEE Transactions on Power Systems*, vol. 31, no. 4, pp. 3008–3018, July 2016.

[10] H. Hijazi, C. Coffrin, and P. Van Hentenryck, "Convex quadratic relaxations of nonlinear programs in power systems," in *Optimization Online: http://www.optimization-online.org/DB HTML/2013/09/4057.html*, 2013.

[11] R. A. Jabr, "Radial distribution load flow using conic programming," *IEEE Transactions on Power Systems*, vol. 21, no. 3, pp. 1458–1459, Aug 2006.

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

[13] G. Ács and C. Castelluccia, "I have a dream!(differentially private smart metering)." in *Information hiding*, vol. 6958. Springer, 2011, pp. 118–132.

[14] J. Zhao, T. Jung, Y. Wang, and X. Li, "Achieving differential privacy of data disclosure in the smart grid," in *INFOCOM, 2014 Proceedings IEEE*. IEEE, 2014, pp. 504–512.

[15] X. Liao, P. Srinivasan, D. Formby, and A. R. Beyah, "Di-prida: Differentially private distributed load balancing control for the smart grid," *IEEE Transactions on Dependable and Secure Computing*, 2017.

[16] A. Karapetyan, S. K. Azman, and Z. Aung, "Assessing the privacy cost in centralized event-based demand response for microgrids," *CoRR*, vol. abs/1703.02382, 2017. [Online]. Available: http://arxiv.org/abs/1703.02382

[17] F. Zhou, J. Anderson, and S. H. Low, "Differential privacy of aggregated dc optimal power flow data."

Appendix A
Missing Proofs

This section provides the missing proofs. It first reviews the sensitivity of the queries adopted in the PLO mechanisms. The characterization of properties discussed below holds true for the α-indistinguishability model of differential privacy [3].

Property *1:* Let $D = \{x_1, \ldots, x_n\} \in \mathbb{R}^n$ be an n-dimensional numerical vector. The sensitivity of the identity query $Q_I(D) = \{x_1, \ldots, x_n\}$ is $\Delta_{Q_I} = \alpha$.

The property above follows directly from the definition of sensitivity of queries in the α-indistinguishability model.

Property *2:* Let $D = \{x_1, \ldots, x_n\} \in \mathbb{R}^n$ be an n-dimensional numerical vector. The sensitivity of the average query $Q_A(D) = \frac{1}{n}\sum_{i=1}^{n} x_i$ is $Q_A = \frac{\alpha}{n}$.

Let D and D' be two datasets such that $D \sim_\alpha D'$, that is D' differs from D in at most one coordinate and for a factor of at most α. Denote by i be the coordinate such that $|x_i - x'_i| \leqslant \alpha$. It follows:

$$
\begin{aligned}
|Q_A(D) - Q_A(D')| &= \left| \frac{1}{n}\sum_{j=1}^{n} x_j - \frac{1}{n}\sum_{j=1}^{n} x'_j \right| \\
&= \frac{1}{n}|x_i - x'_i| \qquad \text{(by Eq. (9))} \\
&\leqslant \frac{1}{n}\alpha.
\end{aligned}
$$

Theorem *4:* For a given α-indistinguishability level, the PLO mechanism is ϵ-differential private.

Proof. Consider an indistinguishability value $\alpha > 0$. Algorithm 1 queries the dataset of real conductance data in three different instances:

1) To compute $\tilde{\mathbf{g}}$: In Equation (15), $\tilde{\mathbf{g}}$ is computed by issuing an identity query over $\mathbf{g}$. The privacy budget used in Equation (15) is $\frac{\epsilon}{3\alpha}$. Thus, since by Property 1, Theorem 4, and parallel composition (Theorem 2), privately computing the conductance values $\tilde{\mathbf{g}}$ is $\epsilon/3$-differentially private.
2) To compute $\tilde{\mu}^v_{\mathbf{g}}$: In Equation (16), for a voltage level v, the mean value $\mu^v_{\mathbf{g}}$ of the conductance vector $\mathbf{g}$ the computation of is computed issuing an average query Q_A on $\mathbf{g}$. The privacy budget used is $\frac{n_v\,\epsilon}{3\alpha}$. Therefore, by Property 2 and Theorem 4 computing $\tilde{\mu}^v_{\mathbf{g}}$ is $\epsilon/3$-differentially private. Computing the vector of mean values $\tilde{\mu}_{\mathbf{g}} = \{\tilde{\mu}^{v_1}_{\mathbf{g}}, \ldots, \tilde{\mu}^{v_{|VL(\mathcal{N})|}}_{\mathbf{g}}\}$ for each voltage level of the network is also $\epsilon/3$-differentially private by parallel composition (Theorem 2) since each line belongs to exactly one voltage level set $E(v)$.
3) To compute $\tilde{\mu}^v_{\mathbf{b}}$: The mean value $\mu_{\mathbf{b}}$ is $\epsilon/3$ differentially private. The argument is analogous to the one above.

Computing a privacy-preserving version of the susceptance vector $\mathbf{b}$ uses exclusively privacy-preserving data ($\mathbf{g}$) and public information ($\boldsymbol{r}$), therefore the vector $\tilde{\mathbf{b}}$ defined in Equation 15 is differentially private by post-processing immunity (Theorem 3).

Note that the optimization model of line (5) uses *exclusively* privacy-preserving data ($\tilde{\mathbf{g}}, \tilde{\mathbf{b}}, \tilde{\mu}_{\mathbf{g}}, \tilde{\mu}_{\mathbf{b}}$) and additional public information (i.e., the optimization problem and its optimal solution value). The result follows by sequential composition (Theorem 1) and post-processing immunity (Theorem 3). □

Theorem *5:* For a given α-indistinguishability level, the MPLO mechanism is ϵ-differential private.

Proof. Note that MPLO differs from PLO exclusively in the optimization model executed on line 4. The optimization model does not operate on the sensitive data and takes as input the same privacy-preserving values as those taken as input by the PLO's optimization model. Therefore, by post-process immunity and Theorem 4 the MPLO mechanism is ϵ-differential private. □

Appendix B
MPLO Algorithm

The MPLO mechanism is outlined in Algorithm 2.

Algorithm 2: *The MPLO mechanism for the AC-OPF*

input : $\langle \{\mathcal{N}_t\}_{t=1}^{h}, \mathcal{O}^*, \epsilon, \alpha, \beta \rangle$

1 $\tilde{\mathbf{g}} \leftarrow \mathbf{g} + Lap(\frac{3\alpha}{\epsilon})$

2 $\tilde{\mathbf{b}} \leftarrow \mathbf{r} \cdot \tilde{\mathbf{g}}$

3 **foreach** $v \in VL(\mathcal{N})$ **do**

4 $\quad \tilde{\mu}^v_{\mathbf{x}} \leftarrow \frac{1}{n}\sum_{(ij)\in E(v)} x_{ij} + Lap(\frac{3\alpha}{n_v\epsilon})$ (for $x = \mathbf{g}, \mathbf{b}$)

5 Solve the following model:

$$
\begin{aligned}
&\textbf{variables: } S^g_i(t), V_i(t) && \forall i \in N, t \in [h] \\
&\qquad\qquad \dot{Y}_{ij}, S_{ij}(t) && \forall (i,j) \in E_k \cup E^R_k, \forall t \in [h] \\
&\textbf{minimize: } \|\dot{\mathbf{g}} - \tilde{\mathbf{g}}\|_2^2 + \|\dot{\mathbf{b}} - \tilde{\mathbf{b}}\|_2^2 && (m_1) \\
&\textbf{subject to: } && \forall t \in [1..h], \\
&\quad \angle V_s(t) = 0 && (m_2) \\
&\quad \frac{\left|\sum_{i\in\mathcal{N}_t} \boldsymbol{cost}(S^g_i(t)) - \mathcal{O}^*(t)\right|}{\mathcal{O}^*(t)} \leqslant \beta && (m_3) \\
&\quad \forall i \in \mathcal{N}_t: \\
&\qquad \boldsymbol{v}^{\boldsymbol{l}}_i \leqslant |V_i(t)| \leqslant \boldsymbol{v}^{\boldsymbol{u}}_i && (m_4) \\
&\qquad \boldsymbol{S}^{\boldsymbol{gl}}_i \leqslant S^g_i(t) \leqslant \boldsymbol{S}^{\boldsymbol{gu}}_i && (m_5) \\
&\qquad S^g_i(t) - \boldsymbol{S}^d_i(t) = \textstyle\sum_{(i,j)\in E_k \cup E^R_k} S_{ij}(t) && (m_6) \\
&\quad \forall (i,j) \in E_k \cup E^R_k: \\
&\qquad -\boldsymbol{\theta}^{\boldsymbol{\Delta}}_{ij} \leqslant \angle(V_i(t)V^*_j(t)) \leqslant \boldsymbol{\theta}^{\boldsymbol{\Delta}}_{ij} && (m_7) \\
&\qquad |S_{ij}(t)| \leqslant \boldsymbol{s}^{\boldsymbol{u}}_{ij} && (m_8) \\
&\qquad S_{ij}(t) = \dot{Y}^*_{ij}|V_i(t)|^2 - \dot{Y}^*_{ij}V_i(t)V^*_j(t) && (m_9) \\
&\qquad\quad \forall v \in \mathbf{VL}(\mathcal{N}): \\
&\qquad\qquad \frac{1}{\lambda}\mu_{\mathbf{g}} \leqslant \dot{g}_{ij} \leqslant \lambda\,\mu_{\mathbf{g}} && (m_{10}) \\
&\qquad\qquad \frac{1}{\lambda}\mu_{\mathbf{b}} \leqslant \dot{b}_{ij} \leqslant \lambda\,\mu_{\mathbf{b}} && (m_{11})
\end{aligned}
$$

output: $\{\dot{\mathcal{N}}_t\}_{t=1}^{h} = \langle N, E, \mathbf{S}_t, \dot{\mathbf{Y}}, \boldsymbol{\theta}^{\boldsymbol{\Delta}}, \mathbf{s}, \mathbf{v} \rangle$