

Differentially Private LQG Control: A System-Level Synthesis Approach

Mohadese Jadidi, Jerome Le Ny and Shuang Gao

Abstract—We investigate the steady-state linear quadratic Gaussian (LQG) control problem for coupled systems with privacy-sensitive input signals. To protect these signals from information leakage through shared control actions, we propose two differentially private controller design approaches, perturbing either the measurements or the controls with Gaussian noise. Standard LQG design methods lead to a circular dependency between setting the magnitude of the privacy-preserving noise and designing the Kalman filter, as each problem depends on the other. We address this issue by employing the system-level synthesis framework to directly design the closed-loop transfer function, noise level and controller optimizing the privacy-performance trade-off. Numerical simulations on a power system control example with private demand signals demonstrate that the proposed approach can preserve control and estimation performance while ensuring differential privacy.

I. INTRODUCTION

Large-scale monitoring and control systems often rely on collecting and analyzing individuals' private data. Preventing information leakage from this data is essential to encourage user participation and preserve the benefits of these technologies. For example, energy consumption data from smart meters can be used to infer sensitive information about users' daily activities and preferences [1]. Similarly, in the coordination of electric vehicle charging, adversaries may extract private user information from publicly shared coordination signals [2]. Several approaches have been developed for privacy-preserving data processing, including cryptographic methods, measurement transmission scheduling, and data perturbation techniques [3]. Among these, differential privacy (DP) enables the *release* of statistical analyses derived from sensitive datasets by introducing carefully calibrated noise. It provides formal privacy guarantees by ensuring that the inclusion or exclusion of any single individual's data has a negligible impact on the published results.

Although DP was originally developed in the context of statistical databases [4]–[6], it has also been applied to signal processing [7] and control problems, including estimation and filtering [8], [9], distributed optimization [10], consensus [11], and optimal control [12], [13]. A common approach to enforce DP is to add noise directly to the sensitive signals or parameters, which could be the system's initial conditions [11], inputs [14], states [15], or measurements [12]. In [13], [14], noise is added to the measurements available to the controller. Further performance improvements can be achieved by combining signal processing with noise injection. For

instance, aggregating measurements [12] before perturbation can reduce the required noise level and improve the overall privacy-performance trade-offs.

In this paper, we study a steady-state linear quadratic Gaussian (LQG) control problem for coupled systems, in which the exogenous inputs represent privacy-sensitive signals. For example, acceleration is a privacy-sensitive exogenous input to the kinematic model of a car, from which the car's position and velocity can be inferred. As another example illustrated in Section VI, variations in a home's electricity demand are privacy-sensitive exogenous inputs to a power system model, revealing information such as users' consumption decisions, behavioral patterns, and peak usage times [1]. Implementing an LQG controller (e.g., for traffic or load-frequency control (LFC)) generally requires sharing signals (sensor measurements, control signals), which can leak information about the private exogenous inputs.

To address this issue, we incorporate DP into the design by simultaneously introducing noise in the measurement or control signals and optimizing the overall controller. Previous work on differentially private (dp) LQG control [12], [13] considers the system's states or sensor measurements to directly represent the sensitive data, which simplifies the noise level calibration step and enables the use of standard LQG design methods based on Riccati equations. In contrast, in our framework, the level of privacy-preserving noise depends on the *closed-loop* mapping from the exogenous inputs to the system's measurement to be controlled, which depends on the Kalman filter gain. On the other hand, the Kalman filter itself depends on the noise statistics, including the privacy-preserving noise. To overcome this circular dependency, we use the system-level synthesis (SLS) approach [16] to optimize the closed-loop response and level of privacy-preserving noise, obtaining the controller as a by-product.

The rest of the paper is organized as follows. Section II formulates the dp LQG control problem and provides some background on DP. Section III recalls the SLS framework for controller design, and Section IV develops the SLS-based methodology for dp LQG control, with details of the optimization algorithms presented in Section V. Section VI illustrates the performance of the methodology through numerical simulations, and Section VII concludes the paper.

II. PRELIMINARIES AND PROBLEM STATEMENT

A. Notation

Let $(\Omega, \mathcal{A}, \mathbb{P})$ denote a probability space, with $\mathcal{A}$ a σ -algebra over the sample space Ω and $\mathbb{P}$ a probability measure on $\mathcal{A}$. A discrete-time white Gaussian noise (WGN) signal

This work was supported by NSERC grant RGPIN-2025-06387.

The authors are with the department of Electrical Engineering, Polytechnique Montreal and GERAD, QC H3T1J4, Montreal, Canada. Email: {mohadese.jadidi, jerome.le-ny, shuang.gao}@polymtl.ca

$\{\eta_k\}_{k \geq 0}$ is a sequence of independent and identically distributed zero-mean Gaussian random vectors. The Frobenius norm of a matrix M is $\|M\|_F = \sqrt{\text{Tr}(M^T M)}$. For M a symmetric matrix, $M \succeq 0$ (respectively $M \succ 0$) means that M is positive semi-definite (respectively positive definite).

The space of n -dimensional discrete-time signals is denoted $\mathcal{S}^n := (\mathbb{R}^n)^\mathbb{N}$. For $\{\eta_k\}_{k \geq 0} \in \mathcal{S}^n$, its ℓ_2 -norm is $\|\eta\|_2 = (\sum_{k=0}^\infty \sum_{i=1}^n |\eta_{k,i}|^2)^{1/2}$, and the boldface symbol $\boldsymbol{\eta}$ denotes its z -transform. For a discrete-time linear time-invariant (LTI) system G with impulse response matrices $\{G_t\}_{t \geq 0}$, $\mathbf{G}$ denotes its transfer matrix, its $\mathcal{H}_2$ -norm is $\|\mathbf{G}\|_{\mathcal{H}_2} = \sqrt{\frac{1}{2\pi} \int_{-\pi}^{\pi} \text{Tr}(\mathbf{G}(e^{j\omega})^* \mathbf{G}(e^{j\omega})) d\omega} = \sqrt{\sum_{t=0}^\infty \text{Tr}(G_t^T G_t)}$, and its $\mathcal{H}_\infty$ -norm is $\|\mathbf{G}\|_{\mathcal{H}_\infty} = \sup_{\omega \in [-\pi, \pi]} \sigma_{\max}(\mathbf{G}(e^{j\omega}))$, where $\sigma_{\max}$ denotes the maximum singular value. The spaces of real rational stable proper and strictly proper transfer matrices are denoted by $\mathcal{RH}_\infty$ and $\frac{1}{z}\mathcal{RH}_\infty$, respectively. Let $\mathcal{F}_H$ denote the finite impulse response (FIR) transfer matrices of order H . The discrete-time unit impulse signal, taking the value 1 at $t = 0$ and 0 otherwise, is denoted δ_t^0 .

B. Privacy-Constrained Control

We consider N discrete-time privacy-sensitive signals denoted $\{w_{k,i}\}_{k \geq 0} \in \mathcal{S}^{m_i}$, for $1 \leq i \leq N$. Let $w_k = [w_{k,1}^T \dots w_{k,N}^T]^T \in \mathbb{R}^m$, with $m = \sum_{i=1}^N m_i$. These signals are inputs to the following LTI state-space model

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k + w_k, \\ y_k &= Cx_k + v_k, \end{aligned} \quad (1)$$

where $x_k \in \mathbb{R}^m$, $u_k \in \mathbb{R}^h$ and $y_k \in \mathbb{R}^p$ are the state, the control input and the measurement, respectively, for all $k \in \mathbb{N}$. The measurement noise $v_k \in \mathbb{R}^p$ is a WGN signal with covariance $V \succ 0$. The overall goal is to regulate the state of (1), assuming A , B , C , and V are publicly known. For *control design purposes*, the a priori unknown input w is modelled as a WGN signal independent of v and of the initial state, with publicly known covariance $W \succ 0$. Then, given matrices $Q \succeq 0$ and $R \succ 0$, we aim to minimize the steady-state LQG control objective

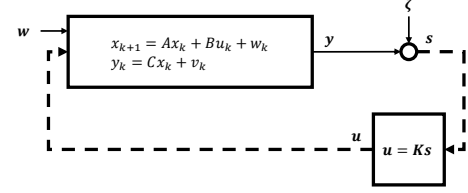
$$\lim_{T \rightarrow \infty} \frac{1}{T} \mathbb{E} \left[\sum_{k=0}^{T-1} x_k^T Q x_k + u_k^T R u_k \right], \quad (2)$$

where the control input u depends causally on the measurements y . We impose the following assumption to ensure the well-posedness of the steady-state LQG control problem.

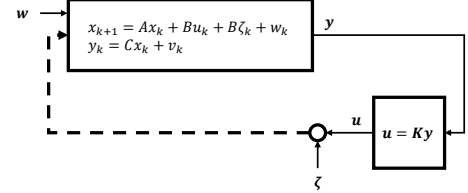
Assumption 1: The pair (A, B) is stabilizable, and the pairs (A, C) and $(A, Q^{1/2})$ are detectable.

We also assume that implementing the controller requires sharing the control actions u publicly, which can leak information about the private signal w . For instance, LFC in power systems is designed to maintain the balance between generation and demand by collecting measurements from different areas and transmitting control signals back to generator units [17]. These signals inherently contain information about local load variations, which are directly

influenced by customers' consumption decisions and reflect users' consumption patterns, habits, and behaviors, potentially leading to privacy leakage [1]. To address this issue, we impose DP constraints on publicly released control actions by introducing perturbations either to the measurements y (see Fig. 1a) or to the control inputs u (see Fig. 1b).



(a) Measurement perturbation.



(b) Control perturbation.

Fig. 1: Enforcing DP by perturbing the measurements (Fig. 1a) or control (Fig. 1b). The WGN signal ζ is added to ensure that the released dashed signals are (ϵ, δ) -dp.

C. Background on Differential Privacy

A dp mechanism is a randomized algorithm that takes private inputs from a data space $\mathcal{W}$ and produces randomized outputs whose distribution changes only slightly when the input data differs by the contribution of a single individual. Such modifications are characterized through a binary symmetric relation on $\mathcal{W}$, referred to as the *adjacency relation*.

Definition 1 ([6]): Let $\epsilon \geq 0$ and $0 \leq \delta \leq 1$. Let $\mathcal{W}$ denote a space equipped with a binary symmetric relation Adj . Let $(\mathcal{R}, \mathcal{A})$ be a measurable space, where $\mathcal{A}$ is a σ -algebra over $\mathcal{R}$. A randomized mechanism $M : \mathcal{W} \rightarrow \mathcal{R}$ is (ϵ, δ) -dp if for every pair $w, w' \in \mathcal{W}$ with $\text{Adj}(w, w')$,

$$\mathbb{P}(M(w) \in S) \leq e^\epsilon \mathbb{P}(M(w') \in S) + \delta, \quad \forall S \in \mathcal{A}. \quad (3)$$

Smaller values of ϵ and δ correspond to stronger privacy guarantees, because closer distributions in (3) for adjacent datasets w, w' make distinguishing between them harder.

The Gaussian mechanism [5], [9] achieves (ϵ, δ) -DP by adding WGN to the output of a mapping. The amount of noise sufficient to guarantee DP scales with how sensitive the mapping is to changes in its input over adjacent elements, which is captured by the following quantity.

Definition 2 ([6]): Let $G : \mathcal{W} \rightarrow S^q$ be a mapping, where $\mathcal{W}$ is equipped with a binary symmetric relation Adj . The ℓ_2 -sensitivity of G is defined as

$$\Delta_2(G) = \sup_{\substack{w, w' \in \mathcal{W} \\ \text{Adj}(w, w')}} \|G(w) - G(w')\|_2.$$

Intuitively, the ℓ_2 -sensitivity of a mapping captures an upper bound on how much the data of a single individual can change the mapping output, and consequently determines how much uncertainty should be introduced to mask the presence of an individual. The following theorem then provides a simple way of publishing (ϵ, δ) -DP signals.

Theorem 1 ([9]): Let $\epsilon > 0$ and $0 < \delta < 1$. Define $k_{\epsilon, \delta} := \frac{1}{2\epsilon} \left(Q^{-1}(\delta) + \sqrt{(Q^{-1}(\delta))^2 + 2\epsilon} \right)$, where $Q(x) := \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-u^2/2} du$. Let $\mathcal{W}$ be a space equipped with the binary symmetric relation Adj. For $G : \mathcal{W} \rightarrow S^q$ and a WGN signal ζ with covariance $\sigma^2 I_q$ satisfying $\sigma \geq \Delta_2(G)k_{\epsilon, \delta}$, the mechanism $M(w) = G(w) + \zeta$ is (ϵ, δ) -dp (for Adj).

In this paper, the input data space $\mathcal{W}$ is the signal space S^m of private exogenous signals w , and is equipped with the following adjacency relation.

Definition 3 ([9]): Let $\rho > 0$. The binary symmetric relation Adj is defined on $\mathcal{W} = S^m$ as

$$\text{Adj}(w, w') \text{ iff } \exists i \in \{1, \dots, N\} \text{ such that} \quad (4)$$

$$\|w_i - w'_i\|_2 \leq \rho \text{ and } w_j = w'_j, \quad \forall j \neq i.$$

In other words, two adjacent signals differ by the data of a single individual. However, we also impose a bound on the allowed signal deviations for which DP will hold, in order to be able to bound the amount of noise necessary.

III. REVIEW OF SLS-BASED CONTROL DESIGN

Our design methodology leverages the SLS parametrization of closed-loop transfer functions under all internally stabilizing controllers [16] and its application to LQG control, as reviewed here. Taking z -transforms in (1), we have

$$\begin{aligned} z\mathbf{x} &= A\mathbf{x} + B\mathbf{u} + \mathbf{w}, \\ \mathbf{y} &= C\mathbf{x} + \mathbf{v}. \end{aligned} \quad (5)$$

Consider an output feedback control $\mathbf{u} = \mathbf{K}\mathbf{y}$, with $\mathbf{K}$ a transfer matrix from $\mathbf{y}$ to $\mathbf{u}$, and substitute it in (5) to get

$$(zI - A - B\mathbf{K}C)\mathbf{x} = \mathbf{w} + B\mathbf{K}\mathbf{v}.$$

For any proper $\mathbf{K}$, the inverse of $(zI - A - B\mathbf{K}C)$ exists. Therefore, the closed-loop system responses from the exogenous inputs $\mathbf{w}$ on the *state* and $\mathbf{v}$ on the *measurement* to the state $\mathbf{x}$ and the control input $\mathbf{u}$ are

$$\begin{bmatrix} \mathbf{x} \\ \mathbf{u} \end{bmatrix} = \begin{bmatrix} \Phi_{xs} & \Phi_{xm} \\ \Phi_{us} & \Phi_{um} \end{bmatrix} \begin{bmatrix} \mathbf{w} \\ \mathbf{v} \end{bmatrix}, \quad (6)$$

where

$$\begin{aligned} \Phi_{xs} &= (zI - A - B\mathbf{K}C)^{-1}, \\ \Phi_{xm} &= (zI - A - B\mathbf{K}C)^{-1}B\mathbf{K}, \\ \Phi_{us} &= \mathbf{K}C(zI - A - B\mathbf{K}C)^{-1}, \\ \Phi_{um} &= \mathbf{K} + \mathbf{K}C(zI - A - B\mathbf{K}C)^{-1}B\mathbf{K}. \end{aligned} \quad (7)$$

The SLS framework provides a complete characterization of all achievable closed-loop system responses, along with a corresponding controller realization, as recalled next.

Theorem 2 ([16]): In the context of output feedback control, the following statements hold:

- 1) All system responses in (7) achievable by an internally stabilizing controller $\mathbf{K}$ are characterized by the affine subspace defined by

$$\begin{aligned} [zI - A \quad -B] \begin{bmatrix} \Phi_{xs} & \Phi_{xm} \\ \Phi_{us} & \Phi_{um} \end{bmatrix} &= [I \quad 0], \\ \begin{bmatrix} \Phi_{xs} & \Phi_{xm} \\ \Phi_{us} & \Phi_{um} \end{bmatrix} \begin{bmatrix} zI - A \\ -C \end{bmatrix} &= \begin{bmatrix} I \\ 0 \end{bmatrix}, \end{aligned} \quad (8)$$

$$\Phi_{xs}, \Phi_{us}, \Phi_{xm} \in \frac{1}{z}\mathcal{RH}_\infty, \quad \Phi_{um} \in \mathcal{RH}_\infty.$$

- 2) Let $\{\Phi_{xs}, \Phi_{us}, \Phi_{xm}, \Phi_{um}\}$ be a set of transfer matrices satisfying (8). Then, the controller $\mathbf{K} = \Phi_{um} - \Phi_{us}\Phi_{xs}^{-1}\Phi_{xm}$ achieves the system responses described in (7). Furthermore, under the following state-space realization of the controller

$$\begin{aligned} z\mathbf{x}_c &= \tilde{\Phi}_{xs}\mathbf{x}_c + \tilde{\Phi}_{xm}\mathbf{y}, \\ \mathbf{u} &= \tilde{\Phi}_{us}\mathbf{x}_c + \Phi_{um}\mathbf{y}, \end{aligned} \quad (9)$$

where $\mathbf{x}_c$ denotes the controller state in the z -domain, $\tilde{\Phi}_{xs} = z(I - z\Phi_{xs})$, $\tilde{\Phi}_{us} = z\Phi_{us}$, $\tilde{\Phi}_{xm} = -z\Phi_{xm}$ with $\tilde{\Phi}_{xs}, \tilde{\Phi}_{us}, \tilde{\Phi}_{xm} \in \mathcal{RH}_\infty$, the controller is internally stabilizing.

Then, the expression of the LQG objective (2) in terms of the $\mathcal{H}_2$ norm [18, Section 9.3.3] leads to the following.

Proposition 1: Under Assumption 1, minimizing the steady-state LQG objective (2) is equivalent to solving

$$\min_{\substack{\Phi_{xs}, \Phi_{us}, \\ \Phi_{xm}, \Phi_{um}}} \left\| \begin{bmatrix} Q^{1/2} & 0 \\ 0 & R^{1/2} \end{bmatrix} \begin{bmatrix} \Phi_{xs} & \Phi_{xm} \\ \Phi_{us} & \Phi_{um} \end{bmatrix} \begin{bmatrix} W^{1/2} & 0 \\ 0 & V^{1/2} \end{bmatrix} \right\|_{\mathcal{H}_2}^2 \quad (10)$$

subject to the constraints (8).

Finally, to turn (10) into a finite-dimensional optimization problem, a common strategy is to impose FIR constraints on the system responses, i.e., solve, for some fixed order H ,

$$\min_{\substack{\Phi_{xs}, \Phi_{us}, \\ \Phi_{xm}, \Phi_{um}}} \left\| \begin{bmatrix} Q^{1/2} & 0 \\ 0 & R^{1/2} \end{bmatrix} \begin{bmatrix} \Phi_{xs} & \Phi_{xm} \\ \Phi_{us} & \Phi_{um} \end{bmatrix} \begin{bmatrix} W^{1/2} & 0 \\ 0 & V^{1/2} \end{bmatrix} \right\|_{\mathcal{H}_2}^2 \quad (11)$$

s.t. (8) holds and $\Phi_{xs}, \Phi_{us}, \Phi_{xm}, \Phi_{um} \in \mathcal{F}_H$.

IV. SLS-BASED DESIGN WITH DP CONSTRAINTS

We now develop two approaches (see Fig. 1) to solve the LQG control problem when the control signal u is publicly shared, while enforcing (ϵ, δ) -DP for the sensitive exogenous inputs w , with the adjacency relation of Definition 3.

In the first approach, illustrated in Fig. 1a, a WGN signal is added to make the measurements y dp before transmission to the controller. By the resilience to post-processing property of DP [6], [9], the control signal u , computed from y , is also dp. Since y is dp, it can be publicly released if needed, in addition to u . However, a potential disadvantage of this

approach is that it may require adding more noise than strictly necessary. This scheme is discussed in Section IV-A.

In the second approach, see Fig. 1b, a WGN signal is added directly to u , enforcing DP at the controller's output. This scheme, discussed in Section IV-B, requires a trusted controller to collect the measurements and add enough noise to the control signal before releasing it. But compared to the first approach, it may require less noise because the controller can directly act to reduce the sensitivity of u to w .

Finally, one could consider adding noise directly to the exogenous inputs w to enforce DP. However, this may not be feasible in practice, for instance when w represents a physical input to the system (acceleration, power consumption, etc.). Moreover, if such an approach is feasible, the added privacy noise simply modifies the input covariance W , leaving the LQG design problem essentially unchanged [9].

A. Measurement Perturbation

Under the adjacency relation (4), the ℓ_2 -sensitivity of the mapping $G_{w \rightarrow y} : \mathcal{S}^m \rightarrow \mathcal{S}^p$ is

$$\begin{aligned} \Delta_2(G_{w \rightarrow y}) &= \sup_{\substack{w, w' \in \mathcal{W} \\ \text{Adj}(w, w')}} \|G_{w \rightarrow y}(w) - G_{w \rightarrow y}(w')\|_2 \\ &= \rho \max_{1 \leq i \leq N} \|C\Phi_{xs}(:, i)\|_{\mathcal{H}_\infty}, \end{aligned}$$

where $\Phi_{xs}(:, i)$ denotes the i^{th} column of the transfer matrix Φ_{xs} defined in (7). According to Theorem 1, adding a WGN signal ζ to y (see Fig. 1a) with covariance $(\max_{1 \leq i \leq N} \|C\Phi_{xs}(:, i)\|_{\mathcal{H}_\infty} \rho)^2 k_{\epsilon, \delta}^2 I_p$ ensures that $s = y + \zeta$ is (ϵ, δ) -dp.

For the measurement perturbation approach, the system dynamics are described by the state-space model

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k + w_k, \\ s_k &= Cx_k + v_k + \zeta_k. \end{aligned}$$

Consider an output feedback control $\mathbf{u} = \mathbf{K}s$, where $\mathbf{K}$ is the transfer matrix from s to the control input $\mathbf{u}$. The closed-loop system responses from the exogenous input $\mathbf{w}$ on the state and the total noise $\mathbf{v} + \zeta$ on the measurement to the state $\mathbf{x}$ and the control input $\mathbf{u}$ are

$$\begin{bmatrix} \mathbf{x} \\ \mathbf{u} \end{bmatrix} = \begin{bmatrix} \Phi_{xs} & \Phi_{xm} \\ \Phi_{us} & \Phi_{um} \end{bmatrix} \begin{bmatrix} \mathbf{w} \\ \mathbf{v} + \zeta \end{bmatrix},$$

i.e., the same as in (7). Theorem 2 also holds.

Extending the optimization problem (10) to include the effect of the added DP noise yields the following optimization problem for the measurement perturbation approach

$$\begin{aligned} \min_{\substack{\Phi_{xs}, \Phi_{us}, \\ \Phi_{xm}, \Phi_{um}}} & \left\| \begin{bmatrix} Q^{1/2} & 0 \\ 0 & R^{1/2} \end{bmatrix} \begin{bmatrix} \Phi_{xs} & \Phi_{xm} \\ \Phi_{us} & \Phi_{um} \end{bmatrix} \right. \\ & \left. \begin{bmatrix} W^{1/2} & 0 \\ 0 & (V + \max_{1 \leq i \leq N} \|C\Phi_{xs}(:, i)\|_{\mathcal{H}_\infty}^2 \rho^2 k_{\epsilon, \delta}^2 I_p)^{1/2} \end{bmatrix} \right\|_{\mathcal{H}_2}^2 \\ \text{s.t. } & (8), \end{aligned}$$

which is equivalent to

$$\begin{aligned} \min_{\substack{\Phi_{xs}, \Phi_{us}, \\ \Phi_{xm}, \Phi_{um}}} & \left\| \begin{bmatrix} Q^{1/2} & 0 \\ 0 & R^{1/2} \end{bmatrix} \begin{bmatrix} \Phi_{xs} & \Phi_{xm} \\ \Phi_{us} & \Phi_{um} \end{bmatrix} \right. \\ & \left. \begin{bmatrix} W^{1/2} & 0 \\ 0 & (V + \lambda^2 \rho^2 k_{\epsilon, \delta}^2 I_p)^{1/2} \end{bmatrix} \right\|_{\mathcal{H}_2}^2 \\ \text{s.t. } & (8), \text{ and } \|C\Phi_{xs}(:, i)\|_{\mathcal{H}_\infty} \leq \lambda, \forall 1 \leq i \leq N. \end{aligned} \quad (12)$$

This formulation allows for the simultaneous design of the controller and selection of the appropriate noise covariance $\lambda^2 \rho^2 k_{\epsilon, \delta}^2 I_p$ for ζ to ensure that s is (ϵ, δ) -dp.

B. Control Input Perturbation

Under the adjacency relation (4), the ℓ_2 -sensitivity of the mapping $G_{w \rightarrow u} : \mathcal{S}^m \rightarrow \mathcal{S}^h$ is given by

$$\begin{aligned} \Delta_2(G_{w \rightarrow u}) &= \sup_{\substack{w, w' \in \mathcal{W} \\ \text{Adj}(w, w')}} \|G_{w \rightarrow u}(w) - G_{w \rightarrow u}(w')\|_2 \\ &= \rho \max_{1 \leq i \leq N} \|\Phi_{us}(:, i)\|_{\mathcal{H}_\infty}. \end{aligned}$$

According to Theorem 1, adding a WGN signal ζ with covariance $(\max_{1 \leq i \leq N} \|\Phi_{us}(:, i)\|_{\mathcal{H}_\infty} \rho)^2 k_{\epsilon, \delta}^2 I_h$ to the control input u (see Fig. 1b) ensures that $u + \zeta$ is (ϵ, δ) -dp.

For the control input perturbation approach, the system dynamics are described by

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k + B\zeta_k + w_k, \\ y_k &= Cx_k + v_k. \end{aligned}$$

Consider an output feedback control $\mathbf{u} = \mathbf{K}\mathbf{y}$, where $\mathbf{K}$ is the transfer matrix from the measurement $\mathbf{y}$ to the control input $\mathbf{u}$. Then, the closed-loop system responses from $\mathbf{w} + B\zeta$ and the noise $\mathbf{v}$ to the state $\mathbf{x}$ and the control input $\mathbf{u}$ are

$$\begin{bmatrix} \mathbf{x} \\ \mathbf{u} \end{bmatrix} = \begin{bmatrix} \Phi_{xs} & \Phi_{xm} \\ \Phi_{us} & \Phi_{um} \end{bmatrix} \begin{bmatrix} \mathbf{w} + B\zeta \\ \mathbf{v} \end{bmatrix},$$

i.e., the same as in (7). Theorem 2 continues to hold.

In view of (11), incorporating the effect of DP noise under the control input perturbation approach leads to the following optimization problem

$$\begin{aligned} \min_{\substack{\Phi_{xs}, \Phi_{us}, \\ \Phi_{xm}, \Phi_{um}}} & \left\| \begin{bmatrix} Q^{1/2} & 0 \\ 0 & R^{1/2} \end{bmatrix} \begin{bmatrix} \Phi_{xs} & \Phi_{xm} \\ \Phi_{us} & \Phi_{um} \end{bmatrix} \right. \\ & \left. \begin{bmatrix} (W + \max_{1 \leq i \leq N} \|\Phi_{us}(:, i)\|_{\mathcal{H}_\infty}^2 \rho^2 k_{\epsilon, \delta}^2 BB^T)^{1/2} & 0 \\ 0 & V^{1/2} \end{bmatrix} \right\|_{\mathcal{H}_2}^2 \\ \text{s.t. } & (8), \end{aligned}$$

which is equivalent to

$$\begin{aligned} \min_{\substack{\Phi_{xs}, \Phi_{us}, \\ \Phi_{xm}, \Phi_{um}}} & \left\| \begin{bmatrix} Q^{1/2} & 0 \\ 0 & R^{1/2} \end{bmatrix} \begin{bmatrix} \Phi_{xs} & \Phi_{xm} \\ \Phi_{us} & \Phi_{um} \end{bmatrix} \right. \\ & \left. \begin{bmatrix} (W + \lambda^2 \rho^2 k_{\epsilon, \delta}^2 BB^T)^{1/2} & 0 \\ 0 & V^{1/2} \end{bmatrix} \right\|_{\mathcal{H}_2}^2 \\ \text{s.t. } & (8), \text{ and } \|\Phi_{us}(:, i)\|_{\mathcal{H}_\infty} \leq \lambda, \forall 1 \leq i \leq N. \end{aligned} \quad (13)$$

Again, this formulation enables the joint design of the controller and selection of the appropriate noise covariance $\lambda^2 \rho^2 k_{\epsilon, \delta}^2 I_h$ for ζ to ensure that $u + \zeta$ is (ϵ, δ) -dp.

V. NUMERICAL CONTROLLER DESIGN SCHEMES

As mentioned for (11), a common way to turn the previous optimization problems into finite-dimensional problems is to impose FIR constraints on the closed-loop system responses. Assuming a fixed order H for all transfer functions and the appropriate strict properness constraints, we can write

$$\begin{aligned}\Phi_{xs} &= \sum_{t=1}^H \Phi_{xs,t} z^{-t}, & \Phi_{us} &= \sum_{t=1}^H \Phi_{us,t} z^{-t}, \\ \Phi_{xm} &= \sum_{t=1}^H \Phi_{xm,t} z^{-t}, & \Phi_{um} &= \sum_{t=0}^H \Phi_{um,t} z^{-t},\end{aligned}$$

where $\Phi_{xs,t} \in \mathbb{R}^{m \times m}$, $\Phi_{us,t} \in \mathbb{R}^{h \times m}$, $\Phi_{xm,t} \in \mathbb{R}^{m \times p}$, and $\Phi_{um,t} \in \mathbb{R}^{h \times p}$ denote the FIR filter coefficient matrices (taps). The following propositions then provide numerical schemes for the optimization problems (11), (12), and (13) stated in the previous sections. Recall also that once the system responses are computed, the controller can be implemented using the state-space realization (9).

Proposition 2: The optimization problem (11) is equivalent to the following convex quadratic program

$$\begin{aligned}\min_{\substack{\Phi_{xs,t}, \Phi_{us,t}, \\ \Phi_{xm,t}, \Phi_{um,t}}} & \sum_{t=0}^H \left\| \begin{bmatrix} Q^{1/2} & 0_{m \times h} \\ 0_{h \times m} & R^{1/2} \end{bmatrix} \begin{bmatrix} \Phi_{xs,t} & \Phi_{xm,t} \\ \Phi_{us,t} & \Phi_{um,t} \end{bmatrix} \right\|_F^2 \\ & \left\| \begin{bmatrix} W^{1/2} & 0_{m \times p} \\ 0_{p \times m} & V^{1/2} \end{bmatrix} \right\|_F^2\end{aligned}\quad (14a)$$

s.t.

$$\begin{aligned}\forall 0 \leq t \leq H, & \quad \Phi_{xs,t+1} = A\Phi_{xs,t} + B\Phi_{us,t} + \delta_t^0 I, \\ \forall 0 \leq t \leq H, & \quad \Phi_{xm,t+1} = A\Phi_{xm,t} + B\Phi_{um,t}, \\ \forall 0 \leq t \leq H, & \quad \Phi_{xs,t+1} = \Phi_{xs,t}A + \Phi_{xm,t}C + \delta_t^0 I, \\ \forall 0 \leq t \leq H, & \quad \Phi_{us,t+1} = \Phi_{us,t}A + \Phi_{um,t}C, \\ \forall j \in \{xs, xm, us\}, & \quad \Phi_{j,0} = 0, \\ \forall t > H, \quad \forall j \in \{xs, xm, us, um\}, & \quad \Phi_{j,t} = 0.\end{aligned}\quad (14b)$$

Proof: The objective function in (11) is converted from its frequency-domain $\mathcal{H}_2$ -norm definition to the equivalent time-domain representation in (14a). Similarly, the system constraints in (8) are transformed from the z -domain to the time-domain by applying the inverse z -transform, resulting in (14b). Finally, imposing an FIR structure of order H together with the corresponding (strict) properness requirements on the system responses yields the constraints in (14c). ■

Proposition 3: The optimization problem (12), with the additional constraints $\Phi_{xs}, \Phi_{us}, \Phi_{xm}, \Phi_{um} \in \mathcal{F}_H$, is equivalent to

alent to

$$\begin{aligned}\min_{\substack{\Phi_{xs,t}, \Phi_{us,t}, \\ \Phi_{xm,t}, \Phi_{um,t}, \\ \lambda > 0, P_i > 0 \text{ for } 1 \leq i \leq N}} & \sum_{t=0}^H \left\| \begin{bmatrix} Q^{1/2} & 0_{m \times h} \\ 0_{h \times m} & R^{1/2} \end{bmatrix} \begin{bmatrix} \Phi_{xs,t} & \Phi_{xm,t} \\ \Phi_{us,t} & \Phi_{um,t} \end{bmatrix} \right\|_F^2 \\ & \left\| \begin{bmatrix} W^{1/2} & 0_{m \times p} \\ 0_{p \times m} & (V + \lambda^2 \rho^2 k_{\epsilon, \delta}^2 I_p)^{1/2} \end{bmatrix} \right\|_F^2\end{aligned}\quad (15a)$$

s.t. (14b), (14c),

$\forall 1 \leq i \leq N,$

$$\begin{bmatrix} \Omega_i^T P_i \Omega_i - P_i & \Omega_i^T P_i \Theta_i & \Lambda_i^T \\ * & \Theta_i^T P_i \Theta_i - \lambda I_{m_i} & 0_{m_i \times m} \\ * & * & -\lambda I_m \end{bmatrix} \preceq 0, \quad (15b)$$

$$\text{with } \Omega_i = \begin{bmatrix} 0_{m_i \times (H-2)m_i} & 0_{m_i \times m_i} \\ I_{(H-2)m_i} & 0_{(H-2)m_i \times m_i} \end{bmatrix},$$

$$\Theta_i = \begin{bmatrix} I_{m_i} \\ 0_{(H-2)m_i \times m_i} \end{bmatrix},$$

$$\Lambda_i = [C\Phi_{xs,1}(:, i), \dots, C\Phi_{xs,H}(:, i)]_{p \times (H-1)m_i},$$

and $*$ denoting symmetric terms in matrices.

Proof: After imposing the FIR constraint of order H on the system responses, we use the FIR state-space realization. Following [19, Section 4.2.2], we can equivalently represent the $\mathcal{H}_\infty$ -norm constraint in (12) by the linear matrix inequality (LMI) (15b). ■

Proposition 4: The optimization problem (13), with the additional constraints $\Phi_{xs}, \Phi_{us}, \Phi_{xm}, \Phi_{um} \in \mathcal{F}_H$, is equivalent to

$$\begin{aligned}\min_{\substack{\Phi_{xs,t}, \Phi_{us,t}, \\ \Phi_{xm,t}, \Phi_{um,t}, \\ \lambda > 0, P_i > 0 \text{ for } 1 \leq i \leq N}} & \sum_{t=0}^H \left\| \begin{bmatrix} Q^{1/2} & 0_{m \times h} \\ 0_{h \times m} & R^{1/2} \end{bmatrix} \begin{bmatrix} \Phi_{xs,t} & \Phi_{xm,t} \\ \Phi_{us,t} & \Phi_{um,t} \end{bmatrix} \right\|_F^2 \\ & \left\| \begin{bmatrix} (W + \lambda^2 \rho^2 k_{\epsilon, \delta}^2 B B^T)^{1/2} & 0_{m \times p} \\ 0_{p \times m} & V^{1/2} \end{bmatrix} \right\|_F^2\end{aligned}\quad (16a)$$

s.t. (14b), (14c),

$\forall 1 \leq i \leq N,$

$$\begin{bmatrix} \Omega_i^T P_i \Omega_i - P_i & \Omega_i^T P_i \Theta_i & \Lambda_i^T \\ * & \Theta_i^T P_i \Theta_i - \lambda I_{m_i} & 0_{m_i \times h} \\ * & * & -\lambda I_h \end{bmatrix} \preceq 0, \quad (16b)$$

$$\text{with } \Omega_i = \begin{bmatrix} 0_{m_i \times (H-2)m_i} & 0_{m_i \times m_i} \\ I_{(H-2)m_i} & 0_{(H-2)m_i \times m_i} \end{bmatrix},$$

$$\Theta_i = \begin{bmatrix} I_{m_i} \\ 0_{(H-2)m_i \times m_i} \end{bmatrix},$$

$$\Lambda_i = [\Phi_{us,1}(:, i), \dots, \Phi_{us,H}(:, i)]_{h \times (H-1)m_i}.$$

Proof: The proof is similar to that of Proposition 3. ■

Due to the coupling between $\{\Phi_{xs,t}, \Phi_{us,t}, \Phi_{xm,t}, \Phi_{um,t}\}$ and λ in the objective functions (15a) and (16a), the optimization problems (15) and (16) are non-convex. However, for each fixed λ , the problems are convex semi-definite programs, and hence, a grid search over λ in a bounded interval $[\underline{\lambda}, \bar{\lambda}]$ can be performed, where $\underline{\lambda} < \bar{\lambda}$ are positive constants.

For small values of λ , the problems can become infeasible, while large values degrade the system performance.

In the rest of this section, we consider the optimization problem (15), with the discussion of (16) being identical. For each value of λ for which (15) with λ fixed is feasible, denote by $J(\lambda)$ the corresponding optimal value. We first search for a small value $\underline{\lambda}$ such that (15) is feasible, i.e., $J(\underline{\lambda})$ is finite. Note then that (15) is feasible for all fixed $\lambda \geq \underline{\lambda}$, so that J can be defined on the interval $[\underline{\lambda}, \infty)$. The function J is then evaluated over a discretized set of λ values up to some value $\bar{\lambda} > \underline{\lambda}$, and the value that yields the minimum over the grid is selected. We have the following results.

Proposition 5: The function J is continuous on $[\underline{\lambda}, \bar{\lambda}]$.

Proof: We invoke Berge's Maximum Theorem [20, Section 17.5] to establish the continuity of J . Since the objective function is continuous in both the decision variables and λ , and the feasible set is defined by LMI constraints that are affine (and thus continuous) in λ , the optimal value function $J(\lambda)$ is continuous on any compact set $[\underline{\lambda}, \bar{\lambda}]$ over which it is defined (i.e., where the problem is feasible). ■

Proposition 6: Consider the minimization problem

$$\min_{\lambda \in [\underline{\lambda}, \bar{\lambda}]} J(\lambda), \quad (17)$$

where the minimum is attained since J is continuous. Let Γ_n be a uniform grid over the compact interval $[\underline{\lambda}, \bar{\lambda}]$ with mesh size $\Delta_n \rightarrow 0$ as $n \rightarrow \infty$. Let λ_n^* be the grid-based optimizer defined by

$$\lambda_n^* \in \arg \min_{\lambda \in \Gamma_n} J(\lambda).$$

Then, the sequence of objective values converges to the global minimum, that is,

$$\lim_{n \rightarrow \infty} J(\lambda_n^*) = \min_{\lambda \in [\underline{\lambda}, \bar{\lambda}]} J(\lambda).$$

Proof: Let $\lambda^* \in [\underline{\lambda}, \bar{\lambda}]$ be a global minimizer for (17), i.e., such that $J(\lambda^*) \leq J(\lambda)$ for all $\lambda \in [\underline{\lambda}, \bar{\lambda}]$. There must exist a sequence of grid points $\hat{\lambda}_n \in \Gamma_n$, for $n \geq 0$, such that $|\hat{\lambda}_n - \lambda^*| \leq \Delta_n$. As $n \rightarrow \infty$, $\hat{\lambda}_n \rightarrow \lambda^*$. By the continuity of $J(\lambda)$, it follows that $J(\hat{\lambda}_n) \rightarrow J(\lambda^*)$. By the definition of the grid optimizer λ_n^* , we have $J(\lambda_n^*) \leq J(\hat{\lambda}_n)$. Since we also have $J(\lambda^*) \leq J(\lambda_n^*)$, we conclude that $J(\lambda_n^*) \rightarrow J(\lambda^*)$ as $n \rightarrow \infty$. ■

VI. SIMULATIONS

In this section, we illustrate the dp controller design methodology for an LFC problem. In a power system, variations in power demand arise from private customers' consumption decisions and induce deviations in grid frequency (i.e., the rotational speed of generators). If this issue is not addressed properly, it can lead to equipment damage or even blackouts.

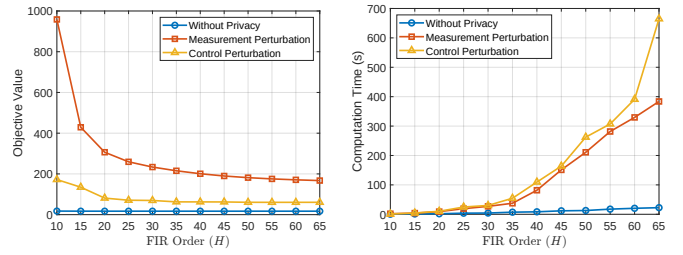
The state-space model for bus i in a power system [16] can be expressed as

$$\begin{aligned} x_{k+1,i} &= A_{ii}x_{k,i} + \sum_{j \in \mathcal{N}_i} A_{ij}x_{k,j} + B_{ii}u_{k,i} + w_{k,i}, \\ y_{k,i} &= C_{ii}x_{k,i} + v_{k,i}, \end{aligned}$$

where $x_{k,i} = [\theta_{k,i} \ \dot{\theta}_{k,i}]^T$ is the state ($\theta_{k,i}$ and $\dot{\theta}_{k,i}$ denote the phase angle deviation and frequency deviation), $u_{k,i}$ is the control input, $y_{k,i}$ is the measured output, $w_{k,i}$ represents the aggregated load variation driven by the privacy-sensitive consumption decisions of users connected to bus i , and $v_{k,i}$ denotes the measurement noise. The model matrices for bus i are defined as

$$\begin{aligned} A_{ii} &= \begin{bmatrix} 1 & \Delta t \\ -\frac{k_i}{n_i} \Delta t & 1 - \frac{d_i}{n_i} \Delta t \end{bmatrix}, \quad A_{ij} = \begin{bmatrix} 0 & 0 \\ \frac{k_{ij}}{n_i} \Delta t & 0 \end{bmatrix}, \\ B_{ii} &= \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad C_{ii} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \end{aligned}$$

where n_i is the inertia, d_i is the damping, k_{ij} represents the coupling between bus i and its neighbor bus j , and $k_i = \sum_{j \in \mathcal{N}_i} k_{ij}$, with $\mathcal{N}_i$ the set of buses neighboring bus i .



(a) Objective value versus FIR order H . (b) Computation time versus FIR order H .

Fig. 2: Effect of the FIR order H under three scenarios: non-private setting, measurement perturbation, and control perturbation: (a) objective value and (b) computation time.

We consider a network of $N = 10$ subsystems interconnected through a randomly generated undirected spanning tree. The system is discretized with the sampling time $\Delta t = 0.2$. The system parameters are generated such that n_i^{-1} , d_i , and k_{ij} are uniformly distributed in $[0, 2]$, $[1, 1.5]$, and $[0.5, 1]$, respectively. The covariance and weighting matrices are set as $W = I_{10} \otimes \text{diag}(10^{-4}, 1)$, $V = 10^{-2}I_{20}$, $Q = I_{20}$, and $R = I_{10}$. The privacy parameters are set as $\epsilon = \log(3)$, $\delta = 0.05$, and $\rho = 1$. To investigate the effect of the FIR order, we show the objective value and computation time for different values of H under the three considered scenarios in Fig. 2a and Fig. 2b, respectively. As H increases, the objective value improves, but the improvement becomes progressively smaller as H approaches 40, while the computation time increases substantially. Therefore, $H = 40$ is selected for the remaining simulations as a practical trade-off between control performance and computational cost.

The performance of the proposed controller design is evaluated on the power system model under three scenarios, including the non-private setting, measurement perturbation, and control perturbation. In the non-private case, the objective value is 16.9976. Under measurement perturbation and control perturbation, the objective values increase to 200.9130 and 62.5811, corresponding to $\lambda = 18.2$ and $\lambda = 0.9$ selected via grid search, respectively. These results indicate that control perturbation provides a more favorable

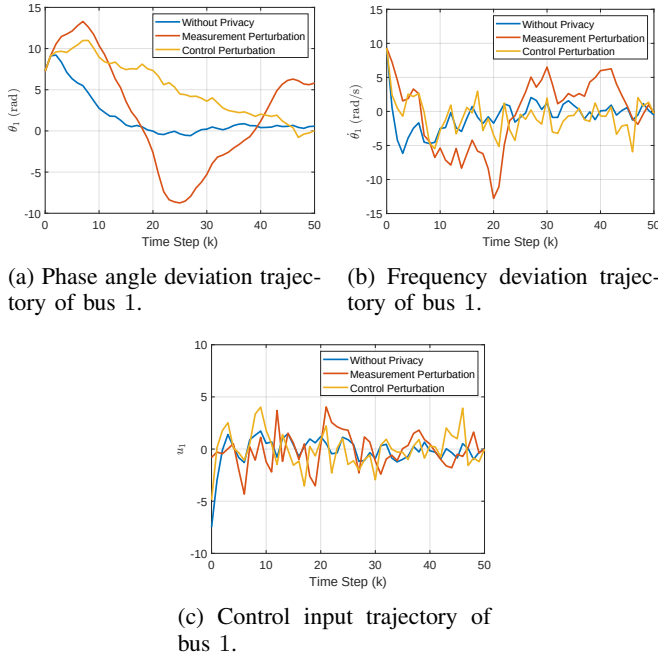


Fig. 3: Phase angle deviation (Fig. 3a), frequency deviation (Fig. 3b), and control input (Fig. 3c) trajectories of bus 1 under three scenarios: non-private setting, measurement perturbation, and control perturbation.

trade-off between privacy and control performance compared to measurement perturbation. In all scenarios, the phase angle deviation and frequency deviation of all buses are regulated to zero, with Fig. 3a and Fig. 3b illustrating trajectories for bus 1. Moreover, the control inputs remain bounded throughout the simulation horizon for all buses. Fig. 3c shows a control trajectory of bus 1.

VII. CONCLUSIONS

In this paper, we address a steady-state LQG control problem with privacy-sensitive exogenous input signals and publicly shared control signals. We overcome the circular dependency between setting the magnitude of the DP noise and designing the Kalman filter gain by employing the SLS framework. We propose and compare two dp control strategies, perturbing either measurements or control inputs. We provide a systematic optimization-based approach to balance control performance and privacy guarantees. Numerical simulations on a power system model with private consumption signals illustrate our theoretical results. One limitation of the control perturbation approach is its reliance on a trusted controller with access to unperturbed measurements and control signals. Future work will investigate whether homomorphic-encryption-based dynamic controllers [21], [22] can be combined with the proposed DP mechanism to remove this trust requirement.

REFERENCES

- [1] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid – the new and improved power grid: A survey," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 4, pp. 944–980, 2012.
- [2] S. Han, U. Topcu, and G. J. Pappas, "Differentially private distributed constrained optimization," *IEEE Transactions on Automatic Control*, vol. 62, no. 1, pp. 50–64, 2017.
- [3] X. Yan, G. Zhou, D. E. Quevedo, C. Murguia, B. Chen, and H. Huang, "Privacy-preserving state estimation in the presence of eavesdroppers: A survey," *IEEE Transactions on Automation Science and Engineering*, vol. 22, pp. 6190–6207, 2024.
- [4] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography*. Springer Berlin Heidelberg, 2006, pp. 265–284.
- [5] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, "Our data, ourselves: privacy via distributed noise generation," in *Proceedings of the 24th Annual International Conference on The Theory and Applications of Cryptographic Techniques*, 2006, pp. 486–503.
- [6] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Foundations and Trends in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2014.
- [7] A. D. Sarwate and K. Chaudhuri, "Signal processing and machine learning with differential privacy: Algorithms and challenges for continuous data," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 86–94, 2013.
- [8] K. H. Degue and J. Le Ny, "Differentially private Kalman filtering with signal aggregation," *IEEE Transactions on Automatic Control*, vol. 68, no. 10, pp. 6240–6246, 2023.
- [9] J. Le Ny and G. J. Pappas, "Differentially private filtering," *IEEE Transactions on Automatic Control*, vol. 59, no. 2, pp. 341–354, 2014.
- [10] Y. Wang and A. Nedić, "Differentially-private distributed optimization with guaranteed optimality," in *Proceedings of the 62nd IEEE Conference on Decision and Control (CDC)*, 2023, pp. 4162–4169.
- [11] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design," *Automatica*, vol. 81, pp. 221–231, 2017.
- [12] K. H. Degue and J. Le Ny, "Cooperative differentially private LQG control with measurement aggregation," *IEEE Control Systems Letters*, vol. 7, pp. 1093–1098, 2023.
- [13] K. Yazdani, A. Jones, K. Leahy, and M. Hale, "Differentially private LQ control," *IEEE Transactions on Automatic Control*, vol. 68, no. 2, pp. 1061–1068, 2023.
- [14] Y. Kawano and M. Cao, "Design of privacy-preserving dynamic controllers," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3863–3878, 2020.
- [15] Y. Wang, Z. Huang, S. Mitra, and G. E. Dullerud, "Differential privacy in linear distributed control systems: Entropy minimizing mechanisms and performance tradeoffs," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 118–130, 2017.
- [16] J. Anderson, J. C. Doyle, S. H. Low, and N. Matni, "System level synthesis," *Annual Reviews in Control*, vol. 47, pp. 364–393, 2019.
- [17] L. Jiang, W. Yao, Q. H. Wu, J. Y. Wen, and S. J. Cheng, "Delay-dependent stability for load frequency control with constant and time-varying delays," *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 932–941, 2012.
- [18] S. Skogestad and I. Postlethwaite, *Multivariable feedback control: Analysis and Design*. John Wiley, 2005.
- [19] R. J. Caverly and J. R. Forbes, "LMI properties and applications in systems, stability, and control theory," arXiv preprint arXiv:1903.08599, 2024.
- [20] C. D. Aliprantis and K. C. Border, *Infinite Dimensional Analysis: A Hitchhiker's Guide*. Springer, 2006.
- [21] A. B. Alexandru and G. J. Pappas, "Encrypted LQG using labeled homomorphic encryption," in *Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPs)*, 2019, pp. 129–140.
- [22] J. Kim, H. Shim, and K. Han, "Dynamic controller that operates over homomorphically encrypted data for infinite time horizon," *IEEE Transactions on Automatic Control*, vol. 68, no. 2, pp. 660–672, 2023.