Modular control under privacy protection

Kawano, Yu; Kashima, Kenji; Cao, Ming

Published in:
Automatica

DOI:
10.1016/j.automatica.2021.109518

Publication date:
2021

Automatica 127 (2021) 109518

Contents lists available at ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Modular control under privacy protection: Fundamental trade-offs[☆]

Yu Kawano[a,*], Kenji Kashima[b], Ming Cao[c]

[a] Graduate School of Advanced Science and Engineering, Hiroshima University, Higashi-Hiroshima 739-8527, Japan
[b] Graduate School of Informatics, Kyoto University, Kyoto 606-8501, Japan
[c] Faculty of Science and Engineering, University of Groningen, Groningen, 9747 AG, The Netherlands

ARTICLE INFO

Article history:
Received 12 June 2020
Received in revised form 21 September 2020
Accepted 22 December 2020
Available online 15 February 2021

Keywords:
Differential privacy
Privacy limits
Discrete-time linear systems
Modular design
Tracking control

ABSTRACT

In privacy-preserving controller design, there is usually a trade-off between the privacy level and control performances, and we show in this paper that this trade-off in particular determines a lower bound on the differential privacy level of the closed-loop system. The control task we consider is reference tracking in a plug-and-play setting, and the plant under control is a networked system of modules, each of which has no access to the models of the others. For a module, we first identify the whole set of tracking local controllers based on the Youla parametrization. At the same time, each module, to protect its own privacy, tries to prevent the other interconnected modules to identify its private information; in this context, for example, the tracking reference signal (say, the target production amount if each module is a workshop in a factory) can be viewed as a piece of private information. Each module can tune the parameters of its local controller to increase the privacy level of its reference signal. However, if the distribution of Laplace (resp. uniform) noise is fixed, the differential privacy level of a Laplace (resp. uniform) mechanism cannot be further improved from a ceiling value no matter how one tunes parameters. In other words, for modular systems under local reference tracking control, there is a lower bound on the differential privacy level.

1. Introduction

In the beginning, statistical disclosure control technologies for protecting private data have been developed for static data; see e.g. Dwork, Kenthapadi, McSherry, Mironov and Naor (2006), Dwork, McSherry, Nissim and Smith (2006) and Willenborg and De Waal (1996, 2012). Later on, partly motivated by the fact that private data generated by IoT technologies are sometimes outputs of dynamic processes as modules, privacy has started to be studied in the context of dynamical systems, and privacy protection is gradually becoming an active research topic in systems and control communities; see e.g. recent publications (Cortés et al., 2016; Farokhi & Sandberg, 2019) and references therein. It is well known that there is in general a trade-off between data utility and privacy protection; however, such trade-offs have not been adequately quantitatively investigated.

In a networked system of modules, e.g. those created through IoT technologies, the sharing of data generated by individual modules through the network may create the risk of private information of one module being inferred by other modules. On the other hand, sharing information is necessary when controllers for such modular network systems are designed since each module may only have part of the information that is needed. By considering these data privacy and network control problems at the same time, this paper aims at advancing the existing trade-off analysis one step further by focusing on the tracking problem of a module. In this context, the concept of *retrofit control* is proposed for characterizing a class of stabilizing local controllers with the Youla parametrization (Ishizaki, Kawaguchi, Sasahara, & Imura, 2019; Sasahara, Ishizaki, & Imura, 2019). By extending this method to tracking control, we provide the complete characterization of the local tracking controllers, which enables us to proceed with privacy analysis for all possible local tracking controllers. Even for stabilization, our result is more general than that of Ishizaki et al. (2019) in the sense that we provide a necessary and sufficient condition; in contrast, Ishizaki et al. (2019) give a sufficient condition.

For the privacy issue, we consider a scenario where the reference signal (e.g. the target production amount) of a module is required to be private. As a privacy preserving data mining technique, we employ differential privacy (Dwork, Kenthapadi et al., 2006; Dwork, McSherry et al., 2006), where the main idea

[☆] This work was supported in part by JSPS, Japan KAKENHI under Grant JP18H01461, the European Research Council (ERC-CoG-771687) and the Dutch Organization for Scientific Research, The Netherlands (NWO-vidi-14134). The material in this paper was partially presented at the 21st IFAC World Congress (IFAC 2020), July 12–17, 2020, Berlin, Germany. This paper was recommended for publication in revised form by Associate Editor Linda Bushnell under the direction of Editor Sophie Tarbouriech.

[*] Corresponding author.
E-mail addresses: ykawano@hiroshima-u.ac.jp (Y. Kawano), kk@i.kyoto-u.ac.jp (K. Kashima), m.cao@rug.nl (M. Cao).

https://doi.org/10.1016/j.automatica.2021.109518
0005-1098/

is to add noise to signals before sending them to other modules for making the estimation of the reference difficult from those sent data. Given that differential privacy has been employed in dynamical settings (Hale & Egerstedt, 2017; Han, Topcu, & Pappas, 2017; He & Cai, 2016; Huang, Mitra, & Vaidya, 2015; Ito, Kawano, & Kashima, 2021; Kawano & Cao, 2020; Le Ny & Mohammady, 2018; Le Ny & Pappas, 2014; Yazdani, Jones, Leahy, & Hale, 2018), the main advance of this paper is to show that for both Laplace and uniform mechanisms, lower bounds on the differential privacy levels can be constructed for given i.i.d. Laplace and uniform distributions. That is, given distributions, there are ceiling values for the differential privacy levels to be achieved by tuning the parameters in general. It is worth mentioning that these results are obtained based on necessary and sufficient conditions proven in this paper for the differential privacy of Laplace and uniform mechanisms, where the condition for the Laplace mechanism without the proof can be found in the preliminary conference version (Kawano, Kashima, & Cao, 2020). In most of differential privacy analysis, only sufficient conditions have been studied.

As relevant researches, Le Ny and Mohammady (2018) and Le Ny and Pappas (2014) provide ways to publish output data while protecting the private state or input data of dynamical systems, and Kawano and Cao (2020) analyze differential privacy in terms of observability and proposes a control design methodology while guaranteeing privacy of the plant data. The paper (Yazdani et al., 2018) designs a cloud-based LQ controller while protecting the privacy of the state of each agent against the cloud. The privacy protecting methods in these four papers mainly rely on adding the Gaussian noise, and some results for differential privacy analysis in Kawano and Cao (2020) are extended to the case of using a stable distribution. None of Kawano and Cao (2020), Le Ny and Mohammady (2018) and Le Ny and Pappas (2014) mathematically investigates the trade-offs between filtering/control and privacy performances. The paper (Yazdani et al., 2018) provides a sufficient condition for differential privacy for given cost functions; however, even with the help of this sufficient condition, it is difficult to derive a lower bound on the differential privacy level to be achieved by tuning cost functions. Some works (Han et al., 2017; He & Cai, 2016; Huang et al., 2015; Wang, Huang, Mitra, & Dullerud, 2017) have studied the trade-offs between differential privacy and optimality in distributed optimizations, but the problem formulations are fundamentally different from what is studied in this paper; in particular, these papers do not analyze ceiling values for the differential privacy levels.

A preliminary conference version of this work can be found in Kawano et al. (2020). The main contributions of this paper is then for MIMO systems, the finding of a necessary and sufficient condition for tracking control (the conference version only gives a conservative sufficient condition for more restrictive classes of systems), the analysis of the uniform mechanism, and computing the tracking error under each noise. The uniform mechanism involving the dynamical system has not been studied before to our best knowledge. In addition, we show that the proposed lower bounds are tight for positive systems, which implies that the constructed lower bounds are not conservative.

The remainder of this paper is organized as follows. In Section 2, we formulate a tracking control problem in the context of modular control design and provide the class of tracking local controllers for a constant reference. In Section 3, we estimate the ceiling levels of the differential privacy for Laplace and uniform mechanisms. Section 4 illustrates our results by an example of tracking the prescribed power supply in a DC microgrid while keeping the electricity consumption of each user private. Concluding remarks are given in Section 5.

Notations: The sets of real numbers, non-negative integers, and positive integers are denoted by $\mathbb{R}$, $\mathbb{Z}_{\geq 0}$, and $\mathbb{Z}_{>0}$, respectively. For the sequence $u : \mathbb{Z}_{\geq 0} \to \mathbb{R}^m$, a vector consisting of its subsequence is denoted by $u_t := [u^\top(0) \ \cdots \ u^\top(t)]^\top \in \mathbb{R}^{(t+1)m}$. Both the vector q-norm and matrix norm induced by the vector q-norm are denoted by $|\cdot|_q$ for $q \in \mathbb{Z}_{>0} \cup \{\infty\}$. For a sequence, its q-norm is denoted by $\|\cdot\|_q$. A sequence $u : \mathbb{Z}_{\geq 0} \to \mathbb{R}^m$ is said to belong to $L_q^m[0,\infty)$ if $\|u\|_q$ is bounded. The set of stable, proper, and rational transfer function matrices is denoted by $\mathcal{RH}_\infty$.

Let $\nu \in \mathbb{R}^n$ be an i.i.d. random variable with mean zero. The Laplace distribution with the variance $2b^2$ ($b > 0$) has the following probability density:

$$p(\nu; b) = \frac{1}{(2b)^n} \mathrm{e}^{-\frac{|\nu|_1}{b}}.$$

The uniform distribution on $[-d/2, d/2]^n$ ($d > 0$) has the following probability density:

$$p(\nu; d) = \begin{cases} \dfrac{1}{d^n} & \text{if } \nu \in [-d/2, d/2]^n \\ 0 & \text{otherwise,} \end{cases}$$

and the variance is $d^2/12$.

2. Tracking control for modules

2.1. Problem formulation

In this section, we formulate a tracking control problem of interconnected systems in the framework of retrofit control proposed by Ishizaki et al. (2019). Consider the following discrete-time linear system:

$$\begin{bmatrix} w \\ y \end{bmatrix} = \underbrace{\begin{bmatrix} G_{w,v}(z) & G_{w,u}(z) \\ G_{y,v}(z) & G_{y,u}(z) \end{bmatrix}}_{=:G(z)} \begin{bmatrix} v \\ u \end{bmatrix} \tag{1}$$

that we call a local plant. This local plant as a module is influenced by other modules through the signal v as shown in Fig. 1:

$$v = \mathbf{G_{v,w}}(z) w. \tag{2}$$

The transfer function matrix of the interconnected system from u to y is

$$\mathbf{G_{pre}} := G_{y,u} + G_{y,v}\mathbf{G_{v,w}}(I - G_{w,v}\mathbf{G_{v,w}})^{-1}G_{w,u}, \tag{3}$$

where the argument z is omitted hereafter. Suppose that $\mathbf{G_{pre}}$ is internally stable. This is a natural assumption for real-life systems including factories and power systems having a stable functioning mode.

For controlling interconnected systems, it can happen that only one module needs to be updated for improving its control performance or satisfying an additional control requirement. Such an update can be done by implementing a local controller in this module. However, such a module may not always be able to access the model information $\mathbf{G_{v,w}}$ of the other modules. For instance, another module may belong to a different provider or management party which can implement its own local controller. Therefore, a local controller is required to be designed without knowing $\mathbf{G_{v,w}}$. This is a standard assumption in decentralized control. On the other hand, implementing a local controller can destroy the internal stability of the overall interconnected system. For instance, consider a local controller $u = K_y y + \delta u$. Then, the transfer function matrix from $\delta u \to y$ becomes $(I + \mathbf{G_{pre}}K_y)^{-1}\mathbf{G_{pre}}$. Without knowing $\mathbf{G_{v,w}}$, the gain K_y needs to be designed such that the internal stability of the interconnected system is preserved.

As a control objective, we consider tracking control, i.e., $\lim_{t\to\infty}(y(t) - r(t)) = 0$ for the given reference signal r. Since the local plant can access the signals v, w, u, and y, these signals

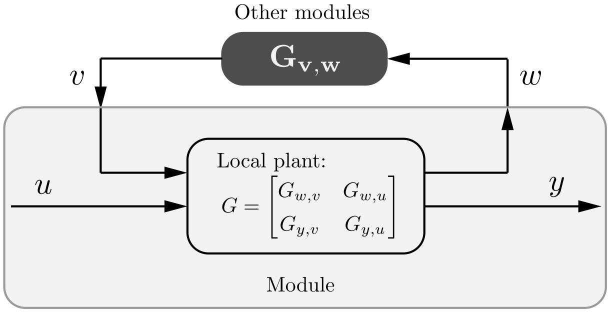
Other modules
$\mathbf{G_{v,w}}$
v
w
u
y
Local plant:
$G = \begin{bmatrix} G_{w,v} & G_{w,u} \\ G_{y,v} & G_{y,u} \end{bmatrix}$
Module

Fig. 1. Interconnection of G and $\mathbf{G_{v,w}}$.

are available for controller design in contrast to $\mathbf{G_{v,w}}$. That is, a local controller can be described as

$$u = \underbrace{\begin{bmatrix} K_y(z) & K_w(z) & K_v(z) \end{bmatrix}}_{=:K(z)} \begin{bmatrix} y-r \\ w \\ v \end{bmatrix}. \tag{4}$$

In summary, the entire system can be illustrated by Fig. 2, and we study the following tracking problem.

Problem 2.1. Let G in (1) be given and internally stable. Find the class of local controllers K in the form of (4), which achieves $y(t) - r \to 0$ as $t \to \infty$ for an arbitrary constant reference $r \in \mathbb{R}^m$ while keeping the internal stability of the entire system in Fig. 2 for each $\mathbf{G_{v,w}} \in \mathcal{G}_{v,w} := \{\mathbf{G_{v,w}} : \mathbf{G_{pre}} \text{ is internally stable}\}$. ◁

In Ishizaki et al. (2019), a specific class of stabilizing local controllers (namely controllers solving Problem 2.1 for $r = 0$) has been provided based on the Youla parametrization in the continuous-time problem setting; such controllers are called output-rectifying retrofit controllers. As Ishizaki et al. (2019), this paper assumes the internal stability of G to avoid unnecessary complication of controller parametrization; this assumption can be relaxed via a doubly coprime factorization, see e.g., Sasahara et al. (2019). In the next subsection, we generalize the results of Ishizaki et al. (2019) to solve Problem 2.1.

Recently, other parametrizations than the Youla parametrization have been proposed for describing the set of all stabilizing controllers (Furieri, Zheng, Papachristodoulou, & Kamgarpour, 2019; Wang, Matni, & Doyle, 2019) and are shown to be all equivalent (Furieri et al., 2019; Zheng, Furieri, Papachristodoulou, Li, & Kamgarpour, 2020). Note that the equivalence to the parametrization in Wang et al. (2019) is analyzed when the feed-though term is zero, while this assumption is not imposed in this paper. In our problem setting, the so-called input–output parametrization (IOP) in Furieri et al. (2019) can also be used to obtain an equivalent condition for the solvability of Problem 2.1 as explained later. In this paper, to utilize some existing results on retrofit control (Ishizaki et al., 2019; Sasahara et al., 2019), we employ the Youla parametrization for solving Problem 2.1.

2.2. Local controller design

To proceed with local controller design, let $G_{(y,w,v),v}$ (resp. $G_{(y,w,v),u}$) denote the transfer function matrix of the system in Fig. 1 from v (resp. u) to (y, w, v), i.e.,

$$G_{(y,w,v),v} := \begin{bmatrix} G_{y,v} \\ G_{w,v} \\ I \end{bmatrix}, \quad G_{(y,w,v),u} := \begin{bmatrix} G_{y,u} \\ G_{w,u} \\ 0 \end{bmatrix}.$$

From the internal stability of G, the Youla parametrization gives the class of all stabilizing controllers as follows:

$$K = (I + QG_{(y,w,v),u})^{-1}Q, \tag{5}$$

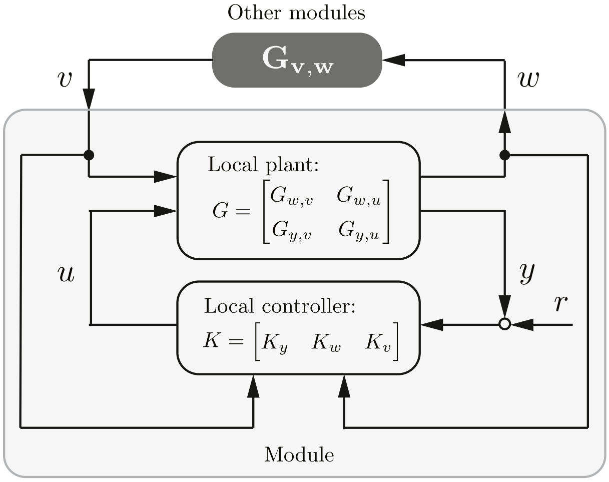
Other modules
$\mathbf{G_{v,w}}$
v
w
Local plant:
$G = \begin{bmatrix} G_{w,v} & G_{w,u} \\ G_{y,v} & G_{y,u} \end{bmatrix}$
u
y
r
Local controller:
$K = \begin{bmatrix} K_y & K_w & K_v \end{bmatrix}$
Module

Fig. 2. Entire system after local controller K is implemented.

$$Q := \begin{bmatrix} Q_y & Q_w & Q_v \end{bmatrix} \in \mathcal{RH}_\infty.$$

From tracking and internal stability requirements, constraints are imposed to Q as follows.

Theorem 2.2. *A local controller (5) solves Problem 2.1 if and only if $Q \in \mathcal{RH}_\infty$ satisfies*

$$G_{w,u}QG_{(y,w,v),v} = 0 \tag{6}$$

and

$$I + \bar{\mathbf{G}}_{\mathbf{y,r}}(1)Q_y(1) = 0, \tag{7}$$

where

$$\bar{\mathbf{G}}_{\mathbf{y,r}} := G_{y,u} + (G_{y,v} + G_{y,u}QG_{(y,w,v),v})(I - \mathbf{G_{v,w}}G_{w,v})^{-1}\mathbf{G_{v,w}}G_{w,u}. \tag{8}$$

Proof. The proof is given in Appendix A.1. □

If (7) has a solution $Q_y(1)$, one can always construct at least a $Q \in \mathcal{RH}_\infty$ satisfying (6) and (7), namely a local controller achieving tracking control. Otherwise, tracking control is infeasible. For the sake of illustration, we introduce a matrix $\bar{Q}_y$ whose size is the same as that of $Q_y(1)$. First, we solve a matrix equation corresponding to (7), i.e. $I + \bar{\mathbf{G}}_{\mathbf{y,r}}(1)\bar{Q}_y = 0$ with respect to $\bar{Q}_y$, where one can check its solvability. If it has a solution $\bar{Q}_y$, we can find $Q_y \in \mathcal{RH}_\infty$ satisfying $Q_y(1) = \bar{Q}_y$. For instance, such a Q_y is $Q_y = \bar{Q}_y/z$. Next, by using the block elements of $G_{(y,w,v),v}$ and Q, Eq. (6) can be rewritten as

$$G_{w,u}(G_{y,v}Q_y + G_{w,v}Q_w + Q_v) = 0.$$

Therefore, for arbitrary $Q_y \in \mathcal{RH}_\infty$ and $Q_w \in \mathcal{RH}_\infty$, (6) is satisfied by choosing Q_v as $Q_v = -(G_{y,v}Q_y + G_{w,v}Q_w)$. Note that $Q_v \in \mathcal{RH}_\infty$ because of $G_{y,v}, G_{w,v} \in \mathcal{RH}_\infty$.

Although the constraints (6) and (7) can be described in terms of K, a condition corresponding to (5) in terms K is not clear. Therefore, to obtain the complete characterization of K solving Problem 2.1, we employ the Youla parametrization. On the other hand, the controller (5) can be rewritten as

$$K = X^{-1}Q,$$

where X is a solution to

$$\begin{bmatrix} X & Q \end{bmatrix} \begin{bmatrix} I \\ -G_{(y,w,v),v} \end{bmatrix} = I. \tag{9}$$

This is in essence an IOP. All conditions (6), (7), and (9) are linear with respect to parameters $Q \in \mathcal{RH}_\infty$ and X or the value of Q at

$z = 1$. IOP enables us to formulate controller design as a convex optimization problem. For unstable systems, controller design by IOP can be done without computing doubly coprime factorization in contrast to the Youla parametrization (Furieri et al., 2019). This fact can be used to simplify retrofit control design for unstable systems. However, this is not the main interest of this paper because the results on privacy analysis do not depend on the methods for parametrizing the set of controllers.

Remark 2.3. Even when $r = 0$, Theorem 2.2 is more general than (Ishizaki et al., 2019, Proposition 2.2) because $QG_{(y,w,v),v} = 0$ is required instead of (6). If $QG_{(y,w,v),v} = 0$ (or weakly $G_{y,u}QG_{(y,w,v),v} = 0$), then $\bar{\mathbf{G}}_{\mathbf{y},\mathbf{r}}$ becomes the following $\hat{\mathbf{G}}_{\mathbf{y},\mathbf{r}}$,

$$\hat{\mathbf{G}}_{\mathbf{y},\mathbf{r}} := G_{y,u} + G_{y,v}(I - \mathbf{G}_{\mathbf{v},\mathbf{w}}G_{w,v})^{-1}\mathbf{G}_{\mathbf{v},\mathbf{w}}G_{w,u}. \tag{10}$$

Note that $\hat{\mathbf{G}}_{\mathbf{y},\mathbf{r}}$ does not depend on tuning parameters Q anymore. Moreover, if $\mathbf{G}_{\mathbf{v},\mathbf{w}}$ is square and satisfies

$$(I - \mathbf{G}_{\mathbf{v},\mathbf{w}}G_{w,v})^{-1}\mathbf{G}_{\mathbf{v},\mathbf{w}} = \mathbf{G}_{\mathbf{v},\mathbf{w}}(I - \mathbf{G}_{\mathbf{v},\mathbf{w}}G_{w,v})^{-1},$$

then $\hat{\mathbf{G}}_{\mathbf{y},\mathbf{r}} = \mathbf{G}_{\mathbf{pre}}$; recall (3). Therefore, the tracking condition (7) reduces to

$$I + \mathbf{G}_{\mathbf{pre}}(1)Q_y(1) = 0 \tag{11}$$

that is the MIMO version of the condition obtained in the preliminary version (Kawano et al., 2020). In the SISO case, (6) and $QG_{(y,w,v),v} = 0$ are equivalent. In this case, the condition (11) is directly derived without introducing the transfer function matrix $\bar{\mathbf{G}}_{\mathbf{y},\mathbf{r}}$ in contrast to (7). This is an example of that considering the SISO case simplifies the whole analysis. ◁

One notices that from (3), tracking controller design requires the information of $\mathbf{G}_{\mathbf{v},\mathbf{w}}(1)$ although $\mathbf{G}_{\mathbf{v},\mathbf{w}}(z)$ is not available for local controller design. Sharing only the information of $\mathbf{G}_{\mathbf{v},\mathbf{w}}(1)$ may not be that difficult. Even if this information is not shared, it can be estimated by adding constant inputs $w(t) = c$, $t \in \mathbb{Z}_{\geq 0}$. For instance, when v and w are scalar, an approximation of the DC gain is obtained as

$$\mathbf{G}_{\mathbf{v},\mathbf{w}}(1) = \lim_{t\to\infty}\frac{v(t)}{c} \simeq \frac{v(\bar{t})}{c}$$

for sufficiently large $\bar{t} \in \mathbb{Z}_{\geq 0}$.

The condition (7) can be extended to an arbitrary reference $r(t)$ for which the final value theorem is available. If $\lim_{t\to\infty} r(t)$ does not exist, the final value theorem is not applicable. However, an alternative condition can be derived based on the internal model principle (Levine, 2018).

3. Fundamental performance limits for privacy protection

In the previous section, we have provided a condition for tracking control of each local plant in a decentralized control setting. Decentralized control has advantages in view of privacy preservation because the local plant does not need to share information of the local controller (i.e. control algorithms) and reference r (e.g. a target produced amount) with the other modules $\mathbf{G}_{\mathbf{v},\mathbf{w}}$. However, there is still a possibility that the owner(s) of $\mathbf{G}_{\mathbf{v},\mathbf{w}}$ estimates the reference r from the signal w it receives. In this section, our objective is to design the local controller which makes estimating r difficult, i.e. r is highly private against the owner(s) of $\mathbf{G}_{\mathbf{v},\mathbf{w}}$. As a criterion for privacy, we employ differential privacy proposed by Dwork, Kenthapadi et al. (2006) and Dwork, McSherry et al. (2006), which has been applied to state–space representations of dynamical systems; see e.g. Ito et al. (2021), Kawano and Cao (2020) and Le Ny and Pappas (2014). In this section, we proceed with differential privacy analysis by using state–space models.

3.1. State–space models

Suppose that a controller satisfying the conditions in Theorem 2.2 is implemented. From (2) and (A.2), the transfer function matrix from r to w of the entire system is computed as

$$w = -(I - G_{w,v}\mathbf{G}_{\mathbf{v},\mathbf{w}})^{-1}G_{w,u}Q_y r. \tag{12}$$

Note that this is internally stable.

Proposition 3.1. *The transfer function matrix from r to w in (12) is internally stable.*

Proof. From the assumption in Problem 2.1, the transfer function matrix from u to w of the interconnected system in Fig. 1 is internally stable. By using (1) and (2), the transfer function matrix can be computed as

$$w = (I - G_{w,v}\mathbf{G}_{\mathbf{v},\mathbf{w}})^{-1}G_{w,u}u.$$

Therefore, $Q \in \mathcal{RH}_\infty$ concludes the statement of the proposition. □

For fixed Q_y, consider a minimal realization of (12), which can be computed by using for instance the Ho–Kalman algorithm (Ho & Kálmán, 1966).

$$\Sigma_{w,r} : \begin{cases} x(t+1) = Ax(t) + Br(t), \ x(0) = 0, \\ w(t) = Cx(t) + Dr(t) \end{cases} \tag{13}$$

for $t \in \mathbb{Z}_{\geq 0}$, where $x(t) \in \mathbb{R}^n$, $r(t) \in \mathbb{R}^m$, and $w(t) \in \mathbb{R}^p$ denote the state, input (reference signal), and output, respectively, and $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$, $C \in \mathbb{R}^{p\times n}$, and $D \in \mathbb{R}^{p\times m}$. From Proposition 3.1, this system is Schur stable. Now, we consider the output sequence $w_t \in \mathbb{R}^{(t+1)p}$ of the system (13) with the zero initial state, where the meaning of the subscript t was defined in the notation section. This can be described by

$$w_t = H_t r_t, \tag{14}$$

where $H_t \in \mathbb{R}^{(t+1)p\times(t+1)m}$ is

$$H_t := \begin{bmatrix} D & 0 & \cdots & \cdots & 0 \\ CB & D & \ddots & & \vdots \\ CAB & CB & D & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ CA^{t-1}B & CA^{t-2}B & \cdots & CB & D \end{bmatrix}.$$

Throughout this section, we assume that $H_t \neq 0$; if $H_t = 0$, then $w_t = 0$, and it becomes unnecessary to discuss the privacy of r_t.

For the sake of later analysis, we introduce the q-induced norm ($q \in \mathbb{Z}_{>0} \cup \{\infty\}$) of the system (13),

$$\|\Sigma_{w,r}\|_{q-\text{ind}} := \sup_{\substack{r\in L_q^m[0,\infty) \\ \|r\|_q\neq 0}} \frac{\|w\|_q}{\|r\|_q} = \sup_{t\in\mathbb{Z}_{\geq 0}} |H_t|_q, \tag{15}$$

where the last equality follows from the definition (14) of H_t. Since the system (13) is Schur stable, the induced q-norm is bounded for any $q \in \mathbb{Z}_{>0} \cup \{\infty\}$.

3.2. Differential privacy

In this subsection, we give the definition of differential privacy. Although differential privacy is mainly used for analysis of aggregated data, the criterion for evaluating the privacy level itself is available for our problem. One of the main ideas of differential privacy is to add noise ν to the output w for increasing the difficulty of estimating r. That is, instead of w, the local plant sends the following w_ν to $\mathbf{G_{v,w}}$:

$$w_\nu(t) = w(t) + \nu(t), \ t \in \mathbb{Z}_{\geq 0}. \tag{16}$$

For the zero initial state, the system (13) with the new output (16) induces the mapping $\mathcal{M} : \mathbb{R}^{(t+1)m} \times \mathbb{R}^{(t+1)p} \ni (r_t, \nu_t) \mapsto w_{\nu,t} \in \mathbb{R}^{(t+1)p}$; recall the notation of the sequence. In differential privacy analysis, this mapping is called a *mechanism* (Dwork, Kenthapadi et al., 2006; Dwork, McSherry et al., 2006).

Differential privacy gives an index of the privacy level of a mechanism, which is characterized by the sensitivity of published output data $w_{\nu,t}$ with respect to input data r_t. More specifically, if for a pair of not so distinct input data (r_t, r'_t), the corresponding pair of output data $(w_{\nu,t}, w'_{\nu,t})$ is very different, then input data r_t is easy to estimate, i.e. the mechanism is less private. For such a reason, differential privacy is defined by using a pair of different but "similar" input data, where by similar we mean that the pair satisfies the following adjacency relations.

Definition 3.2. Given $c > 0$ and $p \in Z_{>0} \cup \{\infty\}$, a pair of input data $(r_t, r'_t) \in \mathbb{R}^{(t+1)m} \times \mathbb{R}^{(t+1)m}$ (resp. $(r, r') \in L^m_q[0, \infty) \times L^m_q[0, \infty)$) is said to belong to the binary relation c-adjacency under the q-norm if $|r_t - r'_t|_q \leq c$ (resp. $\|r - r'\|_q \leq c$). The set of all pairs of the input data that are c-adjacent under the q-norm is denoted by Adj^c_q. ◁

Now, we are ready to define differential privacy of the mechanism proposed by Dwork, Kenthapadi et al. (2006) and Dwork, McSherry et al. (2006).

Definition 3.3. The mechanism (induced by (13) and (16)) is said to be (ε, δ)-*differentially private* for Adj^c_q at $t \in \mathbb{Z}_{\geq 0}$ if there exist $\varepsilon, \delta \geq 0$ such that

$$\mathbb{P}(w_{\nu,t} \in S) \leq \mathrm{e}^{\varepsilon}\mathbb{P}(w'_{\nu,t} \in S) + \delta \tag{17}$$

for all sets S of outputs and for any $(r_t, r'_t) \in \mathrm{Adj}^c_q$. If δ (resp. ε) is zero, the mechanism is simply said to be ε-differentially (resp. δ-differentially) private. ◁

If ε and δ are small, then for a different pair of input data (r_t, r'_t), the corresponding pair of probability distributions of output data $(w_{\nu,t}, w'_{\nu,t})$ is small, i.e., a mechanism is highly private. Therefore, the privacy level of a mechanism is evaluated by the variables ε and δ.

3.3. Privacy limits of Laplace mechanisms

From the definition, the variables ε and δ can depend on noise ν. In other words, noise ν needs to be designed based on the required differential privacy level. In this subsection, we consider adding i.i.d. Laplace noise; the corresponding mechanism is called the *Laplace mechanism*. For the Laplace mechanism, a sufficient condition for differential privacy has been proposed; see, e.g., Dwork, Kenthapadi et al. (2006), Dwork, McSherry et al. (2006) and Le Ny and Pappas (2014). However, for our analysis, we need a necessary condition. In fact, a necessary and sufficient condition can be established based on an existing sufficient condition (Le Ny & Pappas, 2014, Theorem 2).

Theorem 3.4. *Consider the i.i.d. Laplace noise with the variance $2b^2$. The Laplace mechanism is ε-differentially private for Adj^c_1 at $t \in \mathbb{Z}_{>0}$ ($t \in \mathbb{Z}_{\geq 0}$ when $D \neq 0$) if and only if $b > 0$ is chosen such that*

$$b \geq \frac{c}{\varepsilon}|H_t|_1. \tag{18}$$

Proof. The proof is given in Appendix A.2. □

Remark 3.5. In this section, we assume that the owner(s) of $\mathbf{G_{v,w}}$ does not know whether the reference r is constant. If the reference is known to be constant, then the condition (18) is replaced by

$$b \geq \frac{c}{\varepsilon}|H_t \mathbb{1}|_1, \tag{19}$$

where $\mathbb{1}$ is the vector whose all elements are one, and c-adjacency means $|r - r'| \leq c$ for constants r and r'. Note that b satisfying (19) is larger than that of (18) in general because $|H_t \mathbb{1}|_1$ is not a bounded function of t in contrast to $|H_t|_1$ even if the system (13) is Schur stable. This corresponds to the natural observation: it is more difficult to protect r when r is known to be constant. ◁

In Theorem 3.4, the system (13) is not necessarily Schur stable because a fixed and bounded time-interval is considered. If we require the Laplace mechanism to be differentially private for any time-interval, Schur stability is required.

Corollary 3.6. *Consider the i.i.d. Laplace noise with the variance $2b^2$. The Laplace mechanism is ε-differentially private for Adj^c_1 at any $t \in \mathbb{Z}_{\geq 0}$ if and only if $b > 0$ is chosen such that*

$$b \geq \frac{c}{\varepsilon}\|\Sigma_{w,r}\|_{1-\mathrm{ind}}. \tag{20}$$

Proof. First, we show the necessity. From (15), for any $\bar{a} > 0$, there exists $t \in \mathbb{Z}_{\geq 0}$ such that $|H_t|_1 \geq \|\Sigma_{w,r}\|_{1-\mathrm{ind}} - \bar{a}$. From Theorem 3.4, if the Laplace mechanism is ε-differentially private at this t, then

$$b \geq \frac{c}{\varepsilon}|H_t|_1 \geq \frac{c}{\varepsilon}\|\Sigma_{w,r}\|_{1-\mathrm{ind}} - a, \ \ a := \frac{\bar{a}c}{\varepsilon}.$$

Since $\bar{a} > 0$ (or equivalently $a > 0$) is arbitrary, we have (20).

Next, we show the sufficiency. From (15), it follows that $|H_t|_1 \leq \|\Sigma_{w,r}\|_{1-\mathrm{ind}}$ for any $t \in \mathbb{Z}_{\geq 0}$. Therefore, from Theorem 3.4, if (20) holds, the Laplace mechanism is ε-differentially private for any $t \in \mathbb{Z}_{\geq 0}$. □

From (20), for fixed c and $\|\Sigma_{w,r}\|_{1-\mathrm{ind}}$, one may conclude naturally that adding large noise ν increases the differential privacy level ε. However, adding noise degenerates control performances, which is specified by the following proposition.

Proposition 3.7. *Let $\Sigma_{y,\nu}$ denote a minimal realization of the transfer function matrix of the whole system from ν to y. For the i.i.d. Laplace noise ν with the variance $2b^2$, the tracking error $y - r$ satisfies*

$$\lim_{t \to \infty} \mathbb{E}[|y(t) - r(t)|^2] = 2b^2\|\Sigma_{y,\nu}\|_{2-\mathrm{ind}}. \tag{21}$$

Proof. The proof is given in Appendix A.3. □

From Corollary 3.6 and Proposition 3.7, one sees clearly the trade-off between differential privacy and tracking control performances. If one chooses the minimum b to achieve ε-differential privacy, the equality in (20) yields

$$\lim_{t \to \infty} \mathbb{E}[|y(t) - r(t)|^2] = 2\left(\frac{c}{\varepsilon}\|\Sigma_{w,r}\|_{1-\mathrm{ind}}\right)^2 \|\Sigma_{y,\nu}\|_{2-\mathrm{ind}}.$$

Therefore, the differential privacy level can be decided by evaluating the utility guarantee of the tracking control performance. To utilize this evaluation, the induced norms $\|\Sigma_{w,r}\|_{1-\mathrm{ind}}$ and $\|\Sigma_{y,\nu}\|_{2-\mathrm{ind}}$ are needed to be estimated, since $\mathbf{G_{v,w}}$ is unknown. It may not be difficult to estimate their upper bounds although the resulting evaluation with these upper bounds becomes conservative. If one designs b based on (19) instead of (18), conservativeness is reduced, since $H_t \mathbb{1}$ can be estimated in arbitrary accuracy.

Note that not only the variance of the Laplace noise is a tuning parameter. The 1-induced norm of the system (13) denoted by $\|\Sigma_{w,r}\|_{1-\mathrm{ind}}$ can be specified by tuning the free controller parameter Q_y. From (12), $\|\Sigma_{w,r}\|_{1-\mathrm{ind}}$ can be made arbitrarily small by making Q_y arbitrarily small even though $\mathbf{G_{v,w}}$ is unknown. However, as clarified in Theorem 2.2, the tracking control requirement of a module imposes the constraints (6) and (7) for Q. Because of them, the parameter Q_y cannot be made arbitrarily small in general. Therefore, in general, given the variance $2b^2$, the differential privacy level ε of the Laplace mechanism cannot be improved from the ceiling value even if one tunes the controller parameters Q. In the special case when $G_{y,u}QG_{(y,w,v),v} = 0$, the limit can be estimated explicitly as follows.

Theorem 3.8. *Consider the i.i.d. Laplace noise with Q solving Problem 2.1. Suppose that Q_y is square, and Q satisfies $G_{y,u}Q\,G_{(y,w,v),v} = 0$. If given variance $2b^2$ and Adj_1^c, the Laplace mechanism is ε-differentially private, then it holds that*

$$\varepsilon \geq \frac{c}{b}\left|(I - G_{w,v}(1)\mathbf{G_{v,w}}(1))^{-1}G_{w,u}(1)\hat{\mathbf{G}}_{\mathbf{y,r}}^{-1}(1)\right|_1. \tag{22}$$

Proof. From the definition of the 1-induced norm of the system, the DC gain gives its lower bound,

$$\|\Sigma_{w,r}\|_{1-\mathrm{ind}} \geq |C(I-A)^{-1}B + D|_1.$$

Since (13) is a state–space representation of (12), we obtain

$$C(I-A)^{-1}B + D = -(I - G_{w,v}(1)\mathbf{G_{v,w}}(1))^{-1}G_{w,u}(1)Q_y(1).$$

Next, the assumptions for Q imply that (7) holds for $\bar{\mathbf{G}}_{\mathbf{y,r}} = \hat{\mathbf{G}}_{\mathbf{y,r}}$, where $\hat{\mathbf{G}}_{\mathbf{y,r}}$ is defined in (10). Thus, Q_y needs to satisfy

$$Q_y(1) = -\hat{\mathbf{G}}_{\mathbf{y,r}}^{-1}(1).$$

By combining the above, we have

$$\|\Sigma_{w,r}\|_{1-\mathrm{ind}} \geq \left|(I - G_{w,v}(1)\mathbf{G_{v,w}}(1))^{-1}G_{w,u}(1)\hat{\mathbf{G}}_{\mathbf{y,r}}^{-1}(1)\right|_1.$$

Therefore, (22) is obtained from (20). □

Theorem 3.8 implies that given variance $2b^2$ and c, the differential privacy level ε cannot be made smaller than the value given by the right-hand side of (22) for any Q satisfying the conditions. It is worth emphasizing that this lower bound can be computed only by estimating the value of $\mathbf{G_{v,w}}(z)$ at $z = 1$. As mentioned at the paragraph immediately after Remark 2.3, this may not be that difficult. From Remark 3.5, the lower bound can be larger if r is known to be constant.

Remark 3.9. From (21), one may think that tracking control performance can be made less degenerated against noise ν if $\|\Sigma_{y,\nu}\|_{2-\mathrm{ind}}$ is made arbitrary small. From (2) and (A.1), the transfer function matrix from ν to y is obtained as

$$y = (G_{y,v} + G_{y,u}QG_{(y,w,v),v})(I - \mathbf{G_{v,w}}G_{w,v})^{-1}\mathbf{G_{v,w}}\nu.$$

Therefore, $\|\Sigma_{y,\nu}\|_{2-\mathrm{ind}}$ can be specified by tuning Q. However, as for the differential privacy level ε, the constraints (6) and (7) can give a lower bound on $\|\Sigma_{y,\nu}\|_{2-\mathrm{ind}}$. ◁

Remark 3.10. When each signal is scalar, from the definition (10) of $\hat{\mathbf{G}}_{\mathbf{y,r}}$, we have

$$(I - G_{w,v}\mathbf{G_{v,w}})^{-1}G_{w,u}\hat{\mathbf{G}}_{\mathbf{y,r}}^{-1} = \frac{G_{w,u}}{G_{y,u} + (G_{y,v}G_{w,u} - G_{y,u}G_{w,v})\mathbf{G_{v,w}}}. \tag{23}$$

If $G_{y,u}(1)G_{w,v}(1) = G_{y,v}(1)G_{w,u}(1)$, the condition (22) reduces to

$$\varepsilon \geq \frac{c}{b}\frac{G_{w,u}(1)}{G_{y,u}(1)}.$$

In this case, the lower bound on the differential privacy level is determined only by the local plant. On the other hand, if $\mathbf{G_{v,w}}$ is designed such that $G_{y,u} + (G_{y,v}G_{w,u} - G_{y,u}G_{w,v})\mathbf{G_{v,w}} = 0$, then (23) does not exist, and the condition (22) does not hold for any finite $\varepsilon \geq 0$. In this case, we have $\mathbf{G_{pre}} = 0$ from (3). This implies that if $\mathbf{G_{v,w}}$ is designed to make $\mathbf{G_{pre}}$ small, large noise is required to make r highly private. ◁

Remark 3.11. For positive systems, $\|\Sigma_{w,r}\|_{1-\mathrm{ind}} = |C(I-A)^{-1}B + D|_1$ can be shown in a similar manner as for SISO systems (Rantzer, 2011, Theorem 6). Therefore, for the positive system and b satisfying the equality in (20), the equality holds in (22), i.e., the lower bound (22) is tight. ◁

3.4. Privacy limits of uniform mechanisms

In the previous subsection, we have shown that for the Laplace mechanism, there exists the limit of the differential privacy level when achieving tracking control. As an evaluation of data utility, we have estimated the tracking error in the mean-square sense, but the worst-case error cannot be specified due to the structure of its probability distribution. In contrast, this is possible for the *uniform mechanism*, the mechanism obtained by adding noise following a uniform distribution. Furthermore, we will obtain in this sub-section similar conclusions for a differential privacy level and mean-square tracking error.

The differential privacy of the uniform mechanism has been studied (Geng, Ding, Guo, & Kumar, 2018; He & Cai, 2016) for scalar static data, but not in a dynamical setting. First, we provide a necessary and sufficient condition for differential privacy.

Theorem 3.12. *Consider the i.i.d. noise with uniform distribution on $[-d/2, d/2]$. The uniform mechanism is δ-differentially private for Adj_∞^c at $t \in \mathbb{Z}_{>0}$ ($t \in \mathbb{Z}_{\geq 0}$ when $D \neq 0$) if and only if $d > 0$ is chosen such that*

$$d \geq \frac{c}{\delta}|H_t|_\infty. \tag{24}$$

Proof. The proof is given in Appendix A.4. □

Corollary 3.13. *Consider the i.i.d. noise with uniform distribution on $[-d/2, d/2]$. The uniform mechanism is δ-differentially private for Adj_∞^c at any $t \in \mathbb{Z}_{\geq 0}$ if and only if $d > 0$ is chosen such that*

$$d \geq \frac{c}{\delta}\|\Sigma_{w,r}\|_\infty.$$

Proof. The proof can be shown in a similar way as that of Corollary 3.6 based on Theorem 3.12. □

Remark 3.14. The definition of δ-differential privacy implies $\delta \leq 1$, and thus we implicitly assume $d \geq c|H_t|_\infty$ (resp. $d \geq c\|\Sigma_{w,r}\|_\infty$) in Theorem 3.12 (resp. Corollary 3.13). ◁

As for the Laplace mechanism, there is a trade-off between the privacy level and tracking control performances for the uniform mechanism. To see this, we provide the following proposition.

Proposition 3.15. *For the i.i.d. noise ν with uniform distribution on $[-d/2, d/2]$, the tracking error $y - r$ satisfies*

$$\lim_{t\to\infty}\mathbb{E}[|y(t) - r(t)|^2] = \frac{d^2}{12}\|\Sigma_{y,\nu}\|_{2-\mathrm{ind}}. \tag{25}$$

Proof. The proof is similar to that of Proposition 3.7, where the variance is $d^2/12$ for the considered noise here. □

From Corollary 3.13, to make the uniform mechanism highly differentially private (i.e., to make δ small), d needs to be large. From Proposition 3.15, this can cause a large tracking error. Therefore, we again here design a local controller such that the ∞-induced norm of the system (13) becomes small, which is another approach to increase the differential privacy level. However, again due to the constraint (7) for tracking control, the differential privacy level δ cannot be improved from the ceiling value in general.

As for Theorem 3.8, the limit can be estimated explicitly in a specific case.

Theorem 3.16. *Consider the i.i.d. noise with uniform distribution. Suppose that Q satisfies the assumptions in Theorem 3.8. If given interval $[-d/2, d/2]$ and Adj^c_∞, the uniform mechanism is differentially private, then*

$$\delta \geq \frac{c}{d} |(I - G_{w,v}(1)\mathbf{G}_{\mathbf{v},\mathbf{w}}(1))^{-1} G_{w,u}(1) \hat{\mathbf{G}}_{\mathbf{y},\mathbf{r}}(1)^{-1}|_\infty .$$

Proof. The proof is similar to that of Theorem 3.8. □

Remark 3.17. Again for the positive system, the lower bound obtained in Theorem 3.16 is tight because $\|\Sigma_{w,r}\|_{\infty-\mathrm{ind}} = |C(I-A)^{-1}B + D|_\infty$. This equality can be shown in a similar manner as for the SISO system (Rantzer, 2011, Theorem 6). ◁

4. Examples

4.1. Problem setting

Consider the DC microgrids (Cucuzzella et al., 2018) whose dynamics are described by

$$\begin{aligned} L_i \dot{I}_i(t) &= -R_i I_i(t) - V_i(t) + u_i(t), \\ C_i \dot{V}_i(t) &= I_i(t) - I_{L,i} - \sum_{j \in \mathcal{N}_i} R_{i,j}^{-1}(V_i(t) - V_j(t)), \\ y_i(t) &= I_i(t) \end{aligned} \tag{26}$$

for $i = 1, \dots, n$, where $I_i(t) \in \mathbb{R}$, $V_i(t) > 0$, and $u_i(t)$ denote the generator current, load voltage, and control input of node (i.e. module) i, respectively, and $I_{L,i} \in \mathbb{R}$ denote the load current of node i, which can be viewed as a constant in the time scale of controller design. The positive parameters L_i, R_i, $R_{i,j}(= R_{j,i})$, and C_i denote the inductance, resistances, and capacitance, respectively. The set of neighbors of node i is denoted by $\mathcal{N}_i$. Note that the subsystem of each node (with $V_j = 0$) and the whole interconnected system are Hurwitz.

The control objective is to maintain the stability of the system by keeping $V_i(t)$ to the prescribed value V^* and the difference between the generator and load currents to zero. Therefore, the control objective of each module i is

$$\lim_{t\to\infty} V_i(t) = V^*, \ \lim_{t\to\infty} I_i(t) = I_{L,i}. \tag{27}$$

In contrast to V^*, the consumption $I_{L,i}$ depends on each module i and contains information of consumption patterns. Therefore, this needs to be private against the other modules.

To simplify the local controller design process, we apply the changes of variables $\hat{I}_i = I_i - I_{L,i}$, $\hat{V}_i = V_i - V^*$, $\hat{y}_i = y_i - I_{L,i}$, and $\hat{u}_i = u_i - RI_{L,i} - V^*$. Then, (26) becomes

$$\begin{aligned} L_i \dot{\hat{I}}_i(t) &= -R_i \hat{I}_i(t) - \hat{V}_i(t) + \hat{u}_i(t), \\ C_i \dot{\hat{V}}_i(t) &= \hat{I}_i(t) - \sum_{j \in \mathcal{N}_i} R_{i,j}^{-1}(\hat{V}_i(t) - \hat{V}_j(t)), \\ \hat{y}_i(t) &= \hat{I}_i(t), \end{aligned} \tag{28}$$

and the control objective (27) becomes regulation, i.e., $r = 0$. Our objective is to design a local controller of node i for achieving regulation while increasing the differential privacy level of r (that is $I_{L,i}$ in the original coordinates), where the differential privacy level does not depend on the changes of variables.

4.2. Tracking controller design

For designing a local controller, we use the zero-order-hold discretization with the sampling period 10^{-3} [s], since each output information is collected and sent to the power company digitally. Note that the discretization of a Hurwitz system is Schur, and thus the assumptions in Problem 2.1 are satisfied.

We consider the case when $n = 2$. Based on Cucuzzella et al. (2018), the parameters are chosen as $L_1 = 2.0$ [mH], $L_2 = 1.8$ [mH], $R_1 = 0.5$ [Ω], $R_2 = 0.2$ [mΩ], $R_{1,2} = 50$ [mΩ], $C_1 = 2.5$ [mF], and $C_2 = 2.2$ [mF]. We design a local controller for node 1. Then, $v = \hat{V}_2$, $u = \hat{u}_1$, and $w = \hat{V}_1$, and $y = \hat{y}_1$. The transfer functions are obtained as

$$G_{y,v} = \frac{-0.389z - 0.0493}{z^2 - 0.759z + 2.61 \times 10^{-4}},$$

$$G_{y,u} = \frac{0.4382z + 9.06 \times 10^{-6}}{z^2 - 0.759z + 2.61 \times 10^{-4}},$$

$$G_{w,v} = \frac{0.983z - 0.764}{z^2 - 0.759z + 2.61 \times 10^{-4}},$$

$$G_{w,u} = \frac{(19.5z + 2.46) \times 10^{-3}}{z^2 - 0.759z + 2.61 \times 10^{-4}},$$

and

$$\mathbf{G}_{\mathbf{v},\mathbf{w}} = \frac{0.979z - 0.875}{z^2 - 0.870z + 1.01 \times 10^{-4}}.$$

First, we write down the conditions in Theorem 2.2 for tracking control. Since $G_{w,u}$ is scalar, (6) holds if and only if $QG_{(y,w,v),v} = 0$, i.e.,

$$Q_v = -(Q_y G_{y,v} + Q_w G_{w,v}).$$

Next, since $\mathbf{G}_{\mathbf{v},\mathbf{w}}$ and $G_{w,v}$ are scalar, the tracking condition becomes (11) that is

$$1 + 1.33 Q_y(1) = 0. \tag{29}$$

Therefore, Q_y cannot be made arbitrarily small, and thus the differential privacy levels of the Laplace and uniform mechanisms cannot be improved from the ceiling values. In fact, all conditions in Theorems 3.8 and 3.16 hold, and we have

$$(I - G_{w,v}(1)\mathbf{G}_{\mathbf{v},\mathbf{w}}(1))^{-1} G_{w,u}(1) \hat{\mathbf{G}}^{-1}_{\mathbf{y},\mathbf{r}}(1) = 0.25.$$

For the Laplace (resp. uniform) mechanism, the differential privacy level is lower bounded by $\varepsilon \geq 0.25c/b$ (resp. $\delta \geq 0.25c/d$.)

Remark 4.1. If one takes the outputs as $y_i = [I_i, V_i]^\top$, then it is possible to show that given distributions, the lower bounds on the differential privacy levels of $I_{L,i}$ can be made arbitrarily small by tuning Q. Therefore, our results can suggest how to choose outputs for improving the privacy performance. ◁

Since $QG_{(y,w,v),v} = 0$ needs to hold, the transfer function from noise v to y is computed as

$$y = \frac{G_{y,v}\mathbf{G}_{\mathbf{v},\mathbf{w}}}{1 - \mathbf{G}_{\mathbf{v},\mathbf{w}} G_{w,v}} v,$$

where recall Remark 3.9. Its H_∞-norm, namely $\|\Sigma_{y,v}\|_{2-\mathrm{ind}}$, is 1.82, which cannot be improved by tuning the local controller. From Proposition 3.7 (resp. Proposition 3.15), the tracking error is $3.64b^2$ for the Laplace mechanism (resp. $0.152d^2$ for the uniform mechanism).

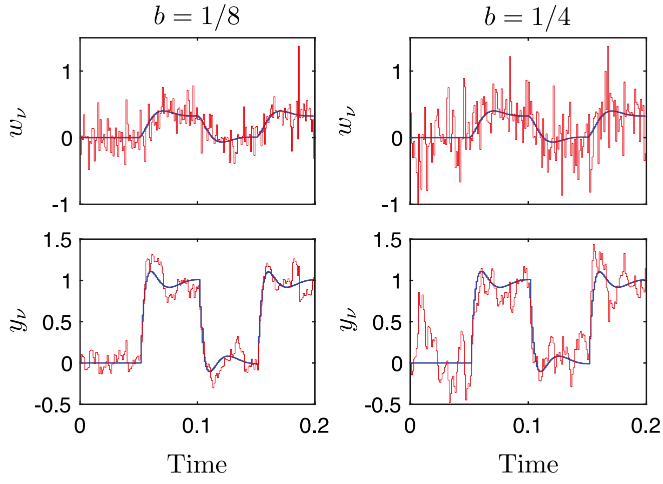

Fig. 3. Responses of w_ν and y_ν of the Laplace mechanism for Q_y without noise (blue line) and with noise (red line). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

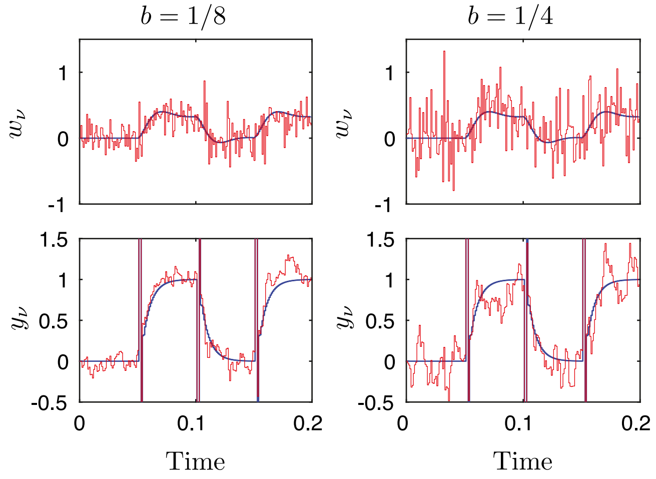

Fig. 4. Responses of w_ν and y_ν of the Laplace mechanism for $\bar{Q}_y$ without noise (blue line) and with noise (red line). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

4.3. Simulation results

When noise ν is added, the output of the considered module (i.e. node 1) y_ν and the signal sent to the other module (i.e. node 2) w_ν are respectively computed as

$$y_\nu = -\mathbf{G}_{\mathbf{pre}} Q_y r + \frac{G_{y,v}G_{v,w}}{1 - G_{w,v}\mathbf{G}_{\mathbf{v,w}}}\nu,$$

$$w_\nu = -\frac{G_{w,u}}{1 - G_{w,v}\mathbf{G}_{\mathbf{v,w}}}Q_y r + \nu.$$

The controller parameter here is only $Q_y \in \mathcal{RH}_\infty$. A parameter Q_y satisfying (29) is, for instance,

$$Q_y = -\frac{1}{1.33z}.$$

As a comparison, we also consider a controller achieving the lower bounds on the differential privacy levels; towards this end, we use the information of $\mathbf{G}_{\mathbf{v,w}}$ even though this is not supposed to be available. Such a controller parameter is

$$\bar{Q}_y = -\frac{1}{4z}\frac{1 - G_{w,v}\mathbf{G}_{\mathbf{v,w}}}{G_{w,u}},$$

where the coefficient 1/4 is determined by (29).

We consider a scenario where the reference r is switched between 0 and 1. By adding noise, we protect from r being identified from w_ν and also evaluate the tracking control performance under noise. Fig. 3 (resp. Fig. 4) shows w_ν and y_ν of the Laplace mechanism for controller parameter Q_y (resp. $\bar{Q}_y$) when $b = 1/8$ and $b = 1/4$. It is observed that Q_y has similar privacy performance as $\bar{Q}_y$ achieving the lower bound on the differential privacy level. Namely, the differential privacy level is impossible to improve further. In contrast to slight improvement of privacy performance, the tracking control performance is significantly degenerated for $\bar{Q}_y$ when the reference signal is switched. A possible reason of Q_y having better tracking control performance is that Q_y is the one having the smallest H_∞-norm satisfying (29). That is, y_ν with Q_y is less sensitive with respect to the change of r.

Next, Fig. 5 shows w_ν and y_ν of the uniform mechanism for controller parameter Q_y when $d = \sqrt{3/8}$ and $d = \sqrt{3/2}$, where these values are chosen such that tracking errors are equivalent under both noises. The maximum tracking error is smaller than the Laplace mechanism as expected.

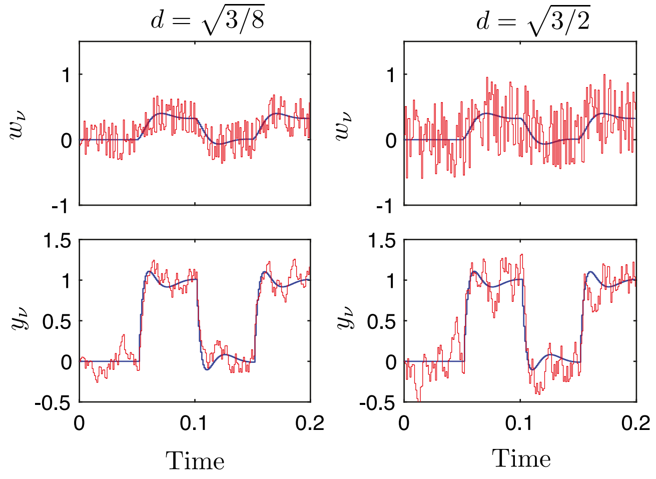

Fig. 5. Responses of w_ν and y_ν of the uniform mechanism for Q_y without noise (blue line) and with noise (red line). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

5. Conclusion

In the framework of modular control design, we have analyzed lower bounds on the differential privacy levels for the Laplace and uniform mechanisms in terms of the 1- and ∞-induced system norms, respectively. In systems and control, the 2-induced norm, namely the H_∞-norm plays an important role, which is connected to the Gaussian mechanism by Kawano and Cao (2020) and Le Ny and Pappas (2014). As for the 1- and ∞-induced norms, the 2-induced norm can be lower bounded due to the constraints on the local controller. Therefore, in general, the differential privacy level of the Gaussian mechanism cannot be improved from a ceiling value even one tunes parameters of the local controller although it is not easy to estimate the ceiling value explicitly. Future work includes estimating ceiling values of differential privacy levels in more general problem settings, e.g. for general nonlinear systems. As to mechanisms, we have focused on Laplace and uniform mechanisms, and it may be possible to estimate a ceiling value from the definition of differential privacy itself without specifying the types of noise to be added.

Appendix. Proofs

A.1. Proof of Theorem 2.2

By generalizing Ishizaki et al. (2019, Proposition 2.2) with the argument after Ishizaki et al. (2019, Proposition 2.1), it is possible to show that a controller (5) solves Problem 2.1 for $r = 0$ if and only if it satisfies (6). That is, (6) gives a characterization of all stabilizing controllers. Since a tracking controller is a specific stabilizing controller, we investigate an additional condition to achieve tracking.

A tracking condition is derived based on the final value theorem (see e.g. Levine, 2018). To compute the transfer function matrix from r to y of the entire system in Fig. 2, we apply the changes of variables $\hat{y} = y - G_{y,v}v$ and $\hat{w} = w - G_{w,v}v$, which yields

$$\begin{aligned} v &= \mathbf{G}_{\mathbf{v},\mathbf{w}}(\hat{w} + G_{w,v}v),\\ \hat{w} &= G_{w,u}u,\\ \hat{y} &= G_{y,u}u,\\ u &= -K_y r + K_y\hat{y} + K_w\hat{w} + KG_{(y,w,v),v}v. \end{aligned}$$

The last three equations lead to

$$u = (I - KG_{(y,w,v),u})^{-1}(-K_y r + KG_{(y,w,v),v}v).$$

By using (5), $KG_{(y,w,v),u}$ can be computed as

$$\begin{aligned} KG_{(y,w,v),u} &= (I + QG_{(y,w,v),u})^{-1}QG_{(y,w,v),u}\\ &= I - (I + QG_{(y,w,v),u})^{-1}, \end{aligned}$$

and consequently

$$\begin{aligned} u &= (I + QG_{(y,w,v),u})(-K_y r + KG_{(y,w,v),v}v)\\ &= -Q_y r + QG_{(y,w,v),v}v, \end{aligned}$$

where again (5) is used. Then, y and w are respectively computed as

$$y = -G_{y,u}Q_y r + (G_{y,v} + G_{y,u}QG_{(y,w,v),v})v \tag{A.1}$$

and

$$w = -G_{w,u}Q_y r + G_{w,v}v, \tag{A.2}$$

where (6) is used. From (2) and (A.2), it follows that

$$v = -(I - \mathbf{G}_{\mathbf{v},\mathbf{w}}G_{w,v})^{-1}\mathbf{G}_{\mathbf{v},\mathbf{w}}G_{w,u}Q_y r.$$

Substituting this into (A.1) yields

$$y = -\bar{\mathbf{G}}_{\mathbf{y},\mathbf{r}}Q_y r$$

for $\bar{\mathbf{G}}_{\mathbf{y},\mathbf{r}}$ in (8). From the final value theorem, tracking control is achieved for a constant reference $r \in \mathbb{R}^m$ if and only if

$$\lim_{z\to 1} -\frac{z-1}{z}\bar{\mathbf{G}}_{\mathbf{y},\mathbf{r}}(z)Q_y(z)\frac{z}{z-1}r = r,$$

where $z/(z-1)r$ is the z-transformation of a constant signal r. This holds for arbitrary r if and only if (7) holds. □

A.2. Proof of Theorem 3.4

The sufficiency follows from that of Le Ny and Pappas (2014, Theorem 2) with the definition of the matrix induced norm.

For the necessity proof, we show that if the Laplace mechanism is ε-differentially private, the equality holds in (18) for specific choices of (r_t, r_t') and S. Since the system is linear, let $r_t = 0$ without loss of generality. Then, $|r_t'|_1 = c$ from the definition of Adj_1^c. From the definition of the induced matrix 1-norm, there exists r_t' such that $|H_t r_t'|_1 = |H_t|_1|r_t'|_1$ and $|r_t'|_1 = c$, and consequently

$$|H_t r_t'|_1 = c|H_t|_1. \tag{A.3}$$

Next, let $S = S_1 \times \cdots \times S_{(t+1)p}$, where $S_i = (-1, 0)$ if the ith element of $H_t r_t'$ is positive; $S_i = (0, 1)$ otherwise. This implies

$$|H_t r_t' - \nu_t|_1 = |H_t r_t'|_1 + |\nu_t|_1 = c|H_t|_1 + |\nu_t|_1, \ \forall \nu_t \in S \tag{A.4}$$

where (A.3) is used.

For these (r_t, r_t') and S, it follows from (A.4) that

$$\begin{aligned} \mathbb{P}(w_{\nu,t} \in S) &= \frac{1}{(2b)^{(t+1)p}}\int_{\mathbb{R}^{(t+1)p}} 1_S(\nu_t)e^{-\frac{|\nu_t|_1}{b}}d\nu_t\\ &= e^{\frac{c}{b}|H_t|_1}\frac{1}{(2b)^{(t+1)p}}\int_{\mathbb{R}^{(t+1)p}} 1_S(\nu_t)e^{-\frac{|H_t r_t' - \nu_t|_1}{b}}d\nu_t. \end{aligned}$$

The change of variables $\nu_t = H_t r_t' + \bar{\nu}_t$ yields

$$\mathbb{P}(w_{\nu,t} \in S) = e^{\frac{c}{b}|H_t|_1}\mathbb{P}(w_{\nu,t}' \in S).$$

Therefore, if the Laplace mechanism is ε-differentially private, ε cannot be smaller than $\frac{c}{b}|H_t|_1$, i.e., b satisfies (18). □

A.3. Proof of Proposition 3.7

When noise ν is added, the output y can be described by

$$y = -\bar{\mathbf{G}}_{\mathbf{y},\mathbf{r}}Q_y r + (G_{y,\nu} + G_{y,u}QG_{(y,w,\nu),\nu})(I - \mathbf{G}_{\mathbf{v},\mathbf{w}}G_{w,\nu})^{-1}\mathbf{G}_{\mathbf{v},\mathbf{w}}\nu,$$

where the first and second terms on the right-hand side are computed in Appendix A.1 and Remark 3.9, respectively. To analyze y in the time domain, we consider a minimal realization of the above transfer function matrix:

$$\bar{\Sigma} : \begin{cases} \bar{x}(t+1) = \bar{A}\bar{x}(t) + \bar{B}_r r(t) + \bar{B}_\nu \nu(t), \ \bar{x}(0) = 0,\\ y(t) = \bar{C}\bar{x}(t) + \bar{D}_r r(t) + \bar{D}_\nu \nu(t). \end{cases}$$

By defining

$$h_r(t) := \begin{cases} \bar{D}_r, & t = 0\\ \bar{C}\bar{A}^{t-1}\bar{B}_r + \bar{D}_r, & \text{otherwise}, \end{cases}$$

$$h_\nu(t) := \begin{cases} \bar{D}_\nu, & t = 0\\ \bar{C}\bar{A}^{t-1}\bar{B}_\nu + \bar{D}_\nu, & \text{otherwise}, \end{cases}$$

the output can be described as

$$y(t) = \sum_{k=0}^{t}(h_r(k)r(t-k) + h_\nu(k)\nu(t-k)),$$

and consequently the tracking error at time instant t is

$$y(t) - r(t) = \sum_{k=0}^{t}(h_r(k)r(t-k) + h_\nu(k)\nu(t-k)) - r(t),$$

Since $\nu(t)$ is i.i.d. Laplace noise with $\mathbb{E}[\nu(t)] = 0$ and $\mathbb{E}[\nu^2(t)] = 2b^2$, it follows that

$$\mathbb{E}[|y(t) - r(t)|^2] = \left|\sum_{k=0}^{t} h_r(k)r(t-k) - r(t)\right|^2 + 2b^2\sum_{k=0}^{t}|h_\nu(k)|^2.$$

Now, the controller is designed to achieve tracking control, i.e.,

$$\lim_{t\to\infty}\left|\sum_{k=0}^{t} h_r(k)r(t-k) - r(t)\right|^2 = 0.$$

Furthermore, from the assumptions in Problem 2.1 and $Q \in \mathcal{RH}_\infty$, the system $\Sigma_{y,\nu}$ is internally stable, and consequently

$$\lim_{t\to\infty}\sum_{k=0}^{t}|h_\nu(k)|^2 = \|\Sigma_{y,\nu}\|_{2-\mathrm{ind}}.$$

Therefore, by taking $t \to \infty$, we obtain (21). □

A.4. Proof of Theorem 3.12

First, we consider the necessity. As in the proof of Theorem 3.12, we show that if the system is δ-differentially private, the equality holds in (24) for specific choices of (r_t, r'_t) and S. Let $r_t = 0$ without loss of generality. From the definitions of Adj^c_∞ and the induced matrix ∞-norm, there exists r'_t such that $|H_t r'_t|_\infty = c|H_t|_\infty$. Furthermore, from the definition of the vector ∞-norm, for some ith element of $H_t r'_t$, denoted by $y'_{t,i}$, we have

$$|y'_{t,i}| = |H_t r'_t|_\infty = c|H_t|_\infty. \tag{A.5}$$

Now, we choose $S = S_1 \times \cdots \times S_{(t+1)p}$, where $S_j = (-\infty, \infty)$, $j \neq i$, and $S_i = [-c|H_t|_\infty/2, \infty)$ (resp. $S_i = (-\infty, c|H_t|_\infty/2]$) if $y'_{t,i} > 0$ (resp. $y'_{t,i} < 0$); note that $y'_{t,i} \neq 0$ from the assumption $H_t \neq 0$.

For these (r_t, r'_t) and S, it follows that

$$\begin{aligned}\mathbb{P}(w_{\nu,t} \in S) &= \frac{1}{d^{(t+1)p}} \int_{\mathbb{R}^{(t+1)p}} 1_S(\nu_t) d\nu_t \\ &= \frac{1}{2d}(d + c|H_t|_\infty),\end{aligned}$$

and

$$\begin{aligned}\mathbb{P}(w'_{\nu,t} \in S) &= \frac{1}{d^{(t+1)p}} \int_{\mathbb{R}^{(t+1)p}} 1_S(H_t r'_t + \nu_t) d\nu_t \\ &= \frac{1}{2d}(d - c|H_t|_\infty).\end{aligned}$$

These two equalities yield

$$\mathbb{P}(w_{\nu,t} \in S) - \mathbb{P}(w'_{\nu,t} \in S) = \frac{c}{d}|H_t|_\infty.$$

Since the system is δ-differentially private, δ cannot be smaller than $c|H_t|_\infty/d$. Therefore, d satisfies (24).

Next, we show sufficiency. Let $r_t = 0$ without loss of generality. Then, $|r'_t|_\infty = c$. Also, let $y'_t := H_t r'_t$. Then, for any S, the definition of the uniform distribution leads to

$$\begin{aligned}&\mathbb{P}(w'_{\nu,t} \in S) - \mathbb{P}(w_{\nu,t} \in S) \\ &= \frac{1}{d^{(t+1)p}} \int_{\mathbb{R}^{(t+1)p}} (1_S(y'_t + \nu_t) - 1_S(\nu_t)) d\nu_t.\end{aligned}$$

Let $y'_{t,i}$, $i = 1, \dots, (t+1)p$ denote the vector whose ith element is that of y'_t, and the other elements are zero. Also, define $y'_{t,-1} := y'_t - y'_{t,1}$. Then, the direct computation yields

$$\begin{aligned}&\int_{\mathbb{R}^{(t+1)p}} (1_S(y'_t + \nu_t) - 1_S(\nu_t)) d\nu_t \\ &= \int_{\mathbb{R}^{(t+1)p}} (1_S(y'_t + \nu_t) - 1_S(y'_{t,-1} + \nu_t)) d\nu_t \\ &\quad + \int_{\mathbb{R}^{(t+1)p}} (1_S(y'_{t,-1} + \nu_t) - 1_S(\nu_t)) d\nu_t.\end{aligned}$$

By applying the change of variables $\bar{\nu}_t = \nu_t + y'_{t,-1}$, the first term on the right-hand side can be rearranged as

$$\begin{aligned}&\int_{\mathbb{R}^{(t+1)p}} (1_S(y'_t + \nu_t) - 1_S(y'_{t,-1} + \nu_t)) d\nu_t \\ &= \int_{\mathbb{R}^{(t+1)p}} (1_S(y'_{t,1} + \bar{\nu}_t) - 1_S(\bar{\nu}_t)) d\bar{\nu}_t.\end{aligned}$$

By repeating similar procedures, we have

$$\begin{aligned}&\mathbb{P}(w'_{\nu,t} \in S) - \mathbb{P}(w_{\nu,t} \in S) \\ &= \frac{1}{d^{(t+1)p}} \sum_{i=1}^{(t+1)p} \int_{\mathbb{R}^{(t+1)p}} (1_S(y'_{t,i} + \nu_t) - 1_S(\nu_t)) d\nu_t.\end{aligned}$$

For any S, it is possible to show that

$$\begin{aligned}&|\mathbb{P}(w'_{\nu,t} \in S) - \mathbb{P}(w_{\nu,t} \in S)| \\ &\le \frac{1}{d^{(t+1)p}} \max_{\substack{i=1,\dots,(t+1)p \\ |r'_t|_\infty = c}} \left| \int_{\mathbb{R}^{(t+1)p}} (1_S(y'_{t,i} + \nu_t) - 1_S(\nu_t)) d\nu_t \right| \\ &\le \max_{\substack{i=1,\dots,(t+1)p \\ |r'_t|_\infty = c}} \frac{|y'_{t,i}|}{d} = \frac{c}{d}|H_t|_\infty.\end{aligned}$$

Therefore, if (24) holds, the uniform mechanism is δ-differentially private. □

References

Cortés, J., Dullerud, G. E., Han, S., Le Ny, J., Mitra, S., & Pappas, G. (2016). Differential privacy in control and network systems. In *Proc. 55th IEEEconference on decision and control* (pp. 4252–4272). IEEE.

Cucuzzella, M., Trip, S., De Persis, C., Cheng, X., Ferrara, A., & van der Schaft, A. J. (2018). A robust consensus algorithm for current sharing and voltage regulation in DC microgrids. *IEEE Transactions on Control Systems Technology*, *27*(4), 1583–1595.

Dwork, C., Kenthapadi, K., McSherry, F., Mironov, I., & Naor, M. (2006). Our data, ourselves: Privacy via distributed noise generation. In *Annual international conference on the theory and applications of cryptographic techniques* (pp. 486–503). Springer.

Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. In *Proc. 3rd theory of cryptography conference* (pp. 265–284).

Farokhi, F., & Sandberg, H. (2019). Ensuring privacy with constrained additive noise by minimizing Fisher information. *Automatica*, *99*, 275–288.

Furieri, L., Zheng, Y., Papachristodoulou, A., & Kamgarpour, M. (2019). An input–output parametrization of stabilizing controllers: Amidst youla and system level synthesis. *IEEE Control Systems Letters*, *3*(4), 1014–1019.

Geng, Q., Ding, W., Guo, R., & Kumar, S. (2018). Optimal noise-adding mechanism in additive differential privacy. arXiv preprint arXiv:1809.10224.

Hale, M., & Egerstedt, M. (2017). Cloud-enabled differentially private multi-agent optimization with constraints. *IEEE Transactions on Control of Network Systems*, *5*(4), 1693–1706.

Han, S., Topcu, U., & Pappas, G. J. (2017). Differentially private distributed constrained optimization. *IEEE Transactions on Automatic Control*, *62*(1), 50–64.

He, J., & Cai, L. (2016). Differential private noise adding mechanism and its application on consensus. arXiv preprint arXiv:1611.08936.

Ho, B. L., & Kálmán, R. E. (1966). Effective construction of linear state-variable models from input/output functions. *Regelungstechnik*, *14*(12), 545–548.

Huang, Z., Mitra, S., & Vaidya, N. (2015). Differentially private distributed optimization. In *Proc. 2015 international conference on distributed computing and networking* (p. 4).

Ishizaki, T., Kawaguchi, T., Sasahara, H., & Imura, J. (2019). Retrofit control with approximate environment modeling. *Automatica*, *107*, 442–453.

Ito, K., Kawano, Y., & Kashima, K. (2021). Differentially private mechanisms for linear dynamical systems with heavy-tailed noise. In *Proc. 24th international symposium on mathematical theory of networks and systems* (in press).

Kawano, Y., & Cao, M. (2020). Design of privacy-preserving dynamic controllers. *IEEE Transactions on Automatic Control*, *65*(9), 3863–3878.

Kawano, Y., Kashima, K., & Cao, M. (2020). A fundamental performance limit of cloud-based control in terms of differential privacy level. In *Proc. 21st IFAC world congress* (pp. 11165–11170).

Le Ny, J., & Mohammady, M. (2018). Differentially private MIMO filtering for event streams. *IEEE Transactions on Automatic Control*, *63*(1), 145–157.

Le Ny, J., & Pappas, G. J. (2014). Differentially private filtering. *IEEE Transactions on Automatic Control*, *59*(2), 341–354.

Levine, W. S. (2018). *The control handbook*. CRC press.

Rantzer, A. (2011). Distributed control of positive systems. In *Proc. 50th IEEE conference on decision and control and european control conference* (pp. 6608–6611). IEEE.

Sasahara, H., Ishizaki, T., & Imura, J. i. (2019). Parameterization of retrofit controllers. arXiv preprint arXiv:1911.04915.

Wang, Y., Huang, Z., Mitra, S., & Dullerud, G. E. (2017). Differential privacy in linear distributed control systems: Entropy minimizing mechanisms and performance tradeoffs. *IEEE Transactions on Control of Network Systems*, *4*(1), 118–130.

Wang, Y.-S., Matni, N., & Doyle, J. C. (2019). A system-level approach to controller synthesis. *IEEE Transactions on Automatic Control*, *64*(10), 4079–4093.

Willenborg, L., & De Waal, T. (1996). *Statistical disclosure control in practice, Vol. 111*. Springer Science & Business Media.

Willenborg, L., & De Waal, T. (2012). *Elements of statistical disclosure control, Vol. 155*. Springer Science & Business Media.

Yazdani, K., Jones, A., Leahy, K., & Hale, M. (2018). Differentially private LQ control. arXiv:1807.05082.

Zheng, Y., Furieri, L., Papachristodoulou, A., Li, N., & Kamgarpour, M. (2020). On the equivalence of youla, system-level and input-output parameterizations. *IEEE Transactions on Automatic Control*, (early access).

Yu Kawano has since 2019 been an Associate Professor in the Graduate School of Advanced Science and Engineering at Hiroshima University. He received the M.S. and Ph.D. degrees in engineering from Osaka University, Japan, in 2011 and 2013, respectively. From 2013 to 2016, he was a Post-Doctoral Researcher at both Kyoto University and JST CREST, Japan. From 2016 to 2019, he was a Post-Doctoral Researcher at the University of Groningen, The Netherlands. He has held visiting research positions at Tallinn University of Technology, Estonia and the University of Groningen. His research interests include nonlinear systems, complex networks, model reduction, and privacy of control systems. He is an Associate Editor for Systems and Control Letters and a member of the EUCA Conference Editorial Board.

Kenji Kashima received his Doctoral degree in Informatics from Kyoto University in 2005, respectively. He was with Tokyo Institute of Technology, Universität Stuttgart, Osaka University, before he joined Kyoto University in 2013, where he is currently an Associate Professor. His research interests include control and learning theory for complex (large scale, stochastic, networked) dynamical systems, as well as its interdisciplinary applications. He received Humboldt Research Fellowship (Germany), IEEE CSS Roberto Tempo Best CDC Paper Award, Pioneer Award of SICE Control Division, and so on. He is a Senior Member of IEEE, an Associate Editor of IEEE Transactions of Automatic Control (2017-), the IEEE CSS Conference Editorial Board (2011-) and Asian Journal of Control (2014-).

Ming Cao has since 2016 been a professor of systems and control with the Engineering and Technology Institute (ENTEG) at the University of Groningen, the Netherlands, where he started as a tenure-track Assistant Professor in 2008. He received the Bachelor degree in 1999 and the Master degree in 2002 from Tsinghua University, Beijing, China, and the Ph.D. degree in 2007 from Yale University, New Haven, CT, USA, all in Electrical Engineering. From September 2007 to August 2008, he was a Postdoctoral Research Associate with the Department of Mechanical and Aerospace Engineering at Princeton University, Princeton, NJ, USA. He worked as a research intern during the summer of 2006 with the Mathematical Sciences Department at the IBM T. J. Watson Research Center, NY, USA. He is the 2017 and inaugural recipient of the Manfred Thoma medal from the International Federation of Automatic Control (IFAC) and the 2016 recipient of the European Control Award sponsored by the European Control Association (EUCA). He is a Senior Editor for Systems and Control Letters, and an Associate Editor for IEEE Transactions on Automatic Control, IEEE Transactions on Circuits and Systems and IEEE Circuits and Systems Magazine. He is a vice chair of the IFAC Technical Committee on Large-Scale Complex Systems. His research interests include autonomous agents and multi-agent systems, complex networks and decision-making processes.