university of groningen

University Medical Center Groningen

University of Groningen

Design of Privacy-Preserving Dynamic Controllers

Kawano, Yu; Cao, Ming

Published in:
IEEE Transaction on Automatic Control

DOI:
10.1109/TAC.2020.2994030

IMPORTANT NOTE: You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

Document Version
Final author's version (accepted by publisher, after peer review)

Publication date:
2020

Link to publication in University of Groningen/UMCG research database

Citation for published version (APA):
Kawano, Y., & Cao, M. (2020). Design of Privacy-Preserving Dynamic Controllers: Special Issue of "Security and Privacy of Distributed Algorithms and Network Systems". *IEEE Transaction on Automatic Control*, *65*(9), 3863-3878. https://doi.org/10.1109/TAC.2020.2994030

Copyright
Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

The publication may also be distributed here under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license. More information can be found on the University of Groningen website: https://www.rug.nl/library/open-access/self-archiving-pure/taverne-amendment.

Take-down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from the University of Groningen/UMCG research database (Pure): http://www.rug.nl/research/portal. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.

Download date: 25-10-2021

Design of Privacy-Preserving Dynamic Controllers

Yu Kawano, *Member,* and Ming Cao, *Senior Member*

***Abstract*—As a quantitative criterion for privacy of "mechanisms" in the form of data-generating processes, the concept of *differential privacy* was first proposed in computer science and has later been applied to linear dynamical systems. However, differential privacy has not been studied in depth together with other properties of dynamical systems, and it has not been fully utilized for controller design. In this paper, first we clarify that a classical concept in systems and control, *input observability* (sometimes referred to as *left invertibility*) has a strong connection with differential privacy. In particular, we show that the Gaussian mechanism can be made highly differentially private by adding *small* noise if the corresponding system is less input observable. Next, enabled by our new insight into privacy, we develop a method to design dynamic controllers for the classic tracking control problem while addressing privacy concerns. We call the obtained controller through our design method the *privacy-preserving controller*. The usage of such controllers is further illustrated by an example of tracking the prescribed power supply in a DC microgrid installed with smart meters while keeping the electricity consumers' tracking errors private.**

***Index Terms*—Discrete-time linear systems, Differential Privacy, Observability, Privacy-Preserving Controllers**

I. Introduction

The trend of the Internet-of-Things (IoT) and cloud computing makes privacy and security become a research area of acute social and technological concerns, see e.g. [1]–[7]. To protect the privacy of data sources, the collected data are usually processed statistically before being publicized for different applications. However, even if one only publishes statistical analytics, not raw data, private personal information may still be identified by smart data mining algorithms that combine the statistics with other third party information, see e.g. [8]–[11]. Motivated by threats on privacy, statistical disclosure control, or more generally privacy preserving data mining, has been intensively studied; see e.g. [12], [13]. Representative techniques include the K-anonymity [14], l-diversity [15], t-closeness [16], and differential privacy [17], [18]. In particular, differential privacy enjoys the mathematical property of being quantifiable and thus has been used in solving various privacy-related problems arising in the domains of smart grids [19]–[21], health monitoring [22], [23], blockchain (or bitcoin) [24], [25] and mechanism design [26].

There is a growing need to treat privacy as a critical property of *dynamical* systems instead of the feature of some *static* time invariant data set. For example, in power grids, consumers' electricity consumption patterns change over time and are coupled in a closed loop with the stabilization actions of various controllers in power systems. To address privacy issues of those datasets that are generated by dynamical systems, the standard concept of *differential privacy* for static data has been extended to discrete-time linear dynamical systems, see e.g. [27], [28], which shows convincingly that the key idea of differential privacy, namely adding noise to data before publishing them, is also effective for privacy protection for dynamical data sets. However, there is still a considerable lack of in-depth understanding of the possible fundamental interplay between differential privacy and other critical properties of dynamical systems [29].

To address this challenge, we propose to take an approach that is deeply rooted in systems and control theory; to be more specific, we study privacy of dynamical systems by taking two major steps: first to study privacy in terms of *input observability* and then to provide a privacy-preserving controller design method. The differential privacy level of a discrete-time linear system can be interpreted as a quantitative criterion for the difficulty of identifying its input, which triggers us to give a refreshing look at rich classic results on uniquely determining the input from the output in systems and control under the name of input observability [30] or left invertibility [31]. For input observability, there are already several qualitative criteria, e.g. the rank condition of the transfer function matrix [31], the PBH type test [30], [32], and Kalman's rank type conditions [31], [33]. However, these existing conditions do not provide quantitative analysis. Therefore, there is a gap between the relatively new concept of differential privacy and the classical concept of input observability. To establish a bridge between this gap, we extend the notion of the Gramian to input observability. Then, we show that the Gaussian mechanism evaluates the maximum eigenvalue of the input observability Gramian; in other words, *small* noise is enough to make the less input observable Gaussian mechanism highly differentially private. This new insight suggests that the input observability Gramian can be used for detailed privacy analysis, not restricted to differential privacy, just like what the standard controllability and observability Gramians can do for detailed controllability and observability analysis.

Next, we consider achieving trajectory tracking while protecting the tracking error as private information. Trajectory tracking itself has been studied as a part of the output regulation problem [34] for which dynamic output feedback controllers have been studied. The differential privacy level increases if the dynamic controllers are designed such that the maximum eigenvalue of the input observability Gramian is small, which is achieved by making the corresponding H_∞-norm small. In this paper, we provide a dynamic controller

This work was supported in part by the European Research Council (ERC-CoG-771687) and the Dutch Organization for Scientific Research (NWO-vidi-14134).

Y. Kawano is with the Graduate School of Advanced Science and Engineering, Hiroshima University, Higashi-Hiroshima, Japan (email: ykawano@hiroshima-u.ac.jp).

Ming Cao is with the Faculty of Science and Engineering, University of Groningen, 9747 AG Groningen, The Netherlands (email: m.cao@rug.nl).

design method in order to address the tracking problem and to specify the H_∞-norm simultaneously based on LMIs. It is worth pointing out that to increase the differential privacy level of the controller, one needs to make the H_∞-norm of the controller small or add large noise, both of which may deteriorate the control performance. Therefore, privacy-preserving controller design reduces to a trade-off between the privacy level and control performance.

Along this line of research on designing privacy-preserving controllers, there are related earlier works. Differential privacy has been employed for privacy-preserving filtering [27], [28], but not for controller design. In particular, [27] also studies the connection between differential privacy and the H_∞-norm of a system; however, differential privacy has not been studied from the input observability perspective, which was considered in our preliminary conference version [35]. Different from [27], [35], in this paper we consider not just i.i.d. noise; although this may seem to be a rather minor technical extension, it is in fact an important step towards obtaining a deeper understanding of the differential privacy level of a dynamical system. Also note that differential privacy has been used for LQ control [36] and distributed optimization [37]–[41], where the controller gains or controller dynamics are designed without considering privacy issues, and consequently privacy-preserving noise is added separately, making protecting privacy independent of the controller design itself. In contrast, we design the controller with the incorporated goal of achieving high privacy levels using small noise.

The remainder of this paper is organized as follows. Section II introduces the concept of differential privacy and analyzes it from several aspects including input observability. Section III provides a privacy-preserving controller design method. Our method is illustrated by an example of DC microgrids installed with smart meters in Section IV. Section V briefly mentions extensions of our results to nonlinear systems, where a part of the results has been presented in a preliminary conference version [42]. Finally, Section VI concludes the paper.

Notations: The set of real numbers, non-negative real numbers, and non-negative integers are denoted by $\mathbb{R}$, $\mathbb{R}_+$ and $\mathbb{Z}_+$, respectively. For vectors $x_1, \dots, x_m \in \mathbb{R}^n$, a collective vector $[x_1^\top \ \cdots \ x_m^\top]^\top \in \mathbb{R}^{nm}$ is also described by $[x_1; \cdots; x_m]$ for the sake of simplicity of description. For the sequence $u(t) \in \mathbb{R}^m$, $t \in \mathbb{Z}_+$, a collective vector consisting of its subsequence is denoted by $U_t(\tau) := [u(\tau); \cdots; u(\tau+t)] \in \mathbb{R}^{(t+1)m}$; when $\tau = 0$, the argument is omitted, i.e., $U_t := [u(0); \cdots; u(t)]$. For a square matrix $A \in \mathbb{R}^{n\times n}$, its determinant is denoted by $\det(A)$, and when its eigenvalues are real, its maximum and minimum eigenvalues are denoted by $\lambda_{\max}(A)$ and $\lambda_{\min}(A)$, respectively. Further, $A \succ 0$ means that A is symmetric and positive definite. The identity matrix of size n is denoted by I_n. For the vector $x \in \mathbb{R}^n$, its norms is denoted by $|x|_p := (\sum_{i=1}^n |x_i|^p)^{1/p}$, where $p \in \mathbb{Z}_+$, and its weighted norm with $A \succ 0$ is denoted by $|x|_A := (x^\top A x)^{1/2}$. A continuous function $\alpha : [0, a) \to \mathbb{R}_+$ is said to be of class $\mathcal{K}$ if it is strictly increasing and $\alpha(0) = 0$. Moreover, it is said to be of class $\mathcal{K}_\infty$ if $a = \infty$ and $\alpha(r) \to \infty$ as $r \to \infty$. A random variable w is said to have a non-degenerate multivariate Gaussian distribution with the mean value $\mu \in \mathbb{R}^n$ and covariance matrix $\Sigma \succ 0$, denoted by $w \sim \mathcal{N}_n(\mu, \Sigma)$, if its distribution has the following probability density:

$$p(w; \mu, \Sigma) = \left(\frac{1}{(2\pi)^n \det(\Sigma)}\right)^{1/2} \mathrm{e}^{-|w-\mu|^2_{\Sigma^{-1}}/2}.$$

The so called Q-function is defined by $\mathsf{Q}(w) := \frac{1}{\sqrt{2\pi}} \int_w^\infty \mathrm{e}^{-\frac{v^2}{2}} dv$, where $\mathsf{Q}(w) < 1/2$ for $w > 0$, and $\mathsf{R}(\varepsilon, \delta) := (\mathsf{Q}^{-1}(\delta) + \sqrt{(\mathsf{Q}^{-1}(\delta))^2 + 2\varepsilon})/2\varepsilon$.

II. Differential Privacy Analysis

In this section, we study differential privacy of discrete-time linear dynamical systems from three aspects. First, we define the differential privacy of a Gaussian mechanism with output noise [17], [18]; the exact definition of a mechanism will become clear later. Second, we investigate the differential privacy of the mechanism in terms of observability. Last, we analyze the differential privacy of the mechanism with input noise. Throughout the paper, we follow the convention by focusing on a finite data sets. In a dynamical system setting, this corresponds to analyzing the system's properties within a finite time.

Consider the following discrete-time linear system:

$$\begin{cases} x(t+1) = Ax(t) + Bu(t), \\ y(t) = Cx(t) + Du(t), \end{cases} \tag{1}$$

for $t \in \mathbb{Z}_+$, where $x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^m$ and $y(t) \in \mathbb{R}^q$ denote the state, input and output, respectively, and $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$, $C \in \mathbb{R}^{q\times n}$ and $D \in \mathbb{R}^{q\times m}$.

For (1), the output sequence $Y_t \in \mathbb{R}^{(t+1)q}$ is described by

$$Y_t = O_t x_0 + N_t U_t, \tag{2}$$

where $O_t \in \mathbb{R}^{(t+1)q\times n}$ and $N_t \in \mathbb{R}^{(t+1)q\times(t+1)m}$ are

$$O_t := \begin{bmatrix} C^\top & CA^\top & \cdots & (CA^t)^\top \end{bmatrix}^\top, \tag{3}$$

$$N_t := \begin{bmatrix} D & 0 & \cdots & \cdots & 0 \\ CB & D & \ddots & & \vdots \\ CAB & CB & D & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ CA^{t-1}B & CA^{t-2}B & \cdots & CB & D \end{bmatrix}. \tag{4}$$

To facilitate future discussion, we also denote the left $(t+1)q$ by $(T+1)m$ submatrix of N_t by $N_{t,T}$, $T \le t$.

Remark 2.1: If $[O_t \quad N_t] = 0$, then Y_t is identically zero. In this pathological case, there is no reason to proceed with privacy analysis, and thus throughout the paper we assume that $[O_t \quad N_t] \neq 0$. ◁

A. Differential Privacy With Output Noise

To proceed with differential privacy analysis, we consider the output $y_w(t) := y(t) + w(t)$ after adding the noise $w(t) \in \mathbb{R}^q$. From (2), $Y_{w,t} \in \mathbb{R}^{(t+1)q}$ can be described by

$$Y_{w,t} = O_t x_0 + N_t U_t + W_t. \tag{5}$$

This defines a mapping $\mathcal{M} : \mathbb{R}^n \times \mathbb{R}^{(t+1)m} \times \mathbb{R}^{(t+1)q} \ni (x_0, U_t, W_t) \mapsto Y_{w,t} \in \mathbb{R}^{(t+1)q}$. In differential privacy analysis, this mapping is called a *mechanism* [17], [18].

It is worth clarifying that the input of the dynamical system (1) is u while the input data of the induced mechanism (5) is (x_0, U_t).

Remark 2.2: Depending on specific applications, x_0 and U_t do not need to be private at the same time. Our results can be readily extended to the scenario where one of x_0 and U_t is confidential, and the other is public. $\lhd$

Differential privacy gives an index of the privacy level of a mechanism, which is characterized by the sensitivity of the published output data $Y_{w,t}$ with respect to the input data (x_0, U_t). More specifically, if for a pair of not so distinct input data $((x_0, U_t), (x_0', U_t'))$, the corresponding pair of output data $(Y_{w,t}, Y_{w,t}')$ are very different, then one can conclude that input data are easy to identify, i.e. the mechanism is less private. Thus, differential privacy is defined using a pair of different but "similar" input data, where by similar we mean that the pair satisfies the following adjacency relations.

Definition 2.3: Given $c > 0$ and $p \in \mathbb{Z}_+$, a pair of input data $((x_0, U_t), (x_0', U_t')) \in (\mathbb{R}^n \times \mathbb{R}^{(t+1)m}) \times (\mathbb{R}^n \times \mathbb{R}^{(t+1)m})$ is said to belong to the binary relation *c-adjacency* under the p norm if $|[x_0; U_t] - [x_0'; U_t']|_p \leq c$. The set of all pairs of the input data that are c-adjacent under the p norm is denoted by Adj_p^c. $\lhd$

The magnitude of c gives an upper bound on the difference of the pair of input data (x_0, U_t) and (x_0', U_t'). Therefore, c can be chosen according to the knowledge of the range or distribution of input data.

Now, we are ready to define differential privacy of the mechanism (5).

Definition 2.4: Let $(\mathbb{R}^{(t+1)q}, \mathcal{F}, \mathbb{P})$ be a probability space. The mechanism (5) is said to be (ε, δ)-*differentially private* for Adj_p^c at a finite time instant $t \in \mathbb{Z}_+$ if there exist $\varepsilon > 0$ and $\delta \geq 0$ such that

$$\begin{aligned} &\mathbb{P}(O_t x_0 + N_t U_t + W_t \in \mathcal{S}) \\ &\leq \mathrm{e}^{\varepsilon} \mathbb{P}(O_t x_0' + N_t U_t' + W_t \in \mathcal{S}) + \delta, \ \forall \mathcal{S} \in \mathcal{F} \end{aligned} \tag{6}$$

for any $((x_0, U_t), (x_0', U_t')) \in \mathrm{Adj}_p^c$. $\lhd$

Remark 2.5: There are two minor differences between Definition 2.3 and the symmetric binary relation in [27]. In [27], it is assumed that $x_0 = x_0'$ in the binary relation and the pair of input sequences (U_t, U_t') are the same except for one element in the sequence, which is a special case of Definition 2.3. Our definition of differential privacy is a direct extension of the original one [17], [18] and slightly different from that defined for linear dynamical systems in [27]; our definition depends on the initial state in addition to the input sequence, and W_t is not necessarily causal. $\lhd$

If ε and δ are large, then for a different pair of input data $((x_0, U_t), (x_0', U_t'))$, the corresponding probability distributions of output data $(Y_{w,t}, Y_{w,t}')$ can be very different, i.e., a mechanism is less private. Therefore, the privacy level of a mechanism can be evaluated by the pair of variables ε and δ. From its definition, one notices that if a mechanism is $(\varepsilon_1, \delta_1)$-differentially private, then it is $(\varepsilon_2, \delta_2)$-differentially private for any $\varepsilon_2 \geq \varepsilon_1$ and $\delta_2 \geq \delta_1$. Therefore, ε and δ give a lower bound on the privacy level, where larger ε and δ imply lower privacy levels.

As is clear from the definition, ε and δ also depend on noise. In fact, we will show that the sensitivity of the dynamical system (1) provides the lower bound on the covariance matrix for the multivariate Gaussian noise to achieve (ε, δ)-differential privacy, which is a generalization of [18], [27, Theorem 3]. In what follows, we call a mechanism with the Gaussian noise a *Gaussian mechanism*.

Theorem 2.6: The Gaussian mechanism (5) induced by $W_t \sim \mathcal{N}_{(t+1)q}(\mu, \Sigma)$ is (ε, δ)-differentially private for Adj_2^c at a finite time $t \in \mathbb{Z}_+$ with $\varepsilon > 0$ and $1/2 > \delta > 0$ if the covariance matrix $\Sigma \succ 0$ is chosen such that

$$\lambda_{\max}^{-1/2}(\mathcal{O}_{\Sigma,t}) \geq c\mathsf{R}(\varepsilon, \delta), \tag{7}$$

where

$$\mathcal{O}_{\Sigma,t} := \begin{bmatrix} O_t & N_t \end{bmatrix}^\top \Sigma^{-1} \begin{bmatrix} O_t & N_t \end{bmatrix}. \tag{8}$$

Proof: Using a similar argument as in the proof for [27, Theorem 3], for arbitrary $\varepsilon > 0$, one has

$$\begin{aligned} &\mathbb{P}(O_t x_0 + N_t U_t + W_t \in \mathcal{S}) \\ &\leq \mathrm{e}^{\varepsilon} \mathbb{P}(O_t x_0' + N_t U_t' + W_t \in \mathcal{S}) + \mathbb{P}\left(\tilde{W} \geq \varepsilon z - 1/2z\right), \end{aligned}$$

where

$$z := |O_t(x_0' - x_0) + N_t(U_t' - U_t)|_{\Sigma^{-1}}^{-1},$$

and $\tilde{W} \sim \mathcal{N}(0, 1)$. Then, the mechanism is (ε, δ)-differentially private if $\mathsf{Q}\left(\varepsilon z - \frac{1}{2z}\right) \leq \delta$, i.e.

$$z \geq \mathsf{R}(\varepsilon, \delta), \tag{9}$$

for any $((x_0, U_t), (x_0', U_t')) \in \mathrm{Adj}_2^c$. The inequality (9) holds if (7) is satisfied because

$$z^{-1} = |O_t(x_0' - x_0) + N_t(U_t' - U_t)|_{\Sigma^{-1}} \leq c\lambda_{\max}^{1/2}(\mathcal{O}_{\Sigma,t}).$$

■

In (7), only the matrix $\begin{bmatrix} O_t & N_t \end{bmatrix}$ depends on the system dynamics (1). We will analyze this matrix in terms of system (1)'s input observability in the next subsection. When the initial state (resp. input sequence) is public, the condition (7) can be replaced by $\lambda_{\max}^{-1/2}(N_t^\top \Sigma^{-1} N_t) \geq c\mathsf{R}(\varepsilon, \delta)$ (resp. $\lambda_{\max}^{-1/2}(O_t^\top \Sigma^{-1} O_t) \geq c\mathsf{R}(\varepsilon, \delta)$). The matrix $\mathcal{O}_{\Sigma,t}$ defined in (8) is in fact the Fisher information matrix of Y_t with respect to $[x_0; \ U_t]$. Therefore, Theorem 2.6 connects differential privacy with Fisher information.

From (8), $\lambda_{\max}^{1/2}(\mathcal{O}_{\Sigma,t})$ is the 2-induced matrix norm of $\Sigma^{-1/2}[O_t \ N_t]$, denoted by $|\Sigma^{-1/2}[O_t \ N_t]|_2$. This can be upper bounded as follows.

$$\begin{aligned} \lambda_{\max}^{1/2}(\mathcal{O}_{\Sigma,t}) &= \left|\Sigma^{-1/2}\begin{bmatrix} O_t & N_t \end{bmatrix}\right|_2 \\ &\leq \left|\Sigma^{-1/2}\right|_2 \left|\begin{bmatrix} O_t & N_t \end{bmatrix}\right|_2 \\ &= \lambda_{\min}^{-1/2}(\Sigma)\lambda_{\max}^{1/2}\left(\mathcal{O}_{I_{(t+1)q},t}\right), \end{aligned}$$

and consequently,

$$\lambda_{\max}^{-1/2}(\mathcal{O}_{\Sigma,t}) \geq \lambda_{\min}^{1/2}(\Sigma)\lambda_{\max}^{-1/2}\left(\mathcal{O}_{I_{(t+1)q},t}\right). \tag{10}$$

Therefore, for any given c, $\varepsilon > 0$ and $1/2 > \delta > 0$, one can make the Gaussian mechanism (ε, δ)-differentially private if one makes the minimum eigenvalue of the covariance matrix Σ sufficiently large such that

$$\lambda_{\min}^{1/2}(\Sigma) \geq c\lambda_{\max}^{1/2}\left(\mathcal{O}_{I_{(t+1)q},t}\right) \mathsf{R}(\varepsilon, \delta) \tag{11}$$

because (10) and (11) imply (7). In the special case where $\Sigma = \sigma^2 I_{(t+1)q}$, $\sigma > 0$ (an i.i.d. Gaussian noise), (11) becomes

$$\sigma \geq c\lambda_{\max}^{1/2}\left(\mathcal{O}_{I_{(t+1)q},t}\right) \mathsf{R}(\varepsilon, \delta). \tag{12}$$

Still one can design σ to make the Gaussian mechanism (ε, δ)-differentially private for arbitrary $\varepsilon > 0$ and $1/2 > \delta > 0$.

Remark 2.7: One can also extend [27, Theorem 2] to use the i.i.d. Laplace noise in our problem setting. However, the extension to the multivariate Laplace noise is not easy because this involves the computation of the modified Bessel function of the second kind. Let $w_i(t)$, $i = 1, \ldots, q$, $t \in \mathbb{Z}_+$ be an i.i.d. Laplace noise with the variance $\mu \in \mathbb{R}$ and distribution $b > 0$. Then, the Laplace mechanism (5) is $(\varepsilon, 0)$-differentially private at a finite time t with $\varepsilon > 0$ if

$$b \geq c \left|\begin{bmatrix} O_t & N_t \end{bmatrix}\right|_1 / \varepsilon,$$

for any $((x_0, U_t), (x_0', U_t')) \in \mathrm{Adj}_1^c$, where $|A|_1 := \max_j \sum_i |a_{i,j}|$ is the induced matrix 1-norm. As for the Gaussian mechanism, the induced matrix norm of $[O_t \ N_t]$ plays a crucial role for the Laplace mechanism too. In the next subsection, we study its 2-norm in terms of system (1)'s input observability. Because of the equivalence of induced matrix norms, the observation for the 2-norm is applicable to an arbitrary norm including the 1-norm. ◁

Remark 2.8: In this subsection, to make the input data private, noise is added to the output data, which makes the output data also private. To analyze the differential privacy level of the output data, one can employ the conventional results for a static data set in [17], [18]. By adding a sufficiently large noise, it is possible to achieve the differential privacy requirements for the input data and output data at the same time. ◁

Note that in Theorem 2.6, the system (1) is not necessarily stable. Now, we focus on asymptotically stable systems. Then, one can characterize the differentially privacy level in terms of the H_∞-norm and the observability Gramian, where the H_∞-norm of the system (1) is the infimum non-negative constant γ satisfying

$$\sum_{\tau=0}^{t} |y(\tau)|_2^2 \leq \gamma^2 \sum_{\tau=0}^{t} |u(\tau)|_2^2, \ \forall t \in \mathbb{Z}_+,$$

for all L_2-bounded input signals, and the observability Gramian is

$$\mathcal{O}_\infty := O_\infty^\top O_\infty = \sum_{t=0}^{\infty} (CA^t)^\top (CA^t), \tag{13}$$

where O_t is defined in (3). Note that $\lambda_{\max}(O_t^\top O_t)$ is non-decreasing with $t \in \mathbb{Z}_+$, and for the asymptotically stable system, $\mathcal{O}_\infty$ is finite. Now, we obtain the following result as a corollary of Theorem 2.6.

Corollary 2.9: The Gaussian mechanism (5) induced by an asymptotically stable system (1) and $W_t \sim \mathcal{N}_{(t+1)q}(\mu, \Sigma)$ is (ε, δ)-differentially private for Adj_2^c at a finite time $t \in \mathbb{Z}_+$ with $\varepsilon > 0$ and $1/2 > \delta > 0$ if the covariance matrix $\Sigma \succ 0$ is chosen such that the following inequality holds

$$\lambda_{\min}^{1/2}(\Sigma) \geq c\left(\lambda_{\max}^{1/2}(\mathcal{O}_\infty) + \gamma\right) \mathsf{R}(\varepsilon, \delta). \tag{14}$$

Proof: It holds that

$$\begin{aligned}
&|O_t(x_0' - x_0) + N_t(U_t' - U_t)|_{\Sigma^{-1}} \\
&\leq |O_t(x_0' - x_0)|_{\Sigma^{-1}} + |N_t(U_t' - U_t)|_{\Sigma^{-1}} \\
&\leq \lambda_{\max}^{1/2}(\Sigma^{-1})(|O_t(x_0' - x_0)|_2 + |N_t(U_t' - U_t)|_2) \\
&\leq c\lambda_{\max}^{1/2}(\Sigma^{-1})\left(\lambda_{\max}^{1/2}(\mathcal{O}_\infty) + \gamma\right).
\end{aligned}$$

Therefore, (14) implies (9), where $1/\lambda_{\max}(\Sigma^{-1}) = \lambda_{\min}(\Sigma)$ is used. ■

If x_0 is public and the multivariate Gaussian is i.i.d, Corollary 2.9 reduces to [27, Corollary 1]. When the initial state (resp. input sequence) is public, the condition (14) can be replaced by $\lambda_{\min}^{1/2}(\Sigma) \geq c\gamma \mathsf{R}(\varepsilon, \delta)$ (resp. $\lambda_{\min}^{1/2}(\Sigma) \geq c\lambda_{\max}^{1/2}(\mathcal{O}_\infty)\mathsf{R}(\varepsilon, \delta)$). From the proof, one notices that for an asymptotically stable system (1), if the covariance matrix Σ is chosen such that (14) holds, then (7) holds for any $t \in \mathbb{Z}_+$. That is, for any asymptotically stable system (1) and for any $\varepsilon > 0$ and $1/2 > \delta > 0$, there exists a non-degenerate multivariate Gaussian noise which makes the induced mechanism (ε, δ)-differentially private for any $t \in \mathbb{Z}_+$. However, this is not always true for unstable systems; a similar statement can be found in [43, Theorem 4.5].

B. Connection with Strong Input Observability

In the previous subsection, we have studied the (ε, δ)-differential privacy of a Gaussian mechanism induced by output noise. However, it is not intuitively clear how differential privacy relates to dynamical systems' other intrinsic properties. For differential privacy, noise is designed to prevent the initial state and input sequence from being identified from the published output sequence. From the systems and control point of view, the property of determining the initial state and input sequence can be interpreted as observability or left invertibility [30], [31]. In this subsection, we study the Gaussian mechanism from the input observability perspective.

First, we define what we mean by strong input observability.

Definition 2.10: The system (1) is said to be *strongly input observable* if there exists $T \in \mathbb{Z}_+$ such that both the initial state $x_0 \in \mathbb{R}^n$ and initial input $u(0) \in \mathbb{R}^m$ can be uniquely determined from the measured output sequence Y_T. ◁

It is worth mentioning that if $(x_0, u(0))$ is uniquely determined from Y_T, then $(x(k), u(k))$ is consequently uniquely determined from Y_{T+k}, $k = 1, 2, \ldots$. Hence, one can focus on $(x_0, u(0))$ in the definition of strong input observability. Note that although strong input observability may seem too strong to hold for many existing engineering systems, more emerging and future systems may very likely possess this property after more sensed data and communicated information become available.

Remark 2.11: There are several similar but different concepts from strong input observability just defined. On the one

hand, if U_T is known, the analysis reduces to determining the initial state x_0, i.e, the standard observability analysis [44]. When U_T is unknown, the property that x_0 can be uniquely determined is called unknown-input (or strong) observability [45]. On the other hand, if x_0 is known, the analysis reduces to determining the initial input $u(0)$; this property is called input observability with the known initial state x_0 [30] or left invertibility [31]. In the case, for the unknown initial state x_0, the property that the initial input $u(0)$ can be uniquely determined is called input observability [30]. Therefore, our strong input observability requires both unknown-input (or strong) observability and input observability. $\lhd$

The results in the existing observability analysis are helpful for the strong input observability analysis. Especially, by extending [31, Theorem 3], we have the following necessary and sufficient condition for strong input observability. Since the proof is similar, it is omitted.

Theorem 2.12: The system (1) is strongly input observable if and only if

$$\operatorname{rank}\left[\begin{array}{cc} O_{2n} & N_{2n,n} \end{array}\right] = n + (n+1)m \tag{15}$$

for O_t in (3) and the submatrix $N_{t,T}$ of N_t in (4), i.e., the matrix $[O_{2n}\ N_{2n,n}]$, has the column full rank. $\lhd$

The following corollary is also used in this paper.

Corollary 2.13: The system (1) is strongly input observable if and only if

$$\operatorname{rank}\left[\begin{array}{cc} O_t & N_{t,T} \end{array}\right] = n + (T+1)m, \tag{16}$$

for any integers $T \geq n$ and $t \geq T + n$. $\lhd$

Proof: From the structures of O_t and $N_{t,T}$, if $[O_{2n}\ N_{2n,n}]$ has the column full rank, then

$$\operatorname{rank}\left[\begin{array}{cc} O_{2n} & N_{2n,n} \end{array}\right] = \operatorname{rank}\left[\begin{array}{cc} O_{2n+t} & N_{2n+t,n} \end{array}\right]$$

for any $t \in \mathbb{Z}_+$. Conversely, from the Cayley-Hamilton theorem [46], if $[O_{2n+t}\ N_{2n+t,n}]$ has the column full rank for some $t \in \mathbb{Z}_+$, then (15) holds. ■

The rank condition (15) or (16) is a *qualitative* criterion for strong input observability, but differential privacy is a *quantitative* criterion. A connection between these two concepts can be established by extending the concept of the observability Gramian to strong input observability because controllability and observability Gramians give both quantitative and qualitative criteria. To extend the concept of the Gramian, we consider a weighted least square estimation problem[1] of the initial state x_0 and input sequences U_T, $T \geq n$, from the output sequence with the measurement noise $Y_{w,t}$, $t \geq T+n$, under the technical assumption $u(\tau) = 0$, $t \geq \tau > T$:

$$J_{(x_0,U_T)} = \min_{(x_0,U_T)\in\mathbb{R}^n\times\mathbb{R}^{(T+1)m}} |Y_{w,t} - O_t x_0 - N_{t,T}U_T|^2_{\Sigma^{-1}}. \tag{17}$$

This problem has a unique solution if (16) holds, i.e., the system is strongly input observable, in which case the solution is

$$\left[\begin{array}{c} \hat{x}_0 \\ \hat{U}_T \end{array}\right] = (\mathcal{O}_{\Sigma,t,T})^{-1}\left[\begin{array}{cc} O_t & N_{t,T} \end{array}\right]^\top \Sigma^{-1} Y_{w,t}, \tag{18}$$

where

$$\mathcal{O}_{\Sigma,t,T} := \left[\begin{array}{cc} O_t & N_{t,T} \end{array}\right]^\top \Sigma^{-1}\left[\begin{array}{cc} O_t & N_{t,T} \end{array}\right]. \tag{19}$$

When there is no measurement noise, i.e., $W_T = 0$, it follows that (18) gives the actual initial state and input sequence.

One notices that $\mathcal{O}_{\Sigma,t,t} = \mathcal{O}_{\Sigma,t}$ for $\mathcal{O}_{\Sigma,t}$ in (8). As for $\mathcal{O}_{\Sigma,t}$, the matrix $\mathcal{O}_{\Sigma,t,T}$ characterizes the differential privacy level of a Gaussian mechanism, which we state as a corollary of Theorem 2.6 without the proof.

Corollary 2.14: Let $T \geq n$ and $t \geq T + n$. For any $((x_0, U_t), (x_0', U_t'))$ belonging to Adj_2^c and satisfying $u(\tau) = u'(\tau)$, $T < \tau \leq t$, the Gaussian mechanism (5) induced by $W_t \sim \mathcal{N}_{(t+1)q}(\mu, \Sigma)$ is (ε, δ)-differentially private at a finite time $t \in \mathbb{Z}_+$ with $\varepsilon > 0$ and $1/2 > \delta > 0$, if the covariance matrix $\Sigma \succ 0$ is chosen such that

$$\lambda_{\max}^{-1/2}(\mathcal{O}_{\Sigma,t,T}) \geq c\mathsf{R}(\varepsilon, \delta). \tag{20}$$

$\lhd$

Notice that if $T = t$, (20) is equivalent to (7). From (20), Corollary 2.14 concludes that the differential privacy of the Gaussian mechanism is characterized by the maximum eigenvalue of the matrix $\mathcal{O}_{\Sigma,t,T}$, where $\mathcal{O}_{\Sigma,t,T}$ is not necessarily non-singular in differential privacy analysis; non-singularity is required to guarantee the uniqueness of a solution to the least square estimation problem (17).

For $\Sigma = I_{(t+1)q}$, we call $\mathcal{O}_{t,T} := \mathcal{O}_{I_{(t+1)q},t,T}$ the *strong input observability Gramian*. The strong input observability Gramian is both qualitative and quantitative for strong input observability. For instance, from Corollary 2.13, the system (1) is strongly input observable if and only if $\mathcal{O}_{t,T}$ is non-singular for any integers $T \geq n$ and $t \geq n + T$. Also, by substituting $(\hat{x}_0, \hat{U}_T)$ of (18) into (x_0, U_T) of (17), one notices that if all eigenvalues of $\mathcal{O}_{t,T}$ is large, then $J_{(x_0,U_T)}$ in (17) with $\Sigma = I_{(t+1)q}$ is small. That is, (x_0, U_T) is relatively easy to be estimated. This observation agrees with (20) because for $\Sigma = \sigma^2 I_{(t+1)q}$, large σ is required if $\lambda_{\max}(\mathcal{O}_{t,T})$ is large; recall (12). In other words, small noise is enough to make the less input observable Gaussian mechanism highly differentially private.

To gain deeper insight following the privacy analysis, we take a further look at the eigenvalues of the strong input observability Gramian $\mathcal{O}_{t,T}$ from three aspects. First, from (3), (4) and (19) with $\Sigma = I_{(t+1)q}$, the first $m \times m$ block diagonal element of $\mathcal{O}_{t,T}$ is

$$(\mathcal{O}_{t,T})_{1,1} := \sum_{k=0}^{t} (CA^k)^\top CA^k,$$

and for $i \geq 2$, the ith $m \times m$ block diagonal element of $\mathcal{O}_{t,T}$ is

$$(\mathcal{O}_{t,T})_{i,i} := D^\top D + \sum_{k=0}^{t-i-2} (CA^kB)^\top CA^kB,$$
$$i = 2, \ldots, T+1$$

[1]Note that the controllability Gramian is originally obtained from the minimum energy control problem [47]. The duals of the controllability Gramian and minimum energy control problem are respectively the observability Gramian and least square estimation problem of the initial state.

where $(\mathcal{O}_{t,T})_{T+1,T+1} := D^\top D$ when $t = T$. One notices that $(\mathcal{O}_{t,T})_{1,1}$ is the standard observability Gramian for the initial state x_0, and $(\mathcal{O}_{t,T})_{i,i}$, $i \geq 2$ can be viewed as the observability Gramian corresponding to the initial input $u(0)$, which we call the *initial input observability Gramian*. Since the trace of a matrix is the sum of all its eigenvalues, and the trace of $\mathcal{O}_{t,T}$ is the sum of the traces of all its block diagonal elements $(\mathcal{O}_{t,T})_{i,i}$, $i = 1, \ldots, T+1$, the sum of the eigenvalues of $\mathcal{O}_{t,T}$ is the sum of the eigenvalues of all $(\mathcal{O}_{t,T})_{i,i}$, $i = 1, \ldots, T+1$. Therefore, if the standard and initial input observability Gramians have large eigenvalues, the strong input observability Gramian $\mathcal{O}_{t,T}$ has large eigenvalues also. In other words, the privacy level of the initial state and whole input sequence is characterized by that of only the initial state and initial input. This fact is natural because of two facts: 1) the output at each time instant contains the information of the initial state and initial input, i.e. these are the least private information; 2) if the initial state and initial input are uniquely determined, the whole input sequence is uniquely determined.

Next, for fixed t, the minimum eigenvalue of $\mathcal{O}_{t,T}$ does not increase with T. For instance,

$$\lambda_{\min}(\mathcal{O}_{t,1}) \leq \lambda_{\min}(\mathcal{O}_{t,0}). \tag{21}$$

Recall that these two Gramians are obtained from the least square estimation problems when $u(t) = 0$ for $t = 2, 3, \ldots$ and $t = 1, 2, \ldots$, respectively. Therefore, (21) corresponds to a natural observation that $u(0)$ is more difficult to estimate if $u(1)$ is unknown compared to the case when $u(1)$ is known to be 0.

Finally, for fixed T, $\lambda_{\max}(\mathcal{O}_{t,T})$ is non-decreasing with t, and thus ε in Corollary 2.14 is non-decreasing with t. This implies that as more data are being collected, less private a mechanism becomes. It is worth emphasizing that this observation is obtained when $\Sigma = I_{(t+1)q}$, or more generally $\Sigma = \sigma^2 I_{(t+1)q}$, $\sigma > 0$, i.e., the output noise is i.i.d. Therefore, by employing non-i.i.d. noise, it is still possible to keep the same privacy level in longer duration; we will discuss this in the next subsection.

The above discussions are based on the minimum or maximum eigenvalue of the strong input observability Gramian. For more detailed privacy (strong input observability) analysis, each eigenvalue and the associated eigen-space can be used as typically done for the standard observability Gramian. Let $v_i \in \mathbb{R}^{n+(T+1)m}$, $i = 1, \ldots, n+(T+1)m$, be the eigenvectors of $\mathcal{O}_{t,T}$ associated with the eigenvalues $\lambda_i \leq \lambda_{i+1}$. If there is k such that $\lambda_k \ll \lambda_{k+1}$, then $(x_0, U_T) \in \operatorname{span}\{v_{k+1}, \ldots, v_T\}$ is relatively easy to observe. Especially, if $0 < \lambda_{k+1}$, then such (x_0, U_T) can be uniquely determined, and the projection of $\operatorname{span}\{v_{k+1}, \ldots, v_T\}$ onto the $(x_0, u(0))$-space gives the strongly input observable subspace. For the (non-strong) input observability with known initial state (i.e., left invertibility), the input observable and unobservable subspaces have been studied based on an extension of Kalman's canonical decomposition [48], but quantitative analysis has not been established yet.

The quantitative analysis of subspaces can be used for designing noise to make a system more private. Let $\lambda_k \ll \lambda_{k+1}$, and consider the projection of $\operatorname{span}\{v_{k+1}, \ldots, v_T\}$ onto the $(x_0, u(0))$-space, which we denote by $\mathcal{X} \times \mathcal{U} \subset \mathbb{R}^n \times \mathbb{R}^m$. Then, the output of the system is sensitive to the initial states and inputs in $\mathcal{X} \times \mathcal{U}$; in other words, such initial states and inputs are less private. To protect less private input information, one can directly add noise $v \in \mathcal{X} \times \mathcal{U}$ to the initial state and the input channel instead of the output channel. This motivates us to study differential privacy with input noise.

C. Differential Privacy With Input Noise

In this subsection, we study the scenario where noise is added to the input channel. In this case, one can directly decide the distribution of estimated input data. However, additional effort is needed for studying the utility of the output data. Furthermore, differential privacy analysis is technically more involved because the output variables are not necessarily non-degenerate (while they are Gaussian if the input noise is Gaussian). To address this issue, even though artificial, some technical procedure is required, which is essentially equivalent to selecting a different base measure using the disintegration theorem [49]. As the main result of this subsection, we show that the differential privacy levels of the Gaussian mechanisms induced by the input noise and output noise can be made the same for suitable choices of the input noise and output noise.

To proceed with analysis, we assume that the system (1) is strongly input observable, i.e., the matrix in (16) has the column full rank for any $T \geq n$ and $t \geq T + n$, which implicitly implies $(t+1)q \geq n + (T+1)m$. Then, there exists a $(t+1)q - (n + (T+1)m)$ by $(t+1)q$ matrix $\overline{N}_{t,T}$ such that

$$\operatorname{rank} \overline{N}_t = (t+1)q,$$

and

$$\begin{bmatrix} O_t & N_{t,T} \end{bmatrix}^\top \overline{N}_{t,T} = 0, \tag{22}$$

where

$$\overline{N}_t := \begin{bmatrix} O_t & N_{t,T} & \overline{N}_{t,T} \end{bmatrix}. \tag{23}$$

Remark 2.15: If a system is strongly input unobservable, i.e., (16) does not hold, then one can use the singular value decomposition of $[O_t \; N_{t,T}]$ for similar analysis. $\lhd$

Now, we consider the following system with the initial state, input and output noises,

$$\begin{cases} x(t+1) = Ax(t) + B(u(t) + v(t)), x(0) = x_0 + v_x \\ y_v(t) = Cx(t) + D(u(t) + v(t)) + v_d(t), \end{cases} \tag{24}$$

where the output noise v_d is generated by the dummy variables $\overline{V}_{d,t,T} \in \mathbb{R}^{(t+1)q-(n+(T+1)m)}$ as

$$\begin{bmatrix} v_d(0); & v_d(1); & \cdots; & v_d(t) \end{bmatrix} = \overline{N}_{t,T} \overline{V}_{d,t,T}. \tag{25}$$

The reason we call them the dummy variables is that $\overline{V}_{d,t,T}$ does not affect the differential privacy level, which will be explained later. By recalling the notation of a sequence introduced in the introduction, define

$$\overline{V}_t := \begin{bmatrix} v_x; & V_t; & \overline{V}_{d,t,T} \end{bmatrix} \in \mathbb{R}^{(t+1)q}. \tag{26}$$

From (23) and (26), for $v(\tau)=0$, $\tau>T$, the output sequence $Y_{v,t}\in\mathbb{R}^{(t+1)q}$ can be described by

$$\begin{aligned}Y_{v,t}&=O_t(x_0+v_x)+N_t(U_t+V_T)+\overline{N}_{t,T}\overline{V}_{d,t,T}\\&=O_tx_0+N_tU_t+\overline{N}_t\overline{V}_t.\end{aligned}\tag{27}$$

We study the connection between the differential privacy levels of mechanisms (5) and (27). The important fact is that the numbers of the elements of W_t and $\overline{V}_t$ are the same, and from (23), $\overline{N}_t$ is non-singular. For mechanisms (5) and (27), the generated output sequences are the same if and only if $W_t=\overline{N}_t\overline{V}_t$. Therefore, the designs of the noises W_t and $\overline{V}_t$ are equivalent problems. In the previous subsection, we have studied the differential privacy of the Gaussian mechanism (5). Similarly, for the Gaussian mechanism (27), we have the following corollary of Theorem 2.6.

Corollary 2.16: Let $T\geq n$ and $t\geq T+n$. Also let $\overline{V}_t\sim\mathcal{N}_{(t+1)q}(\overline{\mu},\mathrm{diag}\{\overline{\Sigma}_1,\overline{\Sigma}_2\})$ be a non-degenerate multivariate Gaussian noise, where $\overline{\Sigma}_1\in\mathbb{R}^{(n+(T+1)m)\times(n+(T+1)m)}$ is the covariance matrix of the initial state and input noise $[v_x;V_t]$, and $\overline{\Sigma}_2$ is that of the dummy variable $\overline{V}_{d,t,T}$. Then, for any $((x_0,U_t),(x_0',U_t'))$ belonging to Adj_2^c and satisfying $u(\tau)=u'(\tau)$, $T<\tau\leq t$, the Gaussian mechanism (27) induced by the strongly input observable system (1) and $\overline{V}_t$ is (ε,δ)-differentially private at a finite time $t\in\mathbb{Z}_+$ if the covariance matrix $\overline{\Sigma}_1$ is chosen such that

$$\lambda_{\min}^{1/2}(\overline{\Sigma}_1)\geq c\mathsf{R}(\varepsilon,\delta).\tag{28}$$

Proof: Instead of (7), one has

$$\begin{aligned}&\lambda_{\max}^{-1/2}\left(\begin{bmatrix}O_t & N_{t,T}\end{bmatrix}^\top\overline{N}_t^{-\top}\overline{\Sigma}^{-1}\overline{N}_t^{-1}\begin{bmatrix}O_t & N_{t,T}\end{bmatrix}\right)\\&\geq c\mathsf{R}(\varepsilon,\delta).\end{aligned}$$

From (23), it follows that

$$\begin{aligned}&\begin{bmatrix}O_t & N_{t,T}\end{bmatrix}^\top\overline{N}_t^{-\top}\overline{\Sigma}^{-1}\overline{N}_t^{-1}\begin{bmatrix}O_t & N_{t,T}\end{bmatrix}\\&=\begin{bmatrix}I_{n+(T+1)m} & 0\end{bmatrix}\overline{N}_t^\top\overline{N}_t^{-\top}\overline{\Sigma}^{-1}\overline{N}_t^{-1}\overline{N}_t\begin{bmatrix}I_{n+(T+1)m}\\0\end{bmatrix}\\&=\overline{\Sigma}_1^{-1}.\end{aligned}$$

Therefore, (28) holds. ∎

Corollary 2.16 concludes that the differential privacy level only depends on the covariance $\overline{\Sigma}_1$ of the input noise $[v_x;V_T]$, i.e., the differential privacy level does not depend on the system itself. The covariance $\overline{\Sigma}_1$ gives an intuitive interpretation of the privacy level of the input. Therefore, Corollary 2.14 can help understanding the interpretation of the magnitudes of (ε,δ) from the perspective of the privacy level of the input.

In Corollary 2.14 and Theorem 2.16, the differential privacy levels of both mechanisms are the same if

$$\mathcal{O}_{\Sigma,t,T}=\begin{bmatrix}O_t & N_t\end{bmatrix}^\top\Sigma^{-1}\begin{bmatrix}O_t & N_t\end{bmatrix}=\overline{\Sigma}_1^{-1},\tag{29}$$

where we recall (19) for the first equality; the converse is not true in general since differential privacy only evaluates the maximum eigenvalues. Therefore, adding the Gaussian noise with the covariance Σ to the output of the system (1) is equivalent to adding the Gaussian noise with the covariance $\mathcal{O}_{\Sigma,t,T}^{-1}$ to the input of the system (1) under the strong input observability assumption.

In the previous subsection, we mentioned that the privacy level of the mechanism (5) with the i.i.d. output noise $\Sigma=\sigma I_{(t+1)q}$ decreases with the growth of duration. In contrast, if one adds noise to the initial state and input channel, the privacy level of a mechanism does not depend on the duration because one can directly decide the distribution of the estimated initial state and input sequence. These two facts do not contradict each other if one allows to add non-i.i.d output noise. From (29), adding suitable non-i.i.d. noise to the output channel has a similar effect as adding noise to the initial state and input channel. Therefore, adding non-i.i.d. noise is a key factor for keeping the same privacy level against the duration when one adds noise to the output channel.

Finally, the reason that the dummy variables $\overline{V}_{d,t,T}$ do not affect the differential privacy level can be explained based on the least square estimation problems of the initial state and input sequence. For a strongly input observable system, the solution to the following least square estimation problem

$$\overline{J}_{(x_0,U_T)}=\min_{(x_0,U_T)\in\mathbb{R}^n\times\mathbb{R}^{(T+1)m}}|Y_{v,t}-O_tx_0-N_{t,T}U_T|_2^2$$

is, from (16), (22), and (27),

$$\begin{bmatrix}\hat{x}_0\\\hat{U}_T\end{bmatrix}=\mathcal{O}_{t,T}^{-1}\begin{bmatrix}O_t & N_{t,T}\end{bmatrix}^\top Y_{v,t}=\begin{bmatrix}x_0\\U_T\end{bmatrix}+\begin{bmatrix}v_x\\V_T\end{bmatrix}.$$

The least square estimation is the actual initial state and input sequence plus the noise added to them. Because of the condition (22), the dummy variable $\overline{V}_{d,t,T}$ is canceled. This is the reason that the dummy variable does not affect differential privacy analysis.

III. Privacy-Preserving Controllers

A. Motivating Example

We start with a motivating example. Consider DC microgrids [50] installed with smart meters whose dynamics are described by

$$\begin{aligned}L_i\dot{I}_i(t)&=-R_iI_i(t)-V_i(t)+u_i(t),\ I_i(t):=I_{T,i}(t)-I_{L,i},\\C_i\dot{V}_i(t)&=I_i(t)-\sum_{j\in\mathcal{N}_i}I_{i,j}(t),\\L_{i,j}\dot{I}_{i,j}(t)&=(V_i(t)-V_j(t))-R_{i,j}I_{i,j}(t),\\y_{i,1}(t)&=V_i(t),\ y_{i,2}(t)=I_i(t),\end{aligned}\tag{30}$$

where $I_{T,i}(t)\in\mathbb{R}$, $V_i(t)>0$, and $I_{i,j}(t)\in\mathbb{R}$ denote the generator current, load voltage, the current between nodes i and j, respectively, and $I_{L,i}\in\mathbb{R}$ denote the load current, which can be viewed as a constant in the time scale of controller design. The parameters $L_i,L_{i,j},R_i,R_{i,j},C_i>0$ denote inductances, resistances, and capacitance, respectively. The set of neighbors of node i is denoted by $\mathcal{N}_i$, and the number of the neighbors is denoted by n_i. For analysis and controller design, we use its zero-order-hold discretization, since each output information is collected and sent to the power company digitally.

One objective of the power company is to maintain the stability of the system by keeping $V_i(t)$ to the prescribed value V^* and the difference between the generator current

(i.e. supply) and load current (i.e. demand), denoted by $I_i(t)$, to zero. Therefore, the control objective is

$$\lim_{t\to\infty} V_i(t) = V^*, \ \lim_{t\to\infty} I_i(t) = 0. \tag{31}$$

Owing to developments of IoT technologies, smart meters are becoming more widely available, which can be used to monitor and send the value of $I_i(t)(= I_{T,i}(t) - I_{L,i})$ to the power company online. However, the desired load current $I_{L,i}$ is determined by each user and thus contains the information of each user's lifestyle. Since this load current of privacy concern is static, one can use existing results for static differential privacy, e.g. [21].

However, there is bigger privacy issue that needs to be addressed. Our observations in the previous section indicate the possibility that a user i can identify the other users' $[V_i, I_i]$ from its own dynamical control input data sets u_i. So the privacy of user i here is concerned with her wish not letting the other users be able to identify that her consumption pattern has changed, and such a privacy issue depends on controller dynamics. Thus, one is forced to consider designing a tracking controller by taking privacy into account. The privacy-protection objective is that even if user i's $[V_i, I_i]$ becomes different from $[V^*, 0]$, another user j cannot infer the occurrence of the difference from u_j, $j \neq i$. This privacy requirement should not conflict with the control objective (31) of tracking the desired signals.

In the following subsections, first we summarize the standard result for tracking controller design based on the internal model principle. Then, we impose a differential privacy requirement for a tracking controller. In the end, we consider estimating private information and evaluate its difficulty.

B. Tracking Controllers

To be self-contained, in this subsection, an existing tracking controller is shown. This controller has tuning parameters that will be adjusted based on a privacy requirement in the next subsection.

Consider the following plant

$$\begin{cases} x_p(t+1) = A_p x_p(t) + B_p u_p(t), \\ y_p(t) = C_p x_p(t) + D_p u_p(t), \end{cases} \tag{32}$$

where $x_p(t) \in \mathbb{R}^{n_p}$, $u_p(t) \in \mathbb{R}^{m_p}$ and $y_p(t) \in \mathbb{R}^{q_p}$ denote the state, input and output, respectively, and $A_p \in \mathbb{R}^{n_p\times n_p}$, $B_p \in \mathbb{R}^{n_p\times m_p}$, $C_p \in \mathbb{R}^{q_p\times n_p}$ and $D_p \in \mathbb{R}^{q_p\times m_p}$.

The control objective is to design an output feedback controller, which achieves $y_p \to y_r$ as $t \to \infty$ for a given reference output $y_r(t) \in \mathbb{R}^{q_p}$. Suppose that the reference output $y_r(t)$ is generated by the following exosystem:

$$\begin{cases} x_r(t+1) = A_r x_r(t), \ x_r(0) = x_{r,0} \in \mathbb{R}^{n_r}, \\ y_r(t) = C_r x_r(t), \end{cases} \tag{33}$$

where $x_r(t) \in \mathbb{R}^{n_r}$ and $y_r(t) \in \mathbb{R}^{q_r}$; $A_r \in \mathbb{R}^{n_r\times n_r}$ and $C_r \in \mathbb{R}^{q_r\times n_r}$. Then, the composite system consisting of the plant (32) and exosystem (33) is

$$\begin{cases} \bar{x}(t+1) = \bar{A}\bar{x}(t) + \bar{B}u_p(t), \\ e(t) = y_p(t) - y_r(t) = \bar{C}\bar{x}(t) + D_p u_p(t), \end{cases}$$

$$\bar{x} := \begin{bmatrix} x_p \\ x_r \end{bmatrix}, \ \bar{A} := \begin{bmatrix} A_p & 0 \\ 0 & A_r \end{bmatrix}, \ \bar{B} := \begin{bmatrix} B_p \\ 0 \end{bmatrix},$$
$$\bar{C} := \begin{bmatrix} C_p & -C_r \end{bmatrix}.$$

The tracking control objective can be rewritten as $\lim_{t\to\infty} e(t) = 0$.

As an output feedback controller, the following observer based stabilizing controller is typically used

$$\begin{cases} u_p(t) = G x_c(t), \\ x_c(t+1) = A_c x_c(t) - L e(t), \end{cases} \tag{34}$$

where

$$A_c := \bar{A} + L\bar{C} + (\bar{B} + LD_p)G,$$

and $G = [G_1 \ G_2] \in \mathbb{R}^{m_p\times(n_p+n_r)}$ and $L = [L_1^\top \ L_2^\top]^\top \in \mathbb{R}^{(n_p+n_r)\times q_p}$ are design parameters. The tracking problem is solvable by the above dynamic output feedback controller under the following standard assumptions [34].

Assumption 3.1: The matrix A_r has no eigenvalue in the interior of the unit circle. ◁

Assumption 3.2: The pair (A_p, B_p) is stabilizable. ◁

Assumption 3.3: The pair $(\bar{C}, \bar{A})$ is detectable. ◁

Assumption 3.4: The following two equations:

$$XA_r = A_p X + B_p U,$$
$$0 = C_p X + D_p U - C_r,$$

have a pair of solutions $X \in \mathbb{R}^{n_p\times n_r}$ and $U \in \mathbb{R}^{m_p\times n_r}$. ◁

Remark 3.5: Assumption 3.4 guarantees that for any given $x_r(t)$ generated by (33), there exist $x_{p,s}(t)$ and $u_{p,s}(t)$ simultaneously satisfying (32) and $e(t) = y_p(t) - y_r(t) = 0$ for all $t \in \mathbb{Z}_+$. Assumption 3.1 guarantees that such $x_{p,s}(t)$ and $u_{p,s}(t)$ uniquely exist; this assumption is for the ease of discussion and is not necessarily to be imposed as mentioned in [34]. ◁

Under Assumption 3.4, the tracking problem is solvable if the closed-loop system consisting of the plant (32) and the controller (34) is asymptotically stable. From the separation principle [44], the closed loop system can be made asymptotically stable by finding a pair of G_1 and L that makes $A_p + B_p G_1$ and $\bar{A} + L\bar{C}$ asymptotically stable, respectively. Then, G_2 can be designed as $G_2 = U - G_1 X$ for U and X in Assumption 3.4.

C. Privacy Requirements for Controllers

The privacy requirement imposed in the motivating example is to make a user j not be able to distinguish whether another user i's $[V_i, I_i]$ has deviated from $[V^*, 0]$ using its input u_j, $j \neq i$. This corresponds to designing a controller (34) such that e is always inferred to be zero using u_p. Note that this privacy requirement is different from protecting the privacy of y_p, in which case if y_r is a piece of public information, the information $e = y_p - y_r = 0$ cannot be published, and thus in which case protecting y_p conflicts with the tracking control objective, implying one may have to regulate y_p to a different value than y_r. In contrast, the privacy requirement for e does not conflict with the goal of tracking control.

For protecting the information of e, we consider adding noise to u_p. As mentioned in the previous section, adding

sufficiently large noise always achieves the prescribed privacy level. However, large noise can change a control input significantly. Therefore, it is desirable to design a controller which becomes highly private by adding small noise. According to Theorem 2.9, such a controller has a small H_∞-norm.

Remark 3.6: One may consider controller design from different perspectives. Based on Theorem 2.6, differential privacy analysis itself is possible for an unstable controller. However, this theorem does not give a clear indication on how to choose design parameters G_1 and L_1. On the other hand, if a strongly input unobservable controller is designed, the information in the strongly input unobservable space is protected without adding noise as mentioned in Section II-B. However, from Theorem 2.12, this reduces to a rank constraint problem that is difficult to solve in general as the rank minimization problem is known to be NP-hard [51]. Therefore, we design a controller having a small H_∞-norm. $\lhd$

Remark 3.7: In Theorem 2.9, the differential privacy level also depends on the standard observability Gramian of the initial state. However, it is not straightforward to simultaneously specify the maximum eigenvalues of the observability Gramian and H_∞-norm. In fact, it is known that the maximum Hankel singular value, the square root of the maximum eigenvalue of the product of the controllability and observability Gramians, is bounded by the H_∞-norm [52]. Therefore, making H_∞-norm small can result in making the maximum eigenvalue of the observability Gramian small. $\lhd$

Remark 3.8: Even if one adds different noise than the Gaussian noise such as the Laplace noise as in Remark 2.7, making H_∞-norm small can increase the differential privacy level. Making H_∞-norm small can result in making $\lambda_{\max}^{1/2}([\ O_t \quad N_t\ ]^\top[\ O_t \quad N_t\ ])$ small. Then, from the equivalence of the norm, any matrix induced norm of $[\ O_t \quad N_t\ ]$ becomes small. Therefore, from Remark 2.7, the differential privacy level increases also for the Laplace mechanism. $\lhd$

In general, a controller having a bounded H_∞-norm needs to be asymptotically stable. Unfortunately, stable controller design is not always possible because of its structure in (34).

Proposition 3.9: Under Assumptions 3.1-3.4, the controller (34) solving the linear output regulation problem is not asymptotically stable if $D_p = 0$.

Proof: Assumption 3.4, (34), and $G_2 = U - G_1X$ yield

$$\begin{aligned}&\begin{bmatrix} \lambda I_{n_p} - A_p - B_pG_1 & -B_pG_2 \\ 0 & \lambda I_{n_r} - A_r \\ C_p & -C_r \end{bmatrix}\begin{bmatrix} X \\ I_{n-r} \end{bmatrix}\\ &= \begin{bmatrix} \lambda X - A_pX - B_pU \\ \lambda I_{n_r} - A_r \\ C_pX - C_r \end{bmatrix} = \begin{bmatrix} X(\lambda I_{n_r} - A_r) \\ \lambda I_{n_r} - A_r \\ -D_pU \end{bmatrix}.\end{aligned}$$

If $D_p = 0$, this becomes zero when λ is an eigenvalue of A_r. Therefore, for the pair $(\bar{C}, \bar{A} + \bar{B}G)$, any eigenvalue of A_r is not observable. That is, the set of eigenvalues of A_c contains that of A_r, which are marginally stable according to Assumption 3.1. ■

If $D_p \neq 0$, one can use the output regulation controller (34) addressing the privacy requirement. However, there are plenty of systems for which $D_p = 0$. To deal with these systems, we modify the output regulation controller (34) in the next subsection.

D. Controller Design with Privacy Concern

In order to address the case $D_p = 0$, we consider the following controller dynamics:

$$\begin{cases} u_p(t) = G_1\bar{x}_c(t) + G_2x_r(t), \\ \bar{x}_c(t+1) = \bar{A}_c\bar{x}_c(t) + \bar{A}_rx_r(t) - L_1e(t), \end{cases} \tag{35}$$

where

$$\begin{aligned}\bar{A}_c &:= A_p + B_pG_1 + L_1(C_p + D_pG_1),\\ \bar{A}_r &:= L_1C_r + (B_p + L_1D_p)G_2.\end{aligned}$$

The difference of (35) from the previous controller (34) is to use the actual state x_r of the exosystem (33) instead of its estimation. Since we do not need to estimate x_r, (35) can have better control performance than (34).

Privacy-preserving tracking controller design requires the following three conditions for the new controller parameters G_1 and L_1:

1) $A_p + B_pG_1$ is asymptotically stable;
2) $A_p + L_1C_p$ is asymptotically stable;
3) Given $\gamma > 0$, the H_∞-norm of the controller (35) from e to u_p is bounded as

$$\| - G_1(zI_{n_p+n_r} - \bar{A}_c)^{-1}L_1\|_{H_\infty} \leq \gamma. \tag{36}$$

As mentioned in the previous subsection, the third condition implicitly requires the stability of the new controller (35). Stabilization of a plant by a stable controller is called strong stabilization. Its necessary and sufficient condition is described in terms of a parity interlacing property (PIP) of the transfer function matrix [53]. However, the PIP condition does not provide a controller design method. For continuous-time systems, the papers [54], [55] provide ways of designing a controller satisfying Condition 3) based on the LMI. We employ one of these methods.

It is not easy to simultaneously finding G_1 and L_1 satisfying all three conditions; the reason will be explained later. Therefore, first, we find G_1 stabilizing $A_p + B_pG_1$, which can be done by multiple methods under Assumption 3.2. Then, we find L_1 satisfying 2) and 3) as follows.

Lemma 3.10: Suppose that G_1 is chosen such that $A_p + B_pG_1$ is asymptotically stable. If there exist $P \in \mathbb{R}^{n_p\times n_p}$ and $\hat{L}_1 \in \mathbb{R}^{n_p\times q_p}$ satisfying the following LMIs:

$$\begin{bmatrix} P & PA_p + \hat{L}_1C_p \\ (PA_p + \hat{L}_1C_p)^\top & P \end{bmatrix} \succ 0, \tag{37}$$

and

$$\begin{bmatrix} P & 0 & \overline{P}_{13} & G_1^\top \\ 0 & \gamma^2 I_{q_p} & -\hat{L}_1^\top & 0 \\ \overline{P}_{13}^\top & -\hat{L}_1 & P & 0 \\ G_1 & 0 & 0 & I_{m_p} \end{bmatrix} \succ 0, \tag{38}$$

$$\overline{P}_{13}^\top := P(A_p + B_pG_1) + \hat{L}_1(C_p + D_pG_1),$$

then $A_p + L_1C_p$ with $L_1 := P^{-1}\hat{L}_1$ is asymptotically stable, and (36) holds.

Proof: If (37) holds, $A_p + L_1 C_p$ is asymptotically stable. Next, (38) implies (36) [56, Theorem 4.6.6]. ■

Remark 3.11: For any given G_1 stabilizing $A_p + B_p G_1$, it is possible to verify if there exist P, L_1, and $\gamma > 0$ satisfying (36) by replacing (38) by

$$\begin{bmatrix} P & \overline{P}_{13} \\ \overline{P}_{13}^\top & P \end{bmatrix} \succ 0. \tag{39}$$

That is, given G_1, the LMIs (37) and (39) have a solution P only if strong stabilization is achievable. ◁

An alternative way of controller design is to find $\hat{L}_1$ satisfying 2) and then to use similar LMIs for finding G_1 that satisfies 1) and 3) simultaneously. If one tries to find G_1 and $\hat{L}_1$ at the same time, then one encounters BMIs, e.g. there is a cross term of G_1 and P or G_1 and $\hat{L}_1$ in $\overline{P}_{13}$ in (38). BMIs are more difficult to handle than LMIs, since a BMI describes those sets that are not necessarily convex.

E. Differential Privacy of Controllers

To make the designed controller in the previous subsection differentially private, one can add noise to the output u_p or the input e of the controller. As clarified in Corollary 2.16, the differential privacy level under the input Gaussian noise only depends on the covariance matrix of the noise. Under the output Gaussian noise, we obtain the following theorem by combining Corollary 2.9 and Lemma 3.10. Since the proof directly follows, it is omitted.

Theorem 3.12: Consider the controller dynamics (35) satisfying the requirements 1) – 3) with the output $u_p(t) + w(t)$, where $w(t) \in \mathbb{R}^{m_p}$ is the noise. Then, the Gaussian mechanism induced by the controller dynamics and $W_t \sim \mathcal{N}_{(t+1)m_p}(\mu, \Sigma)$ is (ε, δ)-differentially private for Adj_2^c at a finite time $t \in \mathbb{Z}_+$ with $\varepsilon > 0$ and $1/2 > \delta > 0$ if the covariance matrix $\Sigma \succ 0$ is chosen such that (14) holds for $(A, B, C, D) = (\bar{A}_c, -L_1, G_1, 0)$. ◁

In summary, the privacy-preserving controller with the prescribed differential privacy level is designed as follows. First, one designs the controller dynamics (35) based on the LMIs (37) and (38) and then design the noise w based on the above theorem with (14). In the LMIs, the design parameters reduce to γ, the H_∞-norm of the controller (35).

From (14) (and Remark 3.7), a smaller γ gives a smaller lower bound on the covariance matrix of the Gaussian noise, but making γ small may result in deterioration of the control performance. Moreover, adding noise w may result in deterioration of the control performance also. Let $H(z)$ and $K(z)$ denote the transfer functions of the plant (32) from u_p to y_p and controller (35) from e to u_p, respectively. The transfer function matrices of the closed-loop system from w to y_p is $(I - H(z)K(z))^{-1}P(z)$. If the controller is designed such that the H_∞-norm of $K(z)$ is sufficiently large, the output y_p of the closed-loop system is less influenced by w. In contrast, this causes a decrease in the privacy level. Therefore, there is a trade-off between the control performance and the privacy level for privacy-preserving controller design.

If one additionally requires the H_∞-norm of the closed-loop system not to be greater than $\bar{\gamma} > 0$, then one can use the following LMI:

$$\begin{bmatrix} Q & 0 & 0 & * & * & * \\ 0 & P & 0 & * & * & * \\ 0 & 0 & \bar{\gamma}^2 I_{q_p} & * & * & * \\ QA_p & QB_pG_1 & QB_p & Q & 0 & 0 \\ -\hat{L}_1 C_p & \overline{P}_{25}^\top & -\hat{L}_1 D_p & 0 & P & 0 \\ C_p & D_pG_1 & D_p & 0 & 0 & I_{m_p} \end{bmatrix} \succ 0, \tag{40}$$

$$\overline{P}_{25}^\top = P(A_p + B_pG_1) + \hat{L}_1 C_p,$$

where $*$ are suitable elements to make the matrix symmetric. The H_∞-norms of the controller and closed-loop system are made less than γ and $\bar{\gamma}$, respectively, if LMIs (37), (38) and (40) have solutions P, Q, and $\hat{L}_1$.

F. Private Data Estimation

In the previous subsections, we have studied privacy-preserving controller design. An approach to evaluating the privacy level of the proposed controller is to utilize differential privacy. In systems and control, filtering is a central problem, and one may ask whether existing filtering techniques can be used for estimating private data. Therefore, in this subsection, we consider this estimation problem. It is expected that the obtained observations in this subsection can help in improving the privacy-preserving controller design method.

For state estimation, one can use the standard techniques of the optimal linear filters or smoothers. Thus, we reformulate the input estimation problem as a state estimation problem inspired by unknown input observer design [57], [58]. Suppose that the designed controller (35) is strongly input observable for the output u_p and input e. Recall the notations for sequences $U_{p,2n}(t)$ and $E_{2n}(t)$ introduced in the introduction. In a similar manner as (2), the output sequence $U_{p,t}$ of the controller can be described by

$$U_{p,2n}(t) = O_{2n}\bar{x}_c(t) + N_{2n}E_{2n}(t) + N_{r,2n}X_{r,2n}(t), \tag{41}$$

where $A = \bar{A}_c$, $B = -L_1$, $C = G_1$, and $D = 0$ for O_{2n} and N_{2n}, and $N_{r,t}$ denotes N_t for $A = \bar{A}_c$, $B = \bar{A}_r$, $C = G_1$, and $D = G_2$.

From (15), there exists a (not necessarily unique) matrix $K \in \mathbb{R}^{(n+(n+1)m)\times(2n+1)q}$ such that

$$K \begin{bmatrix} O_{2n} & N_{2n,n} \end{bmatrix} = I_{n+(n+1)m}. \tag{42}$$

By using this K, define

$$K_x := \begin{bmatrix} I_n & 0 \end{bmatrix} K,$$
$$K_u := \begin{bmatrix} 0 & I_m & 0 \end{bmatrix} K.$$

Then, from (41),

$$\begin{aligned} &K_x(U_{p,2n} - N_{r,2n}X_{r,2n}) \\ &= \begin{bmatrix} I_n & 0 \end{bmatrix} K \begin{bmatrix} O_{2n} & N_{2n,n} \end{bmatrix} \begin{bmatrix} \bar{x}_c(0) \\ E_n \end{bmatrix} \\ &= \begin{bmatrix} I_n & 0 \end{bmatrix} \begin{bmatrix} \bar{x}_c(0) \\ E_n \end{bmatrix} = \bar{x}_c(0), \end{aligned} \tag{43}$$

and

$$K_u(U_{p,2n}(t) - N_{r,2n}X_{r,2n}(t))$$

$$= \begin{bmatrix} 0 & I_m & 0 \end{bmatrix} \begin{bmatrix} \bar{x}_c(t) \\ E_n(t) \end{bmatrix} = e(t), \tag{44}$$

By substituting them into (35), we have

$$\begin{cases} u_p(t) = G_1\bar{x}_c(t) + G_2x_r(t), \\ \bar{x}_c(t+1) = \bar{A}_c\bar{x}_c(t) + \bar{A}_rx_r(t) \\ \qquad\qquad -L_1K_u(U_{p,2n}(t) - N_{r,2n}X_{r,2n}(t)), \\ \bar{x}_c(0) = K_x(U_{p,2n} - N_{r,2n}X_{r,2n}), \end{cases} \tag{45}$$

where recall that the state of the exosystem x_r is a piece of public information. This system corresponds to a left inverse system of the controller. In order to estimate e from u_p, one can use the state estimation of this model with the process and measurement noises $\tilde{v}(t) \in \mathbb{R}^{(2n+1)m_p}$ and $\tilde{w}(t) \in \mathbb{R}^{m_p}$.

Let $\tilde{x}_c(t)$ denote the state estimation of (45). Then, define

$$\tilde{u}_p(t) = G_1\tilde{x}_c(t) + G_2x_r(t).$$

Finally from (44) and $\tilde{U}_{p,2n}(t)$, the estimation of $e(t)$ denoted by $\tilde{e}(t)$ can be computed by

$$\tilde{e}(t) = K_u(\tilde{U}_{p,2n}(t) - N_{r,2n}X_{r,2n}(t)). \tag{46}$$

It is worth mentioning that in (45), future information of $u_p(t)$, namely $U_{p,2n}(t)$ is used in order to estimate $e(t)$. In other words, at time t, one can estimate the historic data $e(t-2n)$, and thus the private data estimation can be formulated as a smoothing problem. There are several techniques for designing filters or smoothers such as the Kalman filter or its smoother, and one of them can be employed for the state estimation. Typically, for the filtering and smoothing problems, i.i.d. Gaussian noises are used as the process and measurement noises. Therefore, adding non-i.i.d. or non-Gaussian noises to the privacy-preserving controller could be useful for protecting the private data than adding i.i.d. Gaussian noises.

The above is one approach to input data estimation. For strongly input observable systems, one can directly estimate $(x_0, u(0))$ from E_t and the probability density function of noise by extending the results in [59]. The paper [59] further develops an updating algorithm of the estimation forward in time.

IV. Examples

We revisit the DC microgrids (30) with parameters in [50] for $i = 1, 2$, where $R_i = 0.2[\Omega]$, $R_{i,j} = 70[\mathrm{m}\Omega]$, $L_i = 1.8[\mathrm{mH}]$, and $C_i = 2.2[\mathrm{mF}]$ and design a privacy-preserving controller, where the sampling period is $10^{-3}[\mathrm{s}]$. We consider that originally $I_i = 0[\mathrm{A}]$ and $V_i = 380[\mathrm{V}]$ are achieved with $I_{1,2} = 0[\mathrm{A}]$. Then the user 1 starts to use more electricity, which causes $I_1 = -4[\mathrm{A}]$. The goal is to achieve $I_i = 0[\mathrm{A}]$ and $V_i = 380[\mathrm{V}]$ again by protecting from user 2 the information that user 1 changes its electricity consumption. From the control objective (31), the exosystem (33) is given by $A_r = C_r = I_4$. In this problem setting, Assumptions 3.1-3.4 hold.

We design a privacy-preserving tracking controller. First, we design G_1 stabilizing $A_p + B_pG_1$ based on the following optimal control problem:

$$J = \sum_{t=0}^{\infty} |x_p(t)|_2^2 + |u_p(t)|_2^2.$$

Solving the corresponding Riccati equation, G_1 is obtained as

$$G_1 = \begin{bmatrix} -0.850 & 0.037 & -0.0461 & -0.0007 & 0.229 \\ 0.0370 & -0.850 & -0.0007 & -0.0461 & -0.229 \end{bmatrix}.$$

With X and U in Assumption 3.4, $G_2 = U - G_1X$ is computed as

$$G_2 = \begin{bmatrix} 0.869 & -0.0019 & 0.873 & 0.174 \\ -0.0019 & 0.869 & 0.174 & 0.873 \end{bmatrix}.$$

Second, the LMIs (37) and (38) have solutions P and $\hat{L}_1$ for $\gamma = 0.365$. The matrix $L_1 = P^{-1}\hat{L}_1$ is

$$L_1 = \begin{bmatrix} -0.193 & 0.0088 & 0.0828 & 0.0111 \\ 0.0088 & -0.193 & 0.0111 & 0.0828 \\ -0.0717 & 0.0072 & -0.134 & -0.0129 \\ 0.0072 & -0.0717 & -0.0129 & -0.134 \\ 0.0253 & -0.0253 & -0.0504 & 0.0504 \end{bmatrix}.$$

In this scenario, the initial state of the controller is chosen as $[0\ 0\ 380\ 380\ 0]^\top$ because the state of the controller takes this value when the control objective is achieved.

Suppose that each user adds the Gaussian noise to I_i and V_i before sending them to the power company. Based on our observation for input observability, we design input noises from the principal components of $N_{10,5}^\top N_{10,5}$ of the controller, where the initial state of the controller is assumed to be a piece of public information. Its eigenvalues are shown in Fig. 1. Let $v_{j,i}$ be the projection of the normalized eigenvectors corresponding to the eigenvalue λ_j onto the $u_i(0)$-space. By using non-zero λ_j, we compute

$$\sum_{j=21}^{40} \lambda_j v_{1,j}v_{1,j}^\top = \sum_{j=21}^{40} \lambda_j v_{2,j}v_{2,j}^\top = \begin{bmatrix} 0.0347 & -0.0106 \\ -0.0106 & 0.0129 \end{bmatrix}.$$

Since larger λ_j characterizes less private information of $u_i(0)$, it is reasonable to add larger noise to $u_i(0)$ corresponding to larger λ_j. Therefore, we scale by a positive constant a, namely

$$\overline{\Sigma}_1 = a^2 \begin{bmatrix} 0.0347 & -0.0106 \\ -0.0106 & 0.0129 \end{bmatrix}$$

as the covariance matrix of the input noise for each user. The condition (28) for (ε, δ)-differential privacy holds if

$$a \geq 10.8c\mathsf{R}(\varepsilon, \delta).$$

Let $c = 1$. In privacy related literatures in systems and control [27], [28], [37], ε and δ are chosen to be values in $[0.3, 1.6]$ and $[0.01, 0.05]$, respectively. We use similar values. For instance, for $\varepsilon = 0.3$ and $\delta = 0.0446$ or $\varepsilon = 0.42$ and $\delta = 0.00820$, the condition holds for $a = 64.3$. For $\varepsilon = 0.3$ and $\delta = 0.0446$ or $\varepsilon = 0.69$ and $\delta = 0.00820$, the condition holds for $a = 39.7$. For $\varepsilon = 1.4$ and $\delta = 0.0446$, the condition holds for $a = 15.8$.

Figure 2 shows y_p and u_p of the closed-loop system for the four cases: no noise, $a = 15.8$, $a = 39.7$, and $a = 64.3$. If there is no noise, the tracking error converges to zero. However, the change of I_1 affects clearly I_2, V_2, and u_2. Therefore, user 2 can identify that user 1 starts to use more electricity. In contrast, privacy-preserving controllers with noises mask the effects caused by the electricity consumption of user 1 against

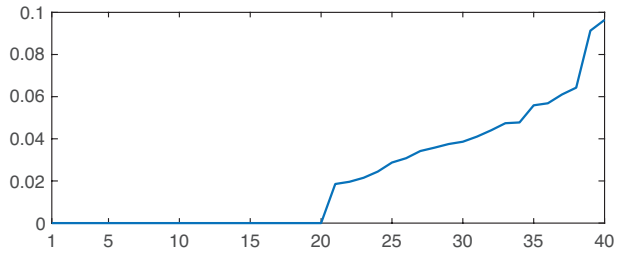

Fig. 1. The value of each eigenvalue of $N_{10,5}^{\top} N_{10,5}$

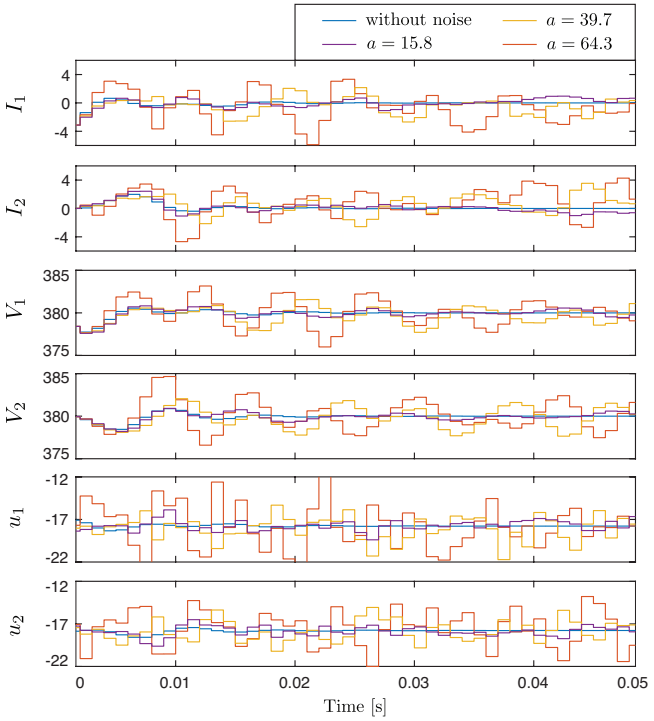

Fig. 2. The outputs and inputs of the closed-loop system controlled by the privacy-preserving controller

user 2. Although adding large noise increases the privacy level, it unfortunately makes I_i, V_i, and u_i fluctuate. Therefore, the balance between required control and privacy performances is needed when designing the noise. In this case, the noise with $a = 15.8$ is enough to protect the fluctuation of the input u_2.

V. Toward Nonlinear Mechanisms

The objective in this section is to extend some of our results to nonlinear mechanisms toward nonlinear privacy-preserving controller design. The output regulation and H_∞-norm analysis are extended to nonlinear systems at least locally; see e.g. [34], [60]. Therefore, if differential privacy analysis is extended, one can design a nonlinear privacy-preserving controller at least locally in a similar manner as the linear case. In this section, we proceed with differential privacy analysis of the Gaussian mechanism induced by a nonlinear dynamical system and output Gaussian noise. For nonlinear dynamical systems, even if Gaussian noise is added to the input channel, the output variable is not Gaussian in general, and thus we do not analyze the mechanisms induced by input noise.

A. Differential Privacy with Output Noise

Consider the following nonlinear discrete-time control system with output noise

$$\begin{cases} x(t+1) = f(x(t), u(t)), \\ y_w(t) = h(x(t), u(t)) + w(t), \end{cases} \tag{47}$$

where $f : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ and $h : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^q$ are continuous. Its solution $x(t)$ starting from x_0 controlled by U_{t-1} is denoted by $\phi(t, x_0, U_{t-1})$, where $\phi(0, x_0, U_{-1}) := x_0$. The output sequence $Y_{w,t}$ can be described by

$$Y_{w,t} = H_t(x_0, U_t) + W_t, \tag{48}$$

where $H_t : \mathbb{R}^n \times \mathbb{R}^{(t+1)m} \to \mathbb{R}^{(t+1)q}$ is

$$H_t(x_0, U_t) := \begin{bmatrix} h(\phi(0, x_0, U_{-1}), u(0)) \\ h(\phi(1, x_0, U_0), u(1)) \\ \vdots \\ h(\phi(t, x_0, U_{t-1}), u(t)) \end{bmatrix}. \tag{49}$$

Now, we are ready to obtain an extension of Theorem 2.6 to the nonlinear Gaussian mechanism by using input data dependent Gaussian noise.

Theorem 5.1: The Gaussian mechanism (48) induced by $W_t \sim \mathcal{N}_{(t+1)q}(\mu(x_0, U_t), \Sigma(x_0, U_t))$ is (ε, δ)-differentially private for Adj_2^c at a finite time t with $\varepsilon(x_0, U_t) > 0$ and $1/2 > \delta(x_0, U_t) > 0$ if the covariance matrix $\Sigma(x_0, U_t) \succ 0$ is chosen such that

$$\inf_{|[\bar{x}_0; \bar{U}_t]|_2 \le c} \frac{1}{\bar{H}_t(x_0, U_t, \bar{x}_0, \bar{U}_t)} \ge c\mathsf{R}\left(\varepsilon(x_0, U_t), \delta(x_0, U_t)\right), \tag{50}$$

where

$$\bar{H}_t(x_0, U_t, \bar{x}_0, \bar{U}_t) := |H_t(x_0 + \bar{x}_0, U_t + \bar{U}_t) - H_t(x_0, U_t)|_{\Sigma^{-1}(x_0, U_t)}$$

for any $(x_0, U_t) \in \mathbb{R}^n \times \mathbb{R}^{(t+1)m}$.

Proof: In a similar manner as for Theorem 2.6, one obtains (9) for

$$z = |H_t(x_0, U_t) - H_t(x_0', U_t')|^{-1}_{\Sigma^{-1}(x_0, U_t)}.$$

Define $\bar{x}_0 = x_0' - x_0$ and $\bar{U}_t = U_t' - U_t$. Then, $((x_0, U_t), (x_0', U_t')) \in \mathrm{Adj}_2^c$ implies $|[\bar{x}_0; \bar{U}_t]|_2 \le c$. It follows that

$$z = \bar{H}_t(x_0, U_t, \bar{x}_0, \bar{U}_t) \le \sup_{|[\bar{x}_0; \bar{U}_t]|_2 \le c} \bar{H}_t(x_0, U_t, \bar{x}_0, \bar{U}_t),$$

for any $((x_0, U_t), (x_0', U_t')) \in \mathrm{Adj}_2^c$. Therefore, if (50) holds, (9) holds. ■

In Theorem 5.1, the mean value and variance can be made functions of (x_0, U_t) under the reasonable assumption that a system manager designing noise knows the initial state and inputs of the system. Even if the system manager does not know them exactly, noise can still be designed by using a constant mean value and variance. Note that using (x_0, U_t)-dependent noise does not break privacy guarantee because information of noise is not published in general.

The paper [61] studies nonlinear observer design based on differential privacy in the contraction framework with constant

metrics. The provided results can be extended to differential privacy analysis of nonlinear systems, but as they stand, only for stable systems. In contrast, Theorem 5.1 can be used for unstable systems and considers a more general mean value and variance depending on (x_0, U_t).

In a similar manner as Remark 2.7, for the i.i.d. Laplace noise $w_i(t)$, $i = 1, \dots, q$, $t \in \mathbb{Z}_+$ with the variance $\mu(x_0, U_t) \in \mathbb{R}$ and distribution $b(x_0, U_t) > 0$, the mechanism (48) is $(\varepsilon, 0)$-differentially private for Adj_1^c at a finite time t with $\varepsilon > 0$ if

$$b(x_0, U_t) \geq \sup_{|[\bar{x}_0; \bar{U}_t]|_1 \leq c} \frac{\left| H_t(x_0 + \bar{x}_0, U_t + \bar{U}_t) - H_t(x_0, U_t) \right|_1}{\varepsilon(x_0, U_t)} \tag{51}$$

for any $(x_0, U_t) \in \mathbb{R}^n \times \mathbb{R}^{(t+1)m}$. Furthermore, suppose that f and h are smooth. Let $\gamma(s) = x_0 + s(\bar{x}_0 - x_0)$ and $\nu(s) = U_t + s(\bar{U}_t - U_t)$ for $s \in [0, 1]$. Then,

$$\begin{aligned}
&\left| H_t(x_0 + \bar{x}_0, U_t + \bar{U}_t) - H_t(x_0, U_t) \right|_1 \\
&= \left| \int_0^1 \frac{\partial H_t(\gamma(s), \nu(s))}{\partial (x_0, U_t)} \begin{bmatrix} x_0 \\ U_t \end{bmatrix} ds \right|_1 \\
&\leq c \left| \int_0^1 \frac{\partial H_t(\gamma(s), \nu(s))}{\partial (x_0, U_t)} ds \right|_1 \\
&\leq c \sup_{(x_0, U_t) \in \mathbb{R}^n \times \mathbb{R}^{(t+1)m}} \left| \frac{\partial H_t(x_0, U_t)}{\partial (x_0, U_t)} \right|_1 .
\end{aligned}$$

Therefore, (51) holds if

$$b(x_0, U_t) \geq \frac{c}{\varepsilon(x_0, U_t)} \sup_{(x_0, U_t) \in \mathbb{R}^n \times \mathbb{R}^{(t+1)m}} \left| \frac{\partial H_t(x_0, U_t)}{\partial (x_0, U_t)} \right|_1 .$$

Note that in the linear case $\partial H_t(x_0, U_t) / \partial (x_0, U_t)$ is nothing but the matrix $\begin{bmatrix} O_t & N_t \end{bmatrix}$.

For Laplacian noise, differential privacy is characterized by the matrix $\partial H_t(x_0, U_t) / \partial (x_0, U_t)$. This matrix has a strong connection with the *local strong input observability* of the nonlinear system (47); the concept of strong observability can be extended to nonlinear systems as for local observability [62] based on the distinguishability of a pair of initial states and initial inputs. In fact, one can derive a necessary and sufficient condition for *local strong input observability* in terms of the differential one-forms corresponding to $\partial H_t(x_0, U_t) / \partial (x_0, U_t)$ as follows: there exists $t \in \mathbb{Z}_+$ such that

$$\mathrm{span}\{\mathrm{d}H_t(x_0, U_t)\} \cap \mathrm{span}\{\mathrm{d}x, \mathrm{d}u_0\} = \mathrm{span}\{\mathrm{d}x, \mathrm{d}u_0\}$$

under the constant dimensional assumption for all $(x_0, U_t) \in \mathbb{R}^n \times \mathbb{R}^{(t+1)q}$; see e.g. [62] for similar discussions for local observability. This is an extension of the condition (42). In contrast to the qualitative criterion for strong input observability, it is still not straightforward to extend the concept of Gramians. In fact, there is no clear extension of Gramians to nonlinear systems even for controllability and observability although the concept of controllability and observability and their corresponding energy functions have been extended [62]–[64].

B. Incrementally Input-to-Output Stable Systems

In Section II-A, we mention that the H_∞-norm gives an upper bound of the differential privacy level. This observation can help the privacy-preserving controller design. In this subsection, we aim at extending this result to the nonlinear case based on the concept of the incremental input-to-output stability (IOS).

For a nonlinear system, several types of gains (or called estimations) are defined; e.g. see [65]. Especially, $L^2 \to L^2$ estimation is extended to nonlinear systems as input-to-state stability (ISS) [65], which is also extended to incremental properties in [66]. Incremental ISS can be readily extended to input-to-output operators, discrete-time systems, and arbitrary $L^p \to L^p$ estimations as follows. In Appendix, we give its Lyapunov characterization.

Definition 5.2: A nonlinear system (47) is said to be *incrementally IOS* (with respect to the p-norm) if the output $h(\phi(t, x_0, U_{t-1}), u(t))$ exists for all $t \in \mathbb{Z}_+$, for any $x_0 \in \mathbb{R}^n$ and $u : \mathbb{Z}_+ \to \mathbb{R}^m$, and there exist class $\mathcal{K}$ functions α and γ such that

$$\begin{aligned}
&\sum_{\tau=0}^{t} |h(\phi(\tau, x_0, U_{t-1}), u(t)) - h(\phi(\tau, x_0', U_{t-1}'), u'(t))|_p \\
&\leq \alpha(|x_0 - x_0'|_p) + \sum_{\tau=0}^{t} \gamma(|u(\tau) - u'(\tau)|_p), \ t \in \mathbb{Z}_+
\end{aligned} \tag{52}$$

for any $(x_0, x_0') \in \mathbb{R}^n \times \mathbb{R}^n$ and $(U_t, U_t') \in \mathbb{R}^{(t+1)m} \times \mathbb{R}^{(t+1)m}$. $\lhd$

In fact, α and γ do not need to belong to class $\mathcal{K}$ for differential privacy analysis, and non-negative functions are enough. To connect differential privacy analysis with ISS, we consider class $\mathcal{K}$ functions.

In the linear case, as shown in Corollary 2.9, the H_∞-norm can be used for designing the Gaussian noise. Now, we obtain an extension of Corollary 2.9 to the nonlinear IOS system based on Theorem 5.1. The proof directly follows, and thus is omitted.

Corollary 5.3: Let $W_t \sim \mathcal{N}_{(t+1)q}(\mu(x_0, U_t), \Sigma(x_0, U_t))$ be a non-degenerate multivariate Gaussian noise. Then, the Gaussian mechanism (48) induced by an incrementally IOS nonlinear system (47) (with respect to 2-norm) is (ε, δ)-differentially private for Adj_2^c at a finite time t with $\varepsilon(x_0, U_t) > 0$ and $1/2 > \delta(x_0, U_t) > 0$ if the covariance matrix $\Sigma(x_0, U_t) \succ 0$ is chosen such that

$$\begin{aligned}
&\lambda_{\min}^{1/2}(\Sigma(x_0, U_t)) \\
&\geq (\alpha(c) + (t+1)\gamma(c)) \mathsf{R}\left(\varepsilon(x_0, U_t), \delta(x_0, U_t)\right)
\end{aligned}$$

for any $x_0 \in \mathbb{R}^n$ and $U_t \in \mathbb{R}^{(t+1)m}$. $\lhd$

VI. Conclusion

In this paper, we have studied differential privacy of Gaussian mechanisms induced by discrete-time linear systems. First, we have analyzed differential privacy in terms of strong input observability and then have clarified that the differential privacy level is characterized by the maximum eigenvalue of the input observability Gramian. In other words, small noise is enough to make the less input observable Gaussian mechanism

highly differentially private. Moreover, we have shown that the mechanisms induced by input and output noises have the same differential privacy level for suitable covariance matrices. Next, we have developed a privacy-preserving controller design method, which can make a linear system highly private by adding small noise. Finally, we have briefly mentioned differential privacy analysis of incrementally IOS nonlinear systems.

Although we have focused on differential privacy in this paper, our analysis and controller design can be tools for studying more general privacy issues of control systems. Differential privacy has been originally proposed in static data analysis, and one may extend this concept to dynamical systems further or develop new privacy concepts for dynamical systems. For privacy-preserving controller design, we have first designed a controller satisfying a certain control performance and then added noise to protect private information. There remain several interesting research directions. One is to investigate an updating method for the covariance matrix of noise forward in time based on the idea of Kalman filter design. Another is to develop a randomized control mechanism guaranteeing a certain control performance, which may enable us to design the controller and noise at the same time.

In general, measurement and input noises, disturbance and model error make analysis and controller design difficult and deteriorate the control performance, and thus they are regarded as troubles. However, they improve the system's privacy level. Therefore, the privacy-preserving controller design reduces to the trade-off between the privacy level and control performance.

Acknowledgement: We thank Dr. Michele Cucuzzella, University of Groningen for fruitful discussions on DC microgrids.

APPENDIX

In this appendix, we provide a sufficient condition for incremental IOS.

Theorem A: A nonlinear system (47) is incrementally IOS if there exist a continuous function $V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_+$, constants $c_1 > 0$, $\lambda \in (0,1)$, class $\mathcal{K}$ functions σ_1, σ_2, and a class $\mathcal{K}_\infty$ function α_2 such that

$$c_1|h(x_0,u) - h(x_0',v)|_p \le V(x_0,x_0') + \sigma_1(|u-u'|_p), \quad (53)$$

$$V(x_0,x_0') \le \alpha_2(|x_0 - x_0'|_p), \quad (54)$$

$$V(f(x_0,u), f(x_0',u')) \le \lambda V(x_0,x_0') + \sigma_2(|u-u'|_p) \quad (55)$$

for any $(x_0,x_0') \in \mathbb{R}^n \times \mathbb{R}^n$ and $(u,u') \in \mathbb{R}^m \times \mathbb{R}^m$.

Proof: Recursively using the inequality (55) for $\tau \ge 1$ yields

$$\begin{aligned}
&V(\phi(\tau,x_0,U_{\tau-1}),\phi(\tau,x_0',U'_{\tau-1}))\\
&\le \lambda V(\phi(\tau-1,x_0,U_{\tau-2}),\phi(\tau-1,x_0',U'_{\tau-2}))\\
&\quad + \sigma(|u(\tau-1)-u'(\tau-1)|_p)\\
&\le \lambda^2 V(\phi(\tau-2,x_0,U_{\tau-3}),\phi(\tau-2,x_0',U'_{\tau-3}))\\
&\quad + \lambda\sigma_2(|u(\tau-2)-u'(\tau-2)|_p)\\
&\quad + \sigma_2(|u(\tau-1)-u'(\tau-1)|_p)\\
&\le \lambda^\tau V(x_0,x_0') + \sum_{r=0}^{\tau-1}\lambda^{\tau-1-r}\sigma_2(|u(r)-u'(r)|_p).
\end{aligned}$$

From (53),

$$\begin{aligned}
&c_1|h(\phi(\tau,x_0,U_{\tau-1},u(\tau)) - h(\phi(\tau,x_0',U'_{\tau-1}),u'(\tau))|_p\\
&\le \lambda^\tau\alpha_2(|x_0-x_0'|_p) + \sum_{r=0}^{\tau-1}\lambda^{\tau-1-r}\sigma_2(|u(r)-u'(r)|_p)\\
&\quad + \sigma_1(|u(\tau)-u'(\tau)|_p).
\end{aligned}$$

By taking the summation, we have

$$\begin{aligned}
&c_1\sum_{\tau=0}^{t}|h(\phi(\tau,x_0,U_{\tau-1},u(\tau)) - h(\phi(\tau,x_0',U'_{\tau-1}),u'(\tau))|_p\\
&\le \sum_{\tau=0}^{t}\Bigg(\lambda^\tau\alpha_2(|x_0-x_0'|_p) + \sigma_1(|u(\tau)-u'(\tau)|_p)\\
&\quad + \sum_{r=0}^{\tau-1}\lambda^{\tau-r-1}\sigma_2(|u(r)-u'(r)|_p)\Bigg)\\
&\le \frac{1-\lambda^t}{1-\lambda}\alpha_2(|x_0-x_0'|_p) + \sum_{\tau=0}^{t}\sigma_1(|u(\tau)-u'(\tau)|_p)\\
&\quad + \sum_{r=0}^{t-1}\frac{1-\lambda^{t-1-r}}{1-\lambda}\sigma_2(|u(r)-u'(r)|_p)\\
&\le \frac{\alpha_2(|x_0-x_0'|_p)}{1-\lambda}\\
&\quad + \sum_{r=0}^{t}\left(\frac{\sigma_2(|u(r)-u'(r)|_p)}{1-\lambda} + \sigma_1(|u(\tau)-u'(\tau)|_p)\right),
\end{aligned}$$

where in the second last inequality, $\lambda \in (0,1)$ is used. Therefore, the system is incrementally IOS. ■

Remark B: We mentioned that for differential privacy analysis, α and γ are required to be only non-negative functions. Here, we obtain a similar characterization by using non-negative functions σ_1, σ_2, and α_2. ◁

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] R. H. Weber, "Internet of things–new security and privacy challenges," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, 2010.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," *Proc. 2010 IEEE International Conference on Computer Communications*, pp. 1–9, 2010.

[5] D. D. Ryan, "Cloud computing privacy concerns on our doorstep," *Communications of the ACM*, vol. 54, no. 1, pp. 36–38, 2011.

[6] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security & Privacy*, no. 6, pp. 24–31, 2010.

[7] J. Mervis, "Can a set of equations keep US census data private," *Science Magazine*, 2019.

[8] L. Sweeney, "Weaving technology and policy together to maintain confidentiality," *The Journal of Law, Medicine & Ethics*, vol. 25, no. 2-3, pp. 98–110, 1997.

[9] B. Malin and L. Sweeney, "How (not) to protect genomic data privacy in a distributed network: using trail re-identification to evaluate and design anonymity protection systems," *Journal of biomedical informatics*, vol. 37, no. 3, pp. 179–192, 2004.

[10] S. Hansell, "AOL removes search data on vast group of web users," *New York Times*, vol. 8, p. C4, 2006.

[11] A. A. Narayanan and V. Shmatikov, "How to break anonymity of the netflix prize dataset," *arXiv: cs/0610105*, 2006.

[12] L. Willenborg and T. D. Waal, *Statistical Disclosure Control in Practice*. Springer Science & Business Media, 1996, vol. 111.

[13] ——, *Elements of Statistical Disclosure Control*. Springer Science & Business Media, 2012, vol. 155.

[14] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[15] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam, "l-diversity: Privacy beyond k-anonymity," *Proc. 22nd International Conference on Data Engineering*, pp. 24–24, 2006.

[16] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," *Proc. 23rd IEEE International Conference on Data Engineering*, pp. 106–115, 2007.

[17] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," *Proc. 3rd Theory of Cryptography Conference*, pp. 265–284, 2006.

[18] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, "Our data, ourselves: Privacy via distributed noise generation," *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 486–503, 2006.

[19] J. Zhao, T. Jung, Y. Wang, and X. Li, "Achieving differential privacy of data disclosure in the smart grid," *Proc. 2014 IEEE International Conference on Computer Communications*, pp. 504–512, 2014.

[20] W. Jia, H. Zhu, Z. Cao, X. Dong, and C. Xiao, "Human-factor-aware privacy-preserving aggregation in smart grid," *IEEE Systems Journal*, vol. 8, no. 2, pp. 598–607, 2013.

[21] H. Sandberg, G. Dán, and R. Thobaben, "Differentially private state estimation in distribution networks with smart meters," *Proc. 54th IEEE Conference on Decision and Control*, pp. 4492–4498, 2015.

[22] F. K. Dankar and K. E. Emam, "The application of differential privacy to health data," *Proc. 2012 International Conference on Extending Database Technology*, pp. 158–166, 2012.

[23] F. K. Dankar, K. Fida, and K. E. Emam, "Practicing differential privacy in health care: A review," *Transactions on Data Privacy*, vol. 6, no. 1, pp. 35–67, 2013.

[24] M. Yang, A. Margheri, R. Hu, and V. Sassone, "Differentially private data sharing in a cloud federation with blockchain," *IEEE Cloud Computing*, vol. 5, no. 6, pp. 69–79, 2018.

[25] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin," *Proc. International Conference on Financial Cryptography and Data Security*, pp. 34–51, 2013.

[26] F. McSherry and K. Talwar, "Mechanism design via differential privacy," *Proc. 48th Annual Symposium on Foundations of Computer Science*, vol. 7, pp. 94–103, 2007.

[27] J. Le Ny and G. J. Pappas, "Differentially private filtering," *IEEE Transactions on Automatic Control*, vol. 59, no. 2, pp. 341–354, 2014.

[28] J. Le Ny and M. Mohammady, "Differentially private mimo filtering for event streams," *IEEE Transactions on Automatic Control*, vol. 63, no. 1, pp. 145–157, 2018.

[29] P. Kairouz, S. Oh, and P. Viswanath, "The composition theorem for differential privacy," *IEEE Transactions on Information Theory*, vol. 63, no. 6, pp. 4037–4049, 2017.

[30] M. Hou and R. J. Patton, "Input observability and input reconstruction," *Automatica*, vol. 34, no. 6, pp. 789–794, 1998.

[31] M. K. Sain and J. L. Massey, "Invertibility of linear time-invariant dynamical systems," *IEEE Transactions on Automatic Control*, vol. 14, no. 2, pp. 141–149, 1969.

[32] P. J. Moylan, "Stable inversion of linear systems," *IEEE Transactions on Automatic Control*, vol. 22, no. 1, pp. 74–78, 1977.

[33] J. L. Massey and M. K. Sain, "Inverses of linear sequential circuits," *IEEE Transactions on Computers*, vol. 17, no. 4, pp. 330–337, 1968.

[34] J. Huang, *Nonlinear Output Regulation: Theory and Applications*. SIAM, 2004, vol. 8.

[35] Y. Kawano and M. Cao, "Revisit input observability: A new approach to attack detection and privacy preservation," *Proc. 57th IEEE Conference on Decision and Control*, pp. 7095–7100, 2018.

[36] K. Yazdani, A. Jones, K. Leahy, and M. Hale, "Differentially private LQ control," *arXiv:1807.05082*, 2018.

[37] M. Hale and M. Egerstedt, "Cloud-enabled differentially private multi-agent optimization with constraints," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 4, pp. 1693–1706, 2017.

[38] Z. Huang, S. Mitra, and G. Dullerud, "Differentially private iterative synchronous consensus," *Proc. 2012 ACM Workshop on Privacy in the Electronic Society*, pp. 81–90, 2012.

[39] Z. Huang, S. Mitra, and N. Vaidya, "Differentially private distributed optimization," *Proc. 2015 International Conference on Distributed Computing and Networking*, p. 4, 2015.

[40] 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.

[41] S. Song, K. Chaudhuri, and A. D. Sarwate, "Stochastic gradient descent with differentially private updates," *Proc. 2013 IEEE Global Conference on Signal and Information Processing*, pp. 245–248, 2013.

[42] Y. Kawano and M. Cao, "Differential privacy and qualitative privacy analysis for nonlinear dynamical systems," *Proc. 7th IFAC Workshop on Distributed Estimation and Control in Networked Systems*, pp. 52–57, 2018.

[43] J. Cortés, G. E. Dullerud, S. Han, J. Le Ny, S. Mitra, and G. J. Pappas, "Differential privacy in control and network systems," *Proc. 55th IEEE Conference on Decision and Control*, pp. 4252–4272, 2016.

[44] T. Kailath, *Linear Systems*. New Jersey: Prentice-Hall, 1980, vol. 156.

[45] W. Kratz, "Characterization of strong observability and construction of an observer," *Linear Algebra and Its Applications*, vol. 221, pp. 31–40, 1995.

[46] S. Lang, *Algebra*. New York: Springer-Verlag, 2002.

[47] R. E. Kalman, "Contributions to the theory of optimal control," *Boletín de la Sociedad Matemática Mexicana*, vol. 5, no. 2, pp. 102–119, 1960.

[48] P. Sannuti and A. Saberi, "Special coordinate basis for multivariable linear systems – finite and infinite zero structure, squaring down and decoupling," *International Journal of Control*, vol. 45, no. 5, pp. 1655–1704, 1987.

[49] P. Billingsley, *Probability and measure*, 3rd ed. New York: Wiley, 2008.

[50] M. Cucuzzella, S. Trip, C. D. Persis, X. Cheng, A. Ferrara, and A. J. van der Schaft, "A robust consensus algorithm for current sharing and voltage regulation in dc microgrids," *IEEE Transactions on Control Systems Technology*, vol. 27, no. 4, pp. 1583–1595, 2018.

[51] L. Vandenberghe and S. Boyd, "Semidefinite programming," *SIAM Review*, vol. 38, no. 1, pp. 49–95, 1996.

[52] K. Zhou, J. C. Doyle, and K. Glover, *Robust and optimal control*. New Jersey: Prentice Hall, 1996, vol. 40.

[53] M. Vidyasagar, *Control System Synthesis: A Factorization Approach*. Morgan & Claypool Publishers, 2011.

[54] M. Zeren and H. Özbay, "On the strong stabilization and stable H^∞-controller design problems for MIMO systems," *Automatica*, vol. 36, no. 11, pp. 1675–1684, 2000.

[55] S. Gumussoy and H. Özbay, "Remarks on strong stabilization and stable $\mathcal{H}^\infty$ controller design," *IEEE Transactions on Automatic Control*, vol. 50, no. 12, pp. 2083–2087, 2005.

[56] R. E. Skelton, T. Iwasaki, and D. E. Grigoriadis, *A Unified Algebraic Approach to Control Design*. CRC Press, 1997.

[57] S. Bhattacharyya, "Observer design for linear systems with unknown inputs," *IEEE transactions on Automatic Control*, vol. 23, no. 3, pp. 483–484, 1978.

[58] M. Hou and P. C. Muller, "Design of observers for linear systems with unknown inputs," *IEEE Transactions on Automatic Control*, vol. 37, no. 6, pp. 871–875, 1992.

[59] J. He, L. Cai, and X. Guan, "Preserving data-privacy with added noises: Optimal estimation and privacy analysis," *IEEE Transactions on Information Theory*, vol. 64, no. 8, pp. 5677–5690, 2018.

[60] W. Lin and C. I. Byrnes, "H_∞-control of discrete-time nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 41, no. 4, pp. 494–510, 1996.

[61] J. L. Ny, "Differentially private nonlinear observer design using contraction analysis," *International Journal of Robust and Nonlinear Control*, 2020, early access.

[62] H. Nijmeijer and A. van der Schaft, *Nonlinear Dynamical Control Systems*. New York: Springer-Verlag, 1990.

[63] J. M. A. Scherpen, "Balancing for nonlinear systems," *Systems & Control Letters*, vol. 21, no. 2, pp. 143–153, 1993.

[64] Y. Kawano and J. M. A. Scherpen, "Model reduction by differential balancing based on nonlinear Hankel operators," *IEEE Transactions on Automatic Control*, vol. 62, no. 7, pp. 3293–3308, 2017.

[65] E. D. Sontag, "Input to state stability: Basic concepts and results," in *Nonlinear and optimal control theory*. Springer, 2008, pp. 163–220.

[66] D. Angeli, "Further results on incremental input-to-state stability," *IEEE Transactions on Automatic Control*, vol. 54, no. 6, pp. 1386–1391, 2009.

Yu Kawano (M'13) is currently 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 October 2013 to November 2016, he was a Post-Doctoral researcher at both Kyoto University and JST CREST, Japan. From November 2016 to March 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 and served as a Research Fellow of the Japan Society for the Promotion Science. He is an Associate Editor for Systems and Control Letters. His research interests include nonlinear systems, complex networks, and model reduction.

Ming Cao (SM'16) 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.