A Fundamental Performance Limit of Cloud-based Control in Terms of Differential Privacy Level [⋆]

Yu Kawano [*] **Kenji Kashima** [**] **Ming Cao** [***]

[*] *Y. Kawano is with the Graduate School of Engineering, Hiroshima University, Higashi-Hiroshima 739-8527, Japan (email: ykawano@hiroshima-u.ac.jp).*
[**] *K. Kashima is with the Graduate School of Informatics, Kyoto University, Kyoto 606-8501, Japan (e-mail: kk@i.kyoto-u.ac.jp).*
[***] *M. Cao is with the Faculty of Science and Engineering, University of Groningen, Groningen, 9747 AG, The Netherlands (e-mail: m.cao@rug.nl).*

Abstract: In this paper, we address a privacy issue raised by cloud based control. In a cloud based control framework, a plant typically has no access to the models of the cloud system and other plants connected via the cloud system. Under restricted information, the plant is required to design its local controller for achieving control objectives. As a control objective, we consider a tracking problem, and for constant reference signals, a class of tracking controllers is identified based on Youla parametrization. More importantly, as local tracking controllers are implemented, there is a possibility that the cloud system or other plants connected via the cloud system may be able to identify private information of the plant by using the collected signal from the plant; for example, the reference signal (say, the target production amount) of the plant can be viewed as a piece of private information. In order to evaluate the privacy level of the reference signal, we employ the concept of differential privacy. For the Laplace mechanism induced by the entire system, we show that the differential privacy level cannot be further improved from a ceiling value for any parameters of the local controller. In other words, there is a performance limit in terms of differential privacy level, which is determined by the plant and cloud system only.

Keywords: Differential privacy, privacy limit, cloud-based control, discrete-time linear systems

1. INTRODUCTION

As a key technology of Industry 4.0, cloud-based control has attracted both social and research attentions; see e.g. Lim et al. (2009). Although this is expected to dramatically improve the quality and flexibility of production processes, it leads to potential privacy threat because users share various information through the networks, and from the shared information, there is a possibility that private information of each user is identified by the cloud system or other users.

Privacy threat is a big issue not only for cloud-based control but also for data-based IoT technologies. To deal with privacy issues, statistical disclosure control technologies have been developed; see e.g. Willenborg and Waal (1996, 2012). Originally, these techniques were proposed for static data sets and, recently, have been developed for dynamical data sets, since IoT systems can be dynamical systems. For instance, differential privacy (Dwork et al. (2006a,b)) of dynamical systems are studied by Le Ny and Pappas (2014); Kawano and Cao. Also, there are research results in the context of information entropies (Tanaka et al. (2017); Farokhi and Sandberg (2019)).

In this paper, we study a privacy issue raised by cloud-based control, where as a control objective, we address a tracking problem of a plant. The control objective itself is challenging, since the plant is supposed not to have full information of the cloud system and other plants connected via the cloud system, and other plants can design their own local controllers. Therefore, each plant needs to design its local controller under the assumption that models of the cloud system (and other plants) are not available. In this context, the concept of retrofit control is proposed for characterizing a class of stabilizing local controllers with Youla parametrization by Ishizaki et al. (2019). By extending this method to tracking control, we obtain a set of tracking local controllers. Although we consider a constant reference for the sake of simplicity of analysis, the obtained result can be extended to an arbitrary superposition of periodic signals.

Next, we focus on the privacy issue. Especially, we consider to protect privacy in the situation where the reference signal (e.g. the target production amount) of the plant cannot

[⋆] This work was supported in part by JSPS KAKENHI under Grant JP18H01461, the European Research Council (ERC-CoG-771687) and the Dutch Organization for Scientific Research (NWO-vidi-14134).

be identified by the cloud system from the plant's sent signals. As a privacy preserving data mining technique, we employ differential privacy, where the main idea is to add noise to the signal sent to the cloud system for making the estimation of the reference difficult. For the Laplace mechanism induced by the entire system, we construct a lower bound on the differential privacy level for a given distribution of the i.i.d. Laplace noise. In fact, this lower bound does not depend on the parameters of the local controllers. That is, given distribution, there is a ceiling value for the differential privacy level to be achieved by tuning the parameters, which is determined by the plant and cloud system (and the other plants connected via the cloud system) only.

The remainder of this paper is organized as follows. In Section 2, we formulate a tacking control problem in the context of cloud based control and provide a class of tracking local controllers for a constant reference. In Section 3, we estimate the ceiling level of differential privacy. Section 4 illustrates our results by an academic example. Finally, Section 5 concludes the paper.

Notations: The sets of real numbers and non-negative integers are denoted by $\mathbb{R}$ and $\mathbb{Z}_+$, respectively. For the sequence $u : \mathbb{Z}_+ \to \mathbb{R}$, a vector consisting of its subsequence is denoted by $u_t := [u(0) \ \cdots \ u(t)]^\top \in \mathbb{R}^{t+1}$. For the vector $x \in \mathbb{R}^n$ and sequence $u : \mathbb{Z}_+ \to \mathbb{R}$, their norms are denoted by $|x|_p := (\sum_{i=1}^n |x_i|^p)^{1/p}$ and $\|u\|_p := (\sum_{t=0}^\infty |u(t)|^p)^{1/p}$, respectively, where $p \in \mathbb{Z}_+ \setminus \{0\}$. A sequence $u : \mathbb{Z}_+ \to \mathbb{R}$ is said to be $u \in L_p[0,\infty)$ if $\|u\|_p$ is bounded. The set of stable, proper, and rational transfer functions is denoted by $\mathcal{RH}_\infty$. A scalar random variable ν is said to have a Laplace distribution with the mean value $\mu \in \mathbb{R}$ and the distribution $b > 0$, denoted by $\nu \sim \mathrm{Lap}(\mu, b)$ if its distribution has the following probability density:

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

Moreover, $\nu \in \mathbb{R}^n$ with i.i.d. $\nu_i \sim \mathrm{Lap}(\mu_i, b)$ is denoted by $\nu \sim \mathrm{Lap}^n(\mu, b)$, where its probability density is

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

2. CLOUD-BASED CONTROL

In this section, we formulate cloud-based control in the framework of retrofit control proposed by Ishizaki et al. (2019). Consider the interconnected discrete-time linear system of the plant and cloud system in Fig. 1. The transfer function matrices of the plant and cloud system are respectively given by

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

and

$$\Gamma : v = \mathbf{G}_{\mathbf{v},\mathbf{w}}(z) w, \tag{2}$$

where each signal is supposed to be a scaler for the sake of simplicity of the discussion. Suppose that the plant does not know $\mathbf{G}_{\mathbf{v},\mathbf{w}}(z)$. This is a reasonable assumption for cloud-based control because the plant and cloud system can belong to different parties, or because the cloud system can be connected to other plants possessed by other parties

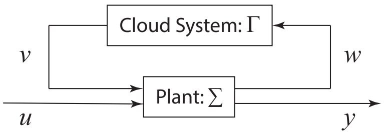

Fig. 1. Pre-existing system.

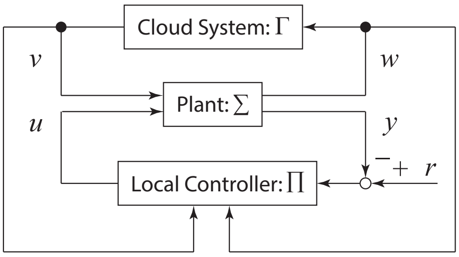

Fig. 2. Entire system.

(in this case, the cloud system represents the system consisting of the cloud itself and other plants). In this setting, the transfer function of the interconnected system of the plant and cloud from u to y becomes

$$G_{\mathrm{pre}}(z) := G_{y,u}(z) + \frac{G_{y,v}(z)\mathbf{G}_{\mathbf{v},\mathbf{w}}(z)G_{w,u}(z)}{1 - G_{w,v}(z)\mathbf{G}_{\mathbf{v},\mathbf{w}}(z)}, \tag{3}$$

which is assumed to be internally stable.

The control objective considered in this paper is tracking, i.e., $y(t) \to r$ as $t \to \infty$ for a given constant reference $r \in \mathbb{R}$. To this end, the plant designs its local controller. Since the plant can access the signals v, w, u, and y, these signals are available for controller design in contrast to $\mathbf{G}_{\mathbf{v},\mathbf{w}}(z)$. In summary, the entire system becomes the one shown in Fig 2.

A tracking controller can be interpreted as a part of a stabilizing controller. In Ishizaki et al. (2019), a class of local controllers making the entire system internally stable has been provided based on the Youla parameterization in the continuous-time problem setting. We apply its discrete-time counterpart and then identify a subset of controllers additionally having the tracking performance. As for the continuous-time case, in order to avoid unnecessary complication of controller parametrization, suppose that the plant (1) is internally stable. Then, the class of stabilizing controllers is obtained as

$$u = K_y(z)(y - r) + K_w(z)w + K_v(z)v, \tag{4}$$

where

$$K_y(z) := \frac{Q_1(z)}{1 + Q_1(z)G_{y,u}(z) + Q_2(z)G_{w,u}(z)},$$
$$K_w(z) := \frac{Q_2(z)}{1 + Q_1(z)G_{y,u}(z) + Q_2(z)G_{w,u}(z)},$$
$$K_v(z) := -\frac{Q_1(z)G_{y,v}(z) + Q_2(z)G_{w,v}(z)}{1 + Q_1(z)G_{y,u}(z) + Q_2(z)G_{w,u}(z)}.$$

The transfer functions $Q_1(z)$, $Q_2(z) \in \mathcal{RH}_\infty$ are free design parameters.

In order to find the classes of $Q_1(z)$ and $Q_2(z)$ achieving tracking control $y(t) \to r$ as $t \to \infty$, we compute the transfer function from r to y as

$$y = -G_{\mathrm{pre}}(z)Q_1(z)r. \tag{5}$$

See Appendix A for the detailed computation of obtaining (5). From the final value theorem (see e.g. Levine

(2018)), tracking control is achieved if and only if

$$Q_1(1) = -\frac{1}{G_{\mathrm{pre}}(1)}. \tag{6}$$

Therefore, the controller (4) with the constraint (6) solves the tracking control problem.

One notices that from (3), tracking controller design requires the information of the DC gain of the cloud system, namely $\mathbf{G}_{\mathbf{v},\mathbf{w}}(1)$ while the plant cannot access the transfer function of the cloud system $\mathbf{G}_{\mathbf{v},\mathbf{w}}(z)$. It is relatively easy to estimate its value at some point $\mathrm{e}^{j\omega^*}$, namely $\mathbf{G}_{\mathbf{v},\mathbf{w}}(\mathrm{e}^{j\omega^*})$ from the output v by sending a signal w whose frequency is ω^*. For the DC gain, this a constant input $w(t) = a$, $\forall t \in \mathbb{Z}_+$. An approximation of the DC gain is obtained as

$$\mathbf{G}_{\mathbf{v},\mathbf{w}}(1) \simeq \frac{v(t)}{w(t)} = \frac{v(t)}{a}$$

for sufficiently large $t \in \mathbb{Z}_+$.

Remark 2.1. In this section, a reference r is supposed to be a constant for the sake of simplicity of the discussion. The condition (6) can be extended to an arbitrary superposition of periodic signals. ◁

3. DIFFERENTIAL PRIVACY BOUND

3.1 Differential Privacy

The local controller is designed after the plant is interconnected to the cloud system. This has advantages in view of privacy preservation because the plant does not need to share information of the local controller (i.e. control algorithms) and reference r (e.g. a target produced amount) when the cloud system is designed. However, there is still a possibility that the cloud system estimates the reference r from the signal w sent to it. In this section, our objective is to design the local controller which makes the estimation difficult, i.e. r is highly private against the cloud system. As a criterion for privacy, we employ differential privacy proposed by Dwork et al. (2006a,b), which has been applied to state-space representations of dynamical systems; see e.g. Le Ny and Pappas (2014); Kawano and Cao. In this subsection, we summarize existing results on differential privacy.

Consider a minimal representation of the transfer function from r to w of the entire system in Fig 2:

$$\begin{cases} x(t+1) = Ax(t) + br(t), \\ w(t) = c^\top x(t), \end{cases} \tag{7}$$

for $t \in \mathbb{Z}_+$, where $x(t) \in \mathbb{R}^n$, $r(t) \in \mathbb{R}$ and $w(t) \in \mathbb{R}$ denote the state, input and output, respectively, and $A \in \mathbb{R}^{n\times n}$ and $b, c \in \mathbb{R}^n$.

One of the main ideas of differential privacy is to add noise $\nu(t) \in \mathbb{R}$ to the output $w(t) \in \mathbb{R}$ for increasing the difficulty of estimating $r(t)$. That is, instead of $w(t)$, the plant sends the following $w_\nu(t)$ to the cloud system:

$$w_\nu(t) = w(t) + \nu(t). \tag{8}$$

For the zero initial state, the system (7) with the new output (8) induces the mapping $\mathcal{M} : \mathbb{R}^{t+1} \times \mathbb{R}^{t+1} \ni (r_t, \nu_t) \mapsto w_{\nu,t} \in \mathbb{R}^{t+1}$; recall the notation of the sequence in the notation part of the introduction. In differential privacy analysis, this mapping is called a *mechanism* (Dwork et al. (2006b,a)).

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

Definition 3.1. Given $c > 0$ and $p \in \mathbb{Z}$, a pair of input data $(r_t, r'_t) \in \mathbb{R}^{t+1} \times \mathbb{R}^{t+1}$ is said to be adjacent $\mathrm{Adj}^c_p(r_t, r'_t)$ if $|r_t - r'_t|_p \leq c$. ◁

The value c gives an upper bound on the similarity of pairs of input data sets (r_t, r'_t). Therefore, c is decided based on the range of input data sets, in which one wants to make the input data difficult to distinguish.

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

Definition 3.2. Let $(\mathbb{R}^{t+1}, \mathcal{F})$ be a measurable space. The mechanism induced by (7) and (8) is said to be *ε-differentially private* for $\mathrm{Adj}^c_p(r_t, r'_t)$ at a finite time instant $t \in \mathbb{Z}_+$ if there exists $\varepsilon > 0$ such that

$$\mathbb{P}(w_{\nu,t} \in S) \leq \mathrm{e}^{\varepsilon}\mathbb{P}(w'_{\nu,t} \in S),\ \forall S \in \mathcal{F} \tag{9}$$

for any $(r_t, r'_t) \in \mathrm{Adj}^c_p(r_t, r'_t)$. ◁

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

3.2 Differential Privacy Bound of Laplace Mechanism

From the definition, the variable ε depends on noise ν. In this subsection, we consider to add an i.i.d. Laplace noise; the corresponding mechanism is called the Laplace mechanism which can be found in Fig. 3. For the Laplace mechanism, we investigate the differential privacy level. In fact, we clarify that there is a limit to the differential privacy level determined by the plant and cloud system.

As preliminary, we introduce the q-induced norm of the system (7),

$$\|\Sigma\|_{q-\mathrm{ind}} := \sup_{\substack{r \in L_q[0,\infty) \\ \|r\|_q \neq 0}} \frac{\|w\|_q}{\|r\|_q}.$$

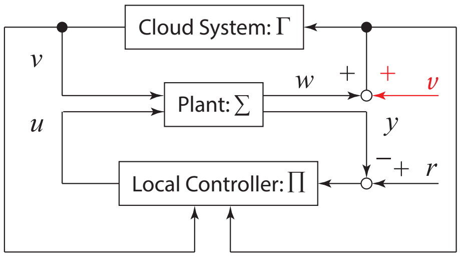

Fig. 3. Target Laplace Mechanism.

For the Laplace mechanism design, the 1-induced norm plays an important role as follows.

Theorem 3.3. The Laplace mechanism with i.i.d. $\nu \sim \mathrm{Lap}^{t+1}(0, b)$ is ε-differentially private for $\mathrm{Adj}_1^c(r_t, r_t')$ for any finite time instant $t \in \mathbb{Z}_+$, $r_t, r_t' \in L_1[0, \infty)$ with $\varepsilon > 0$ if and only if $b > 0$ is chosen such that

$$b \geq \frac{c}{\varepsilon} \|\Sigma\|_{1-\mathrm{ind}} \tag{10}$$

holds.

Theorem 3.3 implies that large noise is required to make the dynamical system (7) having a large 1-induced norm highly differentially private. Since adding noise can degenerate control performance, it is preferable to design the local controller such that its 1-induced norm from r to w is relatively small. This is a new requirement caused by taking privacy issues into account. Therefore, we investigate the 1-induced norm from r to w based on the characterization (4) of the local controller.

Remark 3.4. One may think that tracking control performance is less affected by making the norm of the transfer function from ν to y small even if one adds noise ν. However, the transfer function is $G_{y,v}(z)\mathbf{G}_{\mathbf{v},\mathbf{w}}(z)$, which cannot be changed by local controller design. Therefore, we consider to design the dynamical system (7) being highly private by adding small noise. ◁

The transfer function from r to w of the entire system (7) is computed as

$$w = -\frac{G_{w,u}(z)}{1 - G_{w,v}(z)\mathbf{G}_{\mathbf{v},\mathbf{w}}(z)} Q_1(z) r. \tag{11}$$

See Appendix A for the detailed computation of obtaining (11). From (11), one notices that even when the local controller does not know the transfer function $\mathbf{G}_{\mathbf{v},\mathbf{w}}(z)$ of the cloud system, the 1-induced norm can be made arbitrary small by making the free parameter $Q_1(z)$ arbitrary small. However, there is the constraint (6) for $Q_1(z)$ because of the requirement for tracking control. This is formally stated as follows.

Theorem 3.5. Consider the entire system (7). The 1-induced norm from r to w is lower bounded by

$$\|\Sigma\|_{1-\mathrm{ind}} \geq \left| \frac{G_{w,u}(1)}{1 - G_{w,v}(1)\mathbf{G}_{\mathbf{v},\mathbf{w}}(1)} \frac{1}{G_{\mathrm{pre}}(1)} \right|. \tag{12}$$

for any $Q_1(z)$, $Q_2(z) \in \mathcal{RH}_\infty$ achieving $y(t) \to r$ as $t \to \infty$. ◁

As a corollary of Theorems 3.3 and 3.5, we have the following lower bound on the differential privacy level.

Corollary 3.6. If the Laplace mechanism with i.i.d. $\nu \sim \mathrm{Lap}^{t+1}(0, b)$ is ε-differentially private for $\mathrm{Adj}_1^c(r_t, r_t')$ for any finite time instant $t \in \mathbb{Z}_+$, then

$$\varepsilon \geq \frac{c}{b} \left| \frac{G_{w,u}(1)}{1 - G_{w,v}(1)\mathbf{G}_{\mathbf{v},\mathbf{w}}(1)} \frac{1}{G_{\mathrm{pre}}(1)} \right| \tag{13}$$

holds. ◁

It is worth mentioning that the lower bound (13) on the differential privacy level is independent from the design parameters $Q_1(z)$ and $Q_2(z)$ of the local controller. Therefore, if the distribution of the Laplace noise is fixed, the differential privacy level ε cannot be made smaller than the value determined by the plant and cloud even if one tunes the controller parameters. Therefore, there is a ceiling privacy level achieved by cloud-based control.

Remark 3.7. Recall that $G_{\mathrm{pre}}(z)$ is given in (3). By using this, the transfer function in the right hand side of (13) becomes

$$\begin{aligned}
&\frac{G_{w,u}(1)}{1 - G_{w,v}(1)\mathbf{G}_{\mathbf{v},\mathbf{w}}(1)} \frac{1}{G_{\mathrm{pre}}(1)} \\
&= \frac{G_{w,u}(1)}{1 - G_{w,v}(1)\mathbf{G}_{\mathbf{v},\mathbf{w}}(1)} \frac{1}{G_{y,u}(1) + \frac{G_{y,v}(1)\mathbf{G}_{\mathbf{v},\mathbf{w}}(1)G_{w,u}(1)}{1 - G_{w,v}(1)\mathbf{G}_{\mathbf{v},\mathbf{w}}(1)}} \\
&= \frac{G_{w,u}(1)}{G_{y,u}(1)(1 - G_{w,v}(1)\mathbf{G}_{\mathbf{v},\mathbf{w}}(1)) + G_{y,v}(1)\mathbf{G}_{\mathbf{v},\mathbf{w}}(1)G_{w,u}(1)}
\end{aligned}$$

In a specific case when $G_{y,u}(1)G_{w,v}(1) = G_{y,v}(1)G_{w,u}(1)$, this becomes $G_{w,u}(1)/G_{y,u}(1)$, which implies that the privacy limit is determined only by the plant. ◁

4. EXAMPLES

Consider the following plant and cloud system,

$$\begin{aligned}
G_{w,v}(z) = G_{w,u}(z) &= \frac{5}{2z + 1}, \\
G_{y,v}(z) = G_{y,u}(z) &= \frac{8}{4z + 1}, \\
\mathbf{G}_{\mathbf{v},\mathbf{w}}(z) &= \frac{1}{4z - 2}.
\end{aligned}$$

Then, $G_{\mathrm{pre}}(z)$ in (3) is computed as

$$G_{\mathrm{pre}}(z) = \frac{80z^2 - 20z - 10}{32z^3 + 8z^2 - 24z - 10}.$$

It is possible to confirm that both plant and $G_{\mathrm{pre}}(z)$ are internally stable.

From the requirement of tracking control, $Q_1(z) \in \mathcal{RH}_\infty$ is required to satisfy (6), namely

$$Q_1(1) = -\frac{1}{G_{\mathrm{pre}}(1)} = -\frac{3}{25}.$$

As such a controller, we choose

$$Q_1(z) = -\frac{25(1 + a_1)}{3(z + a_1)},$$

where $a_1 \in (-1, 1)$. Next, we choose $Q_2(z) \in \mathcal{RH}_\infty$ as

$$Q_2(z) = \frac{b_2}{z + a_2},$$

where $a_2 \in (-1, 1)$ and $b_2 \in \mathbb{R}$. The blue lines in Fig. 4 and Fig. 5 show the trajectories (y, w) of the system (7) for $r(t) = 1$, $t = ([0, 100] \cup [101, 200]) \cap \mathbb{Z}_+$ and $r(t) = 2$, $t = [201, 300] \cap \mathbb{Z}_+$ when $a_1 = 1/2$, $a_2 = a_1$, and $b_2 = -b_1$. Tracking control, i.e. $y \to r$ is achieved without using $\mathbf{G}_{\mathbf{v},\mathbf{w}}(z)$; one can further confirm that the tracking performance does not depend on the choice of $Q_2(z)$.

On the other hand, from the signal w sent to the cloud, the cloud can easily estimate that r has changed twice, and the first and third values are the same; see the blue lines in Fig. 4 and Fig. 5. Therefore, information of the reference r can be viewed as less private. In order to increase the privacy level of r, we consider to add i.i.d. Laplace noise ν to w. In view of Remark 3.7, the lower bound (13) on the differential privacy level is obtained as

$$\varepsilon \geq \frac{c}{b} \left| \frac{G_{w,u}(1)}{G_{y,u}(1)} \right| = \frac{25}{24} \frac{c}{b}.$$

Moreover, adding noise ν causes degeneration of tracking performance. As mentioned in Remark 3.4, the sensitivity of the output y with respect to the noise ν cannot be improved by tuning the local controller. In fact, the transfer function from ν to y is obtained as

$$G_{y,v}(z)\mathbf{G}_{\mathbf{v},\mathbf{w}}(z) = \frac{8}{4z+1}\frac{1}{4z-2},$$

whose H_∞-norm is 0.526. Since both privacy level of r and sensitivity of y depend on the plant and cloud system only, it is very difficult to achieve both precise tracking and tight privacy preservation.

The red line in Fig. 4 shows the trajectories (y, w_ν) when the i.i.d. Laplace noise with the distribution $b = 0.1$ is added to w. In this case, tracking performance is less degenerate against the noise. However, simultaneously r is less private. Next, the red line in Fig. 5 shows the trajectories (y, w_ν) when $b = 0.5$. It becomes more difficult to estimate r from w_ν while tracking performance is significantly degenerate. Therefore, it is difficult to increase the differential privacy level while keeping high tracking performance.

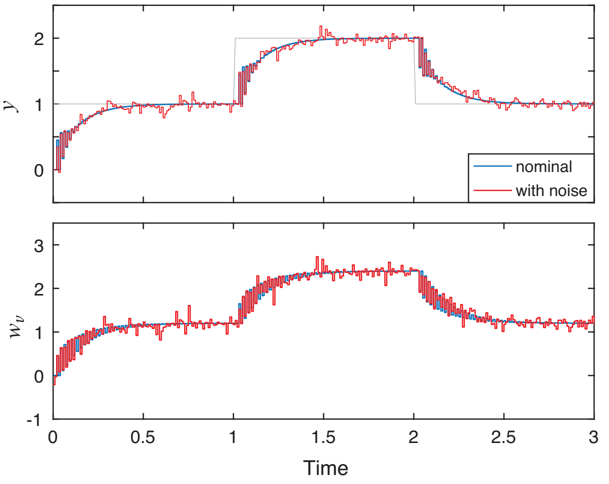

Fig. 4. The trajectories (y, w) of the Laplace mechanism with $b = 0.1$, where the sampling time is 0.01.

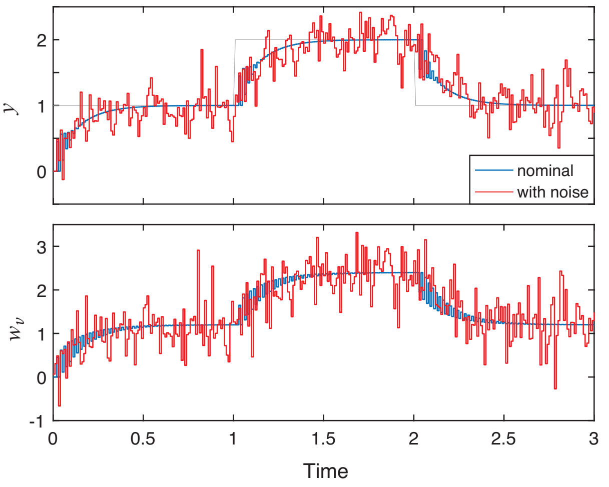

Fig. 5. The trajectories (y, w) of the Laplace mechanism with $b = 0.5$, where the sampling time is 0.01.

5. CONCLUSION

In this paper, we have analyzed the differential privacy level of the Laplace mechanism in the context of cloud based control. We have revealed that there is a ceiling level of differential privacy achieved by tuning the local controller. Also, the degeneration property of the control performance caused by adding noise, cannot be changed. Therefore, there is a fundamental performance limit in terms of differential privacy which is rooted in the fact that it is difficult to improve both privacy level and control performance by tuning parameters of the local controller.

Appendix A. COMPUTATIONS OF (5) AND (11)

In this appendix, we consider to obtain (5) and (11). First, we compute the transfer function from $(r, v) \to y$. The changes of variables $\hat{y} = y - G_{y,v}v$ and $\hat{w} = w - G_{w,v}v$ for (1), (2), and (4) yield

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

where in the last equality, the definitions of $K_y(z)$, $K_w(z)$, and $K_v(z)$ are used. From these four equations, the transfer function from r to $\hat{y}$ is computed as

$$\begin{aligned}
\hat{y} =& -\frac{G_{y,u}(z)K_y(z)}{1 - K_w(z)G_{w,u}(z) - G_{y,u}(z)K_y(z)}r\\
=& -G_{y,u}(z)Q_1(z)r,
\end{aligned}$$

where again the definitions of $K_y(z)$ and $K_w(z)$ are used. Therefore, the change of variables $\hat{y} = y - G_{y,v}v$ yields

$$y = -G_{y,u}(z)Q_1(z)r + G_{y,v}(z)v. \tag{A.1}$$

On the other hand, the transfer function from r to $\hat{w}$ is obtained as

$$\hat{w} = -G_{w,u}(z)Q_1(z)r.$$

The change of variables $\hat{w} = w - G_{w,v}v$ yields

$$w = -G_{w,u}(z)Q_1(z)r + G_{w,v}(z)v \tag{A.2}$$

From (2), it follows that

$$v = -\frac{\mathbf{G}_{\mathbf{v},\mathbf{w}}(z)G_{w,u}(z)}{1 - \mathbf{G}_{\mathbf{v},\mathbf{w}}(z)G_{w,v}(z)}Q_1(z)r \tag{A.3}$$

Then, (A.1) and (A.3) yield

$$\begin{aligned}
y =& -\left(G_{y,u}(z) + \frac{G_{y,v}(z)\mathbf{G}_{\mathbf{v},\mathbf{w}}(z)G_{w,u}(z)}{1 - \mathbf{G}_{\mathbf{v},\mathbf{w}}(z)G_{w,v}(z)}\right)Q_1(z)r\\
=& -G_{\mathrm{pre}}Q_1(z)r.
\end{aligned}$$

This is nothing but (5).

Finally, (11) is obtained from (A.2) and (A.3).

REFERENCES

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

Dwork, C., McSherry, F., Nissim, K., and Smith, A. (2006b). Calibrating noise to sensitivity in private data analysis. *Proc. 3rd Theory of Cryptography Conference*, 265–284.

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

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

Kawano, Y. and Cao, M. (2021). Design of privacy-preserving dynamic controllers. *IEEE Transactions on Automatic Control*. (to appear: arXiv preprint arXiv:1901.07384).

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

Levine, W.S. (2018). *The Control Handbook*. CRC press.

Lim, H.C., Babu, S., Chase, J.S., and Parekh, S.S. (2009). Automated control in cloud computing: challenges and opportunities. *Proc. 1st Workshop on Automated Control for Datacenters and Clouds*, 13–18.

Tanaka, T., Skoglund, M., Sandberg, H., and Johansson, K.H. (2017). Directed information and privacy loss in cloud-based control. *Proc. 2017 American Control Conference*, 1666–1672.

Willenborg, L. and Waal, T.D. (1996). *Statistical Disclosure Control in Practice*, volume 111. Springer Science & Business Media.

Willenborg, L. and Waal, T.D. (2012). *Elements of Statistical Disclosure Control*, volume 155. Springer Science & Business Media.