2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Localized Privacy Preservation by Innovation Perturbation in a Cooperative LQG Control System

Wenliang Sheng Zhiyun Zhao Wen Yang Chao Yang

***Abstract*—We consider a cooperative Linear Quadratic Gaussian (LQG) control system, in which an individual user owns a local plant whose control inputs are provided by a server. In the cooperation, the user takes the plant states as private information and desires to maximize the privacy preservation while ensuring that the server still provides a certain level of control performance. Moreover, the user requires a privacy scheme that is used locally and is unknown to the server, so that it can create a deviation in the server's knowledge of the states from the true value. To achieve this, we propose two privacy schemes localized at the user side, which inject perturbations in the innovation data sent to the server. For both schemes, firstly, we analyze the privacy preservation quality provided by the scheme and the performance loss in the LQG control caused by it. Secondly, based on the trade-off between them, we propose an optimization problem. Thirdly, we propose a recovery procedure by which the control performance is recovered to the optimal one, i.e., the privacy preservation is achieved without any performance loss in control. Finally, simulations are provided, and we give discussions on the two schemes based on the simulation results.**

***Index Terms*—cooperative networked control system, LQG control, privacy preservation, cooperation privacy.**

I. Introduction

Networked control is the current trend for industrial automation and has ever-increasing applications in a wide range of areas, such as smart grids, process control, automated highway systems, and unmanned aerial vehicles [1]. Its flexibility allows the system to be run cooperatively by multiple parties, and we name this type of system as *a cooperative networked control system* [2]. A user-server system is an example of a cooperative networked control system, where one party called the user employs another party called the server to provide service to work cooperatively, as shown in Fig. 1. The cooperative networked control systems are expected to have broader applications in the real world, as cooperation is a natural trend of social development.

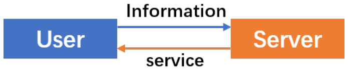

Fig. 1. The user-server system.

Key Laboratory of Smart Manufacturing in Energy Chemical Process, Ministry of Education, Dept. of Automation, East China University of Science and Technology, Shanghai, China, 200237. Email: {y30210936, zyzhao, weny, yangchao}@ecust.edu.cn. The corresponding author is Chao Yang.

However, while this cooperative manner brings efficiency advantages, it may also bring the privacy issue. To achieve cooperation, the user is required to share local information that might be considered private to the server. Meanwhile, the server may also have to be taken as "semi-honest": although it completes the task of cooperation honestly, it may also attempt to infer private information and transfer it to the third parties, causing a risk of privacy breach for the user [3]. Consequently, in order to use the cooperative systems safely, we need to address this privacy issue.

A. Related Studies

The study of privacy was initially considered in the database field [4] and was further studied by the control field [5], [6]. Several different research frameworks on privacy were proposed based on different understandings of privacy. The three main frameworks are differential privacy, information-theoretic approach, and homomorphic encryption.

Le Ny et al. [5] first applied the concept of differential privacy to the field of control. Subsequently, increasing studies on differential privacy are emerging in the field of control [7]–[10]. Wang et al. [9] studied the initial-value privacy problems of linear dynamical systems based on differential privacy. They defined differential initial-value privacy and intrinsic initial-value privacy as metrics of privacy risk. Hawkins and Hale [10] studied the privacy preservation problem in a multi-agent system, where agents add privacy noise to their states before sharing them with other agents.

The information-theoretic approach is the second important framework for privacy preservation, where the quantities based on the information entropy are utilized as privacy metrics. In the existing studies, directional information [11], Kullback-Leibler divergence [12], mutual information [13], etc., have been applied as privacy metrics, and associated problems are further considered.

Unlike the previous two frameworks, where the privacy is usually protected by adding noise, homomorphic encryption provides a completely different methodology. By finding suitable encryption operators or algorithms that ensure the homomorphic nature of the data before and after the encryption operation, it enables the server to do the required computation while keeping unknown with the true data. Fully homomorphic encryption [14], partially homomorphic encryption [15], labeled homomorphic encryption [16], and other homomorphic encryption methods [17] have also been investigated.

Among these three privacy frameworks mentioned above, privacy research in the control field often considers the trade-off between privacy and performance. In this paper, we not only make a parallel analysis but also consider how to achieve good privacy preservation without performance loss.

B. *The Study of This Paper*

We study the privacy preservation problem in a *cooperative LQG control system*, in which a user employs a server to calculate the optimal LQG control input for the local plant. We aim at designing localized privacy schemes to protect the privacy of the user, which is not open to the server.

The study in this paper is novel. Firstly, different from most existing studies, which mainly considered open-loop systems [5], [18], we consider a closed-loop system, which is more difficult to analyze. Secondly, in most existing studies, the proposed privacy scheme is set at the server [19], [20], which does not completely alleviate the user's concern about privacy. The proposed privacy schemes in this paper are designed only at the user side, which better meets the user's requirements.

The main contributions of this paper are summarized as follows.

1) We propose two novel localized privacy-preserving schemes in a cooperative LQG control system, which makes the server's knowledge of the privacy information deviate from the true one.
2) For the proposed schemes, we analyze the performances of privacy preservation and LQG control. Based on the trade-off between them, we further propose an optimization problem.
3) We propose a procedure to recover the perfect optimal control inputs for the user based on the ones provided by the server, under which the privacy is preserved without performance loss in control.

The remainder of the paper is organized as follows. Section II proposes the localized design for privacy preservation in the considered system. Section III and Section IV present the main results. Section V presents a simulation example. At last, Section VI concludes the paper.

Notations: $\mathbb{Z}_+$ is the set of non-negative integers and $k \in \mathbb{Z}_+$ is the time index. $\mathbb{R}$ is the set of real numbers. $\mathbb{R}^n$ is the n-dimensional Euclidean space. $\mathbb{S}^n_+$ (and $\mathbb{S}^n_{++}$) is the set of n by n positive semi-definite matrices (and positive definite matrices); when $X \in \mathbb{S}^n_+$ (and $\mathbb{S}^n_{++}$), it is written as $X \geq 0$ (and $X > 0$). $X \geq Y$ if $X - Y \in \mathbb{S}^n_+$. $\boldsymbol{E}(\cdot)$ is the expectation of a random variable and $\boldsymbol{E}(\cdot|\cdot)$ is the conditional expectation. $\mathrm{tr}(\cdot)$ is the trace of a matrix.

II. Problem Setup

In this section, we present the cooperation model for the user and the server in a basic cooperative LQG control system. Within this basic structure, we propose a localized privacy scheme. Finally, we present the feasible problems to study.

A. *Basic Structure of the Cooperative LQG Control System*

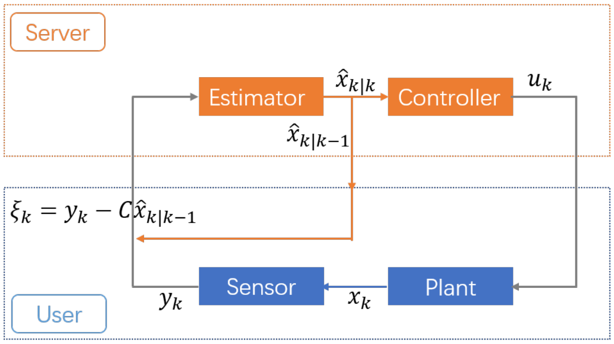

Fig. 2. The basic structure of the cooperative LQG control system.

The basic structure of the LQG cooperative control system consists of a user and a server, which is illustrated in Fig. 2. The user owns a plant whose states are monitored by a sensor, which is a linear time-invariant system. The system state and measurement equations are given as follows:

$$x_{k+1} = Ax_k + Bu_k + w_k, \tag{1}$$

$$y_k = Cx_k + v_k, \tag{2}$$

where $x_k \in \mathbb{R}^n$ is the state of the plant, $u_k \in \mathbb{R}^m$ is the control input at each time k, and $y_k \in \mathbb{R}^m$ is the measurement of x_k at time k. The user cannot directly obtain the actual state x_k of the system and only y_k is accessible. The random variables w_k and v_k are the mutually independent Gaussian white noise with distribution $\mathcal{N}(0, Q)(Q \geq 0)$ and $\mathcal{N}(0, R)(R > 0)$, respectively. We also assume that $(A, \sqrt{Q})$ is stabilizable and (C, A) is detectable.

Because of computational capability limitations, the user employs a remote server to compute the optimal LQG control inputs for its plant. The considered quadratic objective for the LQG control is denoted as $\mathcal{O}_{0:T}$ and is defined as follows:

$$\mathcal{O}_{0:T} \triangleq \boldsymbol{E}[\sum_{k=0}^{T-1}(x_k' W_k x_k + u_k' U u_k) + x_T' W_T x_T], \tag{3}$$

where W and U are weight matrices satisfying $W \geq 0$ and $U > 0$.

To achieve the cooperation, the user needs to provide the server with the following information:

- system matrices A, B, and C;
- noise convariances Q and R;
- weight matrices W and U;
- the initial condition $\mathcal{N}(x_0, \Sigma_0)$.

The server works as an estimator and a controller for the user. It first computes the *a prior* and *a posterior* estimates $\hat{x}_{k|k-1}$ and $\hat{x}_{k|k}$ of the plant's state x_k, which are defined as follows:

$$\hat{x}_{k|k-1} \triangleq \boldsymbol{E}[x_k|y_{k-1}],$$

$$\hat{x}_{k|k} \triangleq \boldsymbol{E}[x_k|y_k].$$

Meanwhile, let $P_{k|k-1}$ and $P_{k|k}$ be the estimation error covariance matrices associated with $\hat{x}_{k|k-1}$ and $\hat{x}_{k|k}$, respectively:

$$P_{k|k-1} \triangleq \boldsymbol{E}[(x_k - \hat{x}_{k|k-1})(x_k - \hat{x}_{k|k-1})'|y_{k-1}],$$
$$P_{k|k} \triangleq \boldsymbol{E}[(x_k - \hat{x}_{k|k})(x_k - \hat{x}_{k|k})'|y_k].$$

The estimates and the associated error covariances are computed by Kalman filtering. The server first does the time update as follows:

$$\hat{x}_{k|k-1} = A\hat{x}_{k-1|k-1} + Bu_{k-1}, \tag{4}$$
$$P_{k|k-1} = AP_{k-1|k-1}A' + Q, \tag{5}$$

and it sends $\hat{x}_{k|k-1}$ back to the user. The user provides the innovation ξ_k to the server, which is defined as

$$\xi_k = y_k - C\hat{x}_{k|k-1}. \tag{6}$$

The server then proceeds the measurement update as follows:

$$K_k = P_{k|k-1}C'(CP_{k|k-1}C' + R)^{-1}. \tag{7}$$
$$\hat{x}_{k|k} = \hat{x}_{k|k-1} + K_k\xi_k, \tag{8}$$
$$P_{k|k} = (I - K_kC)P_{k|k-1}. \tag{9}$$

Based on $\hat{x}_{k|k}$, the server computes the optimal LQG control input u_k:

$$S_T = W, \tag{10}$$
$$S_k = A'S_{k+1}A + W - A'S_{k+1}B(B'S_{k+1}B + U)^{-1}B'S_{k+1}A, \tag{11}$$
$$L_k = -(B'S_{k+1}B + U)^{-1}B'S_{k+1}A, \tag{12}$$
$$u_k = L_k\hat{x}_{k|k}, \tag{13}$$

and sends it back to the user.

B. Local Design of Privacy Scheme

In a basic cooperative LQG control system, the server obtains accurate estimates of the plant's states. However, the user takes the state information as its privacy and wants the server's estimate to deviate from the true one. Therefore, to meet the privacy preservation needs, the user intends to use a localized privacy scheme that is unknown to the server to distort the server's estimate.

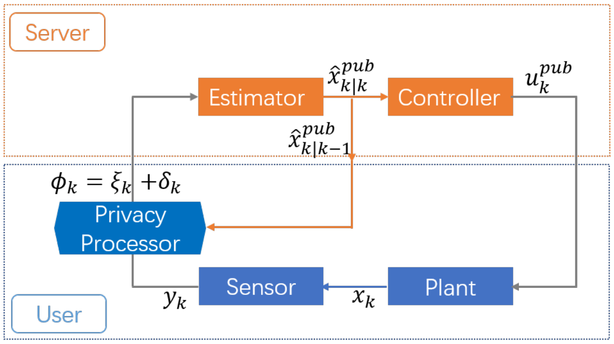

Fig. 3. The structure under the privacy scheme.

We propose a localized privacy scheme in which the user adds a perturbation to the innovation ξ_k before sending it to the server, where the obtained signal is denoted as ϕ_k:

$$\phi_k = \xi_k + \delta_k. \tag{14}$$

The noise δ_k is i.i.d. and follows the Gaussian distribution $\mathcal{N}(0, \Delta)$. This scheme is supposed to make the server's estimate deviate from the true state estimate of the plant.

C. Problem Statement

The proposed privacy scheme increases the privacy preservation quality for the user, which is denoted as $\mathcal{Q}_{privacy}$. Meanwhile, it causes a loss in the LQG performance, which is denoted as $\mathcal{Q}_{Loss}$. In this paper, we consider to work on the following problems:

1) The analysis of the privacy preservation quality $\mathcal{Q}_{privacy}$ provided by the privacy scheme and the control performance loss $\mathcal{Q}_{Loss}$ caused by it.
2) The optimization problem based on the trade-off between the privacy preservation quality and performance loss:

$$\begin{aligned} \max \quad & \operatorname{tr}(\mathcal{Q}_{privacy}) \\ \text{s.t.} \quad & \mathcal{Q}_{Loss} \leq \alpha, \end{aligned}$$

where $\alpha > 0$ represents a given performance level.
3) The recovery of the perfect optimal control u^*_k for the user, which ensures the privacy preservation quality without performance loss.

III. Performance Analysis of Privacy and LQG Control

In this section, we first define the metrics for privacy preservation and the control performance loss, based on which we analyze the proposed localized privacy scheme. We propose an optimization problem to analyze the trade-off between privacy preservation quality and performance loss. Furthermore, we recover the perfect optimal control for the user.

We use the superscript *pub* to represent associated quantities of the server under the privacy scheme. The user computes the innovation as

$$\xi^{drt}_k = y_k - C\hat{x}^{pub}_{k|k-1}, \tag{15}$$

where the superscript *drt* indicates that the user computes the innovation directly based on the prior estimate $\hat{x}^{pub}_{k|k-1}$ sent back by the server. The localized privacy scheme is

$$\phi^{drt}_k = \xi^{drt}_k + \delta_k. \tag{16}$$

Consequently, the estimation process on the server is changed to

$$\hat{x}^{pub}_{k|k-1} = A\hat{x}^{pub}_{k-1|k-1} + Bu^{pub}_{k-1}, \tag{17}$$
$$P^{pub}_{k|k-1} = AP^{pub}_{k-1|k-1}A' + Q, \tag{18}$$
$$K^{pub}_k = P^{pub}_{k|k-1}C'(CP^{pub}_{k|k-1}C' + R)^{-1}, \tag{19}$$
$$\hat{x}^{pub}_{k|k} = \hat{x}^{pub}_{k|k-1} + K^{pub}_k\phi^{drt}_k, \tag{20}$$
$$P^{pub}_{k|k} = (I - K^{pub}_kC)P^{pub}_{k|k-1}. \tag{21}$$

The control input is calculated as follows:

$$u_k^{pub} = L_k \hat{x}_{k|k}^{pub}. \qquad (22)$$

Remark 1. *It can be seen from (10)-(12) that the calculation of L_k is only related to the parameters of the plant. Therefore, regardless of the presence of a privacy scheme, the control gain L_k at time k remains the same.*

Remark 2. *Similarly to Remark 1, parameters $P_{k|k-1}^{pub}$, K_k^{pub}, and $P_{k|k}^{pub}$ are identical to $P_{k|k-1}$, K_k, and $P_{k|k}$ according to (18)(19)(21). In the following discussion, we use the notation without superscripts to represent them.*

A. Privacy Analysis

We define the estimate based on the measurement y_k without privacy scheme as the optimal estimate and represent it with the superscript *opt*. As the plant is determined by u_k^{pub}, it holds that

$$\begin{aligned}\hat{x}_{k|k-1}^{opt} &= A\hat{x}_{k-1|k-1}^{opt} + Bu_{k-1}^{pub},\\ \hat{x}_{k|k}^{opt} &= \hat{x}_{k|k-1}^{opt} + K_k(y_k - C\hat{x}_{k|k-1}^{opt}).\end{aligned}$$

The added noise makes the server's posterior estimate $\hat{x}_{k|k}^{pub}$ deviate from the optimal estimate $\hat{x}_{k|k}^{opt}$. Naturally, this deviation caused by the privacy scheme can be utilized to measure the quality of privacy preservation at each time k and is denoted as $Q_{privacy}^k$:

$$\mathcal{Q}_{privacy}^k \triangleq \boldsymbol{E}[(\hat{x}_{k|k}^{pub} - \hat{x}_{k|k}^{opt})(\hat{x}_{k|k}^{pub} - \hat{x}_{k|k}^{opt})']. \qquad (23)$$

We also take the average of $\mathcal{Q}_{privacy}^k$ as the privacy metric over the duration of time T, denoted as follows:

$$\mathcal{Q}_{privacy} \triangleq \frac{1}{T}\sum_{k=0}^{T-1} \mathcal{Q}_{privacy}^k. \qquad (24)$$

Theorem 1. *Under the localized privacy scheme $\phi_k^{drt} = \xi_k^{drt} + \delta_k$, it holds that*

$$\begin{aligned}\mathcal{Q}_{privacy}^0 &= 0,\\ \mathcal{Q}_{privacy}^k &= (I - K_kC)A\mathcal{Q}_{privacy}^{k-1}A'(I-K_kC)'\\ &\quad + K_k\Delta K_k'. \qquad (25)\end{aligned}$$

Proof. In appendix. ■

B. LQG Control Performance Analysis

Firstly, we define the estimate without any privacy scheme, i.e., under the basic cooperative LQG control system, as the perfect optimal estimate, and denote it by the superscript $*$. In this case, the user's plant is determined by u_k^* and it holds that

$$\begin{aligned}\hat{x}_{k|k-1}^{*} &= A\hat{x}_{k-1|k-1}^{*} + Bu_{k-1}^{*},\\ \hat{x}_{k|k}^{*} &= \hat{x}_{k|k-1}^{*} + K_k(y_k - C\hat{x}_{k|k-1}^{*}).\end{aligned}$$

Remark 3. *It should be noted that there is a difference between the optimal estimate and the perfect optimal estimate, where the optimal estimate is based on the innovation sequence that has been corrupted by noise, while the perfect optimal estimate is based on the optimal innovation sequence.*

Secondly, the quadratic objective in the basic cooperative LQG control system is given as

$$\mathcal{O}_{0:T}^* = \boldsymbol{E}[(x_0^*)'S_0x_0^*] + \sum_{k=0}^{T-1} tr(S_{k+1}Q) + \sum_{k=0}^{T-1} tr(\Phi_kP_k),$$

where

$$\Phi_k = A'S_{k+1}B(B'S_{k+1}B+U)^{-1}B'S_{k+1}A.$$

Under the proposed privacy scheme, the performance loss is defined as $\mathcal{Q}_{Loss}$:

$$\mathcal{Q}_{Loss} = \mathcal{O}_{0:T} - \mathcal{O}_{0:T}^*. \qquad (26)$$

Theorem 2. *Under the localized privacy scheme $\phi_k^{drt} = \xi_k^{drt} + \delta_k$, the LQG performance is*

$$\begin{aligned}\mathcal{O}_{0:T} &= \boldsymbol{E}(x_0'S_0x_0) + \sum_{k=0}^{T-1} tr(S_{k+1}Q) + \sum_{k=0}^{T-1} tr(\Phi_kP_k)\\ &\quad + \sum_{k=0}^{T-1} tr(\Phi_k\mathcal{Q}_{privacy}^k),\\ \Phi_k &= A'S_{k+1}B(B'S_{k+1}B+U)^{-1}B'S_{k+1}A.\end{aligned}$$

Proof. In appendix. ■

Since $x_0 = x_0^*$, the performance loss $\mathcal{Q}_{Loss}$ caused by the privacy scheme is

$$\mathcal{Q}_{Loss} = \sum_{k=0}^{T-1} tr(\Phi_k\mathcal{Q}_{privacy}^k). \qquad (27)$$

C. Optimization Problem

Based on the above analysis, the following optimization problem is proposed to study the trade-off between privacy preservation and control performance: to maximize the privacy metric $\mathcal{Q}_{privacy}$ when the performance loss $\mathcal{Q}_{Loss}$ is required to be under a given level α. The problem is formulated as follows.

Problem 1.

$$\begin{aligned}\max_{\Sigma_\delta, \mathcal{Q}_{privacy}^k} \quad & \mathrm{tr}(\mathcal{Q}_{privacy})\\ \text{s.t.} \quad & \mathcal{Q}_{Loss} \le \alpha,\\ & \mathcal{Q}_{privacy}^k = (I-K_kC)A\mathcal{Q}_{privacy}^{k-1}A'(I-K_kC)'\\ & \qquad + K_k\Sigma_\delta K_k',\\ & k = 1, 2, ..., T.\end{aligned}$$

The problem is a linear programming one and can be solved efficiently by numerical methods.

D. Recovery of Perfect Optimal Control

The implementation of the privacy scheme leads to that the actual state sequence $\mathcal{X} = \{x_0, x_1, ..., x_k\}$ of the plant is different from the perfect optimal state sequence $\mathcal{X}^* = \{x_0^*, x_1^*, ..., x_k^*\}$. In this subsection, we propose a method that is able to recover the perfect optimal control input u_k^* for the user, such that the state sequence $\mathcal{X}$ is identical to $\mathcal{X}^*$, i.e., the performance loss in LQG control is eliminated.

To achieve the recovery of the perfect optimal control u_k^*, the user requires the server to further provide the Kalman gain K_k^{pub} and the LQG control gain L_k. In addition, we require the user to have certain computation and storage capability.

Theorem 3. *Under the localized privacy scheme $\phi_k^{drt} = \xi_k^{drt} + \delta_k$, the perfect optimal control u_k^* can be recovered as follows:*

$$\begin{aligned} d^*_{k|k-1} &= (A + BL_{k-1})d^*_{k-1|k-1}, \\ d^*_{k|k} &= (I - K_k^{pub}C)d^*_{k|k-1} + K_k^{pub}\delta_k, \\ u_k^* &= u_k^{pub} - L_k d^*_{k|k}, \end{aligned}$$

where the recursion starts with $d^*_{0|0} = 0$.

Proof. Let

$$\begin{aligned} d^*_{k|k-1} &= \hat{x}^{pub}_{k|k-1} - \hat{x}^*_{k|k-1}, \\ d^*_{k|k} &= \hat{x}^{pub}_{k|k} - \hat{x}^*_{k|k}. \end{aligned}$$

Since initial condition follows $\hat{x}^{pub}_{0|0} = \hat{x}^*_{0|0} = x_0$, we have $d^*_{0|0} = 0$. By the straightforward calculation, we have

$$\begin{aligned} d^*_{k|k-1} &= (A\hat{x}^{pub}_{k-1|k-1} + Bu^{pub}_{k-1}) - (A\hat{x}^*_{k-1|k-1} + Bu^*_{k-1}) \\ &= (A + BL_{k-1})d^*_{k-1|k-1}, \\ d^*_{k|k} &= [\hat{x}^{pub}_{k|k-1} + K_k(z_k - C\hat{x}^{pub}_{k|k-1})] \\ &\quad -[\hat{x}^*_{k|k-1} + K_k(y_k - C\hat{x}^*_{k|k-1})] \\ &= (I - K_k^{pub}C)d^*_{k|k-1} + K_k^{pub}\delta_k. \end{aligned}$$

Therefore, we can recover the perfect optimal control input as follows:

$$\begin{aligned} u_k^* &= L_k\hat{x}^*_{k|k} \\ &= L_k(\hat{x}^{pub}_{k|k} - d^*_{k|k}) \\ &= u_k^{pub} - L_k d^*_{k|k}. \end{aligned}$$

■

The procedures included in Theorem 3 are presented as follows.

Procedure 1 Recovery of the Perfect Optimal Control u_k^*

Initial condition: $d^*_{0|0} = 0$.
The server:
1) send K_k^{pub} back to the user after the estimation process is completed;
2) send L_k and u_k^{pub} back to the user after the control input calculation is completed;
The user:
3) recover the perfect optimal control input for the user based on Theorem 3.

By Procedure 1, we have $\mathcal{Q}_{Loss} = 0$, since the control input is recovered to the perfect optimal scenario. Accordingly, the privacy performance is given as follows.

Theorem 4. *Under the localized privacy scheme $\phi_k^{drt} = \xi_k^{drt} + \delta_k$ with the control recovery method stated in Theorem 3, it holds that*

$$\begin{aligned} \mathcal{Q}^0_{privacy} &= 0, \\ \mathcal{Q}^k_{privacy} &= (I - K_kC)(A + BL_{k-1})\mathcal{Q}^{k-1}_{privacy} \\ &\quad (A + BL_{k-1})'(I - K_kC)' + K_k\Delta K_k'. \end{aligned} \tag{28}$$

Proof. According to Theorem 3, we can further have

$$d^*_{k|k} = (I - K_kC)(A + BL_{k-1})d^*_{k-1|k-1}.$$

In the scenario of recovering the perfect optimal control input, it holds that $\hat{x}^{opt}_{k|k} = \hat{x}^*_{k|k}$. The remaining proof is similar to that of Theorem 1. ■

IV. Privacy Preservation by Perturbation on True Innovation

In this section, we propose another localized privacy scheme that adds perturbation to the true innovation of the system. This scheme requires the user to recover the optimal prior estimate $\hat{x}^{opt}_{k|k-1}$, which needs the server to provide additional information K_k^{pub}. The structure is shown in Fig. 4.

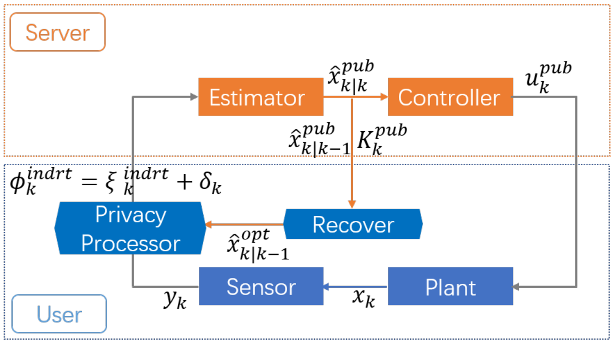

Fig. 4. The structure under privacy scheme $\phi_k^{indrt} = \xi_k^{indrt} + \delta_k$.

A. Privacy Scheme

We use the superscript $indrt$ to denote innovation in the true innovation scheme, which means that the innovation is calculated indirectly. In this case, the innovation is

$$\xi_k^{indrt} = y_k - C\hat{x}^{opt}_{k|k-1},$$

and the privacy scheme is designed as

$$\phi_k^{indrt} = \xi_k^{indrt} + \delta_k.$$

The estimation procedure at the server is updated to

$$\begin{aligned} \hat{x}^{pub}_{k|k-1} &= A\hat{x}^{pub}_{k-1|k-1} + Bu^{pub}_{k-1}, \\ \hat{x}^{pub}_{k|k} &= \hat{x}^{pub}_{k|k-1} + K_k\phi_k^{indrt}. \end{aligned}$$

The recovery procedure of $\hat{x}^{opt}_{k|k}$ at the user is presented as follows.

Theorem 5. *Under the localized privacy scheme $\phi_k^{indrt} = \xi_k^{indrt} + \delta_k$, the optimal prior estimate $\hat{x}_{k|k-1}^{opt}$ can be recovered as follows:*

$$\begin{aligned} d_{k|k-1}^{opt} &= A d_{k-1|k-1}^{opt}, \\ d_{k|k}^{opt} &= d_{k|k-1}^{opt} + K_k^{pub}\delta_k, \\ \hat{x}_{k|k-1}^{opt} &= \hat{x}_{k|k-1}^{pub} - d_{k|k-1}^{opt}, \end{aligned}$$

where the recursion starts with $d_{0|0}^{opt} = 0$.

Proof. Let

$$\begin{aligned} d_{k|k-1}^{opt} &= \hat{x}_{k|k-1}^{pub} - \hat{x}_{k|k-1}^{opt}, \\ d_{k|k}^{opt} &= \hat{x}_{k|k}^{pub} - \hat{x}_{k|k}^{opt}. \end{aligned}$$

Since the initial condition follows $\hat{x}_{0|0}^{pub} = \hat{x}_{0|0}^{opt} = x_0$, we have $d_{0|0}^{opt} = 0$. By the straightforward calculation, we have

$$\begin{aligned} d_{k|k-1}^{opt} &= (A\hat{x}_{k-1|k-1}^{pub} + Bu_{k-1}^{pub}) - (A\hat{x}_{k-1|k-1}^{opt} + Bu_{k-1}^{pub}) \\ &= A d_{k-1|k-1}^{opt}, \\ d_{k|k}^{opt} &= [\hat{x}_{k|k-1}^{pub} + K_k(z_k - C\hat{x}_{k|k-1}^{pub})] \\ &\quad -[\hat{x}_{k|k-1}^{opt} + K_k(y_k - C\hat{x}_{k|k-1}^{opt})] \\ &= d_{k|k-1}^{opt} + K_k^{pub}\delta_k. \end{aligned}$$

Therefore, we can recover the optimal prior estimate.

$$\hat{x}_{k|k-1}^{opt} = \hat{x}_{k|k-1}^{pub} - d_{k|k-1}^{opt}.$$

■

In this scenario, the privacy performance is given as follows.

Theorem 6. *Under the localized privacy scheme $\phi_k^{indrt} = \xi_k^{indrt} + \delta_k$, it holds that*

$$\begin{aligned} \mathcal{Q}_{privacy}^{0} &= 0, \\ \mathcal{Q}_{privacy}^{k} &= A\mathcal{Q}_{privacy}^{k-1}A' + K_k\Delta K_k'. \end{aligned} \tag{29}$$

Proof. The proof is similar to that of Theorem 1. ■

The analysis on the LQG control performance is identical to Theorem 2. Hence, the performance loss $\mathcal{Q}_{Loss}$ can be further obtained:

$$\mathcal{Q}_{Loss} = \sum_{k=0}^{T-1} tr(\Phi_k \mathcal{Q}_{privacy}^{k}). \tag{30}$$

In order to balance privacy preservation quality and performance loss, we have the following optimization problem:

Problem 2.

$$\begin{aligned} \max_{\Sigma_\delta, \mathcal{Q}_{privacy}^{k}} \quad & \mathrm{tr}(\mathcal{Q}_{privacy}) \\ \text{s.t.} \quad & \mathcal{Q}_{Loss} \le \alpha, \\ & \mathcal{Q}_{privacy}^{k} = A\mathcal{Q}_{privacy}^{k-1}A' + K_k\Delta K_k', \\ & k = 1, 2, ..., T. \end{aligned}$$

It is also a linear programming problem and can be solved efficiently by numerical methods.

B. Perfect Optimal Control Recovery

Similarly, we can also recover the perfect optimal control input for the user in this privacy scheme.

Corollary 1. *Under the localized privacy scheme $\phi_k^{indrt} = \xi_k^{indrt} + \delta_k$ with the recovery of the perfect optimal control, the optimal prior estimate $\hat{x}_{k|k-1}^{opt}$ can be recovered as follows:*

$$\begin{aligned} d_{k|k-1}^{opt} &= (A + BL_{k-1}) d_{k-1|k-1}^{opt}, \\ d_{k|k}^{opt} &= d_{k|k-1}^{opt} + K_k^{pub}\delta_k, \\ \hat{x}_{k|k-1}^{opt} &= \hat{x}_{k|k-1}^{pub} - d_{k|k-1}^{opt}. \end{aligned}$$

Proof. The proof is similar to that of Theorem 5. ■

Corollary 2. *Under the localized privacy scheme $\phi_k^{indrt} = \xi_k^{indrt} + \delta_k$, the perfect optimal control u_k^* can be recovered as follows:*

$$\begin{aligned} d_{k|k-1}^{*} &= (A + BL_{k-1}) d_{k-1|k-1}^{*}, \\ d_{k|k}^{*} &= d_{k|k-1}^{*} + K_k^{pub}\delta_k, \\ u_k^{*} &= u_k^{pub} - L_k d_{k|k}^{*}. \end{aligned}$$

Proof. The proof is similar to that of Theorem 3. ■

The procedures included in Corollary 1 and 2 are presented as follows.

Procedure 2 Recovery of the Optimal Prior Estimate $\hat{x}_{k|k-1}^{opt}$ and the Perfect Optimal Control u_k^*

Initial condition: $d_{0|0}^{opt} = 0$, $d_{0|0}^{*} = 0$.
The server:
1) send $\hat{x}_{k|k-1}^{pub}$, K_k^{pub}, and L_k back to the user after the prior estimation process is completed;
The user:
2) recover the optimal prior estimate based on Corollary 1;
3) calculate the true innovation, add the perturbation, and provide it to the server;
The server:
4) send u_k^{pub} back to the user after the control input calculation is completed;
The user:
5) recover the perfect optimal control input for the user based on Corollary 2.

By Procedure 2, we have $\mathcal{Q}_{Loss} = 0$, since the control input is recovered to the perfect optimal scenario. Accordingly, the privacy performance is given as follows.

Theorem 7. *Under the localized privacy scheme $\phi_k^{indrt} = \xi_k^{indrt} + \delta_k$ with the control recovery method stated in Corollary 2, it holds that*

$$\begin{aligned} \mathcal{Q}_{privacy}^{0} &= 0, \\ \mathcal{Q}_{privacy}^{k} &= (A + BL_{k-1})\mathcal{Q}_{privacy}^{k-1}(A + BL_{k-1})' \\ &\quad + K_k\Delta K_k. \end{aligned} \tag{31}$$

Proof. The proof is similar to that of Theorem 1. ■

V. SIMULATION

We consider a higher-order cooperative system, whose parameters are given as follows:

$$A = \begin{bmatrix} 0.2 & 0.4 & 0.2 \\ 0.1 & 0.3 & 0.2 \\ 0.1 & 0.4 & 0.3 \end{bmatrix}, \quad B = \begin{bmatrix} 2.0 & 0.9 \\ 9.1 & 2.1 \\ 1.3 & 8.1 \end{bmatrix},$$

$$C = \begin{bmatrix} 2.0 & 1.6 & 1.2 \\ 2.0 & 2.0 & 1.1 \end{bmatrix}, \quad R = \begin{bmatrix} 7.0 & 1.8 \\ 1.8 & 0.8 \end{bmatrix},$$

$$Q = \begin{bmatrix} 1.9 & 0.9 & 0.4 \\ 0.9 & 2.8 & 2.0 \\ 0.4 & 2.0 & 2.4 \end{bmatrix}, \quad W = \begin{bmatrix} 1.8 & 2.0 & 0.5 \\ 2.0 & 9.8 & 0.9 \\ 0.5 & 0.9 & 5.4 \end{bmatrix},$$

$$U = \begin{bmatrix} 4.5 & 1.0 \\ 1.0 & 8.8 \end{bmatrix}.$$

We analyze the privacy metric $\mathcal{Q}_{privacy}$ and the performance loss $\mathcal{Q}_{Loss}$ under varying noise covariances Δ within time horizon $T = 3000$, which are presented in Fig. 5 and Fig. 6.

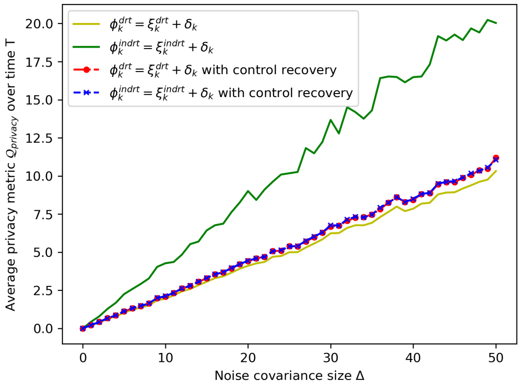

Fig. 5. The impact of different noise covariance Δ on $\mathcal{Q}_{privacy}$.

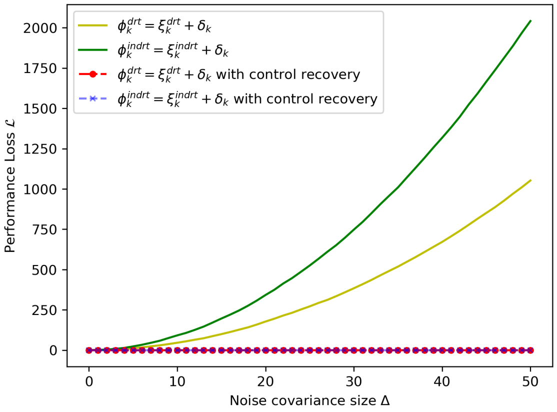

Fig. 6. The impact of different noise covariances Δ on $\mathcal{Q}_{Loss}$.

According to these two figures, we can draw the following conclusions:

1) Without recovering the perfect optimal control u_k^*, the privacy preservation quality $\mathcal{Q}_{privacy}$ and the performance loss $\mathcal{Q}_{Loss}$ are directly proportional. As the privacy preservation quality improves, the performance loss also increases.
2) With recovering the perfect optimal control u_k^*, our scheme ensures the performance loss $\mathcal{Q}_{Loss} = 0$ and provides an acceptable level of privacy preservation.
3) The covariance Δ of the added noise is also directly proportional to the privacy preservation quality $\mathcal{Q}_{privacy}$ and the performance loss $\mathcal{Q}_{Loss}$. Greater covariance of the added noise leads to better privacy preservation quality and greater performance loss.

Conclusions 1) and 2) show that we can add noise arbitrarily, and the larger the noise is, the better the effect of privacy preservation will be, since it always holds that $\mathcal{Q}_{Loss} = 0$.

Comparing these four schemes, we can see that the two schemes of recovering perfect optimal control are the best. They have similar privacy preservation quality and no performance loss. For the two schemes without recovering perfect optimal control, the scheme $\phi_k^{indrt} = \xi_k^{indrt} + \delta_k$ provides better privacy preservation quality but also brings larger performance loss. Which of these two schemes is better depends on how much performance loss the user can accept and how good the privacy preservation quality the user needs.

VI. CONCLUSION

This paper proposes two novel privacy schemes used in a cooperative LQG control system. We evaluate the privacy preservation quality and performance loss of both schemes based on the proposed metrics. We then formulate an optimization problem that considers the trade-off between privacy preservation quality and performance loss. Furthermore, we propose a procedure to recover the perfect optimal control, such that the user's plant has no performance loss in LQG control.

APPENDIX

A. Proof of Theorem 1

From (20), (23), we have

$$\begin{aligned}
\hat{x}_{k|k}^{pub} - \hat{x}_{k|k}^{opt} &= (\hat{x}_{k|k-1}^{pub} + K_k \phi_k^{drt}) \\
&\quad - [\hat{x}_{k|k-1}^{opt} + K_k(y_k - C\hat{x}_{k|k-1}^{opt})] \\
&= [\hat{x}_{k|k-1}^{pub} + K_k(y_k - C\hat{x}_{k|k-1}^{pub} + \delta_k)] \\
&\quad - [\hat{x}_{k|k-1}^{opt} + K_k(y_k - C\hat{x}_{k|k-1}^{opt})] \\
&= (I - K_k C)(\hat{x}_{k|k-1}^{pub} - \hat{x}_{k|k-1}^{opt}) + K_k \delta_k \\
&= (I - K_k C)[(A\hat{x}_{k-1|k-1}^{pub} + Bu_{k-1}^{pub}) \\
&\quad - (A\hat{x}_{k|k-1}^{opt} - Bu_{k-1}^{pub})] + K_k \delta_k \\
&= (I - K_k C)A(\hat{x}_{k-1|k-1}^{pub} - \hat{x}_{k-1|k-1}^{opt}) + K_k \delta_k.
\end{aligned}$$

According to the definition (23), we then calculate

$$
\begin{aligned}
\mathcal{Q}^k_{privacy} =& \boldsymbol{E}[(\hat{x}^{pub}_{k|k} - \hat{x}^{opt}_{k|k})(\hat{x}^{pub}_{k|k} - \hat{x}^{opt}_{k|k})'] \\
=& \boldsymbol{E}\{[(I - K_kC)A(\hat{x}^{pub}_{k-1|k-1} - \hat{x}^{opt}_{k-1|k-1}) + K_k\delta_k] \\
& [(I - K_kC)A(\hat{x}^{pub}_{k-1|k-1} - \hat{x}^{opt}_{k-1|k-1}) + K_k\delta_k]'\} \\
=& (I - K_kC)A\boldsymbol{E}[(\hat{x}^{pub}_{k-1|k-1} - \hat{x}^{opt}_{k-1|k-1})(\hat{x}^{pub}_{k-1|k-1} \\
& -\hat{x}^{opt}_{k-1|k-1})']A'(I - K_kC)' + K_k\boldsymbol{E}[\delta_k\delta_k']K_k' \\
& +(I - K_kC)A\boldsymbol{E}[(\hat{x}^{pub}_{k-1|k-1} - \hat{x}^{opt}_{k-1|k-1})]\boldsymbol{E}[\delta_k']K_k' \\
& +K_k\boldsymbol{E}[\delta_k]\boldsymbol{E}[(\hat{x}^{pub}_{k-1|k-1} - \hat{x}^{opt}_{k-1|k-1})']A'(I - K_kC)' \\
=& (I - K_kC)A\boldsymbol{E}[(\hat{x}^{pub}_{k-1|k-1} - \hat{x}^{opt}_{k-1|k-1})(\hat{x}^{pub}_{k-1|k-1} \\
& -\hat{x}^{opt}_{k-1|k-1})']A'(I - K_kC)' + K_k\boldsymbol{E}[\delta_k\delta_k']K_k' \\
=& (I - K_kC)A\mathcal{Q}^{k-1}_{privacy}A'(I - K_kC)' + K_k\Delta K_k'.
\end{aligned}
$$

The fourth equality holds because the noise δ_k and the state estimate are independent, and $\boldsymbol{E}[\delta_k] = 0$.

B. Proof of Theorem 2

In this scenario, the states are unaccessible. When we calculate the LQG objective $\mathcal{O}_{0:T}$ from backward, the expectation should depend on the information set defined as follows:

$$\mathbb{I}_k = \{y_1, y_2, ..., y_k, u_0, u_1, ..., u_{k-1}\}.$$

First, we have

$$\mathcal{O}_{k:T} = \boldsymbol{E}(x_k'Wx_k + u_k'Uu_k + \mathcal{O}_{k+1:T} \mid \mathbb{I}_k).$$

We calculate the objective in a backward manner.

$$
\begin{aligned}
\mathcal{O}_{T:T} &= \boldsymbol{E}(x_T'Wx_T| \ \mathbb{I}_T). \\
\mathcal{O}_{T-1:T} &= \boldsymbol{E}(x_{T-1}'Wx_{T-1} + u_{T-1}'Uu_{T-1} + \mathcal{O}_{T:T} \mid \mathbb{I}_{T-1}) \\
&= \boldsymbol{E}(x_{T-1}'S_{T-1}x_{T-1} \mid \mathbb{I}_{T-1}) + \mathrm{tr}(S_TQ) \\
&\quad +\mathrm{tr}\big[A'WB(U + B'WB)^{-1}B'WAP_{T-1|T-1}\big] \\
&\quad +\mathrm{tr}\Big[L_{T-1}'(U + B'S_TB)L_{T-1}\mathcal{Q}^{T-1}_{privacy}\Big].
\end{aligned}
$$

Let

$$
\begin{aligned}
r_T &= 0, \\
r_{T-1} &= r_T + \mathrm{tr}(S_TQ), \\
t_T &= 0, \\
t_{T-1} &= t_T + \mathrm{tr}\big[A'WB(U + B'WB)^{-1}B'WAP_{T-1|T-1}\big], \\
\phi_T &= 0, \\
\phi_{T-1} &= \phi_T + \mathrm{tr}\Big[L_{T-1}'(U + B'S_TB)L_{T-1}\mathcal{Q}^{T-1}_{privacy}\Big].
\end{aligned}
$$

Then we have

$$\mathcal{O}_{T-1:T} = \boldsymbol{E}(x_{T-1}'S_{T-1}x_{T-1}| \ \mathbb{I}_{T-1}) + r_{T-1} + t_{T-1} + \phi_{T-1}.$$

Repeating the same reverse iterative calculation, finally we get

$$
\begin{aligned}
\mathcal{O}_{0:T} &= \boldsymbol{E}(x_0'S_0x_0) + r_0 + t_0 + \phi_0 \\
&= \boldsymbol{E}(x_0'S_0x_0) + \sum_{k=0}^{T-1}\mathrm{tr}(S_{k+1}Q) + \sum_{k=0}^{T-1}\mathrm{tr}(\mathit{\Phi}_kP_k) \\
&\quad + \sum_{k=0}^{T-1}\mathrm{tr}\Big(\mathit{\Phi}_k\mathcal{Q}^k_{privacy}\Big).
\end{aligned}
$$

The proof is similar to that of Theorem 3 in the literature [2], and detailed proof can be found.

ACKNOWLEDGEMENT

The work by Wen Yang and Chao Yang is supported by the National Natural Science Foundation of China under Grant 62336005.

REFERENCES

[1] X.-M. Zhang, Q.-L. Han, X. Ge, D. Ding, L. Ding, D. Yue, and C. Peng, "Networked control systems: A survey of trends and techniques," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 1, pp. 1–17, 2019.

[2] C. Yang, W. Yang, and H. Shi, "Privacy preservation by local design in cooperative networked control systems," *arXiv preprint arXiv:2207.03904*, 2022.

[3] A. B. Alexandru, A. Tsiamis, and G. J. Pappas, "Towards private data-driven control," in *2020 IEEE Conference on Decision and Control (CDC)*, 2020, pp. 5449–5456.

[4] C. Dwork, "Differential privacy," in *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP), Part II*, Venice, Italy, July 2006, pp. 1–12.

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

[6] Y. Lu and M. Zhu, "A control-theoretic perspective on cyber-physical privacy: Where data privacy meets dynamic systems," *Annual Reviews in Control*, vol. 47, pp. 423–440, 2019.

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

[8] X. Cao and T. Başar, "Differentially private parameter estimation: Optimal noise insertion and data owner selection," in *2020 IEEE Conference on Decision and Control (CDC)*, 2020, pp. 2887–2893.

[9] L. Wang, I. R. Manchester, J. Trumpf, and G. Shi, "Initial-value privacy of linear dynamical systems," in *2020 IEEE Conference on Decision and Control (CDC)*, 2020, pp. 3108–3113.

[10] C. Hawkins and M. Hale, "Differentially private formation control," in *2020 IEEE Conference on Decision and Control (CDC)*, 2020, pp. 6260–6265.

[11] H. Zhang, Y. Shu, P. Cheng, and J. Chen, "Privacy and performance trade-off in cyber-physical systems," *IEEE Network*, vol. 30, no. 2, pp. 62–66, 2016.

[12] T. Tanaka, M. Skoglund, H. Sandberg, and K. H. Johansson, "Directed information and privacy loss in cloud-based control," in *2017 American control conference (ACC)*. IEEE, 2017, pp. 1666–1672.

[13] E. Ferrari, Y. Tian, C. Sun, Z. Li, and C. Wang, "Privacy-preserving design of scalar lqg control," *Entropy*, vol. 24, no. 7, p. 856, 2022.

[14] J. Kim, C. Lee, H. Shim, J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Encrypting controller using fully homomorphic encryption for security of cyber-physical systems," *IFAC-PapersOnLine*, vol. 49, no. 22, pp. 175–180, 2016.

[15] Y. Shoukry, K. Gatsis, A. Alanwar, G. J. Pappas, S. A. Seshia, M. Srivastava, and P. Tabuada, "Privacy-aware quadratic optimization using partially homomorphic encryption," in *2016 IEEE Conference on Decision and Control (CDC)*, 2016, pp. 5053–5058.

[16] A. B. Alexandru and G. J. Pappas, "Encrypted lqg using labeled homomorphic encryption," in *Proceedings of the 10th ACM/IEEE international conference on cyber-physical systems*, 2019, pp. 129–140.

[17] M. S. Darup, A. Redder, and D. E. Quevedo, "Encrypted cooperative control based on structured feedback," *IEEE control systems letters*, vol. 3, no. 1, pp. 37–42, 2018.

[18] I. Lourenço, R. Mattila, C. R. Rojas, and B. Wahlberg, "How to protect your privacy? a framework for counter-adversarial decision making," in *2020 IEEE Conference on Decision and Control (CDC)*, 2020, pp. 1785–1791.

[19] 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, 2017.

[20] 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, 2016.