This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2021.3077868, IEEE Transactions on Automatic Control

Optimal Privacy-aware Estimation

Ehsan Nekouei, Henrik Sandberg, Mikael Skoglund and Karl H. Johansson

***Abstract*—This paper studies the design of an optimal privacy-aware estimator of a public random variable based on noisy measurements which contain private information. The public variable carries also non-private information, but, its estimate will be correlated with the private information due to the estimation process. The objective is to design an optimal estimator of the public random variable such that the leakage of private information, via the estimation process, is kept below a certain level. The privacy metric is defined as the discrete conditional entropy of the private variable given the output of the estimator. We show that the optimal privacy-aware estimator is the solution of a (possibly infinite-dimensional) convex optimization problem when the estimator has access to either the measurement or the measurement together with the private information. We study the optimal perfect-privacy estimation problem that ensures the estimate of the public variable is independent of the private information. A necessary and sufficient condition is derived guaranteeing that an estimator satisfies the perfect-privacy requirement. It is shown that the optimal perfect-privacy estimator is the solution of a linear optimization problem. A sufficient condition for its existence is derived. The impact of the distribution mismatch on the perfect-privacy condition is studied. Numerical examples are used to illustrate the privacy-accuracy trade-off.**

I. Introduction

A. Motivation

Networked systems play major roles in our society by providing critical services for smart buildings, intelligent transportations and smart grids. The operation of networked systems relies on *estimation* wherein the values of variables are computed based on noisy measurements collected by sensors. In certain applications, sensor measurements contain private information, *e.g.,* the occupancy level of a building which can be inferred from temperature measurements [1]. Since an estimator operates on measurements, its output may be an informative source for inferring private information. For example, the occupancy level of a building can be inferred from temperature estimates.

Due to the distributed structure of networked systems, the output of an estimator is usually shared with untrusted parties, *e.g.,* a cloud-based controller for temperature regulation in a smart building application. Hence, it is important to design privacy-aware estimators which provide accurate estimates of desired variables and simultaneously ensure that the output of the estimator is not a reliable source of information for estimating private data. We refer to the untrusted party with access to the output of an estimator as the "user". The framework developed in this paper is motivated by the growing number of applications in which the service providers want to guarantee that untrusted users do not get access to private information.

E. Nekouei is with the Department of Electrical Engineering, City University of Hong Kong, Kowloon Tong, Hong Kong. enekouei@cityu.edu.hk. H. Sandberg, M. Skoglund and K. H. Johansson are with the School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Stockholm, Sweden. {hsan,skoglund, kallej}@kth.se. This work is supported by the Knut and Alice Wallenberg Foundation, the Swedish Foundation for Strategic Research and the Swedish Research Council.

B. Contributions

We consider an estimation problem wherein measurements contain noisy information about a private random variable and a public random variable. The estimate of the public variable is revealed to an untrusted user. In our set-up, the measurement is modeled as a continuous random variable. The objective is to design an optimal randomized estimator of the public random variable subject to a constraint on the privacy level of the private random variable. The notion of conditional discrete entropy is used to quantify the leakage of private information due to the estimation procedure. This privacy metric captures the uncertainty an untrusted user has about the private random variable after observing the estimate of the public random variable.

We study the optimal privacy-aware estimation problem when the estimator has access to either the discretized measurement or the discretized measurement together with the private random variable. It is shown that the optimal privacy-aware estimator is the solution to a convex optimization problem. Necessary and sufficient optimality conditions are derived. We also consider the optimal perfect-privacy estimation problem which ensures that the output of the estimator is independent of the private information. A necessary and sufficient condition for an estimator to achieve perfect-privacy is derived. It is shown that the optimal perfect-privacy estimator is the solution of a linear optimization problem. The feasible set of this optimization problem is non-empty if the dimension of the null space of a certain matrix is non-zero. The impact of the distribution mismatch on the perfect-privacy condition is studied.

Finally, these results are extended to the case that the estimator has access to the continuous measurement or both the continuous measurement and private information. Our results indicate that the optimal privacy-aware (perfect-privacy) estimation problem is an infinite-dimensional convex (linear) optimization problem in this case.

C. Related Work

The privacy aspect of hypothesis testing problems with a private and a public hypothesis has been studied in the literature, and various privacy-preserving solutions for improving the privacy level of hypothesis testing problems have been proposed, *e.g.,* [2], [3], [4], [5]. In [6], the authors considered a hypothesis test problem with multiple sensors in which

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2021.3077868, IEEE Transactions on Automatic Control

an eavesdropper intercepts the local decisions of a subset of sensors. They studied the optimal decision rule minimizing the Bayes risk at a fusion center subject to a privacy constraint at the eavesdropper. In [7], the authors considered a similar set-up to that of [6] and studied the optimal privacy-aware Neyman-Pearson test with a private hypothesis. The privacy of electricity consumers against an eavesdropper using demand management techniques and storage devices was studied in [8].

Privacy preserving filters, for the state privacy problem in a cloud-based control application, were studied in [9] using the notion of directed information as the privacy metric. A privacy-aware controller design problem for a private Markov decision process problem in presence of an eavesdropper, with access to the input and output of the process, was studied in [10]. The authors of [11] studied the privacy filter design problem for a public Markov chain, correlated with a private Markov chain, when both the private and public chains are directly observable. The interested reader is referred to [12] for an overview of information-theoretic approaches to privacy in estimation and control.

The notion of differential privacy has been used to study privacy-aware estimation, filtering and average consensus problems. The authors of [13] proposed a filtering scheme for preserving the privacy of states or measurements of dynamical systems using the notion of differential privacy. The state estimation problem in a distribution power network subject to differential privacy constraints for the consumers was studied in [14]. The authors of [15] considered a distributed multi-agent control problem and proposed a differential privacy scheme for preserving the privacy of the initial state as well as the preferred target way-points of each agent. Privacy-aware average consensus algorithms, for preserving the privacy of initial states of different agents, have been proposed in [16] and [17].

The authors in [18] studied the optimal trade-off between the privacy and performance in a database privacy problem using rate-distortion theory. Akyol, *et. al.* in [19] considered a strategic information transmission set-up wherein a transmitter communicates private information with a receiver over a noisy channel. They proposed game-theoretic frameworks for the encode-decoder design problem such that the distortion is minimized while a certain privacy level is ensured.

Information-theoretic methods for improving data privacy have been extensively investigated in the literature, *e.g.,* [20], [21], [22], [23] and references therein. In this line of research, the objective is to design privacy preserving filters which operate on a (directly observable) public random variable correlated with a private random variable. The privacy filter is designed such that the distortion between the public variable and its processed version is minimized while a certain level of privacy is guaranteed. The current manuscript is different from this line of research in that, in our set up, neither the public nor the private variables are directly observable, and the sensor observations contain noisy information about the public and private variables. Moreover, in an estimation problem, one is interested in the true value of a variable based on a noisy observation rather than obtaining a low distortion representation of a directly observable random variable.

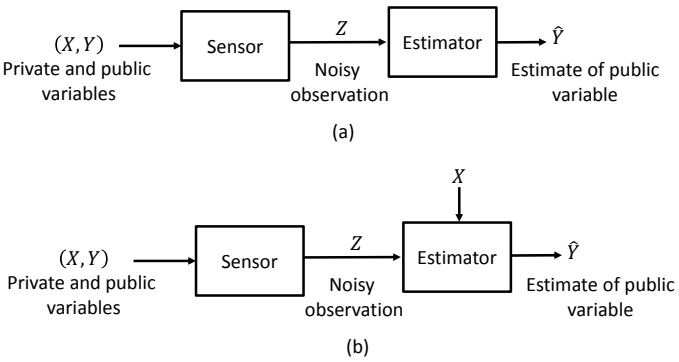


Fig. 1. An estimator of the public random variable Y based on the measurement Z (a), an estimator of the public random variable Y based on the measurement Z and the private random variable X (b).

In [24], the authors considered the problem of adding stochastic distortion to a public variable, which depends on private information, such that (i) the mean square error (MSE) of recovering the original variable from its distorted version is minimized, and (ii) the minimum MSE of recovering the private information from the distorted variable stays above a certain level. The results were extended in [25] under the Hamming distance as the distortion criterion and the efficiency of these methods was analysed in [26].

Perfect-privacy filters in the context of data privacy have been studied in [27]. These results are mainly derived based on the assumption that the public random variable is directly observable and takes finite values. Also, the perfect-privacy condition in [27] requires characterization of the extreme points of a certain convex polytope which depends on the null space of a probability transition matrix. Finally, we note that the relation between the perfect-privacy condition and the notion of maximal correlation has been studied in [28].

Different from the existing work, we consider the estimation of a public random variable, *i.e.,* the sensor does not have direct access to the public random variable. Different from [27], in our work, the optimal perfect-privacy estimator with discretized measurement is obtained by solving a linear optimization problem which does not require finding the extreme points of a convex polytope. In our set-up, the perfect-privacy condition with discretized measurements depends on the null space of a matrix with positive and negative entries which is different from a transition probability matrix. We also study the impact of distribution mismatch on the perfect-privacy condition. The optimal privacy-aware estimation and the optimal perfect-privacy estimation problems are studied, in our work, when the estimator has access to either (possibly continuous) measurement or to both the measurement and private information.

D. Outline of The Paper

The rest of this paper is organized as follows. Our system model and assumptions are described in the next section. Section III presents our results on the optimal privacy-aware

and optimal perfect-privacy estimator design problems when the estimator has access to the discretized measurement. These results are extended to the case with the continuous measurement in Section IV. Our numerical results are presented in Section V, followed by concluding remarks in Section VI.

II. System Model

Consider the estimation problem in Fig. 1 wherein the measurement Z contains noisy information about two, possibly correlated, discrete random variables X and Y. The objective is to estimate Y using either Z or (Z, X). The random variable Y contains *public* information, *i.e.,* its estimate is used by possibly untrusted parties for monitoring or control purposes. The random variable X carries *private* information which should be kept hidden from any untrusted party. Then, the privacy-aware estimation problem can be stated as follows: Find a *reliable* estimate of Y such that the output of the estimator satisfies a certain *privacy* level for X. Note that the estimate of Y is generally correlated with X, thus the estimation process might result in the leakage of private information. Please see Subsection II-D for motivating examples of this estimation problem.

The following notation and assumptions are adopted in the rest of this paper. The support sets of X, Y and Z are denoted by $\mathcal{X} = \{x_1, \dots, x_n\}$, $\mathcal{Y} = \{y_1, \dots, y_m\}$ and $\mathcal{Z} = \mathbb{R}$, respectively. The relation between Z and X, Y can be of the general form $Z = f(X, Y, W)$ where $f(\cdot)$ is a continuous map from $\mathbb{R}^3$ to $\mathbb{R}$, and $W \in \mathbb{R}$ denotes the measurement noise. We assume that the knowledge of the joint distribution of (X, Y, Z) is available at the estimator. It is assumed that the random variable Z is absolutely continuous with respect to the Lebesgue measure on $\mathbb{R}$ with the probability density function $p_Z(z)$. In Section III, we discuss the privacy-aware estimator design problem when the estimator has access to a discretized version of Z. In Section IV, we study the privacy-aware estimation when the estimator has access to the continuous measurement Z.

A. Randomized Estimator Based on Discretized Measurements

In this subsection, the randomized estimation of Y is discussed when the estimator has access to the discretized measurement. To this end, let $\{B_i\}_{i=1}^N$ denote a partition of $\mathbb{R}$ where B_1 and B_N are semi-infinite intervals and where B_i, $2 \leq i \leq N-1$, are of the form $B_i = [a_{i-1}, a_i)$, $a_i > a_{i-1}$. Here, B_i denotes the ith quantization cell, and $a_i, a_{i-1} \in \mathbb{R}$ denote its boundaries. Let $Z_{\rm d}$ denote the discretized version of Z using $\{B_i\}_{i=1}^N$, *i.e.,* $Z_{\rm d}$ is a random variable taking values in $\{1, \dots, N\}$ with $Z_{\rm d} = l$ if Z belongs to B_l. A randomized estimator of Y based on $Z_{\rm d}$ can be defined as

$$\hat{Y}_P(Z_{\rm d}) = \begin{cases} y_1 & \text{w.p.} \quad P_{1l} \\ \vdots & \qquad\qquad \text{if} \quad Z_{\rm d} = l, \\ y_m & \text{w.p.} \quad P_{ml} \end{cases}$$

where w.p. stands for "with probability". Thus, the estimator selects y_i as its output with probability P_{il} when $Z_{\rm d} = l$. Note that an estimator is specified by the randomization probabilities $\{P_{il}\}_{il}$, where $\sum_i P_{il} = 1$ for all l. In the next section, privacy-aware and perfect-privacy estimators are designed by optimizing these randomization probabilities.

In certain applications, the estimator may have access to both $Z_{\rm d}$ and X, see Subsection II-D for more details. In this case, the randomization probabilities are parametrized by the values of $Z_{\rm d}$ and X. A randomized estimator of Y based on $(Z_{\rm d}, X)$ is defined as

$$\hat{Y}_P(Z_{\rm d}, X) = \begin{cases} y_1 & \text{w.p.} \quad P_{1lj} \\ \vdots & \qquad\qquad \text{if} \quad Z_{\rm d} = l, X = x_j \\ y_m & \text{w.p.} \quad P_{mlj} \end{cases}$$

with $\sum_i P_{ilj} = 1$ for all l, j. That is, the estimator selects y_i as its output with probability P_{ilj} given $Z_{\rm d} = l$ and $X = x_j$.

B. Randomized Estimator Based on Continuous Measurements

In this subsection, the structure of a randomized estimator of Y based on the original continuous Z is described. To this end, let $P(z) = \{P_i(z)\}_{i=1}^m$ denote a set of positive functions where $P_i(z)$ is defined on the support set of $\mathcal{Z}$ with $\sum_{i=1}^m P_i(z) = 1$ for all $z \in \mathcal{Z}$. Then, a randomized estimator of Y based on Z can be expressed as

$$\hat{Y}_P(Z) = \begin{cases} y_1 & \text{w.p.} \quad P_1(z) \\ \vdots & \qquad\qquad \text{if} \quad Z = z. \\ y_m & \text{w.p.} \quad P_m(z) \end{cases}$$

According to (1), if the observation Z is equal to z, the estimator declares y_i as the estimate of Y with probability $P_i(z)$.

Similarly, a randomized estimator of Y based on (Z, X) is defined as

$$\hat{Y}_P(Z, X) = \begin{cases} y_1 & \text{w.p.} \quad P_{1j}(z) \\ \vdots & \qquad\qquad \text{if} \quad Z = z, X = x_j, \\ y_m & \text{w.p.} \quad P_{mj}(z) \end{cases}$$

where $\sum_{i=1}^m P_{ij}(z) = 1$ for all $z \in \mathcal{Z}$ and j. In this case, the estimator is specified by the set of positive functions $\{P_{ij}(z)\}_{ij}$.

Remark 1: In real applications, the optimal estimator can be implemented using a random number generator that randomly selects an element of $\mathcal{Y}$ according to the optimal randomization probabilities. A random number generator can be realized via either a dedicated hardware, *e.g.,* linear feedback shift registers, or software executed by generic programmable hardware.

C. Privacy Metric

Since the output of the estimator is usually correlated with X, revealing $\hat{Y}_P$ to the user may result in a privacy loss, *i.e.,* the user can infer about X by observing $\hat{Y}_P$. The privacy level of a generic estimator $\hat{Y}_P$ is defined as the conditional discrete entropy of X given the output of the estimator, denoted by

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2021.3077868, IEEE Transactions on Automatic Control

$\mathsf{H}\left[X\left|\hat{Y}_P\right.\right]$, see (1) for the definition of the privacy level of an estimator with access to $Z_{\rm d}$.

$$\mathsf{H}\left[X\left|\hat{Y}_P\left(Z_{\rm d}\right)\right.\right] = -\sum_{y\in\mathcal{Y}}\mathsf{Pr}\left(\hat{Y}_P\left(Z_{\rm d}\right)=y\right) \times \sum_{x\in\mathcal{X}}\mathsf{Pr}\left(X=x|\hat{Y}_P\left(Z_{\rm d}\right)=y\right)\log\mathsf{Pr}\left(X=x|\hat{Y}_P\left(Z_{\rm d}\right)=y\right). \tag{1}$$

Our choice of privacy metric is motivated by the fact that $\mathsf{H}\left[X\left|\hat{Y}_P\right.\right]$ captures the ambiguity of the user about X after observing $\hat{Y}_P$. Thus, the privacy loss decreases as $\mathsf{H}\left[X\left|\hat{Y}_P\right.\right]$ becomes large since the user becomes more uncertain about the value of X as $\mathsf{H}\left[X\left|\hat{Y}_P\right.\right]$ increases.

Since conditioning reduces entropy [29], we have

$$0 \leq \mathsf{H}\left[X\left|\hat{Y}_P\right.\right] \leq \mathsf{H}\left[X\right],$$

which implies that the maximum privacy is achieved if $\mathsf{H}\left[X\left|\hat{Y}_P\right.\right] = \mathsf{H}\left[X\right]$. Recall that if X and $\hat{Y}_P$ are independent, $\hat{Y}_P$ contains no information about X and the user has maximum ambiguity about X after observing $\hat{Y}_P$, *i.e.,* in this case $\mathsf{H}\left[X\left|\hat{Y}_P\right.\right] = \mathsf{H}\left[X\right]$.

Another motivation for the choice of the privacy metric in this paper is the fact that the error probability of estimating X after observing $\hat{Y}_P$ can be lower bounded in terms of $\mathsf{H}\left[X\left|\hat{Y}_P\right.\right]$ using Fano's inequality [29]:

$$\mathsf{Pr}\left(X\neq\hat{X}\left(\hat{Y}_P\right)\right) \geq \frac{\mathsf{H}\left[X\left|\hat{Y}_P\right.\right]-1}{\log|\mathcal{X}|},$$

where $\hat{X}\left(\hat{Y}_P\right)$ is an arbitrary estimator of X with access to $\hat{Y}_P$ and $|\mathcal{X}|$ is the cardinality of the support set of X. Note that this lower bound is independent of the estimator of X, *i.e.,* it holds for all possible estimators. Thus, by adjusting the value of $\mathsf{H}\left[X\left|\hat{Y}_P\right.\right]$, a desired privacy level of the private random variable can be guaranteed as long as $|\mathcal{X}|>2$.

Remark 2: In this paper, we assume that the sensor and the estimator are co-located. Thus, the adversary can only observe the output of the estimator and does not have access to the sensor measurements. In certain applications, sensor measurements are transmitted over a communication network to a remote estimator. In such applications, an adversary may attempt to infer the private information by overhearing the communication between the sensor and the estimator. This issue can be avoided by securing the information exchange between the sensor and the estimator using information security techniques such as secure multi-party computation or cryptographic techniques.

D. Motivating Examples

In this subsection, we provide three motivating examples of privacy-aware estimation problems.

1) Temperature Estimation: Consider a building application in which the objective is to estimate the temperature level inside an apartment based on noisy sensor measurements. Here, the binary random variable X represents the absence or presence of the tenant which is considered as private information and Y represents the temperature. We assume that when the tenant is present, the temperature is kept at the set temperature T_s by the heating ventilation and air-conditioning (HVAC) system. When the tenant is away, we assume that the HVAC system is off and the temperature is modeled using a random variable distributed between the minimum temperature $T_{\min}$ and the maximum temperature $T_{\max}$. Let the events $X=0$ and $X=1$ denote the absence and presence of the tenant, respectively. Then, the random variable Y can be expressed as

$$Y = \begin{cases} T_s & \text{if} \quad X=1 \\ T & \text{if} \quad X=0, \end{cases}$$

where T is a random variable distributed over $[T_{\min}, T_{\max}]$.

The objective is to provide an accurate estimate of temperature based on the noisy temperature measurement Z, for an untrusted user, *e.g.,* a cloud-based building automation system, while the dependency of the estimator's output on X is kept below a certain level. Note that it is possible to infer the occupancy information in a building using measurements of WiFi signal power see [30]. Hence, if this information is available at the estimator, the temperature can be estimated using (Z,X) which is a richer information set compared with Z.

2) Smart Meter Application: Consider a smart meter application wherein the objective is to estimate the number of active smart appliances in a household based on its electricity consumption level. In this application, the absence/presence of tenants can be modeled using the binary random variable X, which contains private information, Y represents the number of active smart appliances and Z represents the electricity consumption level. An estimate $\hat{Y}$ is provided to an untrusted party such as a utility company. The objective is to design an estimator of Y such that the leakage of the private information, after $\hat{Y}$ is revealed to the untrusted party, is kept below a certain level.

3) Vehicle Density Estimation: Consider the problem of counting vehicles on a road based on position estimates of individual vehicles. In this application, X represents the velocity of a vehicle, which is considered as its private information, Y represents the actual position of the vehicle and Z denotes the noisy measurement of the position of the vehicle. The position estimates can be used by a traffic operator, *i.e.,* an untrusted party, to estimate the number of vehicles on the road at a given time. In this application, the objective is to design an estimator of Y based on Z for individual vehicles such that leakage information about each vehicle's velocity, after revealing its corresponding position estimate $\hat{Y}$ to the traffic operator, is kept below a certain level.

III. Optimal Estimation Using Discretized Measurements

In this section, the optimal privacy-aware and the optimal perfect-privacy estimation problems are studied when the estimator has access to either to $Z_{\rm d}$ or $(Z_{\rm d},X)$. We start our

discussion by introducing the optimal privacy-aware estimator design problem when only $Z_{\rm d}$ is available at the estimator.

A. Optimal Privacy-aware Estimation Using $Z_{\rm d}$

In this subsection, we assume that the estimator has access to the discretized measurement $Z_{\rm d}$. Let $L\left(Y,\hat{Y}_P\left(Z_{\rm d}\right)\right)$ denote the estimation loss which penalizes the deviation of the estimator's output from the true value of Y. Then, the optimal privacy-aware estimator is obtained by minimizing the average estimation loss subject to a lower bound on the privacy of X given the output of the estimator. That is, the optimal privacy-aware estimator is the solution of the following optimization problem

$$\begin{aligned}\underset{\{P_{il}\}_{i,l}}{\text{minimize}}\quad & \mathsf{E}\left[L\left(Y,\hat{Y}_P\left(Z_{\rm d}\right)\right)\right]\\ & P_{il}\geq 0,\forall i,l\\ & \sum_i P_{il}=1,\forall l\\ & \mathsf{H}\left[X\left|\hat{Y}_P\left(Z_{\rm d}\right)\right.\right]\geq \mathsf{H}_0,\end{aligned}\tag{2}$$

where $\mathsf{H}_0\in\mathbb{R}_+$ is a design parameter. Note that the privacy level of the optimal estimator increases as H_0 becomes large. Note that by removing the privacy constraint from the optimization problem above, its feasible set becomes the set of all possible estimators. Thus, the solution of the optimization problem (2) without the privacy constraint will be a classical optimal estimator which may not respect the privacy constraint. By imposing the privacy constraint, we limit the feasible set of the optimization problem to the set of estimators with the privacy level at least H_0, and search for the optimal estimator within this set.

The next theorem shows that the optimal privacy-aware estimator with access to the discretized measurement is the solution of a convex optimization problem.

Theorem 1: The optimal privacy-aware estimator design problem (2) is a convex optimization problem.

Proof: Theorem 1 is a special case of Theorem 3 and its proof is skipped to avoid repetition. ∎

The next lemma states the Karush–Kuhn–Tucker (KKT) necessary and sufficient optimality conditions for the optimization problem (2).

Lemma 1: Let $\boldsymbol{P}^\star$ denote the optimal solution of the optimization problem (2). Then, condition (3) holds where $\mu^\star$ is the dual optimal variable associated with the privacy constraint and $\boldsymbol{\lambda}^\star$ is the vector of dual optimal variables associated with the equality constraints of (2).

Proof: See Appendix A. ∎

B. Optimal Perfect-privacy Estimation Using $Z_{\rm d}$

In this subsection, the design of the optimal perfect-privacy estimator is discussed. To this end, we first define the perfect-privacy condition, and derive a necessary and sufficient condition for an estimator to satisfy the perfect-privacy requirement. Then, we show that the optimal perfect-privacy estimator can be obtained by solving a linear optimization problem.

The next definition states the perfect-privacy condition.

Definition 1: An estimator of the public random variable Y is perfectly private if its output $\hat{Y}$ is independent of the private random variable X.

Before proceeding with the derivation of the perfect-privacy condition, we first define the matrix

$$\Phi=\begin{bmatrix}\phi_{11} & \cdots & \phi_{1N}\\ \vdots & & \vdots\\ \phi_{n1} & \cdots & \phi_{nN}\end{bmatrix},$$

where $\phi_{jl}=\mathsf{Pr}\left(Z\in B_l\middle|\,X=x_j\right)-\mathsf{Pr}\left(Z\in B_l\right)$. Also, the vector $\boldsymbol{P}_i$ is defined as

$$\boldsymbol{P}_i=\begin{bmatrix}P_{i1}\\ \vdots\\ P_{iN}\end{bmatrix},$$

which is the collection of randomization probabilities associated with selecting y_i as the output of the estimator, for different bins. Next lemma derives a necessary and sufficient condition which ensures perfect-privacy.

Lemma 2: An estimator satisfies the perfect-privacy condition if and only if $\boldsymbol{P}_i\in\mathsf{Null}\left(\Phi\right)$ for all $i\in\{1,\ldots,m\}$ where $\mathsf{Null}\left(\Phi\right)$ is the null space of the matrix Φ.

Proof: See Appendix B. ∎

According to this lemma, a randomized estimator satisfies the perfect-privacy condition if the vector of randomization probabilities associated with each element of $\mathcal{Y}$, *i.e.,* the support set of the public random variable, lies in the null space of the matrix Φ. Note that the perfect-privacy requirement is (in general) stricter than the privacy constraint in (2) and coincides with this privacy constraint for $\mathsf{H}_0=\mathsf{H}\left[X\right]$. Hence, the set of estimators which satisfy the perfect-privacy condition is a subset of the set of privacy-aware estimators. The set of perfect-privacy estimators is a convex ploytope.

We note that some other perfect-privacy conditions have already appeared in the literature [27], [31]. For example, the perfect-privacy conditions in [27] require that the dimension of the null space of certain transition probability matrices to be non-zero. The perfect-privacy condition in our set-up requires that the randomization probability vectors $\boldsymbol{P}_i$ lie in the null space of Φ, which is not a transition probability matrix.

We next study the optimal perfect-privacy estimator design problem, *i.e.,* the optimal estimator among all the estimators satisfying the perfect-privacy condition. The optimal perfect-privacy estimator is given by the solution of the following optimization problem

$$\begin{aligned}\underset{\{P_{il}\}_{i,l}}{\text{minimize}}\quad & \mathsf{E}\left[L\left(Y,\hat{Y}_P\left(Z_{\rm d}\right)\right)\right]\\ & P_{il}\geq 0,\forall i,l\\ & \sum_i P_{il}=1,\quad\forall l\\ & \Phi\boldsymbol{P}_i=\boldsymbol{0},\forall i.\end{aligned}\tag{4}$$

Note that the perfect-privacy condition in (4) is linear in the decision variables, *i.e.,* the randomization probabilities. Thus, an important feature of the optimal perfect-privacy estimator

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2021.3077868, IEEE Transactions on Automatic Control

$$\mu^\star \log \prod_j \left(\frac{\sum_l P^\star_{hl} \mathsf{Pr}\left(Z \in B_l | X = x_j\right)}{\sum_l P^\star_{hl} \mathsf{Pr}\left(Z \in B_l\right)} \right)^{\mathsf{Pr}(Z \in B_k, X = x_j)} \begin{cases} = \mathsf{Pr}\left(Z \in B_k | Y = y_h\right) \mathsf{Pr}\left(Y = y_h\right) + \lambda^\star_k & \text{if} \quad 0 < P^\star_{hk} < 1 \\ \leq \mathsf{Pr}\left(Z \in B_k | Y = y_h\right) \mathsf{Pr}\left(Y = y_h\right) + \lambda^\star_k & \text{if} \quad P^\star_{hk} = 0 \\ \geq \mathsf{Pr}\left(Z \in B_k | Y = y_h\right) \mathsf{Pr}\left(Y = y_h\right) + \lambda^\star_k & \text{if} \quad P^\star_{hk} = 1 \end{cases}$$

$$\sum_h P^\star_{hl} = 1 \forall l$$

$$\mu^\star \geq 0$$

$$\mathsf{H}\left[X \left| \hat{Y}_{\boldsymbol{P}^\star}\left(Z\right)\right.\right] \geq \mathsf{H}_0$$

$$\mu^\star \left(\mathsf{H}_0 - \mathsf{H}\left[X \left| \hat{Y}_{\boldsymbol{P}^\star}\left(Z\right)\right.\right] \right) = 0 \tag{3}$$

is that it can be obtained by solving a linear optimization problem. Note that the optimal perfect-privacy estimator can be computed by solving optimization problem (2) for $\mathsf{H}_0 = \mathsf{H}[X]$. However, the privacy constraint in (2) is non-linear and finding the optimal perfect-privacy estimator using (2) is more challenging than solving a linear program, especially in high dimensional problems. From a practical point of view, a perfect-privacy estimator provides the highest level of statistical privacy by ensuring that its output is statistically independent of the private variable, *i.e.,* the output of the estimator does not contain any private information.

We next derive a sufficient condition which ensures that the feasible set of the optimization problem (4) is non-empty.

Lemma 3: If the number of discretization bins, *i.e.,* N, is larger than the size of the support set of the private random variable X, then the feasible set of (4) is non-empty.

Proof: See Appendix C. ∎

The solution of the optimal perfect-privacy estimator design problem depends on the joint distribution of X, Y and Z_d which is typically estimated from data. Thus, there might be a mismatch between the estimated and the true distributions. We next study the impact of such distribution mismatch on the perfect-privacy condition. To this end, we use Θ to denote the collection of random variables $\Theta = (X, Y, Z_\mathrm{d})$ and $p_\Theta\left(\theta\right)$ to denote the *true* distribution of Θ. Let $p_{\hat{\Theta}}\left(\cdot\right)$ denote the estimate of $p_\Theta\left(\cdot\right)$ from data. Hence, the perfect-privacy estimator is designed according to $p_{\hat{\Theta}}(\theta)$ which might be different from the true distribution. Let $\hat{Y}_{\hat{\Theta}}\left(Z_\mathrm{d}\right)$ denote the optimal perfect-privacy estimate derived using $p_{\hat{\Theta}}\left(\theta\right)$.

Next theorem derives an upper bound on the mutual information between private information and the output of the perfect-privacy estimator under distribution mismatch. Before presenting this result, we define the vectors $\boldsymbol{\epsilon} = \left[\epsilon_1, \ldots, \epsilon_N\right]^\top$ and $\boldsymbol{\epsilon}_j = \left[\epsilon_{1j}, \ldots, \epsilon_{Nj}\right]^\top$, $j = 1, \ldots, m$, where

$$\epsilon_l = \mathsf{Pr}_\Theta\left(Z \in B_l\right) - \mathsf{Pr}_{\hat{\Theta}}\left(Z \in B_l\right),$$
$$\epsilon_{lj} = \mathsf{Pr}_\Theta\left(Z \in B_l | X = x_j\right) - \mathsf{Pr}_{\hat{\Theta}}\left(Z \in B_l | X = x_j\right),$$

and $\mathsf{Pr}_\Theta\left(A\right)$ and $\mathsf{Pr}_{\hat{\Theta}}\left(A\right)$ denote the probability of the event A calculated using $p_\Theta\left(\theta\right)$ and $p_{\hat{\Theta}}\left(\theta\right)$, respectively. Also, $\Delta_{i\hat{\Theta}}$ and $\Delta_{ij\hat{\Theta}}$ are defined as

$$\Delta_{i\hat{\Theta}} = \sum_l P^\star_{il\hat{\Theta}} \mathsf{Pr}_{\hat{\Theta}}\left(Z \in B_l\right),$$
$$\Delta_{ij\hat{\Theta}} = \sum_l P^\star_{il\hat{\Theta}} \mathsf{Pr}_{\hat{\Theta}}\left(Z \in B_l | X = x_j\right),$$

where $P^\star_{il\hat{\Theta}}$ is the probability that the optimal perfect-privacy estimator, designed using $p_{\hat{\Theta}}\left(\theta\right)$, selects y_i as its output when the measurement belongs to bin l.

Theorem 2: Consider the optimal perfect-privacy estimator designed using $p_{\hat{\Theta}}\left(\theta\right)$. Let $\hat{Y}_{\hat{\Theta}}\left(Z_\mathrm{d}\right)$ denote the output of this estimator. Assume that $\left\|\boldsymbol{\epsilon}\right\|_1 < \min_i \Delta_{i\hat{\Theta}}$ and $\left\|\boldsymbol{\epsilon}_j\right\|_1 < \min_i \Delta_{ij\hat{\Theta}}$ where $\left\|\cdot\right\|_1$ denotes the one-norm. Then, we have

$$\mathsf{I}\left[X; \hat{Y}_{\hat{\Theta}}\left(Z_\mathrm{d}\right)\right] \leq \sum_j \mathsf{Pr}\left(X = x_j\right) \sum_i \left(\Delta_{ij\hat{\Theta}} + \left\|\boldsymbol{\epsilon}_j\right\|_1\right)\left(\gamma_{ij} + \gamma_i\right),$$

where $\mathsf{I}\left[\cdot;\cdot\right]$ denotes the Shannon mutual-information and

$$\gamma_i = \frac{\left\|\boldsymbol{\epsilon}\right\|_1}{\Delta_{i\hat{\Theta}} - \left\|\boldsymbol{\epsilon}\right\|_1},$$
$$\gamma_{ij} = \frac{\left\|\boldsymbol{\epsilon}_j\right\|_1}{\Delta_{ij\hat{\Theta}} - \left\|\boldsymbol{\epsilon}_j\right\|_1}.$$

Proof: See Appendix D. ∎

Theorem 2 establishes an upper bound on the mutual information between the private random variable and the output of the optimal perfect-privacy estimator under distribution mismatch. According to this theorem, the upper bound on the mutual information is controlled by the norm of the error vectors $\boldsymbol{\epsilon}$ and $\boldsymbol{\epsilon}_j$ which capture the mismatch between the true and the estimated distributions. Thus, the leakage of private information under the perfect-privacy estimator, designed according to $p_{\hat{\Theta}}\left(\theta\right)$, will be negligible when $\max\left(\left\|\boldsymbol{\epsilon}\right\|_1, \max_j \left\|\boldsymbol{\epsilon}_j\right\|_1\right)$ is small and the estimator becomes almost perfectly-private.

C. Optimal Privacy-aware Estimation Using (Z_d, X)

In this subsection, we study the optimal privacy-aware and perfect-privacy estimation problems when the estimator has access to both the discretized measurement and the private random variable.

The optimal privacy-aware estimator based on $(Z_{\rm d}, X)$ is the solution of the following optimization problem

$$\begin{aligned} \underset{\{P_{ilj}\}_{i,l,j}}{\text{minimize}} \quad & \mathsf{E}\left[L\left(Y, \hat{Y}_P\left(Z_{\rm d}, X\right)\right)\right] \\ & P_{ilj} \geq 0, \forall i, l, j \\ & \sum_i P_{ilj} = 1, \forall l, j \\ \mathsf{H}\left[X \left| \hat{Y}_P\left(Z_{\rm d}, X\right)\right.\right] & \geq \mathsf{H}_0. \end{aligned} \tag{5}$$

Note that different from the optimization problem (2), the randomization probabilities depend on both $Z_{\rm d}$ and X in (5). Thus, the availability of X at the estimator provides more degrees of freedom in estimating Y and satisfying the privacy constraint.

The next theorem establishes the convexity of the estimator design problem in (5).

Theorem 3: The optimal privacy-aware estimator design problem using $(Z_{\rm d}, X)$ in (5) is a convex optimization problem.

Proof: See Appendix E. ∎

Note that the expression for objective function and the privacy constraint in (5) are different from those in (2). Nonetheless, the optimal privacy-aware estimator design problem remains convex.

Remark 3: A perfect measurement of the private variable may not be always available, and the estimator might have access to an inaccurate measurement of X. If the statistical structure of the inaccurate measurement is known, the estimator design framework in (5) can be extended to the case that the estimator has access to Z and an inaccurate measurement of X. It is straightforward to show that the estimator design problem, in this case, is also a convex optimization problem.

D. Optimal Perfect-privacy Estimation Using $(Z_{\rm d}, X)$

We next study the optimal perfect-privacy estimation when the estimator has access to $(Z_{\rm d}, X)$. To this end, next lemma derives a necessary and sufficient condition for the perfect-privacy under the information set $(Z_{\rm d}, X)$.

Lemma 4: An estimator of Y based on the information set $(Z_{\rm d}, X)$ satisfies the perfect-privacy condition if and only if we have

$$\Psi \bar{\boldsymbol{P}}_i = \mathbf{0}, \quad 1 \leq i \leq m$$

where $\bar{\boldsymbol{P}}_i = [\boldsymbol{P}_{i1}, \ldots, \boldsymbol{P}_{in}]^\top$ denotes the vector concatenation of vectors $\boldsymbol{P}_{ij} = [P_{i1j}, \ldots, P_{iNj}]^\top$ for $1 \leq i \leq m$ and $1 \leq j \leq n$, and Ψ is an $n \times Nn$ matrix defined as

$$\Psi = \sum_{j=1}^{n} J_j \otimes \eta_j - I_j \otimes \delta_j,$$

where $\otimes$ denotes the tensor product, the vectors η_j and δ_j are defined as

$$\begin{aligned} \eta_j &= \left[\mathsf{Pr}\left(Z \in B_1 \middle| X = x_j\right), \ldots, \mathsf{Pr}\left(Z \in B_N \middle| X = x_j\right)\right], \\ \delta_j &= \left[\mathsf{Pr}\left(Z \in B_1, X = x_j\right), \ldots, \mathsf{Pr}\left(Z \in B_N, X = x_j\right)\right], \end{aligned}$$

where I_j and J_j are $n \times n$ matrices defined as

$$I_j\left(u, v\right) = \begin{cases} 1 & v = j \\ 0 & \text{otherwise}, \end{cases}$$

and

$$J_j\left(u, v\right) = \begin{cases} 1 & v = u = j \\ 0 & \text{otherwise}. \end{cases}$$

Proof: See Appendix F. ∎

The optimal perfect-privacy estimator is the solution to the following optimization problem

$$\begin{aligned} \underset{\{P_{ilj}\}_{i,l,j}}{\text{minimize}} \quad & \mathsf{E}\left[L\left(Y, \hat{Y}_P\left(Z_{\rm d}, X\right)\right)\right] \\ & P_{ilj} \geq 0, \forall i, l, j \\ & \sum_i P_{ilj} = 1, \forall l, j \\ & \Psi \bar{\boldsymbol{P}}_i = \mathbf{0}, 1 \leq i \leq m. \end{aligned} \tag{6}$$

This optimization problem is linear. Following the proof of Lemma 3, it can be shown that its feasible set is non-empty for $N > n$.

IV. Optimal Estimation Using Continuous Measurement

In this section, we study the optimal privacy-aware and the optimal perfect-privacy estimation problems when the estimator has either access to Z or (Z, X).

The optimal privacy-aware estimator with access to Z is the solution to the following optimization problem

$$\begin{aligned} \underset{\{P_i(z)\}_{i=1}^m}{\text{minimize}} \quad & \mathsf{E}\left[L\left(Y, \hat{Y}_P\left(Z\right)\right)\right] \\ & P_i\left(z\right) \geq 0, \forall i, z \\ & \sum_i P_i\left(z\right) = 1, \forall z \\ \mathsf{H}\left[X \left| \hat{Y}_P\left(Z\right)\right.\right] & \geq \mathsf{H}_0. \end{aligned} \tag{7}$$

Different from the privacy-aware estimator design problems using $Z_{\rm d}$ or $(Z_{\rm d}, X)$, the estimator design problem above is a functional optimization problem defined on the space of bounded Borel measurable functions from $\mathbb{R}$ to $\mathbb{R}$ denoted by $\mathsf{B}\left(\mathbb{R}, \mathbb{R}\right)$. Note that $\mathsf{B}\left(\mathbb{R}, \mathbb{R}\right)$ forms a Banach space under the supremum norm and $P_i\left(z\right)$ belongs to the cone of positive functions in $\mathsf{B}\left(\mathbb{R}, \mathbb{R}\right)$ for all i. The next theorem shows that the optimal privacy-aware estimator design problem in (7) is a convex optimization problem.

Theorem 4: The optimal privacy-aware estimator design problem based on Z in (7) is a convex optimization problem.

Proof: See [32]. ∎

Next lemma studies the perfect-privacy condition when the estimator has access to the continuous measurement.

Lemma 5: An estimator of the public random variable Y using the continuous measurement Z satisfies the perfect-privacy condition if and only if

$$\int P_i\left(z\right)\left(p_Z\left(z\right) - p_Z\left(z \left| X = x_j\right.\right)\right) dz = 0, \forall i, j.$$

Proof: See Appendix G. ∎

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2021.3077868, IEEE Transactions on Automatic Control

Using Lemma 5, the optimal perfect-privacy estimator design problem with continuous measurements can be written as

$$\begin{aligned}\underset{\{P_i(z)\}_{i=1}^m}{\text{minimize}} \quad & \mathsf{E}\left[L\left(Y,\hat{Y}_P\left(Z\right)\right)\right]\\ & P_i\left(z\right)\geq 0,\forall i,z\\ & \sum_i P_i\left(z\right)=1,\forall z\\ & \int P_i\left(z\right)\left(p_Z\left(z\right)-p_Z\left(z\,|X=x_j\right)\right)dz=0\forall i,j. \end{aligned} \tag{8}$$

Note that the perfect-privacy constraint in the optimization problem above is a linear constraint and the objective function is a linear functional in the optimization variables. We next study the feasible set of this problem.

Lemma 6: The feasible set of the optimal perfect-privacy estimator design problem with continuous measurement in (8) is always non-empty.

Proof: See Appendix H. ∎

Finally, we study the optimal privacy-aware and the optimal perfect-privacy estimator design problems when the estimator has access to (Z,X). The optimal privacy-aware estimator based on (Z,X) is the solution of the following optimization problem

$$\begin{aligned}\underset{\{P_{ij}(z)\}_{ij}}{\text{minimize}} \quad & \mathsf{E}\left[L\left(Y,\hat{Y}_P\left(Z,X\right)\right)\right]\\ & P_{ij}\left(z\right)\geq 0,\forall i,j,z\\ & \sum_i P_{ij}\left(z\right)=1,\quad \forall z,j\\ & \mathsf{H}\left[X\left|\hat{Y}_P\left(Z,X\right)\right.\right]\geq \mathsf{H}_0. \end{aligned} \tag{9}$$

It can be shown that this problem is a convex optimization problem. We skip its proof as it follows similar to the proof Theorem 4. When the estimator has access to (Z,X), it can be shown that the perfect-privacy condition can be written as

$$\int P_{ij}\left(z\right)p_Z\left(z\,|X=x_j\right)- \sum_{j'}\mathsf{Pr}\left(X=x_{j'}\right)P_{ij'}\left(z\right)p_Z\left(z\,|X=x_{j'}\right)dz=0,\forall i,j.$$

Thus, the optimal perfect-privacy estimator with access to (Z,X) can be obtained by solving the following optimization problem

$$\begin{aligned}\underset{\{P_{ij}(z)\}_{ij}}{\text{minimize}} \quad & \mathsf{E}\left[L\left(Y,\hat{Y}_P\left(Z,X\right)\right)\right]\\ & P_{ij}\left(z\right)\geq 0,\forall i,j,z\\ & \sum_i P_{ij}\left(z\right)=1,\forall z,j\\ & \int P_{ij}\left(z\right)p_Z\left(z\,|X=x_j\right)\\ & -\sum_{j'}\mathsf{Pr}\left(X=x_{j'}\right)P_{ij'}\left(z\right)p_Z\left(z\,|X=x_{j'}\right)dz=0,\forall i,j. \end{aligned}$$

V. Numerical Results

In this section, we study the performance of the optimal privacy-aware and the optimal perfect-privacy estimators for the temperature estimation problem, introduced in Subsection II-D1. The objective of the temperature estimation problem is to provide an accurate estimate of the temperature while the occupancy information is kept private. In our numerical results, we assume that $\mathsf{Pr}\left(X=0\right)=\mathsf{Pr}\left(X=1\right)=0.5$, $T_{\min}=20$, $T_{\max}=22$ and the temperature is discretized between $T_{\min}$ and $T_{\max}$ with the discretization step equal to 0.2. The sensor noise is assumed to be Gaussian distributed with zero mean and variance σ^2. The estimation loss is captured using the following binary loss function:

$$L\left(Y,\hat{Y}\right)=\begin{cases}1 & \text{if} \quad Y\neq\hat{Y}\\ 0 & \text{if} \quad Y=\hat{Y}\end{cases}$$

To study the privacy of the occupancy information, X was estimated from the output of the optimal privacy-aware estimator using a maximum likelihood estimator. Fig 2 shows the error probability of the maximum likelihood estimator of X using $\hat{Y}\left(Z_{\mathrm{d}}\right)$ for different values of the privacy level H_0 for $\sigma^2=0.01$. Note that in this figure, $\mathsf{H}_0=0$ corresponds to the optimal classical estimator, which is privacy oblivious, and $\mathsf{H}_0=\mathsf{H}\left[X\right]$ corresponds to the optimal perfect-privacy estimator. According to this figure, the estimate of X is reliable when H_0 is small. However, as H_0 becomes large, the performance of the maximum likelihood estimator in recovering X from $\hat{Y}\left(Z_{\mathrm{d}}\right)$ deteriorates. This is due to the fact that the mutual information between X and $\hat{Y}\left(Z_{\mathrm{d}}\right)$ decreases when H_0 increases.

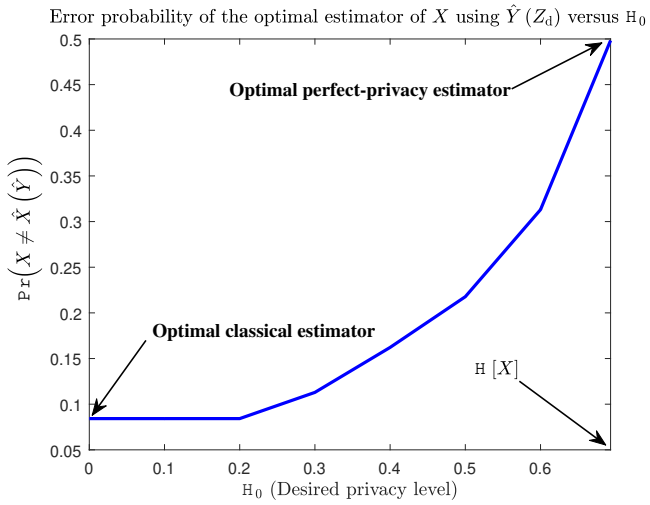
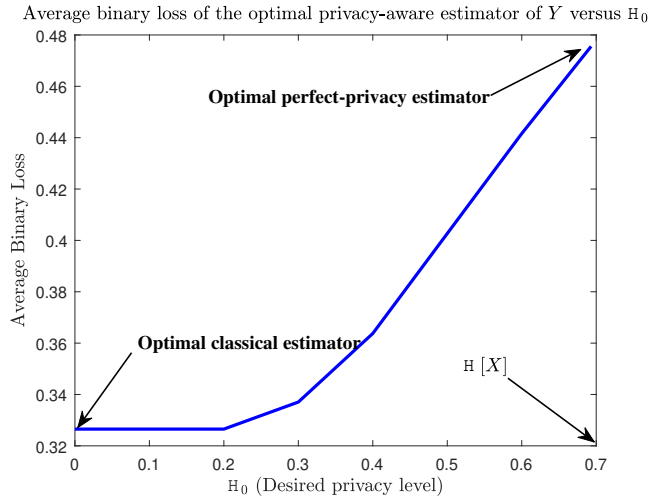


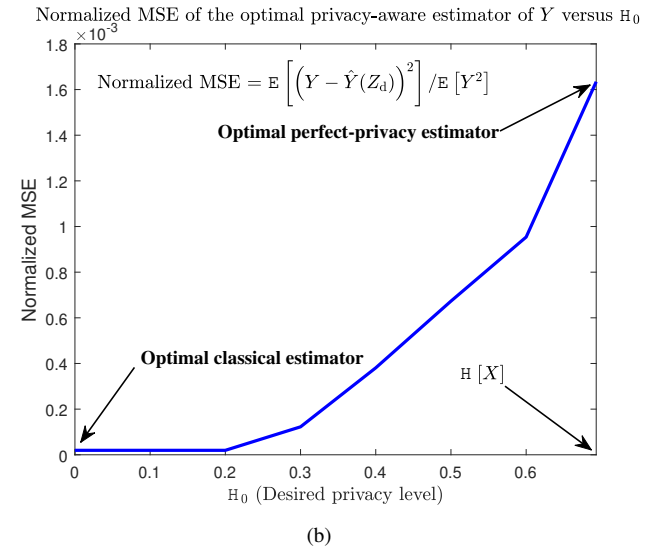
Fig. 2. The error probability of the maximum likelihood estimator of X using the output of the optimal privacy-aware estimator as a function of H_0 with sensor noise variance $\sigma^2=0.01$.

Fig. 3 shows the average binary (estimation) loss and the normalized mean square error of the optimal privacy-aware estimator of Y for different values of H_0. Note that when H_0 is equal to zero, the privacy constraint is inactive. Thus, the optimal classical estimator achieves the best performance. However, as the desired privacy level increases the performance of the optimal estimator in recovering Y drops. This is due to the fact that the set of estimators satisfying the privacy

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2021.3077868, IEEE Transactions on Automatic Control



(a)



(b)

Fig. 3. The average binary loss and the normalized mean square error of the optimal privacy-aware estimator of Y as a function of H_0 with sensor noise variance $\sigma^2 = 0.01$.

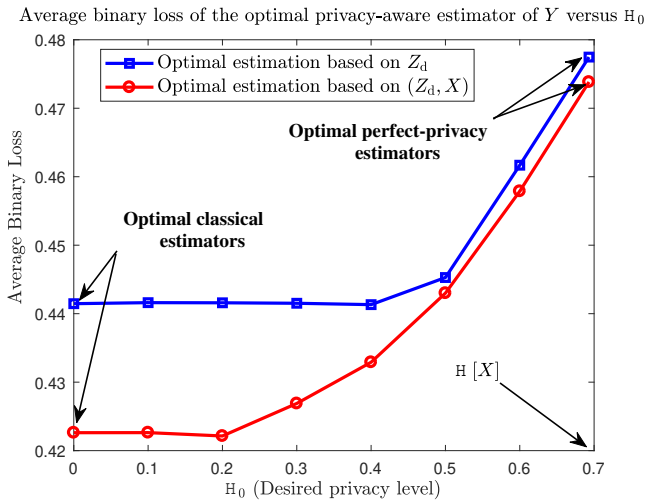


Fig. 4. The average binary loss of the optimal privacy-aware estimator of Y with access to Z_d or (Z_d, X) as a function of H_0 with sensor noise variance $\sigma^2 = 0.1$.

constraint becomes small when H_0 becomes large, *i.e.,* the privacy constraint becomes tight.

Fig. 4 shows the average binary loss of the optimal estimator of Y when the estimator has access to Z_d or (Z_d, X) for sensor noise variance $\sigma^2 = 0.1$. According to this figure, the optimal estimator with access to both Z_d and X incurs less loss in recovering Y, compared with the optimal estimator with only access to Z_d, since the former has more degrees of freedom in meeting the privacy constraint.

VI. Conclusions

In this paper, we studied the optimal privacy-aware estimation of a public random variable using measurements which contain private information. It was shown that the optimal privacy-aware estimator can be obtained by solving (a possibly infinite-dimensional) convex optimization problem when the estimator has access to either the measurement or the measurement as well as private information. It was also shown that the optimal perfect-privacy estimator can be obtained by solving a linear optimization problem. The results of this paper can be extended in multiple directions. An interesting research direction is to investigate the optimal privacy-aware estimator design problem when the measurements, public variable and private variable are vector-valued. The optimal encoder-decoder design for privacy-aware estimation in presence of a strategic sensor is another important avenue of our future research.

Appendix A
Proof of Lemma 1

Note that the mutual information between X and $\hat{Y}_P(Z_\mathrm{d})$ can be expanded as (10). Using (10), the Lagrangian of the optimization problem (2) can be written as (11) where $\boldsymbol{\lambda}$ is the vector of Lagrange multipliers associated with the equality constraints, μ is the Lagrange multiplier associated with the privacy constraint and $\boldsymbol{P} = \{P_{ij}\}_{ij}$.

The partial derivative of the Lagrangian with respect to P_{hk} can be written as (12) where (a) follows from (13). Note that the optimization problem (2) is a convex optimization problem and it is straightforward to show that the Slater's condition holds for this problem. Thus, using the necessary and sufficient Karush–Kuhn–Tucker (KKT) conditions, we have

$$\frac{\partial L(\boldsymbol{P}, \boldsymbol{\lambda}, \mu)}{\partial P_{hk}}\Big|_{\boldsymbol{P}^\star, \boldsymbol{\lambda}^\star, \boldsymbol{\mu}^\star} \begin{cases} = 0 & \text{if} \quad 0 < P^\star_{hk} < 1 \\ \leq 0 & \text{if} \quad P^\star_{hk} = 0 \\ \geq 0 & \text{if} \quad P^\star_{hk} = 1 \end{cases},$$

where $\boldsymbol{P}^\star$ is the optimal solution, and $\boldsymbol{\lambda}^\star$ and $\mu^\star$ are the dual optimal variables.

$$\begin{aligned}\mathsf{I}\left[X;\hat{Y}_P\left(Z_{\mathrm{d}}\right)\right] &= \sum_j \mathsf{Pr}\left(X=x_j\right)\mathsf{D}\left[p_{\hat{Y}_P}\left(y\,|X=x_j\,\right)\middle\|p_{\hat{Y}_P}\left(y\right)\right]\\ &= \sum_j \mathsf{Pr}\left(X=x_j\right)\sum_i\left(\sum_l P_{il}\mathsf{Pr}\left(\,Z\in B_l|\,X=x_j\right)\right)\log\frac{\sum_l P_{il}\mathsf{Pr}\left(\,Z\in B_l|\,X=x_j\right)}{\sum_l P_{il}\mathsf{Pr}\left(Z\in B_l\right)}\end{aligned} \tag{10}$$

$$\begin{aligned}L\left(\boldsymbol{P},\boldsymbol{\lambda},\mu\right) &= \sum_{i=1}^{m}\sum_{l=1}^{N} P_{il}\mathsf{Pr}\left(\,Z\in B_l|\,Y=y_i\right)\mathsf{Pr}\left(Y=y_i\right)\\ &\quad-\mu\sum_j \mathsf{Pr}\left(X=x_j\right)\sum_i\left(\sum_l P_{il}\mathsf{Pr}\left(\,Z\in B_l|\,X=x_j\right)\right)\log\frac{\sum_l P_{il}\mathsf{Pr}\left(\,Z\in B_l|\,X=x_j\right)}{\sum_l P_{il}\mathsf{Pr}\left(Z\in B_l\right)}\\ &\quad+\sum_l\lambda_l\left(\sum_i P_{il}-1\right)\end{aligned} \tag{11}$$

$$\begin{aligned}\frac{\partial L\left(\boldsymbol{P},\boldsymbol{\lambda},\mu\right)}{\partial P_{hk}} &= \mathsf{Pr}\left(\,Z\in B_k|\,Y=y_h\right)\mathsf{Pr}\left(Y=y_h\right)+\lambda_k\\ &\quad-\mu\sum_j \mathsf{Pr}\left(X=x_j\right)\left[\mathsf{Pr}\left(\,Z\in B_k|\,X=x_j\right)\log\frac{\sum_l P_{hl}\mathsf{Pr}\left(\,Z\in B_l|\,X=x_j\right)}{\sum_l P_{hl}\mathsf{Pr}\left(Z\in B_l\right)}\right.\\ &\quad\left.-\left(\sum_l P_{hl}\mathsf{Pr}\left(\,Z\in B_l|\,X=x_j\right)\right)\left(\frac{\mathsf{Pr}\left(\,Z\in B_k|\,X=x_j\right)}{\sum_l P_{hl}\mathsf{Pr}\left(\,Z\in B_l|\,X=x_j\right)}-\frac{\mathsf{Pr}\left(Z\in B_k\right)}{\sum_l P_{hl}\mathsf{Pr}\left(Z\in B_l\right)}\right)\right]\\ &\overset{(a)}{=} \mathsf{Pr}\left(\,Z\in B_k|\,Y=y_h\right)\mathsf{Pr}\left(Y=y_h\right)+\lambda_k\\ &\quad-\mu\sum_j \mathsf{Pr}\left(X=x_j\right)\left[\mathsf{Pr}\left(\,Z\in B_k|\,X=x_j\right)\log\frac{\sum_l P_{hl}\mathsf{Pr}\left(\,Z\in B_l|\,X=x_j\right)}{\sum_l P_{hl}\mathsf{Pr}\left(Z\in B_l\right)}\right]\end{aligned} \tag{12}$$

$$\sum_j \mathsf{Pr}\left(X=x_j\right)\left(\sum_l P_{hl}\mathsf{Pr}\left(\,Z\in B_l|\,X=x_j\right)\right)\left(\frac{\mathsf{Pr}\left(\,Z\in B_k|\,X=x_j\right)}{\sum_l P_{hl}\mathsf{Pr}\left(\,Z\in B_l|\,X=x_j\right)}-\frac{\mathsf{Pr}\left(Z\in B_k\right)}{\sum_l P_{hl}\mathsf{Pr}\left(Z\in B_l\right)}\right)=0 \tag{13}$$

APPENDIX B
PROOF OF LEMMA 2

To satisfy the perfect-privacy condition, we need to have $\mathsf{Pr}\left(\hat{Y}\left(Z_{\mathrm{d}}\right)=y_i,X=x_j\right)=\mathsf{Pr}\left(\hat{Y}\left(Z_{\mathrm{d}}\right)=y_i\right)\mathsf{Pr}\left(X=x_j\right)$ for all i,j. Note that $\mathsf{Pr}\left(\hat{Y}\left(Z_{\mathrm{d}}\right)=y_i,X=x_j\right)$ and $\mathsf{Pr}\left(\hat{Y}\left(Z_{\mathrm{d}}\right)=y_i\right)$ can be expanded as

$$\begin{aligned}&\mathsf{Pr}\left(X=x_j,\hat{Y}\left(Z_{\mathrm{d}}\right)=y_i\right)\\ &=\sum_l \mathsf{Pr}\left(X=x_j,\hat{Y}\left(Z_{\mathrm{d}}\right)=y_i,Z\in B_l\right)\\ &=\mathsf{Pr}\left(X=x_j\right)\sum_l \mathsf{Pr}\left(\hat{Y}\left(Z_{\mathrm{d}}\right)=y_i\middle|\,Z\in B_l\right)\\ &\qquad\qquad\times\mathsf{Pr}\left(\,Z\in B_l|\,X=x_j\right)\\ &=\mathsf{Pr}\left(X=x_j\right)\sum_l P_{il}\mathsf{Pr}\left(\,Z\in B_l|\,X=x_j\right)\end{aligned}$$

and

$$\begin{aligned}&\mathsf{Pr}\left(\hat{Y}\left(Z_{\mathrm{d}}\right)=y_i\right)\\ &=\sum_l \mathsf{Pr}\left(\hat{Y}\left(Z_{\mathrm{d}}\right)=y_i,Z\in B_l\right)\\ &=\sum_l \mathsf{Pr}\left(\hat{Y}\left(Z_{\mathrm{d}}\right)=y_i\middle|\,Z\in B_l\right)\mathsf{Pr}\left(Z\in B_l\right)\\ &=\sum_l P_{il}\mathsf{Pr}\left(Z\in B_l\right).\end{aligned}$$

Thus, for $\mathsf{Pr}\left(X=x_j\right)\neq 0$, the perfect-privacy requirement can be expressed as

$$\sum_l P_{il}\left(\mathsf{Pr}\left(\,Z\in B_l|\,X=x_j\right)-\mathsf{Pr}\left(Z\in B_l\right)\right)=0\quad\forall i,j.$$

The condition above can be expressed as

$$\Phi\boldsymbol{P}_i=\boldsymbol{0},\quad 1\leq i\leq m, \tag{14}$$

which implies that $\boldsymbol{P}_i\in\mathsf{Null}\left(\Phi\right)$.

APPENDIX C
PROOF OF LEMMA 3

Let $\mathcal{P} = \mathcal{P}_1 \times \cdots \times \mathcal{P}_N$ denote the joint probability simplex corresponding to the randomization probabilities of bins, *i.e.,* for each bin l we have $(P_{1l}, \cdots, P_{ml})^\top \in \mathcal{P}_l$. The feasible set of the optimization problem (4) is the intersection of the set $\mathcal{P}$ and the perfect-privacy condition. We show that there are infinity many points in $\mathcal{P}$ which satisfy the perfect-privacy condition if $N > n$.

Note that for $N > n$, the null space of Φ is non-empty. Pick a set of positive real numbers $\{\lambda_i\}_{i=1}^m$ where $0 < \lambda_i < 1$ for all i and $\sum_i \lambda_i = 1$. Let $(\lambda_1, \cdots, \lambda_m)^\top$ be the randomization probability of bin l for all $1 \leq l \leq N$, *i.e.,* $P_{il} = \lambda_i$ for all i, l. Thus, we have $\boldsymbol{P}_i = (\lambda_i, \cdots, \lambda_i)$. Note that $\boldsymbol{P}_i$ belongs to $\mathsf{Null}(\Phi)$ as the sum of the elements in each row of Φ is equal to zero.

APPENDIX D
PROOF OF THEOREM 2

Note that the distribution of $\hat{Y}_{\hat{\Theta}}(Z_{\mathrm{d}})$ can be written as

$$\begin{aligned} p_{\hat{Y}_{\hat{\Theta}}}(y_i) &= \mathsf{Pr}_\Theta\left(\hat{Y}_{\hat{\Theta}}(Z_{\mathrm{d}}) = y_i\right) \\ &= \sum_l \mathsf{Pr}_\Theta\left(\hat{Y}_{\hat{\Theta}}(Z_{\mathrm{d}}) = y_i, Z \in B_l\right) \\ &= \sum_l P^\star_{il\hat{\Theta}} \mathsf{Pr}_\Theta(Z \in B_l) \\ &= \underbrace{\sum_l P^\star_{il\hat{\Theta}} \mathsf{Pr}_{\hat{\Theta}}(Z \in B_l)}_{\Delta_{i\hat{\Theta}}} + \sum_l P^\star_{il\hat{\Theta}} \epsilon_l \\ &= \Delta_{i\hat{\Theta}} + \boldsymbol{\epsilon}^\top \boldsymbol{P}^\star_{i\hat{\Theta}}, \end{aligned}$$

where $\boldsymbol{P}^\star_{i\hat{\Theta}}$ is defined as

$$\boldsymbol{P}^\star_{i\hat{\Theta}} = \left[P^\star_{i1\hat{\Theta}}, \cdots, P^\star_{iN\hat{\Theta}}\right]^\top.$$

Similarly, the conditional distribution of $\hat{Y}_{\hat{\Theta}}(Z_{\mathrm{d}})$ given $X = x_j$ can be written as

$$\begin{aligned} p_{\hat{Y}_{\hat{\Theta}}}(y_i \,|X = x_j) &= \mathsf{Pr}_\Theta\left(\hat{Y}_{\hat{\Theta}}(Z_{\mathrm{d}}) = y_i \middle| X = x_j\right) \\ &= \sum_l P^\star_{il\hat{\Theta}} \mathsf{Pr}_\Theta(Z \in B_l | X = x_j) \\ &= \underbrace{\sum_l P^\star_{il\hat{\Theta}} \mathsf{Pr}_{\hat{\Theta}}(Z \in B_l | X = x_j)}_{\Delta_{ij\hat{\Theta}}} \\ &\quad + \sum_l \epsilon_{lj} P^\star_{il\hat{\Theta}} \\ &= \Delta_{ij\hat{\Theta}} + \boldsymbol{\epsilon}_j^\top \boldsymbol{P}^\star_{i\hat{\Theta}}. \end{aligned}$$

The mutual information between X and $\hat{Y}_{\hat{\Theta}}(Z_{\mathrm{d}})$ can be written as

$$\begin{aligned} &\mathsf{I}\left[X; \hat{Y}_{\hat{\Theta}}(Z_{\mathrm{d}})\right] \\ &= \sum_j \mathsf{Pr}(X = x_j) \sum_i p_{\hat{Y}_{\hat{\Theta}}}(y_i \,|X = x_j) \log \frac{p_{\hat{Y}_{\hat{\Theta}}}(y_i \,|X = x_j)}{p_{\hat{Y}_{\hat{\Theta}}}(y_i)}. \end{aligned}$$

Without loss of generality, assume that $\Delta_{i\hat{\Theta}} > 0$ and $\Delta_{ij\hat{\Theta}} > 0$. Using Taylor expansion, we have

$$\begin{aligned} \log p_{\hat{Y}_{\hat{\Theta}}}(y_i) &= \log\left(\Delta_{i\hat{\Theta}}\right) + \underbrace{\frac{\boldsymbol{\epsilon}^\top \boldsymbol{P}^\star_{i\hat{\Theta}}}{\Delta_{i\hat{\Theta}} + \alpha_i \boldsymbol{\epsilon}^\top \boldsymbol{P}^\star_{i\hat{\Theta}}}}_{\gamma_i(\boldsymbol{\epsilon})} \\ &= \log\left(\Delta_{i\hat{\Theta}}\right) + \gamma_i(\boldsymbol{\epsilon}) \\ \log p_{\hat{Y}_{\hat{\Theta}}}(y_i \,|X = x_j) &= \log\left(\Delta_{ij\hat{\Theta}}\right) + \underbrace{\frac{\boldsymbol{\epsilon}_j^\top \boldsymbol{P}^\star_{i\hat{\Theta}}}{\Delta_{ij\hat{\Theta}} + \alpha_{ij} \boldsymbol{\epsilon}_j^\top \boldsymbol{P}^\star_{i\hat{\Theta}}}}_{\gamma_{ij}(\boldsymbol{\epsilon}_j)} \\ &= \log\left(\Delta_{ij\hat{\Theta}}\right) + \gamma_{ij}(\boldsymbol{\epsilon}_j), \end{aligned}$$

where $\alpha_i, \alpha_{ij} \in [0, 1]$. Thus, $\mathsf{I}\left[X; \hat{Y}_{\hat{\Theta}}(Z_{\mathrm{d}})\right]$ can be written as

$$\begin{aligned} \mathsf{I}\left[X; \hat{Y}_{\hat{\Theta}}(Z_{\mathrm{d}})\right] &= \sum_j \mathsf{Pr}(X = x_j) \sum_i \Delta_{ij\hat{\Theta}} \log \frac{\Delta_{ij\hat{\Theta}}}{\Delta_{i\hat{\Theta}}} \\ &+ \sum_j \mathsf{Pr}(X = x_j) \sum_i \boldsymbol{\epsilon}_j^\top \boldsymbol{P}^\star_{i\hat{\Theta}} \left(\gamma_{ij}(\boldsymbol{\epsilon}_j) - \gamma_i(\boldsymbol{\epsilon})\right) \\ &+ \sum_j \mathsf{Pr}(X = x_j) \sum_i \Delta_{ij\hat{\Theta}} \left(\gamma_{ij}(\boldsymbol{\epsilon}_j) - \gamma_i(\boldsymbol{\epsilon})\right). \end{aligned} \tag{15}$$

Note that $\Delta_{i\hat{\Theta}} = \Delta_{ij\hat{\Theta}}$ for all j, i since $\hat{Y}_{\hat{\Theta}}(Z_{\mathrm{d}})$ satisfies the perfect-privacy condition with respect to $p_{\hat{\Theta}}(\theta)$. Thus, the first term in (15) is equal to zero. Moreover, $\gamma_i(\boldsymbol{\epsilon})$ and $\gamma_{ij}(\boldsymbol{\epsilon}_{ij})$ can be upper bounded as

$$\begin{aligned} \gamma_i(\boldsymbol{\epsilon}) &\leq \frac{\|\boldsymbol{\epsilon}\|_1}{\Delta_{i\hat{\Theta}} - \|\boldsymbol{\epsilon}\|_1} \\ &= \gamma_i \\ \gamma_{ij}(\boldsymbol{\epsilon}_{ij}) &\leq \frac{\|\boldsymbol{\epsilon}_j\|_1}{\Delta_{ij\hat{\Theta}} - \|\boldsymbol{\epsilon}_j\|_1} \\ &= \gamma_{ij}. \end{aligned}$$

Thus, we have

$$\begin{aligned} &\mathsf{I}\left[X; \hat{Y}_{\hat{\Theta}}(Z_{\mathrm{d}})\right] \\ &\leq \sum_j \mathsf{Pr}(X = x_j) \sum_i \left(\Delta_{ij\hat{\Theta}} + \|\boldsymbol{\epsilon}_j\|_1\right)(\gamma_{ij} + \gamma_i). \end{aligned}$$

APPENDIX E
PROOF OF THEOREM 3

The objective function in (5) can be written as

$$\begin{aligned} &\mathsf{E}\left[L\left(Y, \hat{Y}_P(Z_{\mathrm{d}}, X)\right)\right] \\ &= \sum_{ik} L(y_i, y_k) \,\mathsf{Pr}\left(Y = y_i, \hat{Y}_P(Z_{\mathrm{d}}, X) = y_k\right). \end{aligned}$$

Note that the probability of the event $\left(Y=y_i,\hat{Y}_P\left(Z_{\rm d},X\right)=y_k\right)$ can be expressed as

$$\begin{aligned}&\mathsf{Pr}\left(Y=y_i,\hat{Y}_P\left(Z_{\rm d},X\right)=y_k\right)\\&=\sum_{lj}\mathsf{Pr}\left(Y=y_i,\hat{Y}_P\left(Z_{\rm d},X\right)=y_k,Z\in B_l,X=x_j\right)\\&=\sum_{lj}\mathsf{Pr}\left(\hat{Y}_P\left(Z_{\rm d},X\right)=y_k\middle|\,Z\in B_l,X=x_j,Y=y_i\right)\\&\qquad\qquad\times\mathsf{Pr}\left(Z\in B_l,Y=y_i,X=x_j\right)\\&=\sum_{lj}P_{klj}\mathsf{Pr}\left(Z\in B_l,Y=y_i,X=x_j\right),\end{aligned}$$

which implies that the objective function is linear in the randomization probabilities.

We next show that the privacy constraint is convex. Let $\hat{Y}_P\left(Z_{\rm d},X\right)$ denote an estimator of Y based on the randomization probabilities $\{P_{ilj}\}_{ilj}$. Using the definition of the conditional entropy, the privacy constraint can be written as (16) where $p_{\hat{Y}_P}\left(y\right)$ and $p_{\hat{Y}_P}\left(y\,|X=x_j\right)$ denote the probability mass function of $\hat{Y}_P\left(Z_{\rm d},X\right)$ and the conditional probability mass function of $\hat{Y}_P\left(Z_{\rm d},X\right)$ given $X=x_j$, respectively, and $\mathsf{D}\left[\cdot\,\|\cdot\right]$ denotes the Kullback-Leibler (KL) divergence (relative entropy).

The probability mass functions $p_{\hat{Y}_P}\left(y\right)$ and $p_{\hat{Y}_P}\left(y\,|X=x_j\right)$ can be expanded as

$$\begin{aligned}p_{\hat{Y}_P}\left(y_i\right)&=\mathsf{Pr}\left(\hat{Y}_P\left(Z_{\rm d},X\right)=y_i\right)\\&=\sum_{lj}\mathsf{Pr}\left(\hat{Y}_P\left(Z_{\rm d},X\right)=y_i\middle|\,Z\in B_l,X=x_j\right)\\&\qquad\qquad\times\mathsf{Pr}\left(Z\in B_l,X=x_j\right)\\&=\sum_{lj}P_{ilj}\mathsf{Pr}\left(Z\in B_l,X=x_j\right)\end{aligned}$$

and

$$\begin{aligned}p_{\hat{Y}_P}\left(y_i\,|X=x_j\right)&=\mathsf{Pr}\left(\hat{Y}_P\left(Z_{\rm d},X\right)=y_i\middle|\,X=x_j\right)\\&=\sum_{l}\mathsf{Pr}\left(\hat{Y}_P\left(Z_{\rm d},X\right)=y_i\middle|\,Z\in B_l,X=x_j\right)\\&\qquad\qquad\times\mathsf{Pr}\left(\,Z\in B_l|\,X=x_j\right)\\&=\sum_{l}P_{ilj}\mathsf{Pr}\left(\,Z\in B_l|\,X=x_j\right),\end{aligned}$$

respectively. Let $Y_{P'}\left(Z_{\rm d},X\right)$ denote an estimator of Y using the randomization probabilities $\left\{P'_{ilj}\right\}_{ilj}$. Consider an estimator of Y, denoted by $\hat{Y}_{\tilde{P}}\left(Z_{\rm d},X\right)$, with the randomization probabilities $\left\{\tilde{P}_{ilj}\right\}_{ilj}$ which are a convex combination of $\{P_{ilj}\}_{ilj}$ and $\left\{P'_{ilj}\right\}_{ilj}$, *i.e.,* $\tilde{P}_{ilj}=\alpha P_{ilj}+\left(1-\alpha\right)P'_{ilj}$ for all i,l,j. Thus, we have

$$\begin{aligned}p_{\hat{Y}_{\tilde{P}}}\left(y_i\right)&=\alpha p_{\hat{Y}_P}\left(y_i\right)+\left(1-\alpha\right)p_{\hat{Y}_{P'}}\left(y_i\right)\\p_{\hat{Y}_{\tilde{P}}}\left(y_i\,|X=x_j\right)&=\alpha p_{\hat{Y}_P}\left(y_i\,|X=x_j\right)\\&\quad+\left(1-\alpha\right)p_{\hat{Y}_{P'}}\left(y_i\,|X=x_j\right).\end{aligned}$$

Using the convexity of the KL divergence [29], $\mathsf{D}\left[p_{\hat{Y}_{\tilde{P}}}\left(y\,|X=x_j\right)\middle\|p_{\hat{Y}_{\tilde{P}}}\left(y\right)\right]$ can be upper bounded as (17) for $1\le j\le n$. Thus, $\mathsf{H}\left[X\middle|\hat{Y}_P\left(Z_{\rm d},X\right)\right]$ is concave in the randomization probabilities which implies that the privacy constraint, *i.e.,* $\mathsf{H}\left[X\middle|\hat{Y}_P\left(Z_{\rm d},X\right)\right]\ge\mathsf{H}_0$, is convex in $\{P_{ilj}\}_{ilj}$.

Appendix F
Proof of Lemma 4

The perfect-privacy requirement implies

$$\begin{aligned}\mathsf{Pr}\left(\hat{Y}\left(Z_{\rm d},X\right)=y_i,X=x_j\right)&=\mathsf{Pr}\left(\hat{Y}\left(Z_{\rm d},X\right)=y_i\right)\\&\qquad\times\mathsf{Pr}\left(X=x_j\right)\forall i,j.\end{aligned}$$

Note that $\mathsf{Pr}\left(\hat{Y}\left(Z_{\rm d},X\right)=y_i,X=x_j\right)$ and $\mathsf{Pr}\left(\hat{Y}\left(Z_{\rm d},X\right)=y_i\right)$ can be expanded as

$$\begin{aligned}&\mathsf{Pr}\left(X=x_j,\hat{Y}\left(Z_{\rm d},X\right)=y_i\right)\\&=\sum_{l}\mathsf{Pr}\left(X=x_j,\hat{Y}\left(Z_{\rm d},X\right)=y_i,Z\in B_l\right)\\&=\mathsf{Pr}\left(X=x_j\right)\sum_{l}\mathsf{Pr}\left(\hat{Y}\left(Z_{\rm d},X\right)=y_i\middle|\,Z\in B_l,X=x_j\right)\\&\qquad\qquad\times\mathsf{Pr}\left(\,Z\in B_l|\,X=x_j\right)\\&=\mathsf{Pr}\left(X=x_j\right)\sum_{l}P_{ilj}\mathsf{Pr}\left(\,Z\in B_l|\,X=x_j\right)\end{aligned}$$

and

$$\begin{aligned}&\mathsf{Pr}\left(\hat{Y}\left(Z_{\rm d},X\right)=y_i\right)\\&=\sum_{l,j'}\mathsf{Pr}\left(\hat{Y}\left(Z_{\rm d},X\right)=y_i,Z\in B_l,X=x_{j'}\right)\\&=\sum_{l,j'}\mathsf{Pr}\left(\hat{Y}\left(Z_{\rm d},X\right)=y_i\middle|\,Z\in B_l,X=x_{j'}\right)\\&\qquad\qquad\times\mathsf{Pr}\left(Z\in B_l,X=x_{j'}\right)\\&=\sum_{l,j'}P_{ilj'}\mathsf{Pr}\left(Z\in B_l,X=x_{j'}\right).\end{aligned}$$

Thus, for $\mathsf{Pr}\left(X=x_j\right)\ne0$, the perfect-privacy requirement can be expressed as

$$\begin{aligned}&\sum_{l}P_{ilj}\mathsf{Pr}\left(\,Z\in B_l|\,X=x_j\right)\\&\qquad-\sum_{l,j'}P_{ilj'}\mathsf{Pr}\left(Z\in B_l,X=x_{j'}\right)=0\end{aligned}$$

for all i,j. Let $\boldsymbol{P}_{ij}=\left[P_{i1j},\ldots,P_{iNj}\right]^\top$ for $1\le i\le m$ and $1\le j\le n$ and $\bar{\boldsymbol{P}}_i=\left[\boldsymbol{P}_{i1},\ldots,\boldsymbol{P}_{in}\right]^\top$. By direct calculation, it can be shown that the above condition is equivalent to

$$\Psi\bar{\boldsymbol{P}}_i=\boldsymbol{0},1\le i\le m,$$

which implies that $\bar{\boldsymbol{P}}_i\in\mathsf{Null}\left(\Psi\right)$ for all i.

$$\mathsf{H}\left[X\left|\hat{Y}_P\left(Z_{\mathrm{d}},X\right)\right.\right]=\mathsf{H}\left[X\right]-\sum_j \mathsf{Pr}\left(X=x_j\right)\mathsf{D}\left[p_{\hat{Y}_P}\left(y\left|X=x_j\right.\right)\middle\|p_{\hat{Y}_P}\left(y\right)\right] \tag{16}$$

$$\begin{aligned}\mathsf{D}\left[p_{\hat{Y}_{\tilde{P}}}\left(y\left|X=x_j\right.\right)\middle\|p_{\hat{Y}_{\tilde{P}}}\left(y\right)\right]&=\mathsf{D}\left[\alpha p_{\hat{Y}_P}\left(y\left|X=x_j\right.\right)+\left(1-\alpha\right)p_{\hat{Y}_{P'}}\left(y\left|X=x_j\right.\right)\middle\|\alpha p_{\hat{Y}_P}\left(y\right)+\left(1-\alpha\right)p_{\hat{Y}_{P'}}\left(y\right)\right]\\&\leq\alpha\mathsf{D}\left[p_{\hat{Y}_P}\left(y\left|X=x_j\right.\right)\middle\|p_{\hat{Y}_P}\left(y\right)\right]+\left(1-\alpha\right)\mathsf{D}\left[p_{\hat{Y}_{P'}}\left(y\left|X=x_j\right.\right)\middle\|p_{\hat{Y}_{P'}}\left(y\right)\right]\end{aligned} \tag{17}$$

APPENDIX G
PROOF OF LEMMA 5

According to the perfect-privacy definition, the output of the estimator, $\hat{Y}_P\left(Z\right)$, satisfies the perfect-privacy requirement if and only if we have

$$\mathsf{Pr}\left(\hat{Y}_P\left(Z\right)=y_i,X=x_j\right)=\mathsf{Pr}\left(\hat{Y}_P\left(Z\right)=y_i\right)\mathsf{Pr}\left(X=x_j\right)$$

for all i,j. Note that, $\mathsf{Pr}\left(\hat{Y}_P\left(Z\right)=y_i,X=x_j\right)$ and $\mathsf{Pr}\left(\hat{Y}_P\left(Z\right)=y_i\right)$ can be written as

$$\begin{aligned}&\mathsf{Pr}\left(\hat{Y}_P\left(Z\right)=y_i,X=x_j\right)\\&\quad=\int\mathsf{Pr}\left(\hat{Y}_P\left(Z\right)=y_i,X=x_j\middle|Z=z\right)p_Z(z)dz\\&\quad=\mathsf{Pr}\left(X=x_j\right)\int P_i\left(z\right)p_Z\left(z\left|X=x_j\right.\right)dz\end{aligned}$$

and

$$\mathsf{Pr}\left(\hat{Y}_P\left(Z\right)=y_i\right)=\int P_i\left(z\right)p_Z\left(z\right)dz,$$

respectively. Thus, for $\mathsf{Pr}\left(X=x_j\right)\neq 0$, the estimator satisfies the perfect-privacy condition if and only if we have

$$\int P_i\left(z\right)\left(p_Z\left(z\right)-p_Z\left(z\left|X=x_j\right.\right)\right)dz=0,\forall i,j.$$

APPENDIX H
PROOF OF LEMMA 6

Pick $N>n$ and $\{B_i\subset\mathbb{R}\}_{i=1}^N$ where B_i are arbitrary discretization bins. According to Lemma 3, the feasible set of the optimization problem (4) is non-empty. Let $\left\{\bar{P}_l\right\}_l$ denote a point in the feasible set of (4) where $\bar{P}_l=\left(P_{1l},\cdots,P_{ml}\right)^\top$ denotes the randomization probabilities corresponding to bin l. Now, we construct $\left\{P_i\left(z\right)\right\}_i$ as follows. For $z\in B_l$, let $P_i(z)=P_{il}$ for all i. Thus, any feasible solution of (4) corresponds to a piecewise constant solution of (8) which satisfies the perfect-privacy requirement.

REFERENCES

[1] A. Ebadat, G. Bottegal, D. Varagnolo, B. Wahlberg, and K. H. Johansson, "Regularized deconvolution-based approaches for estimating room occupancies," *IEEE Transactions on Automation Science and Engineering*, vol. 12, no. 4, pp. 1157–1168, Oct 2015.

[2] X. He, W. P. Tay, and M. Sun, "Privacy-aware decentralized detection using linear precoding," in *2016 IEEE Sensor Array and Multichannel Signal Processing Workshop (SAM)*, July 2016, pp. 1–5.

[3] M. Sun and W. P. Tay, "Privacy-preserving nonparametric decentralized detection," in *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Mar. 2016, pp. 6270–6274.

[4] X. He and W. P. Tay, "Multilayer sensor network for information privacy," in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Mar. 2017, pp. 6005–6009.

[5] J. Liao, L. Sankar, V. Y. F. Tan, and F. P. Calmon, "Hypothesis testing in the high privacy limit," in *2016 54th Annual Allerton Conference on Communication, Control, and Computing*, Sept. 2016, pp. 649–656.

[6] Z. Li and T. J. Oechtering, "Privacy-aware distributed bayesian detection," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 7, pp. 1345–1357, Oct. 2015.

[7] ——, "Privacy-constrained parallel distributed neyman-pearson test," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 3, no. 1, pp. 77–90, Mar. 2017.

[8] Z. Li, "Privacy-by-design for cyber-physical systems," Ph.D. dissertation, 2017. [Online]. Available: http://kth.diva-portal.org/smash/get/diva2:1131655/FULLTEXT01.pdf

[9] T. Tanaka, M. Skoglund, H. Sandberg, and K. H. Johansson, "Directed information as privacy measure in cloud-based control," KTH Royal Institute of Technology, Sweden, Tech. Rep., 2017. [Online]. Available: https://arxiv.org/abs/1705.02802

[10] P. Venkitasubramaniam, "Privacy in stochastic control: A Markov decision process perspective," in *2013 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Oct 2013, pp. 381–388.

[11] R. Mochaourab and T. J. Oechtering, "Private filtering for hidden Markov models," *IEEE Signal Processing Letters*, vol. 25, no. 6, pp. 888–892, June 2018.

[12] E. Nekouei, T. Tanaka, M. Skoglund, and K. H. Johansson, "Information-theoretic approaches to privacy in estimation and control," *Annual Reviews in Control*, vol. 47, pp. 412 – 422, 2019.

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

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

[15] Y. Wang, Z. Huang, S. Mitra, and G. E. Dullerud, "Differential privacy in linear distributed control systems: Entropy minimizing mechanisms and performance tradeoffs," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 118–130, March 2017.

[16] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design," *Automatica*, vol. 81, pp. 221 – 231, 2017.

[17] Y. Mo and R. M. Murray, "Privacy preserving average consensus," *IEEE Transactions on Automatic Control*, vol. 62, no. 2, pp. 753–765, Feb 2017.

[18] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "Utility-privacy tradeoffs in databases: An information-theoretic approach," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 838–852, 2013.

[19] E. Akyol, C. Langbort, and T. Basar, "Privacy constrained information processing," in *2015 54th IEEE Conference on Decision and Control (CDC)*, 2015, pp. 4511–4516.

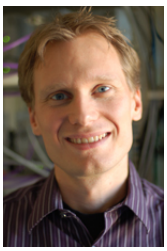
[20] K. Kalantari, L. Sankar, and O. Kosut, "On information-theoretic privacy with general distortion cost functions," in *2017 IEEE International Symposium on Information Theory (ISIT)*, June 2017, pp. 2865–2869.

[21] Y. O. Basciftci, Y. Wang, and P. Ishwar, "On privacy-utility tradeoffs for constrained data release mechanisms," in *2016 Information Theory and Applications Workshop (ITA)*, Jan. 2016, pp. 1–6.

[22] F. du Pin Calmon and N. Fawaz, "Privacy against statistical inference," in *2012 50th Annual Allerton Conference on Communication, Control, and Computing*, Oct. 2012, pp. 1401–1408.

[23] B. Moraffah and L. Sankar, "Information-theoretic private interactive mechanism," in *2015 53rd Annual Allerton Conference on Communication, Control, and Computing*, Sept. 2015, pp. 911–918.
[24] S. Asoodeh, F. Alajaji, and T. Linder, "Privacy-aware MMSE estimation," in *2016 IEEE International Symposium on Information Theory (ISIT)*, July 2016, pp. 1989–1993.
[25] S. Asoodeh, M. Diaz, F. Alajaji, and T. Linder, "Privacy-aware guessing efficiency," in *2017 IEEE International Symposium on Information Theory (ISIT)*, June 2017, pp. 754–758.
[26] ——, "Estimation efficiency under privacy constraints," Tech. Rep., 2017. [Online]. Available: https://arxiv.org/abs/1707.02409
[27] B. Rassouli and D. Gündüz, "On perfect privacy and maximal correlation," December 2017. [Online]. Available: https://arxiv.org/pdf/1712.08500.pdf
[28] F. d. P. Calmon, A. Makhdoumi, M. Médard, M. Varia, M. Christiansen, and K. R. Duffy, "Principal inertia components and applications," *IEEE Transactions on Information Theory*, vol. 63, no. 8, pp. 5011–5038, Aug 2017.
[29] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley-Interscience, 2006.
[30] S. Depatla, A. Muralidharan, and Y. Mostofi, "Occupancy estimation using only wifi power measurements," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 7, pp. 1381–1393, July 2015.
[31] S. Asoodeh, F. Alajaji, and T. Linder, "Notes on information-theoretic privacy," in *2014 52nd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Sept 2014, pp. 1272–1278.
[32] E. Nekouei, H. Sandberg, M. Skoglund, and K. H. Johansson, "Optimal privacy-aware estimation," KTH Royal Institute of Technology, Tech. Rep., 2019. [Online]. Available: https://www.dropbox.com/s/0u8jqxsn64qtb41/Privacy19.pdf?dl=0

Ehsan Nekouei (S'11, M'14) is currently an Assistant Professor with the Department of Electrical Engineering, City University of Hong Kong. From 2014 to 2019, he held postdoctoral positions at the KTH Royal Institute of Technology, Stockholm, Sweden, and The University of Melbourne, Australia. His current research interests include privacy in networked control systems and integrated processing of human decision-making data.



Henrik Sandberg Henrik Sandberg is Professor at the Division of Decision and Control Systems, KTH Royal Institute of Technology, Stockholm, Sweden. He received the M.Sc. degree in engineering physics and the Ph.D. degree in automatic control from Lund University, Lund, Sweden, in 1999 and 2004, respectively. From 2005 to 2007, he was a Post-Doctoral Scholar at the California Institute of Technology, Pasadena, USA. In 2013, he was a visiting scholar at the Laboratory for Information and Decision Systems (LIDS) at MIT, Cambridge, USA. He has also held visiting appointments at the Australian National University and the University of Melbourne, Australia. His current research interests include security of cyber-physical systems, power systems, model reduction, and fundamental limitations in control. Dr. Sandberg was a recipient of the Best Student Paper Award from the IEEE Conference on Decision and Control in 2004, an Ingvar Carlsson Award from the Swedish Foundation for Strategic Research in 2007, and a Consolidator Grant from the Swedish Research Council in 2016. He has served on the editorial boards of IEEE Transactions on Automatic Control and the IFAC Journal Automatica.

Mikael Skoglund Mikael Skoglund (S'93-M'97-SM'04-F'19) received the Ph.D. degree in 1997 from Chalmers University of Technology, Sweden. In 1997, he joined the Royal Institute of Technology (KTH), Stockholm, Sweden, where he was appointed to the Chair in Communication Theory in 2003. At KTH, he heads the Division of Information Science and Engineering, and the Department of Intelligent Systems.

Dr. Skoglund has worked on problems in source-channel coding, coding and transmission for wireless communications, Shannon theory, information and control, and statistical signal processing. He has authored and co-authored more than 175 journal and 385 conference papers.

Dr. Skoglund is a Fellow of the IEEE. During 2003–08 he was an associate editor for the IEEE Transactions on Communications and during 2008–12 he was on the editorial board for the IEEE Transactions on Information Theory. He has served on numerous technical program committees for IEEE sponsored conferences, he was general co-chair for IEEE ITW 2019, and he will serve as TPC co-chair for IEEE ISIT 2022.

Karl Henrik Johansson (F'13) received the M.Sc. and Ph.D. degrees from Lund University, Lund, Sweden. He is the Director of the Stockholm Strategic Research Area ICT The Next Generation and a Professor with the School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology. He has held visiting positions with the University of California, Berkeley, California Institute of Technology, Nanyang Technological University, HKUST Institute of Advanced Studies, and Norwegian University of Science and Technology. His research interests include networked control systems, cyber-physical systems, and applications in transportation, energy, and automation. He is a member of the IEEE Control Systems Society Board of Governors, the IFAC Executive Board, and the European Control Association Council. He has received several best paper awards and other distinctions. He has been awarded Distinguished Professor with the Swedish Research Council and Wallenberg Scholar. He is a recipient of the Future Research Leader Award from the Swedish Foundation for Strategic Research and the triennial Young Author Prize from IFAC. He is a Fellow of the Royal Swedish Academy of Engineering Sciences. He is an IEEE Distinguished Lecturer.