Privacy-Aware Kalman Filtering

Yang Song, Chong Xiao Wang, Wee Peng Tay
School of Electrical and Electronic Engineering, Nanyang Technological University

***Abstract*—We are concerned with a privacy-preserving problem in Kalman filter: a sensor releases a set of measurements to fusion center, who has perfect knowledge of the dynamical model, to allow it to estimate the public state, while prevent it from estimating the private state. We propose to linearly transform the original observation into a lower dimensional space before sending them to fusion center. Two privacy-utility tradeoffs are formulated: one concerns only at the current time step and the other concerns over two time steps. The transformation that leads to the optimal tradeoff can be found in closed-form. The privacy (estimation of private state) and utility (estimation of public state) are measured based on recursive Bayesian Cramér-Rao bound.**

***Index Terms*—Kalman filter, inference privacy, compression, linear transformation, parameter estimation, recursive Bayesian Cramér-Rao bound.**

I. Introduction

With the emergence of the data driven information technology, there are increasing concerns over the breach of privacy of personal data collected from sensors. In general, privacy can be categorized into two classes: data privacy and inference privacy. Data privacy protects the original measurements from being inferred by fusion center. The privacy metrics that have been proposed in data privacy include homomorphic encryption [1], [2], [3] and local differential privacy [4], [5], [6], [7]. Inference privacy prevents fusion center from making certain statistical inferences. The privacy metrics have been used in inference privacy include information privacy [8], [9], [10], [11], differential privacy [12] and average information leakage [13], [14]. The interrelation between data privacy and inference privacy has been studied in [15], [16]. The privacy we consider in this paper belongs to inference privacy.

The Kalman filter uses a system's dynamics model and multiple sequential measurements to form an estimate of the system's varying state. The privacy comes from the system's state that can be separated into private state and public state. Our goal is then to find optimal tradeoff between maximizing the estimation error for private state and minimizing that for public state. This can be achieved by transforming the original measurement space into a lower dimensional space. The transformation applied in this paper is restricted to linear form. In practice, a privacy-preserving Kalman filter can operate as: a sensor transform the measurements before releasing them to the fusion center who knows system's dynamical model. By doing so, the estimation the private state suffers a large uncertainty but the estimation of public state has small uncertainty.

Our work is related to the following works which preserve privacy through data compression/linear transformation: 1) information bottleneck (IB) [17], [18], [19], [20] which operates to compress source variable, while preserving information about relevant variable. The compression (privacy) and preserved relevant information (utility) are measured by mutual information; 2) privacy funnel (PF) [21] which operates to suppress information about relevant variable, while minimally compress the source variable. 3) compressive privacy (CP) [22], [23] unifies PF and IB. The privacy and utility in CP are measured by differential mutual information; 4) [24] proposes to compress the observations while maximally retains the estimation accuracy of all signal parameters. The estimation accuracy is measured by Bayesian Cramér-Rao lower bound.

One major difference between our work and the existing ones is that our work is based on a dynamic system, whereas all above mentioned works are based on a static one. The dynamical model encourages us to measure the privacy (estimation error/uncertainty of private state) and utility (estimation error/uncertainty of public state) by *recursive* Bayesian Cramér-Rao bound [25], which is also different from the measure existing works have used. Moreover, our work can be considered as a generalization of [24] in the sense that we can designate which parameters to protect.

II. Problem Formulation

A. Review of Kalman filter

The dynamical and observational models are both assumed in Kalman filter to be linear, and expressible as

$$\mathbf{x}_k = \mathbf{F}_k \mathbf{x}_{k-1} + \mathbf{v}_{k-1}, \tag{1}$$

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{x}_k + \mathbf{n}_k, \tag{2}$$

where $\mathbf{x}_k \in \mathbb{R}^L$ and $\mathbf{z}_k \in \mathbb{R}^N$ are the system's state and observation (measurement), and $\mathbf{F}_k \in \mathbb{R}^{L\times L}$ and $\mathbf{H}_k \in \mathbb{R}^{N\times M}(N \geq L)$ are known matrices defining the linear functions. The state and process noise $\mathbf{v}_{k-1}$ and $\mathbf{n}_k$, which are statistically independent, follow zero-mean Gaussian distribution with covariances being $\mathbf{Q}_{k-1}$ and $\mathbf{R}_k$, respectively.

Kalman filter algorithm contains two distinct phases: "predict" and "update". In the "predict" phase, the state estimate and error covariance are predicted, respectively, by

$$\hat{\mathbf{x}}_{k|k-1} = \mathbf{F}_k \hat{\mathbf{x}}_{k-1|k-1}, \tag{3}$$

$$\mathbf{P}_{k|k-1} = \mathbf{F}_k \mathbf{P}_{k-1|k-1} \mathbf{F}_k^T + \mathbf{Q}_k, \tag{4}$$

with ^{T} denoting transpose operator. In the "update" phase, the state estimate and error covariance are updated, respectively,

through

$$\hat{\mathbf{x}}_{k|k} = \hat{\mathbf{x}}_{k-1|k-1} + \mathbf{K}_k(\mathbf{z}_k - \mathbf{H}_k\hat{\mathbf{x}}_{k|k-1}), \quad (5)$$

$$\mathbf{P}_{k|k} = (\mathbf{I} - \mathbf{K}_k\mathbf{H}_k)\mathbf{P}_{k|k-1}, \quad (6)$$

where $\mathbf{K}_k = \mathbf{P}_{k|k-1}\mathbf{H}_k^T\mathbf{S}_k^{-1}$ denotes the Kalman gain with $\mathbf{S}_k = \mathbf{H}_k\mathbf{P}_{k|k-1}\mathbf{H}_k^T + \mathbf{R}_k$ being the covariance of the innovation term $\mathbf{z}_k - \mathbf{H}_k\hat{\mathbf{x}}_{k|k-1}$.

B. Privacy for Kalman filter

The true state $\mathbf{x}_k$ may be partitioned into two parts as $\mathbf{x}_k = \left[\mathbf{x}_k^{(p)^T}, \mathbf{x}_k^{(q)^T}\right]^T$, where $\mathbf{x}_k^{(p)} \in \mathbb{R}^{L_p}$ contains public state that are shareable with other people whereas $\mathbf{x}_k^{(q)} \in \mathbb{R}^{L_q}$ represents private state containing sensitive information that are accessible only by the authorized parties. The problem that we are going to address is to linearly transform (or compress) $\mathbf{z}_k$ in (2) such that the estimation error of private state $\hat{\mathbf{x}}_{k|k}^{(q)}$ is maximized, while the estimation error of public state $\hat{\mathbf{x}}_{k|k}^{(p)}$ is retained reasonably low. Here, $\hat{\mathbf{x}}_{k|k}^{(p)}$ and $\hat{\mathbf{x}}_{k|k}^{(q)}$ are, respectively, the public and private partitions of $\hat{\mathbf{x}}_{k|k}$ in (5).

To achieve this, a linear mapping from the N-dimensional to the M-dimensional space, $f : \mathbb{R}^N \to \mathbb{R}^M$, $N > M$, is applied:

$$\tilde{\mathbf{z}}_k = \mathbf{C}_k^T\mathbf{z}_k = \underbrace{\mathbf{C}_k^T\mathbf{H}_k}_{:=\tilde{\mathbf{H}}_k}\mathbf{x}_k + \underbrace{\mathbf{C}_k^T\mathbf{n}_k}_{:=\tilde{\mathbf{n}}_k}, \quad (7)$$

where $\tilde{\mathbf{z}}_k \in \mathbb{R}^M$, $\mathbf{C}_k \in \mathbb{R}^{N\times M}$, $\tilde{\mathbf{H}}_k \in \mathbb{R}^{M\times L}$, $\tilde{\mathbf{n}}_k \in \mathbb{R}^M$, and covariance of the compressed $\tilde{\mathbf{n}}_k$ is $\tilde{\mathbf{R}}_k := \mathbf{C}_k^T\mathbf{R}_k\mathbf{C}_k$. After transforming the measurement, the state estimate and error covariance in (5) and (6) become

$$\hat{\mathbf{x}}_{k|k} = \hat{\mathbf{x}}_{k-1|k-1} + \tilde{\mathbf{K}}_k(\tilde{\mathbf{z}}_k - \tilde{\mathbf{H}}_k\hat{\mathbf{x}}_{k|k-1}), \quad (8)$$

$$\tilde{\mathbf{P}}_{k|k} = (\mathbf{I} - \tilde{\mathbf{K}}_k\tilde{\mathbf{H}}_k)\tilde{\mathbf{P}}_{k|k-1}, \quad (9)$$

where $\tilde{\mathbf{K}}_k = \tilde{\mathbf{P}}_{k|k-1}\tilde{\mathbf{H}}_k^T\tilde{\mathbf{S}}_k^{-1}$ with $\tilde{\mathbf{S}}_k = \tilde{\mathbf{H}}_k\tilde{\mathbf{P}}_{k|k-1}\tilde{\mathbf{H}}_k^T + \tilde{\mathbf{R}}_k$ and $\tilde{\mathbf{P}}_{k|k-1} = \mathbf{F}_k\tilde{\mathbf{P}}_{k-1|k-1}\mathbf{F}_k^T + \mathbf{Q}_k$.

The optimal transformation $\mathbf{C}_k$ can be found by solving following two privacy-utility tradeoff problems.

C. Privacy-utility tradeoff at current time step

At current time k, the privacy-utility tradeoff can be cast as the following optimization problem

$$\text{(P1)} \qquad \min_{\mathbf{C}_k} \ \mathrm{Tr}\left(\left[\tilde{\mathbf{P}}_{k|k}\right]_{p,p}\right) - \beta\mathrm{Tr}\left(\left[\tilde{\mathbf{P}}_{k|k}\right]_{q,q}\right)$$

where

$$\tilde{\mathbf{P}}_{k|k} = \begin{bmatrix} \left[\tilde{\mathbf{P}}_{k|k}\right]_{p,p} & \left[\tilde{\mathbf{P}}_{k|k}\right]_{p,q} \\ \left[\tilde{\mathbf{P}}_{k|k}\right]_{p,q}^T & \left[\tilde{\mathbf{P}}_{k|k}\right]_{q,q} \end{bmatrix},$$

and $\left[\tilde{\mathbf{P}}_{k|k}\right]_{p,p} \in \mathbb{R}^{L_p\times L_p}$, $\left[\tilde{\mathbf{P}}_{k|k}\right]_{q,q} \in \mathbb{R}^{L_q\times L_q}$, $\left[\tilde{\mathbf{P}}_{k|k}\right]_{p,q} \in \mathbb{R}^{L_p\times L_q}$, and $\mathrm{Tr}(\cdot)$ denotes the trace operator, and $\tilde{\mathbf{P}}_{k|k}$ defined in (9) is a function of $\mathbf{C}_k$, and the Lagrange parameter β determines the tradeoff between the estimation error of public state and that of private state at current time step.

D. Privacy-utility tradeoff over two time steps

The linear transformation of the system's measurement at time k influences not just the privacy-utility tradeoff at current time step but also that at next time instant. This is because the predicted error covariance $\tilde{\mathbf{P}}_{k+1|k}$ relates to the error covariance $\tilde{\mathbf{P}}_{k|k}$ through (4) i.e. $\tilde{\mathbf{P}}_{k+1|k} = \mathbf{F}_{k+1}\tilde{\mathbf{P}}_{k|k}\mathbf{F}_{k+1}^T + \mathbf{Q}_{k+1}$. Therefore, we consider here a privacy-utility tradeoff over two time steps as below

$$\begin{aligned}\text{(P2)} \ \min_{\mathbf{C}_k} \ & g_{k|k} + \epsilon g_{k+1|k} \\ \text{s.t. } & g_{k|k} = \mathrm{Tr}\left(\left[\tilde{\mathbf{P}}_{k|k}\right]_{p,p}\right) - \beta\mathrm{Tr}\left(\left[\tilde{\mathbf{P}}_{k|k}\right]_{q,q}\right) \\ & g_{k+1|k} = \mathrm{Tr}\left(\left[\tilde{\mathbf{P}}_{k+1|k}\right]_{p,p}\right) - \gamma\mathrm{Tr}\left(\left[\tilde{\mathbf{P}}_{k+1|k}\right]_{q,q}\right),\end{aligned}$$

where $g_{k|k}$ reflects the privacy-utility tradeoff at current time step as described in (P1), while $g_{k+1|k}$ represents the predicted privacy-utility tradeoff which is controlled by the Lagrange parameter γ. The Lagrange parameter ϵ determines the tradeoff between $g_{k|k}$ and $g_{k+1|k}$. When $\epsilon = 0$, (P2) degenerates to (P1). In $g_{k+1|k}$, the block matrices constituting $\tilde{\mathbf{P}}_{k+1|k}$ are constructed in the same ways as those in $\tilde{\mathbf{P}}_{k|k}$

III. Proposed Algorithm

We will solve (P2) by starting solving its special case in (P1).

A. Solution to problem (P1)

We firstly expand $\tilde{\mathbf{P}}_{k|k}$ as

$$\begin{aligned}&\tilde{\mathbf{P}}_{k|k} \\ =&\tilde{\mathbf{P}}_{k|k-1} - \tilde{\mathbf{P}}_{k|k-1}\tilde{\mathbf{H}}_k^T\tilde{\mathbf{S}}_k^{-1}\tilde{\mathbf{H}}_k\tilde{\mathbf{P}}_{k|k-1}, \\ =&\tilde{\mathbf{P}}_{k|k-1} - \tilde{\mathbf{P}}_{k|k-1}\mathbf{H}_k^T\mathbf{C}_k\left(\mathbf{C}_k^T\mathbf{T}_k\mathbf{C}_k\right)^{-1}\mathbf{C}_k^T\mathbf{H}_k\tilde{\mathbf{P}}_{k|k-1},\end{aligned}$$

where $\tilde{\mathbf{S}}_k = \mathbf{C}_k^T\mathbf{T}_k\mathbf{C}_k$ and $\mathbf{T}_k := \mathbf{H}_k\tilde{\mathbf{P}}_{k|k-1}\mathbf{H}_k^T + \mathbf{R}_k$. Replacing $\mathbf{C}_k$ by $\mathbf{T}_k^{-1/2}\mathbf{C}'_k$ leads to

$$\tilde{\mathbf{P}}_{k|k} = \tilde{\mathbf{P}}_{k|k-1} - \tilde{\mathbf{P}}_{k|k-1}\bar{\mathbf{H}}_k^T\mathbf{C}'_k\left(\mathbf{C}'^T_k\mathbf{C}'_k\right)^{-1}\mathbf{C}'^T_k\bar{\mathbf{H}}_k\tilde{\mathbf{P}}_{k|k-1},$$

where $\bar{\mathbf{H}}_k := \mathbf{T}^{-T/2}\mathbf{H}_k$. Let "economy size" singular value decomposition of $\mathbf{C}'_k$ be $\mathbf{U}_k\mathbf{\Lambda}_k\mathbf{V}_k^T$, where $\mathbf{U}_k \in \mathbb{R}^{N\times M}$, $\mathbf{\Lambda}_k \in \mathbb{R}^{M\times M}$ and $\mathbf{V}_k \in \mathbb{R}^{M\times M}$. Then, by the fact that $\mathbf{C}'_k\left(\mathbf{C}'^T_k\mathbf{C}'_k\right)^{-1}\mathbf{C}'^T_k = \mathbf{U}_k\mathbf{U}_k^T$, we have

$$\begin{aligned}\tilde{\mathbf{P}}_{k|k} &= \tilde{\mathbf{P}}_{k|k-1} - \tilde{\mathbf{P}}_{k|k-1}\bar{\mathbf{H}}_k^T\mathbf{U}_k\mathbf{U}_k^T\bar{\mathbf{H}}_k\tilde{\mathbf{P}}_{k|k-1} \\ &= \tilde{\mathbf{P}}_{k|k-1} - \mathbf{G}_k^T\mathbf{U}_k\mathbf{U}_k^T\mathbf{G}_k, \end{aligned} \quad (10)$$

where $\mathbf{G}_k := \bar{\mathbf{H}}_k\tilde{\mathbf{P}}_{k|k-1}$. Now problem in (P1) can be rewritten as

$$\begin{aligned}\min_{\mathbf{U}_k} \ & \mathrm{Tr}\left(\left[\tilde{\mathbf{P}}_{k|k-1}\right]_{p,p} - \left[\mathbf{G}_k\right]_p^T\mathbf{U}_k\mathbf{U}_k^T\left[\mathbf{G}_k\right]_p\right) \\ & - \beta\mathrm{Tr}\left(\left[\tilde{\mathbf{P}}_{k|k-1}\right]_{q,q} - \left[\mathbf{G}_k\right]_q^T\mathbf{U}_k\mathbf{U}_k^T\left[\mathbf{G}_k\right]_q\right) \quad (11) \\ \text{s.t. } & \mathbf{U}_k^T\mathbf{U}_k = \mathbf{I}_M,\end{aligned}$$

where the partition of $\tilde{\mathbf{P}}_{k|k-1}$ is the same as that of $\tilde{\mathbf{P}}_{k|k}$ in (P1), $\mathbf{G}_k = \left[[\mathbf{G}_k]_p, [\mathbf{G}_k]_q\right]$ with $[\mathbf{G}_k]_p$ and $[\mathbf{G}_k]_q$ containing, respectively, the first L_p columns and the remaining L_q columns of $\mathbf{G}_k$, and $\mathbf{I}_M$ is an identity matrix of size $M \times M$. Now instead of finding original transformation $\mathbf{C}_k$, we may alternatively optimize (P1) over $\mathbf{U}_k$ which relates to $\mathbf{C}_k$ via $\mathbf{C}_k = \mathbf{T}_k^{-1/2}\mathbf{U}_k$.

Ignore $\tilde{\mathbf{P}}_{k|k-1}$ which doesn't depend on $\mathbf{U}_k$, the problem in (11) is equivalent to

$$\begin{aligned}\max_{\mathbf{U}_k}\ & \mathrm{Tr}\left([\mathbf{G}_k]_p^T \mathbf{U}_k\mathbf{U}_k^T [\mathbf{G}_k]_p\right) \\ & -\beta\mathrm{Tr}\left([\mathbf{G}_k]_q^T \mathbf{U}_k\mathbf{U}_k^T [\mathbf{G}_k]_q\right) \\ \text{s.t. }& \mathbf{U}_k^T\mathbf{U}_k = \mathbf{I}_M.\end{aligned} \tag{12}$$

The Lagrange function $L(\mathbf{U}_k, \boldsymbol{\lambda})$ of (12) is

$$\begin{aligned}&\sum_{m=1}^{M} [\mathbf{U}_k]_m^T \left([\mathbf{G}_k]_p [\mathbf{G}_k]_p^T - \beta [\mathbf{G}_k]_q [\mathbf{G}_k]_q^T\right) [\mathbf{U}_k]_m \\ &- \lambda_m \left([\mathbf{U}_k]_m^T [\mathbf{U}_k]_m - 1\right),\end{aligned}$$

where $[\mathbf{U}_k]_m$ is the mth column of $\mathbf{U}_k$ and $\boldsymbol{\lambda} = [\lambda_1, \ldots, \lambda_M]^T$ are the Lagrange multipliers. Differentiating of $L(\mathbf{U}_k, \boldsymbol{\lambda})$ with respect to $[\mathbf{U}_k]_m, m = 1, \ldots, M$ and equating to zero leads to

$$\left([\mathbf{G}_k]_p [\mathbf{G}_k]_p^T - \beta [\mathbf{G}_k]_q [\mathbf{G}_k]_q^T\right) [\mathbf{U}_k]_m = \lambda_m [\mathbf{U}_k]_m,$$

which implies the objective of (12) is maximized when $\mathbf{U}_k$ consists of M eigenvectors of $\mathbf{W}_k := [\mathbf{G}_k]_p [\mathbf{G}_k]_p^T - \beta [\mathbf{G}_k]_q [\mathbf{G}_k]_q^T$ associated with its M largest eigenvalues.

B. Solution to problem (P2)

We firstly express the predicted privacy-utility tradeoff $g_{k+1|k}$ in terms of $\mathbf{U}_k$. Based on (4) and (10), $\tilde{\mathbf{P}}_{k+1|k}$ equals to

$$\begin{aligned}&\tilde{\mathbf{P}}_{k+1|k} \\ =&\mathbf{F}_{k+1}\tilde{\mathbf{P}}_{k|k-1}\mathbf{F}_{k+1}^T - \mathbf{F}_{k+1}\mathbf{G}_k^T\mathbf{U}_k\mathbf{U}_k^T\mathbf{G}_k\mathbf{F}_{k+1}^T + \mathbf{Q}_{k+1} \\ =&\mathbf{F}_{k+1}\tilde{\mathbf{P}}_{k|k-1}\mathbf{F}_{k+1}^T - \mathbf{G}_{k+1|k}^T\mathbf{U}_k\mathbf{U}_k^T\mathbf{G}_{k+1|k} + \mathbf{Q}_{k+1},\end{aligned}$$

where $\mathbf{G}_{k+1|k} := \mathbf{G}_k\mathbf{F}_{k+1}^T$. Then, $g_{k+1|k}$ can be written as

$$\begin{aligned}g_{k+1|k} = \mathrm{Tr}&\left(\left[\mathbf{F}_{k+1}\tilde{\mathbf{P}}_{k|k-1}\mathbf{F}_{k+1}^T + \mathbf{Q}_{k+1}\right]_{p,p}\right. \\ &\left. - \left[\mathbf{G}_{k+1|k}\right]_p^T \mathbf{U}_k\mathbf{U}_k^T \left[\mathbf{G}_{k+1|k}\right]_p\right) \\ &- \gamma\mathrm{Tr}\left(\left[\mathbf{F}_{k+1}\tilde{\mathbf{P}}_{k|k-1}\mathbf{F}_{k+1}^T + \mathbf{Q}_{k+1}\right]_{q,q}\right. \\ &\left. - \left[\mathbf{G}_{k+1|k}\right]_q^T \mathbf{U}_k\mathbf{U}_k^T \left[\mathbf{G}_{k+1|k}\right]_q\right),\end{aligned} \tag{13}$$

where $\mathbf{G}_{k+1|k} = \left[\left[\mathbf{G}_{k+1|k}\right]_p, \left[\mathbf{G}_{k+1|k}\right]_q\right]$ is partitioned in the same manner as $\mathbf{G}_k$. Ignoring the terms in $g_{k|k}$ and $g_{k+1|k}$ that are independent of $\mathbf{U}_k$, after some simple manipulations, the problem in (P2) can be reformulated as

$$\begin{aligned}\max_{\mathbf{U}_k}\ & \mathrm{Tr}\left[\mathbf{U}_k^T\mathbf{W}_{k,k+1}\mathbf{U}_k\right] \\ \text{s.t. }& \mathbf{W}_{k,k+1} = \mathbf{W}_k + \epsilon\mathbf{W}_{k+1|k}, \\ & \mathbf{W}_{k+1|k} = \left(\left[\mathbf{G}_{k+1|k}\right]_p \left[\mathbf{G}_{k+1|k}\right]_p^T\right. \\ & \qquad \left. -\gamma \left[\mathbf{G}_{k+1|k}\right]_q \left[\mathbf{G}_{k+1|k}\right]_q^T\right), \\ & \mathbf{W}_k = [\mathbf{G}_k]_p [\mathbf{G}_k]_p^T - \beta [\mathbf{G}_k]_q [\mathbf{G}_k]_q^T \\ & \mathbf{U}_k^T\mathbf{U}_k = \mathbf{I}_M.\end{aligned} \tag{14}$$

Following the same manner as how we solve problem (12), the solution to (14) will be $\mathbf{U}_k$ that consists of M eigenvectors of $\mathbf{W}_{k,k+1}$ associated with its M largest eigenvalues. The original transformation $\mathbf{C}_k$ will be $\mathbf{T}_k^{-1/2}\mathbf{U}_k$.

IV. Discussion and Simulations

In this section, we discuss how different parameters influence the performance of privacy-utility tradeoff at current time step and tradeoff over two time steps, and provide insights by simulations. To facilitate our analysis, we consider $\mathbf{F}_k$ and $\mathbf{H}_k$ to be time-invariant and their entries are drawn independently from uniform distribution in the interval $(0, 1)$. Moreover, the covariances of the state and process noise $\mathbf{Q}_k$ and $\mathbf{R}_k$ are chosen to be $\mathbf{I}_L$ and $\mathbf{I}_N$, respectively. Let the error covariance of the initial state $\mathbf{P}_{0|0}$ be $10\mathbf{I}_L$. For the following simulations, we also fix $N = 20$ and $L = 8$ in which $L_p = 3$ and $L_q = 5$, and $\gamma = \beta = 0.001$.

Figures 1 shows the impact of the dimension M on the privacy-utility tradeoff at current time step. The variance for public state is defined as $\mathrm{Tr}\left(\left[\tilde{\mathbf{P}}_{k|k}\right]_{p,p}\right)$ and that for private state is $\mathrm{Tr}\left(\left[\tilde{\mathbf{P}}_{k|k}\right]_{q,q}\right)$. Here, k goes from 0 to 10, and the results shown in Figures 1 are obtained after 10 time steps. Two values of M i.e. $M = L_p$ and $M = N - L_q$ are critical because it can be proved by Weyl's inequality (due to lack of space we will skip the proof) that $\mathbf{W}_k$ defined in the solution to (P1) has L_p number of positive eigenvalues, L_q number of negative eigenvalues and $N - L$ number of zero eigenvalues. Therefore, the subspace spanned by L_p eigenvectors associated with the L_p largest eigenvalues captures all public information, while the subspace spanned by L_q eigenvectors associated with the L_q smallest eigenvalues retains all private information. Figures 1 shows that both public and private variances will not change in the interval of $L_p \leq M \leq N - L_q$. However, if M is smaller than L_p, not all public information will be captured thus rendering higher public variance. If M is greater than $N - L_q$, some private information will be included thus private variance is decreasing from $M = N - L_q + 1$ onwards. Above observations suggest that M should be chosen between L_p and $N - L_q$ for solving (P1). Note that if $M = N$, then $\mathbf{C}_k$ (or $\mathbf{U}_k$) becomes a square matrix (no data compression anymore) and it degenerates to the original Kalman filter which preserves no privacy.

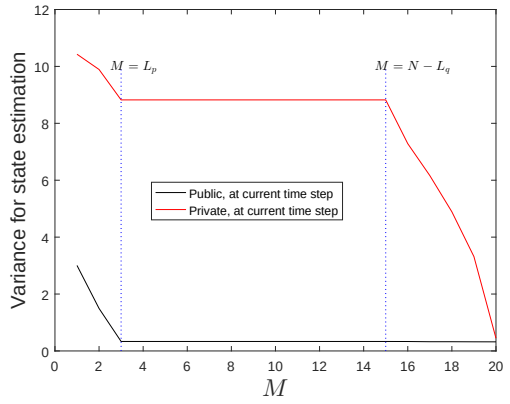

Fig. 1. By solving (P1), public and private variances at current time step vs. transformation dimension M, with $N = 20$, $L_p = 3$ and $L_q = 5$. The results are obtained after 10 time steps.

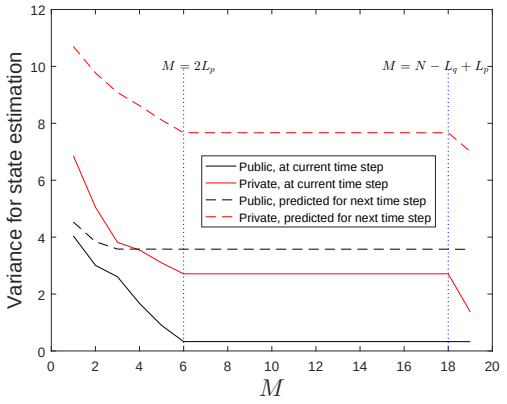

Fig. 2. By solving (P2), public and private variances at current time step and predicted for next time step vs. transformation dimension M. The Lagrange ϵ in (P2) is set to 100, and $N = 20$, $L_p = 3$ and $L_q = 5$. The results are obtained after 10 time steps.

In Figure 2, we study how different M affect problem (P2). The variances at the current time step are defined as same as those in Figure 1. The public and private variances predicted for next time step are defined, respectively, as $\mathrm{Tr}\left(\left[\tilde{\mathbf{P}}_{k+1|k}\right]_{p,p}\right)$ and $\mathrm{Tr}\left(\left[\tilde{\mathbf{P}}_{k+1|k}\right]_{q,q}\right)$. To understand how M affect the privacy-utility tradeoff over two time steps, we need to look into the distribution of eigenvalues of $\mathbf{W}_{k,k+1}$ which is a sum of $\mathbf{W}_k$ and $\epsilon\mathbf{W}_{k+1|k}$, where ϵ is set to 100. It can be proved by Wely's inequality that $\mathbf{W}_{k,k+1}$ has $\min(2L_p, L)$ number of positive eigenvalues and $L - \min(2L_p, L)$ number of negative eigenvalues and the remaining $N - L$ number of eigenvalues are zeros. Recall that $L_p = 3$ and $L_q = 5$ in our setting. Figure 2 shows that the variances for both public and private states keep unchanged for M between $2L_p = 6$ and $N - L_q + L_p = 18$, and all public information will be captured if M is greater than $2L_p$, and some private information will be captured if M is greater than $N - L_q + L_p = 18$. Therefore, we should choose M between $2L_p$ and $N - L_q + L_p$ for solving (P2).

In Figure 3, we study the tradeoff between $g_{k|k}$ (privacy-utility tradeoff at current time step) and $g_{k+1|k}$ (privacy-utility tradeoff predicted for next time step) in (P2) by varying the Lagrange parameter ϵ from 0 to 10000. Now M is fixed at $N - L_q + L_p = 18$, and the results shown in Figure 3 are obtained after 10 time steps. When ϵ is small, the tradeoff between $g_{k|k}$ and $g_{k+1|k}$ is not obvious since the impact of $g_{k+1|k}$ is negligible. From $\epsilon = 100$ onwards, the difference between public and private variances at the current time step starts shrinking indicating worse privacy-utility tradeoff at current time step, whereas the privacy-utility predicted for next time step is improving because the predicted public variance remains almost unchanged while the predicted private variance is increasing.

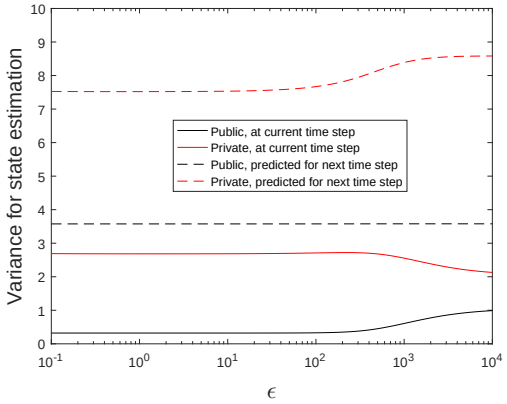

Fig. 3. By solving (P2), public and private variances at current time step and predicted for next time step vs. Lagrange parameter ϵ. Here, M is chosen to be $N - L_q + L_p = 18$. The results are obtained after 10 time steps.

V. Conclusion

In this paper, we have formulated two privacy-preserving problems in a dynamical system. Problem (P1) balances the estimation of public state and that of private state at current time step, and problem (P2) balances them over two time steps. Both problems are formulated based on recursive Bayesian Cramér-Rao bound and optimized over a linear transformation matrix. These two optimization problems can be reformulated as eigenvalue decomposition problems, thus resulting in closed-form solutions. Simulations suggest that M should be chosen in $[L_p, N - L_q]$ for solving (P1) and $[\min(2L_p, L), N - L + \min(2L_p, L)]$ for solving (P2). The impact of ϵ on current and predicted privacy-utility tradeoffs are numerically studied.

Acknowledgments

The research was partially supported by the ST Engineering NTU Corporate Lab through the NRF corporate lab@university scheme Project Reference C-RP10B.

REFERENCES

[1] D. Boneh, E. J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *Proc. Int. Conf. on Theory of Cryptography, Cambridge, MA*, 2005, pp. 325–341.

[2] Y. Ishai and A. Paskin, "Evaluating branching programs on encrypted data," in *Proc. Int. Conf. on Theory of Cryptography, Berlin, Heidelberg*, 2007, pp. 575–594.

[3] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. ACM Symp. on Theory of Computing, Bethesda, MD*, 2009, pp. 169–178.

[4] Y. Wang, X. Wu, and H. Donghui, "Using randomized response for differential privacy preserving data collection," in *Proc. ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining, Washington, D.C.*, 2003, pp. 505–510.

[5] A. D. Sarwate and L. Sankar, "A rate-disortion perspective on local differential privacy," in *Proc. Allerton Conf. on Commun., Control and Computing, Monticello, IL*, 2014, pp. 903–908.

[6] S. Xiong, A. D. Sarwate, and N. B. Mandayam, "Randomized requantization with local differential privacy," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2016.

[7] J. Liao, L. Sankar, F. P. Calmon, and V. Y. Tan, "Hypothesis testing under maximal leakage privacy constraints," arXiv:1701.07099, 2017.

[8] F. du Pin Calmon and N. Fawaz, "Privacy against statistical inference," in *the 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2012.

[9] S. Asoodeh, F. Alajaji, and T. Linder, "Privacy-aware MMSE estimation," in *IEEE International Symposium on Information Theory (ISIT)*, 2016.

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

[11] M. Sun, W. P. Tay, and X. He, "Towards information privacy for the internet of things," in *submitted to IEEE Transactions on Signal Processing*, 2017.

[12] C. Dwork, *Differential Privacy*, 2016.

[13] S. Salamatian, A. Zhang, F. du Pin Calmon, S. Bhamidipati, N. Fawaz, B. Kveton, P. Oliveira, and N. Taft, "How to hide the elephant-or the donkey-in the room: Practical privacy against statistical inference for large data," in *Proc. IEEE Global Conf. on Signal and Information Processing, Austin, TX*, no. 269-272, 2013.

[14] H. Yamamoto, "A source coding problem for sources with additional outputs to keep secret from the receiver or wiretappers," *IEEE Transactions on Information Theory*, vol. 29, no. 6, pp. 918–923, November 1983.

[15] W. Wang, L. Ying, and J. Zhang, "On the relation between identifiability, differential privacy, and mutual-information privacy," *IEEE Transactions on Information Theory*, vol. 62, pp. 5018–5029, 2016.

[16] M. Sun and W. P. Tay, "Inference and data privacy in IoT networks," in *the 18th IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2017.

[17] A. Globerson, G. Chechik, and N. Tishby, "Extracting continuous relevant features," in *Proceedings of the 27th Annual Conference of the Gesellschaft fr Klassifikation e.V., Brandenburg*, 2003, pp. 224–238.

[18] G. Chechik and N. Tishby, "Extracting relevant structures with side information," in *Advances in Neural Information Processing Systems*, 2002, pp. 857–864.

[19] G. Chechik, A. Globerson, N. Tishby, and Y. Weiss, "Information bottleneck for gaussian variables," in *Advances in Neural Information Processing Systems*, 2003.

[20] A. Emad and O. Milenkovic, "Compression of noisy signals with information bottlenecks," in *IEEE Information Theory Workshop (ITW)*, 2013.

[21] A. Makhdoumi, S. Salamatian, and N. Fawaz, "From the information bottleneck to the privacy funnel," in *IEEE Information Theory Workshop (ITW 2014)*, 2014.

[22] S. Y. Kung, "Compressive privacy from information estimation," *IEEE Signal Processing Magazine*, vol. 34, no. 1, pp. 94–112, Janurary 2017.

[23] ——, "A compressive privacy approach to generalized information bottleneck and privacy funnel problems," *Journal of the Franklin Institute*, July 2017.

[24] M. Stein, M. Castaeda, and A. Mezghani, "Information-preserving transformations for signal parameter estimation," *IEEE Signal Processing Letters*, vol. 21, no. 7, pp. 866–870, July 2014.

[25] P. Tichavsky, C. H. Muravchik, and A. Nehorai, "Posterior Cramer-Rao bounds for discrete-time nonlinear filtering," *IEEE Transactions on Signal Processing*, vol. 46, no. 5, pp. 1386–1396, May 1998.