TWO-STAGE ARCHITECTURE OPTIMIZATION FOR DIFFERENTIALLY PRIVATE KALMAN FILTERING

Kwassi H. Degue, Jerome Le Ny

Dept. of Electrical Engineering, Polytechnique Montreal and GERAD, QC H3T-1J4, Canada.

ABSTRACT

The problem of Kalman filtering under a differential privacy constraint is considered in this paper. This problem arises in scenarios where an aggregate statistic must be published in real-time based on privacy-sensitive input signals, which can be assumed to originate from a linear Gaussian model. We propose an architecture combining the differentially private Gaussian mechanism with a linear pre-filter for signal shaping and a Kalman filter for output reconstruction. When the signal shaping block is static, it is shown that the optimum differentially private mechanism following this architecture can be computed using semidefinite programming. Performance improvements over the simpler input perturbation mechanism are illustrated analytically and through computer simulations.

Index Terms— Privacy, Kalman Filtering, Estimation, Filtering, Linear Matrix Inequalities

1. INTRODUCTION

Advances in real-time communication technologies play a major role in the evolution of modern infrastructures, e.g., smart grids or intelligent transportation systems, allowing networks of sensors to perform estimation and fault detection more accurately in these complex systems. However, the raw input signals often consist of privacy-sensitive data collected from individuals, such as location or power consumption traces. In the case of smart metering for example, it has been shown that fine-grained measurements of the electricity consumption of a house allows the inference of many personal details such as when and for how long individual appliances are used [1, 2]. Thus, it becomes essential to develop privacy preserving mechanisms protecting individual users.

Many recent privacy-preserving data analysis approaches rely on the notion of differential privacy [3, 4]. In scenarios where a data holder releases the result of a computation based on private data obtained from individuals, differential privacy guarantees to these individuals that providing their data cannot significantly improve the capability of an adversary to make inferences about them, and in exchange they might derive important benefits from the system. The design of privacy preserving mechanisms for data analysis in static databases has been widely studied in previous work [5, 6, 7]. Much less attention has been devoted to dynamic datasets however [8, 9], and in particular to the design of privacy-preserving model-based dynamic estimators [10, 11, 12, 13].

Many applications such as health monitoring [14] or fault detection [15] require model-based estimators dealing with dynamic, time-varying data streams [16, 17]. The main contribution of this paper is to design a new differentially private Kalman filter for dynamic data modelled as the output of a linear Gaussian system, revisiting our previous work in [18, 11]. In these papers, a differentially private filter was designed by adding privacy-preserving noise either directly on the measured signals (input perturbation), or on the released signal (output perturbation). Moreover, a two-stage approximation architecture for differentially private filtering, generalizing both the input and output perturbation mechanisms, is proposed in [19, 11], but has not yet been applied to differentially private Kalman filtering, which is the goal of this paper. We also consider the design of time-varying filters, whereas our previous work only considered the steady-state case. Similar two-stage architectures are considered for example in [6] for batch processing systems, in [20] for an information-theoretic constraint replacing differential privacy in a related Kalman filter design problem, and are in fact reminiscent of joint transmitter-receiver design problems in the communication literature [21, 22].

Section 2 of this paper provides some background on differential privacy and presents the problem statement. In Section 3, we illustrate in a scalar example that a two-stage architecture can provide significant improvement over the input perturbation mechanism. Section 4 describes this architecture more generally, which uses a linear transformation of the inputs signals followed by the standard Gaussian mechanism for differential privacy and finally a Kalman filter. It is shown that the problem of optimizing the input linear transformation can be cast as a Semidefinite Program (SDP). Subsection 4.4 describes an application to syndromic surveillance systems.

Notation: Throughout this paper, we fix a generic probability triple \((\Omega, F, P)\), where \(F\) is a \(\sigma\)-algebra on \(\Omega\) and \(P\) a probability measure defined on \(F\). We denote the \(\ell_p\)-norm of
a vector \( x \in \mathbb{R}^k \) by \( |x|_p := \left( \sum_{i=1}^k |x_i|^p \right)^{1/p}, \) for \( p \in [1, \infty] \). For a matrix \( A \), the induced 2-norm is denoted \( ||A||_2 = \sqrt{\text{Tr}(A^T A)} \). Finally, for a signal \( x \) we denote \( x^t := \{x_0, \ldots, x_t\} \).

## 2. PROBLEM STATEMENT

Consider a set of \( n \) measured and privacy-sensitive signals \( \{y_i[t]\}_{0 \leq t \leq T}, i = 1, \ldots, n \), with \( y_i[t] \in \mathbb{R}^p \), which could originate from \( n \) distinct individuals for example. We assume that a model explaining this data is publicly known, and consists of a linear system with \( n \) individual vector-valued independent states corresponding to the \( n \) measured signals

\[
x_{i, t+1} = A_{i,t} x_{i,t} + w_{i,t}, \quad t = 0, 1, \ldots, T - 1, \quad (1)
\]

\[
y_{i,t} = C_{i,t} x_{i,t} + v_{i,t}, \quad t = 0, 1, \ldots, T,
\]

for \( i = 1, \ldots, n \), where \( x_{i,t}, w_{i,t} \in \mathbb{R}^p \), with \( w_{i,t} \sim \mathcal{N}(0, W_{i,t}) \) and \( v_{i,t} \sim \mathcal{N}(0, V_{i,t}) \) independent sequences of iid zero-mean Gaussian random vectors with covariance matrices \( W_{i,t}, V_{i,t} > 0 \), for \( i = 1, \ldots, n \). The initial conditions \( x_{i,0} \) are Gaussian random vectors independent of the noise processes \( w_t \) and \( v_t \), with mean \( \Sigma_{i,0} \) and covariance matrices \( \Sigma_{i,0} \) assumed invertible.

A data aggregator aims at releasing a causal minimum mean square estimator \( \hat{y}_i \) of a given set of positive numbers, and \( \hat{y}_i \) for all \( i \) in (2). We also let \( T \to \infty \) and consider the steady-state mean squared error (MSE) \( \lim_{T \to \infty} \sum_{t=0}^T \mathbb{E} \|z_t - \hat{z}_t\|^2 \) as performance measure of a given estimate \( \hat{z} \) of \( z \).

### Basic Differentially Private Mechanism.

Let \( \mathcal{H} \) be a space of datasets of us, in our case, the space of global measurement signals \( y \) with \( y = [y_1^T, \ldots, y_n^T]^T \). A mechanism \( M \) is a random map from \( \mathcal{H} \) to some measurable output space \( \mathcal{O} \). We introduce for a given application a symmetric binary relation Adj on \( \mathcal{H} \), called adjacency \[24\]. For our scenario, we define an adjacency relation by

\[
\text{Adj}(y, y') \iff \|y_i - y'_i\|_2 \leq \rho_i, \quad (2)
\]

and \( y_j = y'_j \) for all \( i \neq j \), with \( \{\rho_i\}_{i=1}^n \in \mathbb{R}^n_+ \) a given set of positive numbers, and

\[
\|v\|_2 := \left( \sum_{i=0}^T |v_i|^2 \right)^{1/2}
\]

where \( |\cdot|_2 \) denotes the Euclidean (vector) norm. Hence, two adjacent global measurement signals differ by the values of a single participant, with only bounded signal deviations allowed for each individual. Differentially private mechanisms produce randomized outputs with distributions that are close for adjacent inputs \[1\].

### Definition 1.

Let \( \mathcal{H} \) be a space equipped with a symmetric binary relation denoted Adj, and let \( (\mathcal{O}, \mathcal{M}) \) be a measurable space, where \( \mathcal{M} \) is a given \( \sigma \)-algebra over \( \mathcal{O} \). Let \( \epsilon, \delta \geq 0 \). A randomized mechanism \( M \) from \( \mathcal{H} \) to \( \mathcal{O} \) is \( (\epsilon, \delta) \)-differentially private (for \( \text{Adj} \)) if for all \( h, h' \in \mathcal{H} \) such that \( \text{Adj}(h, h') \),

\[
\mathbb{P}(M(h) \in S) \leq e^\epsilon \mathbb{P}(M(h') \in S) + \delta, \forall S \in \mathcal{M}. \quad (3)
\]

### Definition 2.

Let \( \mathcal{H} \) be equipped with an adjacency relation \( \text{Adj} \). Let \( \mathcal{O} \) be a vector space with norm \( \parallel \cdot \parallel_\mathcal{O} \). The sensitivity of a query \( q : \mathcal{H} \to \mathcal{O} \) is \( \Delta_{\mathcal{O}q} := \sup_{(h, h') \in \text{Adj}(h, h')} \|q(h) - q(h')\|_\mathcal{O} \). In particular, for \( \mathcal{O} = \mathbb{R}^k \) (with \( k \) possibly equal to \( +\infty \)) equipped with the \( p \)-norm for \( p \in [1, \infty] \), this defines the \( \ell_p \)-sensitivity, denoted \( \Delta_{\ell_p} q \).

The Gaussian mechanism \[5\] consists in adding Gaussian noise proportional to the \( \ell_2 \)-sensitivity to provide \( (\epsilon, \delta) \)-differentially private. We follow here the presentation in \[11\] and consider queries that are dynamical systems with vector-valued input and output signals. Let us define the Q-function \( Q(x) := \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp(-u^2/2)du \) and \( \kappa_{\delta, \epsilon} = \frac{1}{\sqrt{2\pi}} (\mu + \sqrt{\mu^2 + 2\epsilon}), \) with \( \mu = Q^{-1}(\delta) \).

### Theorem 1.

Let \( G \) be a system with \( p \) inputs and \( q \) outputs. Then the mechanism \( M(y) = G y + \nu \), where \( \nu \) is sequence of iid Gaussian vectors with covariance matrix \( \kappa_{\delta, \epsilon}^2 (\Delta_2 G)^2 I_q \), is \( (\epsilon, \delta) \)-differentially private.

### Definition 3.

By resilience to post-processing \[24\], the differentially private signal produced by Theorem 1 can then be processed by a Kalman filter taking into account the privacy-preserving noise \( \nu \) to produce \( \hat{z} \). When \( G = I \), this leads to the input perturbation mechanism discussed in \[18\]. In the rest of this paper, we study more general transformations for \( G \).

### 3. A SCALAR EXAMPLE

The purpose of this section is to illustrate via a simple example with scalar signals that one can improve the performance of the input mechanism significantly by properly combining the input signals before adding the privacy-preserving noise. Consider the scalar case of model \( (1) \) with \( A_{i,t} = a, C_{i,t} = c, W_{i,t} = \sigma^2_w, V_{i,t} = \sigma^2_v \) and \( L_{i,t} = 1 \) (so \( z_t = \sum_{i=1}^n x_{i,t} \)), and assume \( \rho_i := \rho \) for all \( i \) in (2). We also let \( T \to \infty \) and consider the steady-state mean squared error (MSE)

\[
\lim_{T \to \infty} \frac{1}{p} \sum_{t=0}^T \mathbb{E} \|z_t - \hat{z}_t\|^2
\]

as performance measure of a given estimate \( \hat{z} \) of \( z \).

The input perturbation architecture proposed in \[18\] is shown on Fig.1 and is equivalent to the global system

\[
x_{i+1} = A_i x_i + w_i,
\]

\[
y_i = C_i x_i + v_i,
\]

with \( A_i = a I_n, w_i = [w_{i,1} \ldots w_{i,n}]^T, C_i = c I_n \) and \( v_i = [v_{i,1} \ldots v_{i,n}]^T \). Let \( \gamma = \kappa_{\delta, \epsilon} \rho \). Since
\[
\begin{align*}
\text{Fig. 1:} \quad & \text{Differential private Kalman filtering architectures.} \\
\sup_{y,y':A_d(y,y')} \| y - y' \|_2 = \rho, \text{ by Theorem 1}\quad & \text{releasing} \\
\text{with } s_t = y_t + \zeta_t, \text{ with } \zeta_t \sim \mathcal{N}(0, \gamma^2 I_n), \text{ is } (\epsilon, \delta)-\text{differentially private for the adjacency relation (2).} \\
\text{Solving the ARE for } & \hat{z}_t \text{ leads to the following MSE expression for } \hat{z} \\
\text{Fig. 1b, we construct a differentially private estimate } \hat{z}_t \text{ of } z_t \text{ by first multiplying the global signal } y \text{ with a constant matrix } D = [D_1 \ D_2 \ \ldots \ D_n], \text{ with } D_i \in \mathbb{R}^{q \times p_i}. \\
\text{Then, we add white Gaussian noise } \zeta_i \text{ according to the Gaussian mechanism, in order to make the signal } s_t \text{ differentially private, with} \\
\text{Finally, we construct a causal minimum mean square error estimator } \hat{x}_t \text{ of } x_t \text{ from } s_t, \text{ for which it is optimal to use a Kalman filter, since the system producing } s_t \text{ is still linear and Gaussian. We then let } \hat{x}_t = \sum_{i=1}^{n} L_i \hat{x}_t := L \hat{x}_t. \\
\text{For measurement signals } y \text{ and } y' \text{ adjacent according to (2) and differing in user } i, \text{ we have} \\
\text{From Theorem 1 releasing } s_t = Dy_t + \zeta_t, \text{ with } \zeta_t \sim \mathcal{N}(0, (\kappa_{\delta, \epsilon} \Delta_2 D)^2 I_q), \text{ is } (\epsilon, \delta)-\text{differentially private for the adjacency relation (2).} \\
\end{align*}
\]

4. DESIGN OF THE TWO-STAGE MECHANISM

We are now interested in designing the matrix \( D \) in Fig.1b for the more general situation presented in Section 4. Consider the \( n \) individual dynamics 4. They form a global system whose dynamics can be expressed as (4), with \( A_t \) and \( C_t \) block-diagonal matrices having respectively \( A_{t,t} \) and \( C_{t,t} \) on their diagonal, \( w_t = [w_{1,t}^T \ \ldots \ w_{n,t}^T]^T \) and \( v_t = [v_{1,t}^T \ \ldots \ v_{n,t}^T]^T \). Denote by \( W_t = \text{diag}(W_{1,t}, \ldots, W_{n,t}) \) and \( V = \text{diag}(V_1, \ldots, V_n) \) the covariance matrices of respectively \( w_t \) and \( v_t \). Following Fig.1b, we construct a differentially private estimate \( \hat{z}_t \) of \( z_t \) by first multiplying the global signal \( y \) with a constant matrix \( D = [D_1 \ D_2 \ \ldots \ D_n], \) with \( D_i \in \mathbb{R}^{q \times p_i} \) to be designed and \( q \) to be determined.

Recall that we are given the initial covariance matrix \( \Sigma_0 = \text{diag}(\Sigma_{0,1}, \ldots, \Sigma_{0,n}) \) for the state \( x_0 \). With the matrix \( D \) left to design, the estimator \( \hat{z}_t = L_i \hat{x}_t \) of \( z_t = L_i x_t \) with minimum \( MSE \), defined as \( \frac{1}{T+1} \sum_{t=0}^{T} \mathbb{E} \left[ \| z_t - \hat{z}_t \|^2 \right] \), is obtained by finding \( D^* \) and the covariance matrices \( \Sigma_t^* \) solving the fol-
lowing optimization problem

\[
\begin{align*}
\min_{\Sigma_t > 0, D} & \quad \frac{1}{T + 1} \sum_{t=0}^{T} \text{Tr}(L_t \Sigma_t L_t^T) \\
\text{s.t.} & \quad \Sigma_0^{-1} = \Sigma_0^{-1} + C_0^T C_0, \\
\Sigma_{t+1}^{-1} = (A_t \Sigma_t A_t^T + W_t)^{-1} & \quad + C_t^T C_{t+1}, \quad 0 \leq t \leq T - 1, \\
\Pi = D^T (DV D^T + \kappa_{\delta, \epsilon}^2 (\Delta_2 D)^2 I_q)^{-1} D. & \quad (10d)
\end{align*}
\]

Indeed, the Kalman filter gains necessary to construct \( \hat{z}_t \) can be computed from the optimal covariance matrices. With \( V > 0 \), we can deduce an equivalent form of \((10d)\) by using the matrix inversion lemma again

\[
\Pi = V^{-1} - V^{-1} \left( V^{-1} + \frac{D^T D}{\kappa_{\delta, \epsilon}^2 (\Delta_2 D)^2} \right)^{-1} V^{-1},
\]

from which we obtain

\[
k_{\delta, \epsilon}^2 \left[ (V - \text{VIIV})^{-1} - V^{-1} \right] = \frac{D^T D}{\Delta_2 D^2}.
\]

4.2. Semidefinite Programming-based Synthesis

Here we show that the optimization problem \((10a)-(10d)\) can be recast as an SDP and hence solved efficiently \cite{Luo}, if we impose the following additional constraint on \( D \)

\[
\Delta_2 D = \rho_1 ||D_1||_2 = \ldots = \rho_n ||D_n||_2. \quad (13)
\]

The following Lemma shows that no loss of performance occurs by adding the constraint \((13)\) to \((10a)-(10d)\), i.e., that this constraint is satisfied automatically by a matrix \( D^* \) that is optimal for \((10a)-(10d)\).

**Lemma 1.** For any feasible solution \( \{D, \Sigma_t\}_t \) of \((10a)-(10d)\) that does not satisfy \((13)\), there exists a feasible solution that does satisfy this constraint and gives a lower or equal cost. In particular, there exists an optimum solution to \((10a)-(10d)\) such that the D matrix satisfies \( \Delta_2 D := \max_{j} \{ \rho_j ||D_j||_2 \} = \rho_i ||D_i||_2 \) for all \( 1 \leq i \leq n \).

**Proof.** Consider a feasible solution \( \{D, \Sigma_t\}_t \) for \((10a)-(10d)\). If \((13)\) is not satisfied by \( D \), construct the matrix \( M = D^T D + \text{diag} (\{ \eta_i L_{p_i} \})_{1 \leq i \leq n} \), with \( \eta_i = (\Delta_2 D/\rho_i)^2 - ||D_i||_2^2 \). Then the diagonal block \( i \) of \( M \) is \( M_{i} = D_i^T D_i + [(\Delta_2 D/\rho_i)^2 - ||D_i||_2^2] I_{p_i} \), which has maximum eigenvalue \( \Delta_2 D/\rho_i \). Define some matrix \( \tilde{D} \) such that \( \tilde{D}^T D = M \) and group the columns of \( D \) as \( \tilde{D} = [D_1 \ldots D_n] \) following the notation for the columns of \( D \). In particular \( M_i = D_i^T D_i \), so \( \tilde{D}_i^T D_i \) has maximum eigenvalue \( \Delta_2 D/\rho_i \) and hence \( \tilde{D}_i \) has maximum singular value \( \Delta_2 D/\rho_i \). In other words, \( \tilde{D} \) satisfies \((13)\) with a sensibility \( \Delta_2 D = \Delta_2 \tilde{D} \) that is unchanged, and moreover \( \tilde{D}^T D = M \geq D^T D \).

Hence \( \Delta_2 D \) in the denominator of \((11)\) remains unchanged, and moreover

\[
\left( V^{-1} + \frac{D^T D}{(\kappa_{\delta, \epsilon} \Delta_2 D)^2} \right)^{-1} \leq \left( V^{-1} + \frac{D^T D}{(\kappa_{\delta, \epsilon} \Delta_2 D)^2} \right)^{-1} \]

where \( \tilde{\Pi} \) and \( \Pi \) are defined according to \((11)\) for \( \tilde{D} \) and \( D \) respectively. Let \( K := \tilde{\Pi} - \Pi \geq 0 \).

Replacing \( \Pi \) by \( \tilde{\Pi} \) in \((10b)\), we obtain a matrix \( \tilde{\Sigma}_0 \) satisfying \( \tilde{\Sigma}_0^{-1} = \Sigma_0^{-1} + C_0^T K C_0 \geq \Sigma_0^{-1}, \) so \( \tilde{\Sigma}_0 \leq \Sigma_0 \). Now if we have two matrices \( \tilde{\Sigma}_t \leq \Sigma_t, \) and \( \tilde{\Sigma}_{t+1}, \Sigma_{t+1} \) defined according to \((10b)\) together with \( \tilde{\Pi} \) and \( \Pi \), then immediately

\[
\tilde{\Sigma}_{t+1}^{-1} = (A_t \tilde{\Sigma}_t A_t^T + W_t)^{-1} + C_t^T \tilde{\Pi} C_{t+1} \geq (A_t \Sigma_t A_t^T + W_t)^{-1} + C_t^T \Pi C_{t+1} \geq \tilde{\Sigma}_{t+1}^{-1} + C_{t+1}^T K C_{t+1}.
\]

In particular \( \tilde{\Sigma}_{t+1} \leq \Sigma_{t+1} \). Hence, by recursion, we construct a feasible solution \( \{ \tilde{D}, \tilde{\Sigma}_{t+1} \} \) such that \( \tilde{\Sigma}_t \leq \Sigma_t \) for all \( t \geq 0 \). This gives a smaller or equal cost

\[
\frac{1}{T + 1} \sum_{t=0}^{T} \text{Tr}(L_t \tilde{\Sigma}_t L_t^T) \leq \frac{1}{T + 1} \sum_{t=0}^{T} \text{Tr}(L_t \Sigma_t L_t^T),
\]

and so the lemma is proved. \( \square \)

By Lemma 1, we can add without loss of optimality the constraint \((13)\) to \((10a)-(10d)\), which allows us in the following to recast the problem as an SDP. Let \( p := \sum_{i=1}^{n} p_i \), and let \( \alpha_i = \kappa_{\delta, \epsilon} \rho_i \), for all \( 1 \leq i \leq n \). Denote \( E_i = [0 \ldots 0_{p_i} 0_{p_i} 0_{p_i}]^T \) the \( p \times p \) matrix whose elements are zero except for an identity matrix in its \( i \)-th block. The following lemma converts constraints \((12)-(13)\) to a form that is appropriate for an SDP.

**Lemma 2.** If \( \Pi, D \) satisfy the constraints \((12)-(13)\), then \( \Pi \) satisfies \( V - \text{VIIV} \geq 0 \) together with the following constraints, for all \( 1 \leq i \leq n \),

\[
\begin{bmatrix}
I_{p_i} / \alpha_i^2 + V_{i}^{-1} & E_i^T \\
E_i & V - \text{VIIV}
\end{bmatrix} \geq 0,
\]

and not \( \begin{bmatrix}
I_{p_i} / \alpha_i^2 + V_{i}^{-1} & E_i^T \\
E_i & V - \text{VIIV}
\end{bmatrix} \prec 0 \).

Conversely, if \( \Pi \) satisfies these constraints, then there exists a matrix \( D \) such that \( \Pi, D \) satisfy \((12)-(13)\). One such \( D \) can be obtained by the factorization of \( \kappa_{\delta, \epsilon}^2 (V - \text{VIIV})^{-1} - V^{-1} \) = \( D^T D \) (e.g., via singular value decomposition), and will then satisfy \( \Delta_2 D = 1 \).

**Proof.** \( V - \text{VIIV} \geq 0 \) is immediate from \((11)\), since it is equal to \( \left( V^{-1} + \frac{D^T D}{(\kappa_{\delta, \epsilon} \Delta_2 D)^2} \right)^{-1} \).
Next, we see from (12) that rescaling $D$ to $\lambda D$ for any
$\lambda \neq 0$ does not impact the constraint. Hence, we can restrict
without loss of generality our design to $\Delta_2 D = 1$. Together
with (13), the right-hand side of (12) then represents any posi-
tive semidefinite matrix $M = \lambda D_1 / D_2$ satisfying the
constraints that its diagonal blocks $M_{ii} = D_i^T D_i$ have maximum eigen-
value equal to $1 / \rho_i^2$, since $||D_i||_2 = 1 / \rho_i$ by (13). These
constraints are equivalent to saying that for all $1 \leq i \leq n$,
\[ E^T_i \left[ (V - V_i \Pi) - V^{-1} \right] E_i \preceq I_{p_i} / \alpha^2_i, \tag{14} \]
and not \[ E^T_i \left[ (V - V_i \Pi) - V^{-1} \right] E_i \prec I_{p_i} / \alpha_i, \tag{15} \]
Indeed, this comes from the standard fact that the maximum
value $\lambda_{i, \max}$ of $M_i$ is the smallest $\lambda$ satisfying $M_i \preceq \lambda I_{p_i}$.
The constraints given in the Lemma are obtained by taking
Schur complements in (14) and (15).

Note that the fact that the left-hand side of (12) is positive
semidefinite is a simple consequence of $V \succeq V - V_i \Pi$, hence adding the constraint $(V - V_i \Pi)^{-1} - V^{-1} \succeq 0$ is
unnecessary.

Next, define the information matrices $\Omega_t = \Sigma_t^{-1}$. If the
matrices $W_t$ are invertible, denoting $E_t = W_t^{-1}$ and using the
matrix inversion lemma in (10c), one gets
\[ C_{t+1} \Pi C_{t+1} - \Omega_{t+1} + \Xi_t - \Xi_t A_t (\Omega_t + A_t \Xi_t A_t)^{-1} A_t^T \Xi_t = 0. \tag{16} \]
Replacing the equality in (16) by $\geq 0$ and taking a Schur
complement, together with the inequalities of Lemma 2, leads to the
following SDP with variables $\Pi \succeq 0, \{X_t \succeq 0, \Omega_t > 0 \}_{t=0}^T$:
\[
\min_{X_t, \Omega_t, \Pi} \frac{1}{T+1} \sum_{t=0}^T \text{Tr}(X_t) \quad \text{s.t.} \quad \tag{17a}
\begin{align*}
X_t & \preceq L_t \Omega_t, \\
L_t^T & \Omega_t \preceq 0, \quad 0 \leq t \leq T, \\
\Omega_0 & = \Sigma_0^{-1} + C_0^T \Pi C_0, \\
C_{t+1} \Pi C_{t+1} - \Omega_{t+1} + \Xi_t - \Xi_t A_t (\Omega_t + A_t \Xi_t A_t)^{-1} A_t^T \Xi_t & \succeq 0, \\
0 & \leq t \leq T - 1, \\
I_{p_i} / \alpha_i^2 + V_i^{-1} E_i^T & \succeq 0, \quad 1 \leq i \leq n. \tag{17c}
\end{align*}
\]
Here the minimization of the cost (10a) has been replaced by the
minimization of (17a), after introducing the slack variable $X_t$ satisfying (17b), or equivalently $X_t \succeq L_t \Omega_{t+1} L_t^T$ by taking a Schur complement. We also used the fact that $E_i^T V_i^{-1} E_i = V_i^{-1}$ in (17c). Once an optimal solution for this
SDP is obtained, we recover an optimal matrix $D$ from $\Pi$ by a
singular value decomposition as explained in Lemma 2.

**Theorem 2.** Let $\Pi^* \succeq 0, \{X_t^* \succeq 0, \Omega_t^* > 0 \}_{0 \leq t \leq T}$ be an
optimal solution for (17a)-(17c). Suppose that for some $0 \leq t \leq T$, we have $L_t (\Omega_t^{-1} - C_t^T) \neq 0$. Then there exists a matrix
$D^*$ such that $||D_t^*||_2 = 1 / \rho_i$ for $1 \leq i \leq n$, satisfying (12)
for $\Pi^*$, and hence (10d). Moreover, one can construct matrices $\Sigma_t^*$ from the sequence $\Omega_t^*$, which together with $D^*$ constitute
an optimal solution for (10a)-(10d) under the additional constraint (13). Finally, the optimal costs of (10a)-(10d) and
(17a)-(17c) are equal, i.e., the SDP relaxation is tight.

**Remark 1.** The condition $L_t (\Omega_t^*)^{-1} C_t^T \neq 0$ for some $t$
appears to be a weak requirement to guarantee the possibility of
reconstructing the matrix $D$, but in future work we would
like to provide a more explicit condition directly in terms of
the problem parameters.

**Remark 2.** The proof shows explicitly in (13) how to construct the sequence $\Sigma_t^*$. The procedure can be shown to reduce to $\Sigma_t^* = (\Omega_t^*)^{-1}$ under certain conditions, such as
$L_t$ invertible for all $t$. Note however that in practice, we are
mostly interested in $D^*$, from which the design of the Kalman
filter and the computation of its estimation performance can
also be recovered by other standard methods, e.g., based on
the Riccati difference equations (10b)-(10c).

**Proof.** Consider $\Pi^*, \{X_t^*, \Omega_t^* \}_{t=0}^T$ an optimal solution of the
SDP (17a)-(17c). One can remark that inequality (17c)
is equivalent to
\[ \alpha_i^2 E_i^T \left[ (V - V_i \Pi)^{-1} - V^{-1} \right] E_i \succeq I_{p_i} \]
by taking a Schur complement. We show that we cannot have
\[ \alpha_i^2 E_i^T \left[ (V - V_i \Pi)^{-1} - V^{-1} \right] E_i \prec I_{p_i}. \]
Indeed, otherwise there exists $\eta > 0$ such that the matrix $\hat{\Pi} = \Pi^* + \eta I_{p_i}$
still satisfies (17c). Using this matrix $\hat{\Pi}$ in (17c), we obtain a
matrix $\tilde{\Omega}_0 = \Omega_0^* + \eta C_0^T C_0$ feasible for (17c).
Now define $\Omega_t = \Omega_t^* + \eta C_t^T C_t$. One can immediately check that $\hat{\Pi}, \tilde{\Omega}_0$ and $\tilde{\Omega}_0$ satisfy
(17d) for $t = 0$, using the fact that $\Omega_0^*, \Omega_t^*, \Pi^*$
are feasible and that $C_t^T C_t \succeq 0$. Similarly one checks that
the matrices $\tilde{\Omega}_t = \Omega_t^* + \eta C_t^T C_t$ are feasible in (17c)
for all $0 \leq t \leq T$. Now in (17b), taking a Schur complement, we
obtain that the matrices $X_t = L_t \tilde{\Omega}_t^{-1} L_t^T$ are feasible. By the
matrix inversion lemma we can write
\[ \tilde{X}_t = X_t^* - L_t (\Omega_t^*)^{-1} C_t^T K_t C_t (\Omega_t^*)^{-1} L_t^T. \]
for some matrices $K_t > 0$. These matrices $\tilde{X}_t$ give a cost
\[ \frac{1}{T+1} \sum_{t=0}^T \text{Tr}(X_t^*) - \| L_t (\Omega_t^*)^{-1} C_t^T K_t^2 / 2 \|_F, \]
which is a strict improvement over the assumed optimal solution as soon as
one matrix $L_t (\Omega_t^*)^{-1} C_t^T$ is not zero (since the $K_t$’s are invertible).
Hence, we have a contradiction and so we cannot have
\[ \alpha_i^2 E_i^T \left[ (V - V_i \Pi)^{-1} - V^{-1} \right] E_i \prec I_{p_i}. \]
This proves that $\Pi^*$ satisfies (10d).
Note that the optimum value $V^*$ of (17a)-(17e) is at most that of (10a)-(10d), since the constraints have been relaxed. We now show how to construct a sequence $\Sigma_t^*$, which together with $\Pi_t^*$ satisfy the constraints of (10a)-(10d) and achieve the same cost $V^*$, thereby proving the remaining claims of the theorem. Note that since $\Omega_t^* + A_t^T \Xi_t A_t \succeq 0$, (17d) is equivalent to $R_t(\Omega_t^*, \Omega_{t+1}^*) \succeq 0$, where

$$R_t(\Omega_1, \Omega_2) := C_t^T \Pi_t^* C_{t+1} - \Omega_2 - \Xi_t - \Xi_t A_t(\Omega_1 + A_t^T \Xi_t A_t)^{-1} A_t^T \Xi_t.$$ 

First, we take $\Sigma_t^0 = (\Omega_t^*)^{-1}$. If $R_t(\Omega_t^*, \Omega_{t+1}^*) = 0$ for all $0 \leq t \leq T - 1$, then the matrices $\Omega_t^*$ satisfy (16) and we can take $\Sigma_t^* = (\Omega_t^*)^{-1}$ for all $t$, since these matrices satisfy the equivalent condition (10c). Otherwise, let $\tilde{t}$ be the first time index such that $R_t(\Omega_t^*, \Omega_{t+1}^*)$ is not zero. For $t \leq \tilde{t}$, we take $\Sigma_t^* = (\Omega_t^*)^{-1}$ and so in particular we have $R_t((\Sigma_t^*)^{-1}, \Omega_{t+1}^*) \succeq 0$ and not zero. Consider the matrix $\tilde{\Omega}_{t+1}^* = \Omega_t^* + R_t(\Omega_t^*, \Omega_{t+1}^*)$, which then satisfies $R_t(\tilde{\Omega}_t^*, \tilde{\Omega}_{t+1}^*) = 0$ by definition. We set $\Sigma_{t+1}^* = \tilde{\Omega}_{t+1}^*$.

Now note that we again have $R_{\tilde{t}+1}((\Sigma_{\tilde{t}+1}^*)^{-1}, \tilde{\Omega}_{\tilde{t}+2}^*) \succeq 0$, by verifying that (17d) is satisfied at $t + 1$, using the fact that $(\Sigma_{\tilde{t}+1}^*)^{-1} = \tilde{\Omega}_{\tilde{t}+1}^* \succeq \Omega_{\tilde{t}+1}^*$. From here we can proceed by immediate induction, assuming that $\Sigma_t^*, \ldots, \Sigma_{\tilde{t}}^*$ are set and taking

$$\Sigma_{\tilde{t}+1}^* = (\tilde{\Omega}_{\tilde{t}+1}^*)^{-1} := (\Omega_{\tilde{t}+1}^* + R_t((\Sigma_{\tilde{t}+1}^*)^{-1}, \Omega_{\tilde{t}+1}^*))^{-1},$$

which reduces to $(\Omega_{\tilde{t}+1}^*)^{-1}$ if $R_t((\Sigma_{\tilde{t}+1}^*)^{-1}, \Omega_{\tilde{t}+1}^*) = 0$.

The procedure above provides a solution $\Pi_t^*, (\Sigma_t^*)^T_{t=0}$ satisfying the constraints of the original program (10a)-(10d). Because by construction we have $(\Sigma_t^*)^{-1} \succeq \Omega_t^*$ and the matrices $(\Sigma_t^*)^{-1}$ also satisfy (17d), taking $\Omega_t = (\Sigma_t^*)^{-1}$ in (17a)-(17e) gives a cost $V$ for (17a) that is at most the cost $V^*$ corresponding to $\Omega_t^*$, hence equal to $V^*$ by optimality of $\Omega_t^*$. But this cost $V$ is equal to $\frac{1}{T} \sum_{t=0}^{T-1} \text{Tr}(L_t \Sigma_t^* L_t^T)$ of (10a). Hence, we have shown that (10a)-(10d) and (17a)-(17e) have the same value, and constructed an optimal solution $\Pi^*, (\Sigma_t^*)^T_{t=0}$ to (10a)-(10d), achieving this value.

\[\square\]

4.3. Stationary problem

In the stationary case ($T \to \infty$), with the model (4) now assumed time-invariant, a time-invariant filter and a matrix $D$ can be constructed by solving the following SDP with variables $\Pi \succeq 0, X \succeq 0, \Omega \succeq 0$.

\[
\min_{\Pi, X, \Omega, \Omega} \text{Tr}(X) \quad \text{s.t.} \quad \begin{bmatrix} X & L \\ L^T & \Omega \end{bmatrix} \succeq 0, \\
C^T \Pi C - \Omega \succeq \Xi A \succeq 0, \\
I_{p_i} + \frac{1}{2} V_{i-1} E_i^T V - V_i \succeq 0, \quad 1 \leq i \leq n. \tag{19d}
\]

4.4. Application Example

Consider a scenario where the Public Health Services have to publish the number $E_t$ of people in a population exposed/infected by a disease, using data collected from $n = 10$ hospital emergency departments, to perform epidemic outbreak detection. The states $x_{i,t}$ evolve as a stationary system [26] with $A_t = \begin{bmatrix} -0.4 & 0.5 \\ 0.6 & 0.75 \end{bmatrix}$. Let $C_{i,t} = I_2$, $W_{i,t} = W = 0.15 \begin{bmatrix} 1 & 0.2 \\ 0.2 & 2 \end{bmatrix}$, and $V_i = 0.4 I_2$.

Fix $\rho_1 = 5, l = 1, 2$ and $\rho_j = 10, j = 3, \ldots, 10$. The aim is to create an estimate of $z_t = \sum_{i=1}^{10} \left[ \begin{array}{c} 1 \\ 0 \end{array} \right] x_{i,t}$.

We design the architecture of Fig. 2(b) by solving (19a)-(19d), setting the privacy parameters to $\delta = 0.01$ and $\epsilon = \ln(3)$. This leads to an steady-state MSE of 4.91. On the other hand, the steady-state MSE for the input perturbation architecture is 7.06.

5. CONCLUSION

This paper considers the Kalman filtering problem under a differential privacy constraint. An architecture combining the differentially private Gaussian mechanism with a signal shaping matrix and a time-varying Kalman filter for output reconstruction is proposed, and it is shown that optimizing the parameters of this architecture can be done via semi-definite programming. Examples illustrate the achievable performance gains compared to the input perturbation mechanism.

6. REFERENCES

[1] M. A. Lisovich, D. K. Mulligan, and S. B. Wicker, “Infering personal information from demand-response systems,” IEEE Security and Privacy, vol. 8, no. 1, pp. 11–20, 2010.

[2] G. Bauer, K. Stockinger, and P. Lukowicz, “Recognizing the use-mode of kitchen appliances from their current consumption,” EuroSSC, pp. 163–176, 2009.

[3] C. Dwork, “Differential privacy,” in Proceedings of the 33rd International Colloquium on Automata, Languages
and Programming (ICALP). 2006, vol. 4052 of Lecture Notes in Computer Science, Springer-Verlag.

[4] C. Dwork, F. McSherry, K. Nissim, and A. Smith, “Calibrating noise to sensitivity in private data analysis,” in Proceedings of the Third Theory of Cryptography Conference, 2006, pp. 265–284.

[5] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, “Our data, ourselves: Privacy via distributed noise generation,” Advances in Cryptology-EUROCRYPT, vol. 4004, pp. 486–503, 2006.

[6] C. Li, M. Hay, V. Rastogi, G. Miklau, and A. McGregor, “Optimizing linear counting queries under differential privacy,” Principles of Database Syst. (PODS), 2010.

[7] A. Roth, New algorithms for preserving differential privacy, Ph.D. thesis, Carnegie Mellon Univ., Pittsburgh, PA, USA, 2010.

[8] C. Dwork, M. Naor, T. Pitassi, and G. N. Rothblum, “Differential privacy under continual observations,” in Proceedings of the ACM Symposium on the Theory of Computing (STOC), Cambridge, MA, June 2010.

[9] L. Sankar, S. R. Rajagopalan, and V. H. Poor, “A theory of privacy and utility in databases,” Tech. Rep., Princeton Univ., Princeton, NJ, USA, 2011.

[10] S. Tonyali, O. Cakmak, K. Akkaya, M. Mahmoud, and I. Guvenc, “Secure data obfuscation scheme to enable privacy-preserving state estimation in smart grid AMI networks,” IEEE Internet of Things Journal, vol. 2, no. 3, pp. 709–719, October 2016.

[11] J. Le Ny and G. J. Pappas, “Differential private filtering,” IEEE Transactions on Automatic Control, vol. 59, no. 2, pp. 341–354, February 2014.

[12] L. Fan and L. Xiong, “An adaptive approach to real-time aggregate monitoring with differential privacy,” IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 9, pp. 2094–2106, 2014.

[13] J. Le Ny, “Privacy-preserving nonlinear observer design using contraction analysis,” in Proceedings of the 54rd IEEE Conference on Decision and Control, Osaka, Japan, December 2015.

[14] K. H. Degue, D. Efimov, and A. Iggidr, “Interval estimation of sequestered infected erythrocytes in malaria patients,” in Proceedings of European Control Conference (ECC16), Aalborg, Denmark, June 2016.

[15] K. H. Degue, D. Efimov, and J. Le Ny, “Interval observer approach to output stabilization of linear impulsive systems,” in Proceedings of the 20th World Congress of the International Federation of Automatic Control (IFAC 2017), Toulouse, France, July 2017.

[16] M. Yu and D. Wang, “Model-based health monitoring for a vehicle steering system with multiple faults of unknown types,” IEEE Transactions on Industrial Electronics, vol. 61, no. 7, pp. 3574–3586, July 2014.

[17] N. L. Komarova and C. R. Boland, “Cancer: Calculated treatment,” Nature, vol. 499, pp. 291–292 (News and Views article), July 2013.

[18] J. Le Ny and G. J. Pappas, “Differentially private Kalman filtering,” in Proceedings of the 50th Annual Allerton Conference, Allerton House, UIUC, Illinois, USA, October 2012.

[19] J. Le Ny and G. J. Pappas, “Differentially private filtering,” in Proceedings of the 51st IEEE Conference on Decision and Control, Maui, Hawaii, USA, December 2012.

[20] T. Tanaka, K-K. K. Kim, P. A. Parrilo, and S.K. Mitter, “Semidefinite programming approach to gaussian sequential rate-distortion trade-offs,” IEEE Transactions on Automatic Control, vol. 62, no. 1896-1910, April 2017.

[21] J. Salz, “Digital transmission over cross-coupled linear channels,” AT&T Technical Journal, vol. 64, no. 6, pp. 1147–1159, July-August 1985.

[22] J. Yang and S. Roy, “On joint transmitter and receiver optimization for multiple-input-multiple-output (MIMO) transmission systems,” IEEE Journal on Communications, vol. 42, no. 12, pp. 3221–3231, December 1994.

[23] B. D. O. Anderson and J. B. Moore, Optimal filtering, Dover, New York, NY, USA: Dover, 2005.

[24] Cynthia Dwork and Aaron Roth, “The algorithmic foundations of differential privacy,” Foundations and Trends in Theoretical Computer Science, vol. 9, no. 3-4, pp. 211–407, August 2014.

[25] S. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan, Linear matrix inequalities in system and control theory, vol. 15, SIAM, 1994.

[26] P. J. Costa, J. P. Dunyak, and M. Mohtashemi, “Models, prediction, and estimation of outbreaks of infectious disease,” in Proceedings of IEEE SoutheastCon, Ft. Lauderdale, FL, USA, April 2005.