Gaussian Mechanisms Against Statistical Inference: Synthesis Tools

Haleh Hayati, Carlos Murguia, Nathan van de Wouw

Abstract— In this manuscript, we provide a set of tools (in terms of semidefinite programs) to synthesize Gaussian mechanisms to maximize privacy of databases. Information about the database is disclosed through queries requested by (potentially) adversarial users. We aim to keep part of the database private (private sensitive information); however, disclosed data could be used to estimate private information. To avoid an accurate estimation by the adversaries, we pass the requested data through distorting (privacy-preserving) mechanisms before transmission and send the distorted data to the user. These mechanisms consist of a coordinate transformation and an additive dependent Gaussian vector. We formulate the synthesis of distorting mechanisms in terms of semidefinite programs in which we seek to minimize the mutual information (our privacy metric) between private data and the disclosed distorted data given a desired distortion level – how different actual and distorted data are allowed to be.

I. INTRODUCTION

Scientific and technological advancements in today's hyperconnected world have resulted in a massive amount of user data collected and processed by hundreds of companies over public networks. Companies use this data to provide personalized services and target advertising. However, these technologies have come with the cost of a significant loss of privacy in society. Depending on their resources, adversaries can infer sensitive (private) information about databases from public data available on the internet and/or unsecured networks/servers. A motivating example of this privacy loss is the potential use of data from smart electrical meters by criminals, advertising agencies, and governments for monitoring the activities of occupants [1], [2]. This is why researchers from several fields (e.g., computer science, information theory, and control theory) have been drawn to the broad research subject of privacy and security of Cyber-Physical Systems (CPSs), [3]-[9].

We consider the following setting. Users request data, say Y, from public databases through a set of queries. There is sensitive (private) information in the database, say S, that we aim to keep private. However, due to the statistical dependence between Y and S, adversarial users could use disclosed data to infer private information. To avoid accurate inference, we pass the requested data through distorting (privacy-preserving) mechanisms before transmission and send the distorted data to the user. These mechanisms consist of a linear coordinate transformation, G, and an additive

Haleh Hayati, Carlos Murguia, and Nathan van de Wouw are with the Department of Mechanical Engineering, Dynamics and Control Group, Eindhoven University of Technology, The Netherlands. Emails: & h.hayati@tue.nl, & c.g.murguia@tue.nl, & n.v.d.wouw@tue.nl.

dependent Gaussian vector, V; Therefore, the distorted disclosed data, Z, is given by $Z = GY + V$, $V \sim \mathcal{N}[\mathbf{0}, \Sigma^V]$, for some covariance matrix Σ^V. We formulate the synthesis of the distorting mechanisms (the pair (G, Σ^V)) in terms of semidefinite programs in which we seek to conceal (as much as possible) the private parts of the database. Here we follow an information-theoretic approach to privacy. As *privacy metric*, we use the *mutual information*, $I[S; Z]$, between private data, S, and the disclosed distorted data, Z. Mutual information is a measure of the statistical dependence between S and Z [10]. We cast the design of (G, Σ^V) as a semidefinite program where we minimize $I[S; Z]$. Note, however, that it is not desired to overly distort the original data. We might change original data excessively to maximize privacy. Therefore, when synthesizing (G, Σ^V) (by minimizing $I[S; Z]$), we have to consider the trade-off between *privacy* and *distortion*. As *distortion metric*, we use the *weighted mean squared error* between the original data, Y, and its distorted version, Z. Therefore, the overall optimization problem amounts to minimizing $I[S; Z]$, subject to an upper bound on the mean squared error (how different Y and Z are allowed to be on average), using (G, Σ^V) as optimization variables.

Using additive random vectors is common to promote privacy by avoiding an accurate estimation of private data. Differential privacy is popular approach in the context of privacy of databases [6], [11]. In differential privacy, because it provides certain privacy guarantees, Laplace noise is commonly employed [11], without tackling the problem of finding the maximum level of privacy for a given allowed distortion level. Generally, the additive noise distribution that yields maximum privacy is determined by the particular privacy and distortion metrics being considered, as well as the system configuration [12]-[14]. There are results addressing this subject from an information-theoretic perspective, in which privacy is quantified using information metrics – e.g., mutual information, entropy, Kullback-Leibler divergence, and Fisher information [1], [3], [4], [15], [16], [17].

If the data to be kept private follows continuous probability distributions, the problem of finding the optimal additive noise to maximize privacy is difficult to solve. This issue has been addressed by assuming the data to be kept private is deterministic [3], [13], [14]. However, in the context of databases, unavoidable correlation among features results in statistical dependence and, therefore, deterministic tools often lead to conservative results. Recently, the authors in [9], [18], [19] have proposed a framework for synthesizing optimal transition probabilities to maximize privacy for a class of Cyber-Physical Systems (CPSs) characterized by

discrete multivariate probability distributions. Although this framework is fairly general and leads to distorting mechanisms following arbitrary distributions, the computational complexity induced by exploring all the possible transition probabilities from private to disclosed distorted data is high and grows exponentially with the alphabet of the private data. In [3], the authors neglect quantization and work directly with dynamical systems driven by continuous (Gaussian) disturbances. They prove that in the case of unconstrained additive noise, the optimal noise distribution minimizing Fisher information is Gaussian. When employing mutual information as a privacy metric, the same statement was also proved in [20].

Motivated by these results, we propose a general class of Gaussian mechanisms and seek the optimal parameterization. In [21], [22], we present an optimization-based framework for synthesizing optimal privacy-preserving Gaussian mechanisms for a class of stochastic dynamical systems. Our first contribution in this paper is to extend the optimization-based framework for synthesizing Gaussian mechanisms in the context of databases. Furthermore, we prove that we can allow for prior distributions (the joint probability distributions between private and disclosed data) that are not necessarily Gaussian, as long as they are log-concave [23]. The latter generalizes further the class of databases our framework can deal with.

The structure of the paper is organized as follows. The problem formulation, including adversarial capabilities and privacy and distortion metrics, is presented in Section II. The solution to the Problem 1 formulated in Section II is developed in Section III. Our simulation results are presented in Section IV, followed by concluding remarks in Section V. **Notation:** The notation $X \sim \mathcal{N}[\mu, \Sigma^X]$ stands for a normally distributed random vector $X \in \mathbb{R}^n$ with mean $E[X] = \mu \in \mathbb{R}^n$ and covariance matrix $E[(X - \mu)(X - \mu)^T] = \Sigma^X \in \mathbb{R}^{n \times n}$, where $E[a]$ denotes the expected value of the random vector a. The $n \times n$ identity matrix is denoted by I_n or simply I if n is clear from the context. Similarly, $n \times m$ matrices composed of only zeros are denoted by $\mathbf{0}_{n \times m}$ or simply $\mathbf{0}$ when their dimensions are clear. For positive definite (semidefinite) matrices, we use the notation $P > 0$ ($P \geq 0$). The operators $\log[\cdot]$, $\det[\cdot]$, and $\mathrm{tr}[\cdot]$ stand for logarithm base two, determinant, and trace, respectively.

II. PROBLEM FORMULATION

Let S be part of a database D that must be kept private. We model S as a multivariate Gaussian distribution, $S \sim \mathcal{N}[\mu_S, \Sigma^S]$, with mean $\mu_S \in \mathbb{R}^{n_s}$ and covariance $\Sigma^S \in \mathbb{R}^{n_s \times n_s}$, $\Sigma^S > 0$, $n_s \in \mathbb{N}$. Information about S is obtained through queries of the form $Y = q(S)$, for some (stochastic or deterministic) affine mapping $q : \mathbb{R}^{n_s} \to \mathbb{R}^{n_y}$ characterized by transition probabilities $f_{Y|S}(y \mid s)$. We model Y as a multivariate Gaussian distribution, $Y \sim \mathcal{N}[\mu_Y, \Sigma^Y]$, with mean $\mu_Y \in \mathbb{R}^{n_y}$ and covariance $\Sigma^Y \in \mathbb{R}^{n_y \times n_y}$, $\Sigma^Y > 0$, $n_y \in \mathbb{N}$. To capture statistical dependence between private and disclosed data, we let S and Y be jointly distributed as $\binom{Y}{S} \sim \mathcal{N}\left[\mu^{Y,S}, \Sigma^{Y,S}\right]$ with mean $\mu^{Y,S} \in \mathbb{R}^{(n_s+n_y)}$, joint

covariance $\Sigma^{Y,S} \in \mathbb{R}^{(n_s+n_y) \times (n_s+n_y)}$, $\Sigma^{Y,S} > 0$, and cross-covariance $\Sigma^{YS} \in \mathbb{R}^{n_y \times n_s}$, $\Sigma^{YS} > 0$.

We aim to prevent adversaries from accurately estimating the private data S. To this end, we randomize Y before disclosure and send the corrupted data to the user instead. We randomize Y through a mapping $M(\cdot)$ of the form:

$$Z = M(Y) := GY + V, \tag{1}$$

for some linear transformation $G \in \mathbb{R}^{n_y \times n_y}$ and dependent multivariate Gaussian vector $V \sim \mathcal{N}[\mathbf{0}, \Sigma^V]$ with covariance $\Sigma^V \in \mathbb{R}^{n_y \times n_y}$, $\Sigma^V > 0$. The randomized vector Z is disclosed to the user, see Figure 1. We seek to synthesize distortion variables (G, Σ^V) to make inference of private data, S, as hard as possible from the disclosed data, Z.

A. Adversarial Capabilities

We consider worst-case adversaries that send queries to the server or eavesdrop data at the communication channel. They have access to distorted data Z, and have prior knowledge of the statistical properties of the database, i.e., the adversary knows $(\mu_S, \Sigma^S, \mu_Y, \Sigma^Y, \Sigma^{Y,S})$. We assume the adversary uses a linear Minimum Mean Square Error (MMSE) estimator to reconstruct S from Z and prior knowledge. The MMSE estimator offers the best estimation performance among all unbiased estimators for jointly Gaussian vectors [24]. In practice, actual adversaries are unlikely to have all the capabilities we assume here. However, if we maximize privacy against these worst-case adversaries, we ensure that adversaries with fewer capabilities perform even worse.

B. Metrics and Problem Formulation

The aim of our privacy scheme is to make inference of S from the distorted disclosed data Z as challenging as possible without distorting Y excessively. That is, we do not want to make Y and Z overly different because of the utility of the query output Y for users. Hence, when designing the distorting variables (G, Σ^V), we need to consider the *trade-off between privacy and distortion*. As distortion metric, we use the weighted mean squared error between the original and distorted data, i.e., $E[||W(Z - Y)||^2]$ for a given weighting matrix W of appropriate dimension. Matrix W is used to fine-tune the desired distortion at different channels and/or to model different applications of the distorted data. As a privacy metric, we use the mutual information between private and disclosed data, i.e., $I[S; Z]$, which is a measure of the statistical dependence between S and Z [10]. Hence, we aim at minimizing $I[S; Z]$ subject to the second moment constraint $E[||W(Z - Y)||^2] \leq \epsilon$, for a desired maximum distortion level $\epsilon \in \mathbb{R}^+$, by designing G and Σ^V of the distorting mechanisms (1). In what follows, we present the optimization problem we seek to solve.

Problem 1: Given the private S, disclosed Y, desired maximum distortion level $\epsilon \in \mathbb{R}^+$, weighting matrix $W \in \mathbb{R}^{n_y \times n_y}$, and the distorting mechanism (1), find the distorting
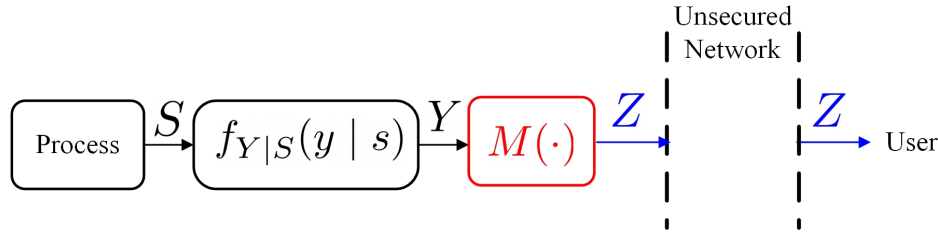
Fig. 1: System configuration.

variables, G and Σ^V, as the solution to:

$$\begin{cases} \min_{G, \Sigma^V} \ I[S;Z], \\ \text{s.t. } E[||W(Z-Y)||^2] \le \epsilon, \\ V \text{ and } Y \text{ independent.} \end{cases} \quad (2)$$

III. SOLUTION TO PROBLEM 1

To solve Problem 1, we first need to write the cost function and constraint in terms of the design variables G and Σ^V.

A. Cost Function: Formulation and Convexity

The mutual information $I[S;Z]$ can be written in terms of differential entropies as $I[S;Z] = h[S] + h[Z] - h[S,Z]$ [10]. Moreover, differential entropies of Gaussian random vectors are fully characterized by their covariance matrices, $h[S] = \frac{1}{2} \log \det\left(\Sigma^S\right) + \frac{n_s}{2} + \frac{n_s}{2} \log(2\pi)$, (see Theorem 8.4.1 in [10]). So, to characterize $I[S;Z]$ in terms of G and Σ^V, we need to write the covariance matrices of S and Z and their joint covariance in terms of design variables, (G, Σ^V). In the following lemma, we give a closed-form expression of the joint density of Z and S.

Lemma 1
$$\left(\begin{smallmatrix} Z \\ S \end{smallmatrix}\right) \sim \mathcal{N}\left[\mu^{Z,S}, \Sigma^{Z,S}\right],$$

with mean $\mu^{Z,S} \in \mathbb{R}^{(n_s + n_y)}$ *and joint covariance matrix* $\Sigma^{Z,S} \in \mathbb{R}^{(n_s+n_y)\times(n_s+n_y)}$, $\Sigma^{Z,S} > 0$, *given by*:

$$\mu^{Z,S} = \begin{bmatrix} G\mu_Y \\ \mu_S \end{bmatrix}, \quad (3)$$

$$\Sigma^{Z,S} = \begin{bmatrix} \Sigma^Z & \Sigma^{ZS} \\ \Sigma^{ZS^\top} & \Sigma^S \end{bmatrix}, \quad (4)$$

$$\Sigma^Z = G\Sigma^Y G^\top + \Sigma^V, \quad (5)$$

$$\Sigma^{ZS} = G\Sigma^{YS}, \quad (6)$$

where Σ^{ZS} *denotes the cross-covariance between* Z *and* S.

Proof: See Lemma 1 in [25]. ∎

In Lemma 1, we have written $(\Sigma^Z, \Sigma^S, \Sigma^{S,Z})$ in terms of the design variables G and Σ^V. Before we write the cost in (2) in terms of these matrices, we notice that Σ^V only appears in the expression for Σ^Z in (5). Moreover, given (G, Σ^Z), matrix Σ^V is fully determined and vice versa. That is, $(G, \Sigma^V) \to (G, \Sigma^Z)$ is an invertible transformation, and therefore, we can pose both cost and constraints in terms of either Σ^V or Σ^Z. By casting the problem in terms of Σ^Z, we can establish a linear distortion constraint and a

convex cost function. Hereafter, the problem is posed in terms of (G, Σ^Z). Then, we extract the optimal Σ^V from the optimal (G, Σ^Z) using (5). The first constraint that we need to enforce is that the extracted Σ^V is always positive definite (as it is a covariance matrix). From (5), it is easy to verify that $\Sigma^V > 0$ if and only if $\Sigma^Z - G\Sigma^Y G^\top > 0$. Using standard Schur complement properties [26], the latter nonlinear inequality can be rewritten as a higher-dimensional linear matrix inequality in Σ^Z and G as follows:

$$\begin{bmatrix} \Sigma^Z & G \\ G^\top & (\Sigma^Y)^{-1} \end{bmatrix} > 0. \quad (7)$$

When we solve the complete optimization problem, we apply inequality (7) to enforce that the optimal Σ^Z and G lead to a positive definite Σ^V.
Finally, given $(\Sigma^Z, \Sigma^S, \Sigma^{S,Z})$ from Lemma 1, we can write the cost $I[S;Z]$ in terms of covariance matrices as follows:

$$I[S;Z] = h[S] + h[Z] - h[S,Z] \quad (8a)$$

$$= \frac{1}{2} \log \frac{\det\left(\Sigma^S\right) \det\left(\Sigma^Z\right)}{\det\left(\Sigma^{Z,S}\right)} \quad (8b)$$

$$= \frac{1}{2} \log \det\left(\Sigma^S\right) - \frac{1}{2} \log \det\left(\Sigma^S - \Sigma^{ZS^\top}\Sigma^{Z^{-1}}\Sigma^{ZS}\right), \quad (8c)$$

where (8b)-(8c) follow from standard determinant and logarithm formulas. We prove in the following lemma that minimizing the cost function $I[S;Z]$ using (G, Σ^Z) as optimization variables is equivalent to solving a convex program subject to some Linear Matrix Inequalities (LMI) constraints.

Lemma 2 *Minimizing* $I[S;Z]$ *in (8) is equivalent to solving the following convex program:*

$$\begin{cases} \min_{\Pi, \Sigma^Z, G} -\log\det(\Pi), \\ \text{s.t. } \Pi \ge \mathbf{0}, \begin{bmatrix} \Sigma^S - \Pi & (G\Sigma^{YS})^\top \\ G\Sigma^{YS} & \Sigma^Z \end{bmatrix} \ge 0. \end{cases} \quad (9)$$

Proof: See Lemma 2 in [25]. ∎

By Lemma 2, minimizing the cost in (2) is equivalent to solving the convex program in (9). Therefore, if the distortion constraint, $E[||W(Z-Y)||^2] < \epsilon$, is convex in the decision variables, we can employ off-the-shelf optimization algorithms to find optimal distorting mechanisms being the solution to Problem 1.

$$\min_{\Pi, \Sigma^Z, G} -\log \det[\Pi],$$

$$\text{s.t.} \begin{cases} \Pi \geq 0, \\ \begin{bmatrix} \Sigma^S - \Pi & (G\Sigma^{YS})^\top \\ G\Sigma^{YS} & \Sigma^Z \end{bmatrix} \geq 0, \\ \begin{bmatrix} \Sigma^Z & G \\ G^\top & (\Sigma^Y)^{-1} \end{bmatrix} > 0, \\ \begin{bmatrix} \theta_Y & \mu^{Y^\top}(G-I)^\top W^\top \\ W(G-I)\mu^Y & I \end{bmatrix} \geq 0, \\ \theta_Y := \epsilon - tr[W^\top(\Sigma^Z + \Sigma^Y - 2\Sigma^Y G)W]. \end{cases} \quad (12)$$

B. Distortion Constraint: Formulation and Convexity

Lemma 3 $E[||W(Z-Y)||^2]$ *is a convex function of* Σ^Z *and* G, *and can be written as follows:*

$$E[||W(Z-Y)||^2] = tr[W^\top(\Sigma^Z + \Sigma^Y - 2\Sigma^Y G)W]$$
$$+ \mu_Y^\top(G-I)^\top W^\top W(G-I)\mu_Y. \quad (10)$$

Proof: See Lemma 3 in [25]. ∎

Remark 1 *The distortion constraint* $E[||W(Z-Y)||^2] \leq \epsilon$ *is nonlinear in the design variables, because the distortion metric* (10) *is linear in* Σ^Z *and quadratic in* G. *However, we can construct an equivalent linear constraint using standard Schur complement properties. It can be proved (see* [26] *for details) that* $E[||W(Z-Y)||^2] \leq \epsilon$ *in* (10) *is equivalent to the following LMI in* Σ^Z *and* G:

$$\begin{cases} \begin{bmatrix} \theta_Y & \mu_Y^\top(G-I)^\top W^\top \\ W(G-I)\mu_Y & I \end{bmatrix} \geq 0, \\ \theta_Y := \epsilon - tr[W^\top(\Sigma^Z + \Sigma^Y - 2\Sigma^Y G)W]. \end{cases} \quad (11)$$

By Lemma 2, Lemma 3, and Remark 1, the cost function $I[S; Z]$ and distortion constraint $E[||W(Z-Y)||^2] \leq \epsilon$ can be written in terms of convex functions in the optimization variables Σ^Z and G. In what follows, we pose the complete nonlinear convex program to solve Problem 1.

Theorem 1 *Consider the distorting mechanism* (1), *desired output distortion level* $\epsilon \in \mathbb{R}^+$, *output distortion weight* $W \in \mathbb{R}^{n_y \times n_y}$, *covariance* Σ^S, *cross-covariance* Σ^{YS}, *and the mean and covariance of* Y, μ^Y *and* Σ^Y, *respectively. Then, the optimization variables* Σ^Z *and* G *that minimize* $I[S; Z]$ *subject to distortion constraint* $E[||W(Z-Y)||^2] \leq \epsilon$, *as in Problem 1, can be found by solving the convex program in* (12).

Proof: The expressions for the cost and constraint and convexity (linearity) of them follow from Lemma 2, Lemma 3, and Remark 1. ∎

Remark 2 *Theorem 1 provides a tool to find optimal*

privacy-preserving mechanisms when the prior distributions are jointly Gaussian. In the following proposition, we prove that we can allow for priors that are not necessarily Gaussian, as long as they are log-concave [23]. *The latter generalizes significantly the class of databases that Theorem 1 can deal with. In particular, we prove that if* S *and* Z *follow non-Gaussian log-concave distributions, their mutual information is upper-bounded by an affine function of the mutual information between* $S_\mathcal{N}$ *and* $Z_\mathcal{N}$, *where* $S_\mathcal{N}$ *and* $Z_\mathcal{N}$ *denote Gaussian random vectors with the same mean and covariance matrix as* S *and* Z, *respectively. Examples of log-concave distributions are normal, exponential, uniform, Laplace, chi, beta, and logistic distributions. We refer the reader to* [27] *for a comprehensive list and properties of log-concave distributions.*

Proposition 1 *Let* S *and* Z *be jointly distributed following log-concave multivariate joint probability distribution. Their mutual information* $I[S; Z]$ *can be upper-bounded as:*

$$I[S; Z] \leq I[S_\mathcal{N}; Z_\mathcal{N}] + C_n, \quad (13)$$

where $C_n = \frac{1}{2} \log(2\pi e c(n))^n$, $n = n_s + n_y$, $c(n) = \frac{e^2 n^2}{4\sqrt{2}(n+2)}$, *and* $S_\mathcal{N}$ *and* $Z_\mathcal{N}$ *denote Gaussian random vectors with the same covariance matrices as* S *and* Z.

Proof: First, we need to prove that for S and Y following log-concave distribution, Z also follows a log-concave distribution. From the fact that the log-concavity of distribution is preserved under affine transformation, we can conclude that GY is log-concave (see [28], Lemma 2.1). Then, based on Hoggar's theorem, the sum of two independent log-concave random variables is itself log-concave, which resulted in log-concavity of Z as a summation of GY and V [29], [30]. Mutual information $I[S; Z]$ can be written in terms of differential entropies as $I[S; Z] = h[S] + h[Z] - h[S, Z]$. Moreover, because Gaussian distributions maximize entropy for a given covariance matrix [10], we can write:

$$\begin{cases} h[S] \leq h[S_\mathcal{N}], \\ h[Z] \leq h[Z_\mathcal{N}], \end{cases} \quad (14)$$

where $S_\mathcal{N}$ and $Z_\mathcal{N}$ denote Gaussian random vectors with the same covariance matrices as S and Z. The authors in [31] prove that the entropy of random vectors following log-concave distributions [32] can be lower bounded as:

$$h[S, Z] \geq \frac{n}{2} \log \frac{\left|\Sigma^{S,Z}\right|^{1/n}}{c(n)}, \quad (15)$$

where $n = n_s + n_z$ and $c(n) = \frac{e^2 n^2}{4\sqrt{2}(n+2)}$. Expanding the lower bound in (15), we obtain

$$\frac{n}{2} \log \frac{\left|\Sigma^{S,Z}\right|^{1/n}}{c(n)} = \frac{n}{2}\left(\frac{1}{n}\log\det\Sigma^{S,Z} - \log c(n)\right)$$
$$= \frac{1}{2}\log\det\Sigma^{S,Z} - \frac{n}{2}\log c(n). \quad (16)$$

Let $(S_\mathcal{N}, Z_\mathcal{N})$ be jointly Gaussian with covariance $\Sigma^{S,Z}$. Then, we can write its differential entropy as $h[S_\mathcal{N}, Z_\mathcal{N}] = $

$\frac{1}{2}\log\det\left(\Sigma^{S,Z}\right) + \frac{n}{2} + \frac{n}{2}\log(2\pi)$ (see Theorem 8.4.1 in [10]). Therefore, using the latter formula for $h[S_\mathcal{N}, Z_\mathcal{N}]$ and (16), we can write the following

$$\frac{n}{2}\log\frac{\left|\Sigma^{S,Z}\right|^{1/n}}{c(n)} = h[S_\mathcal{N}, Z_\mathcal{N}] - \frac{n}{2} - \frac{n}{2}\log(2\pi) - \frac{n}{2}\log c(n). \quad (17)$$

Combining (14), (15), and (17), we can finally conclude that

$$I[S; Z] \leq h[S_\mathcal{N}] + h[Z_\mathcal{N}] - h[S_\mathcal{N}, Z_\mathcal{N}]$$
$$+ \frac{n}{2} + \frac{n}{2}\log(2\pi) + \frac{n}{2}\log c(n), \quad (18)$$

which is equivalent to (13). ∎

Remark 3 *Proposition 1 implies that by minimizing $I[S_\mathcal{N}; Z_\mathcal{N}]$ (based on the optimization problem in Theorem 1), we can effectively decrease the mutual information $I[S; Z]$ for any (S, Z) following a log-concave distribution.*

A tighter bound for the mutual information of log-concave random vectors can be achieved based on their maximum density. The maximum density of a random vector is calculated by its L^∞ norm [33]. In the following proposition, we prove that the mutual information between log-concave random vectors S and Z can be upper-bounded by an affine function of the mutual information of Gaussian random vectors with maximum density being the same as those of S and Z.

Proposition 2 *Let S and Z be jointly distributed following a log-concave multivariate joint probability distribution. For their mutual information $I[S; Z]$, one can write:*

$$\frac{1}{n}I[S; Z] - \frac{1}{n}I[S_\mathcal{N}^*; Z_\mathcal{N}^*] \leq 1, \quad (19)$$

where $n = n_s + n_y$, and $S_\mathcal{N}^*$ and $Z_\mathcal{N}^*$ denote multivariate normally distributed random vectors with maximum density being the same as those of S and Z, respectively.

Proof: Mutual information $I[S; Z]$ can be written in terms of differential entropies as $I[S; Z] = h[S] + h[Z] - h[S, Z]$. Moreover, from the inequality on the entropy of log-concave distributed random vectors, we can conclude that (see Theorem $I.1$ in [33]):

$$\begin{cases} \frac{1}{n_s}h[S] \leq \frac{1}{n_s}h[S_\mathcal{N}^*] + \frac{1}{2}, \\ \frac{1}{n_y}h[Z] \leq \frac{1}{n_y}h[Z_\mathcal{N}^*] + \frac{1}{2}, \\ \frac{1}{n}h[S, Z] \geq \frac{1}{n}h[S_\mathcal{N}^*, Z_\mathcal{N}^*] - \frac{1}{2}, \end{cases} \quad (20)$$

where $n = n_s + n_y$, and $S_\mathcal{N}^*$ and $Z_\mathcal{N}^*$ denote multivariate normally distributed random vectors with maximum density being the same as those of S and Z, respectively.
Combining all these inequalities in (20), we can conclude that

$$\frac{1}{n}I[S; Z] \leq \frac{1}{n}(h[S_\mathcal{N}^*] + h[Z_\mathcal{N}^*] - h[S_\mathcal{N}^*, Z_\mathcal{N}^*]) + 1, \quad (21)$$

which is equivalent to (19). ∎

Remark 4 *In Proposition 2 we prove that the difference between $I[S; Z]$ and $I[S_\mathcal{N}^*; Z_\mathcal{N}^*]$ can be upper-bounded by n. This upper bound is still conservative since it covers all log-concave distributed random vectors. However, the authors in [33] observe that every log-concave random vector has approximately the same entropy per coordinate as a related Gaussian vector (which resulted in approximately the same mutual information) and log-concave distributions resemble log-concave distributions. Therefore, we can imply that by minimizing $I[S_\mathcal{N}^*; Z_\mathcal{N}^*]$ (based on the optimization problem in Theorem 1), we can effectively decrease the mutual information $I[S; Z]$ for any (S, Z) following log-concave distribution.*
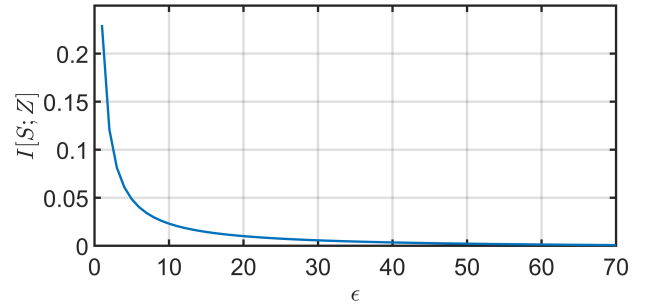

Fig. 2: Cost function for increasing ϵ.

IV. SIMULATION RESULTS

We consider multivariate Gaussian private S and disclosed Y with $n_s = n_y = 3$, and randomly selected means and covariances μ_S, μ_Y, $\Sigma^S > 0$, and $\Sigma^Y > 0$. We first show the effect of the distortion level ϵ on the amount of information leakage, calculated by the optimal cost function $I[S; Z]$, in Figure 2. As expected, the value of the cost decreases monotonically as we increase the maximum allowed distortion ϵ. This figure illustrates that by increasing the distortion level, the decreasing rate of the optimal cost is reduced (we actually have exponential decay). So the best privacy-distortion trade-off is reached for small ϵ.

The effect of the optimal distorting mechanisms is illustrated in Figure 3 for different levels of distortion $\epsilon = \{1, 10, \infty\}$. We contrast realizations of the second elements of Y and distorted Z. The value of $\epsilon = \infty$ means that the optimization problem in (12) is solved without considering the distortion constraint between Z and Y. The difference between Y and Z increases by increasing the distortion level. Next, in Figure 4, we show realizations of the second element of the private S and its MMSE estimate, $\hat{S}_Y^2$, constructed from realizations of the undistorted Y and its MMSE estimate given realizations of the distorted Z, $\hat{S}_Z^2$. We consider different levels of distortion, $\epsilon = \{1, 10, \infty\}$. In Figure 4, we observe that by randomizing Y, we can prevent accurate estimation of S. Because by increasing the distortion level ϵ, the accuracy of the estimation decreases.

Finally, in Figure 5, we show that, as discussed in Remark 3 and Remark 4, for non-Gaussian random vectors S and
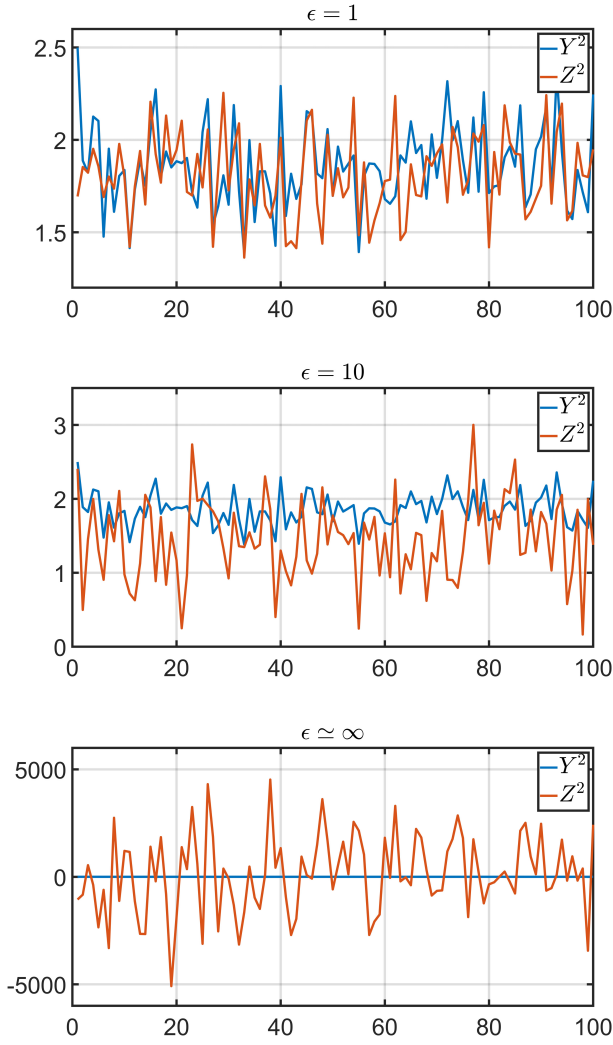
Fig. 3: Comparison between the second element of Y and Z for different distortion levels, $\epsilon = 1, 10, \infty$.

Fig. 4: Comparison between the second element of the private data, S^2, its estimation without distorting Y, $\hat{S}_Y^2$, and its estimation given distorted data Z, $\hat{S}_Z^2$, for different distortion levels $\epsilon = 1, 10, \infty$.

Fig. 5: Comparison between the mutual information of S and Z, with Laplacian S and Y, $I[S; Z]$, and its upper bound, which is based on the mutual information of Gaussian vectors $S_{\mathcal{N}}$ and $Z_{\mathcal{N}}$, $I[S_{\mathcal{N}}; Z_{\mathcal{N}}]$, for increasing ϵ.

Z following joint log-concave distributions, their mutual information can be upper-bounded by affine functions of the mutual information of some Gaussian random vectors. The upper bounds are based on the mutual information of Gaussian random vectors $S_{\mathcal{N}}$ and $Z_{\mathcal{N}}$ with the same mean and covariance matrices as S and Z, and also the mutual information of $S_{\mathcal{N}}^*$ and $Z_{\mathcal{N}}^*$ denote multivariate normally distributed random vectors with maximum density being the same as those of S and Z, respectively. We use S and Y with joint Laplace distribution and solve the optimization problem in (12) for $I[S_{\mathcal{N}}; Z_{\mathcal{N}}]$ to find the optimal distorting parameters G and Σ^V, for increasing amount of distortion level ϵ. Since the maximum density of Gaussian random vectors and Laplace random vectors are the same for the same mean and covariances, we can conclude that for Laplace variables $S_{\mathcal{N}}^* = S_{\mathcal{N}}$, $Z_{\mathcal{N}}^* = Z_{\mathcal{N}}$, and therefore $I[S_{\mathcal{N}}^*; Z_{\mathcal{N}}^*] = I[S_{\mathcal{N}}; Z_{\mathcal{N}}]$. We calculate $I[S_{\mathcal{N}}; Z_{\mathcal{N}}] + C_n$ and $I[S_{\mathcal{N}}^*; Z_{\mathcal{N}}^*] + n$ as the upper bounds of $I[S; Z]$, where in this case study,
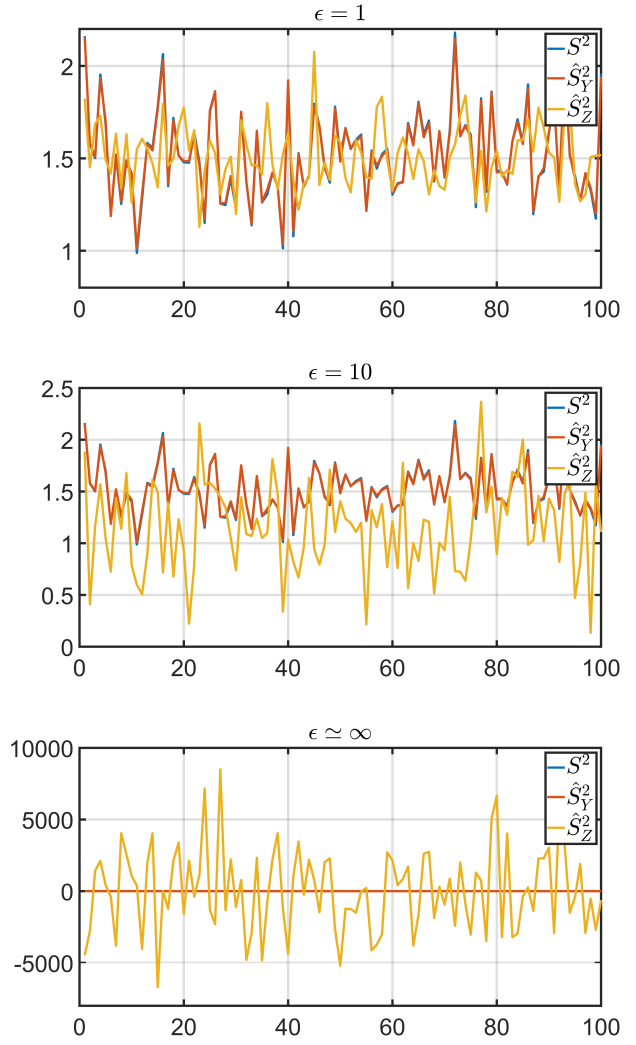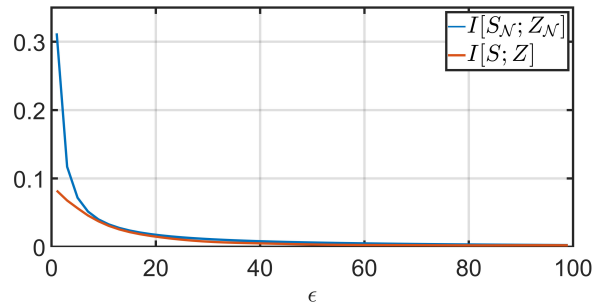
$C_n = 18.6204$ and $n = 6$. Then, we calculate the mutual information between S and Z [34], where S and Y follow Laplace distributions with the same mean and covariance as $S_\mathcal{N}$ and $Y_\mathcal{N}$ and $Z = GY + V$ (with the same distortion variables as Gaussian case). As can be seen in Figure 5, $I[S; Z]$ is even upper-bounded by $I[S_\mathcal{N}; Z_\mathcal{N}]$ without the constant terms n and C_n. It implies that by solving the optimization problem for Gaussian data, the information leakage for Laplace data, which is given by $I[S; Z]$, is decreasing for increasing ϵ, and is upper-bounded by the mutual information $I[S_\mathcal{N}^*; Z_\mathcal{N}^*]$ and $I[S_\mathcal{N}; Z_\mathcal{N}]$. Furthermore, it is apparent that even if the Gaussian upper bounds is loose for these distributions of S and Z, the information leakage $I[S; Z]$ is still decreasing for increasing ϵ. This implies that minimizing $I[S_\mathcal{N}; Z_\mathcal{N}]$ effectively decreases the mutual information $I[S; Z]$ for any log-concave S and Z.

V. CONCLUSIONS

This paper proposes a comprehensive mathematical framework for synthesizing distorting mechanisms to minimize the information leakage caused by public/unsecured communication networks for a class of stochastic databases. We have introduced a class of linear Gaussian distorting mechanisms to randomize data before transmission to prevent adversaries from precisely estimating the private part of the database. Furthermore, for the class of data under study, we have thoroughly characterized an information-theoretic metric (mutual information) to quantify the information between private data and disclosed data for a class of worst-case eavesdropping adversaries. Finally, given the maximum level of distortion tolerated by a particular application, we have provided tools (in terms of convex programs) for designing optimal (in terms of maximizing privacy) distorting mechanisms. We have presented simulation results to illustrate the performance of our tools.

REFERENCES

[1] S. R. Rajagopalan, L. Sankar, S. Mohajer, and H. V. Poor, "Smart meter privacy: A utility-privacy framework," in *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2011, pp. 190–195.

[2] O. Tan, D. Gündüz, and H. V. Poor, "Increasing smart meter privacy through energy harvesting and storage devices," *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 1331–1341, 2013.

[3] F. Farokhi and H. Sandberg, "Optimal privacy-preserving policy using constrained additive noise to minimize the fisher information," in *Proceedings of the IEEE 56th Annual Conference on Decision and Control (CDC)*, 2017.

[4] F. Farokhi, H. Sandberg, I. Shames, and M. Cantoni, "Quadratic Gaussian privacy games," in *Proceedings of the 54th IEEE Conference on Decision and Control (CDC)*, 2015, pp. 4505–4510.

[5] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding sensor outputs for injection attacks detection," in *Proceedings of the 53rd Annual Conference on Decision and Control (CDC)*, 2014, pp. 5776–5781.

[6] J. L. Ny and G. J. Pappas, "Differentially private filtering," *IEEE Transactions on Automatic Control*, vol. 59, pp. 341–354, 2014.

[7] 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.

[8] F. F. Murguia C., Shames I. and N. D., *Information-Theoretic Privacy Through Chaos Synchronization and Optimal Additive Noise. In: Farokhi F. (eds) Privacy in Dynamical Systems*. Singapore: Springer, 2020.

[9] C. Murguia, I. Shames, F. Farokhi, and D. Nešić, "On privacy of quantized sensor measurements through additive noise," in *Proceedings of the 57th IEEE Conference on Decision and Control (CDC)*, 2018.

[10] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York, NY, USA: Wiley-Interscience, 1991.

[11] C. Dwork, "Differential privacy: A survey of results," in *Theory and Applications of Models of Computation*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 1–19.

[12] S. Han, U. Topcu, and G. J. Pappas, "Differentially private convex optimization with piecewise affine objectives," in *Proceedings of the 53rd IEEE Conference on Decision and Control*, 2014.

[13] J. Soria-Comas and J. Domingo-Ferrer, "Optimal data-independent noise for differential privacy," *Information Sciences*, vol. 250, pp. 200 – 214, 2013.

[14] Q. Geng and P. Viswanath, "The optimal mechanism in differential privacy," in *Proceedings of the IEEE International Symposium on Information Theory*, 2014, pp. 2371–2375.

[15] F. Farokhi and G. Nair, "Privacy-constrained communication," *IFAC-PapersOnLine*, vol. 49, pp. 43 – 48, 2016.

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

[17] E. V. Belmega, L. Sankar, and H. V. Poor, "Enabling data exchange in two-agent interactive systems under privacy constraints," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, pp. 1285–1297, 2015.

[18] C. Murguia, I. Shames, F. Farokhi, and D. Nešic, "Privacy against state estimation: An optimization framework based on the data processing inequality," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 7368–7373, 2020.

[19] C. Murguia, I. Shames, F. Farokhi, D. Nešić, and H. V. Poor, "On privacy of dynamical systems: An optimal probabilistic mapping approach," *IEEE Transactions on Information Forensics and Security*, 2021.

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

[21] H. Hayati, C. Murguia, and N. van de Wouw, "Finite horizon privacy of stochastic dynamical systems: A synthesis framework for gaussian mechanisms," in *2021 60th IEEE Conference on Decision and Control (CDC)*. IEEE, 2021, pp. 5607–5613.

[22] ——, "Finite horizon privacy of stochastic dynamical systems: A synthesis framework for dependent gaussian mechanisms," *arXiv preprint arXiv:2108.01755*, 2021.

[23] A. Prékopa, "Logarithmic concave measures and related topics," in *Stochastic programming*. Citeseer, 1980.

[24] M. Huemer, O. Lang, and C. Hofbauer, "Component-wise conditionally unbiased widely linear mmse estimation," *Signal Processing*, vol. 133, pp. 227–239, 2017.

[25] H. Hayati, C. Murguia, and N. van de Wouw, "Gaussian mechanisms against statistical inference: Synthesis tools," *arXiv preprint arXiv:2111.15307*, 2021.

[26] F. Zhang, *The Schur complement and its applications*. Springer Science & Business Media, 2006, vol. 4.

[27] M. Bagnoli and T. Bergstrom, "Log-concave probability and its applications," *Economic Theory*, vol. 26, pp. 445 – 469, 2005.

[28] S. Dharmadhikari and K. Joag-Dev, *Unimodality, convexity, and applications*. Elsevier, 1988.

[29] S. Hoggar, "Chromatic polynomials and logarithmic concavity," *Journal of Combinatorial Theory, Series B*, vol. 16, no. 3, pp. 248–254, 1974.

[30] O. Johnson and C. Goldschmidt, "Preservation of log-concavity on summation," *ESAIM: Probability and Statistics*, vol. 10, pp. 206–215, 2006.

[31] A. Marsiglietti and V. Kostina, "A lower bound on the differential entropy of log-concave random vectors with applications," *Entropy*, vol. 20, no. 3, p. 185, 2018.

[32] J. Wellner, "Log-concave distributions: definitions, properties, and consequences," *Presentation, University of Paris-Diderot*, 2012.

[33] S. Bobkov and M. Madiman, "The entropy per coordinate of a random vector is highly constrained under convexity conditions," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4940–4954, 2011.

[34] J. Delpiano, "Fast mutual information of two images or signals (https://www.mathworks.com/matlabcentral/fileexchange/13289-fast-mutual-information-of-two-images-or-signals)," 2021.