Information-Theoretic Privacy through Chaos Synchronization and Optimal Additive Noise

Carlos Murguia[1,a], Iman Shames[1,b], Farhad Farokhi[1,2,c], and Dragan Nešić[1,d]

[1]Department of Electrical and Electronic Engineering, University of Melbourne, Australia

[2]The Commonwealth Scientific and Industrial Research Organisation (CSIRO), Data61, Australia

[a]carlos.murguia@unimelb.edu.au; [b]iman.shames@unimelb.edu.au; [c]farhad.farokhi@unimelb.edu.au; [d]dnesic@unimelb.edu.au

1 Abstract

We study the problem of maximizing privacy of data sets by adding random vectors generated via synchronized chaotic oscillators. In particular, we consider the setup where information about data sets, queries, is sent through public (unsecured) communication channels to a remote station. To hide private features (specific entries) within the data set, we corrupt the response to queries by adding random vectors. We send the distorted query (the sum of the requested query and the random vector) through the public channel. The distribution of the additive random vector is designed to minimize the mutual information (our privacy metric) between private entries of the data set and the distorted query. We cast the synthesis of this distribution as a convex program in the probabilities of the additive random vector. Once we have the optimal distribution, we propose an algorithm to generate pseudorandom realizations from this distribution using trajectories of a chaotic oscillator. At the other end of the channel, we have a second chaotic oscillator, which we use to generate realizations from the same distribution. Note that if we obtain the same realizations on both sides of the channel, we can simply subtract the realization from the distorted query to recover the requested query. To generate equal realizations, we need the two chaotic oscillators to be synchronized, i.e., we need them to generate exactly the same trajectories on both sides of the channel synchronously in time. We force the two chaotic oscillators into *exponential synchronization* using a driving signal. Exponential synchronization implies that trajectories of the oscillators converge to each other exponentially fast for all admissible initial conditions and are perfectly synchronized in the limit only. Thus, in finite time, there is always a "small" difference between their trajectories. To implement our algorithm, we assume (as it is often done in related work) that systems have been operating for sufficiently long time so that this small difference is negligible and oscillators are practically synchronized. We quantify the worst-case distortion induced by assuming perfect synchronization, and show that this distortion vanishes exponentially fast. Simulations are presented to illustrate our results.

Keywords: Privacy; Data Sets, Queries, Mutual Information, Chaos.

2 Introduction

In a hyperconnected world, scientific and technological advances have led to an overwhelming amount of user data being collected and processed by hundreds of companies over public networks. Companies mine this data to provide targeted advertising and personalized services. However, these new technologies have also led to an alarming widespread loss of privacy in society. Depending on adversary's resources, opponents may infer private user information from public data available on the internet and unsecured/public servers. A motivating example of privacy loss is the potential use of data from smart electrical meters by criminals, advertising agencies, and governments, for monitoring the presence and activities of occupants [1, 2]. Other examples are privacy loss caused by information sharing in distributed control systems and cloud computing [3]; the use of travel data for traffic estimation in intelligent transportation systems [4]; and data collection and sharing by the Internet-of-Things (IoT) [5], which is, most of the time, done without the user's informed consent. These privacy concerns show that there is an acute need for privacy preserving mechanisms capable of handling the new privacy challenges induced by an interconnected world.

In this manuscript, we consider the problem of hiding private information X of users (modeled as discrete random vectors) within datasets when publicly sharing requested queries $Y(X)$ from the same source. In particular, the aim of our privacy scheme is to respond to queries with distorted queries of the form $Z = Y(X)+V$ such that, when releasing Z, the private X is "hidden". Realizations of the vector Z are transmitted over a public (unsecured) communication channel to a remote station. Then, if we do not distort $Y(X)$ before transmission, information about X is directly accessible through the public channel. The first problem that we address is the design of the probability distribution of V to maximize privacy, i.e., the distribution of

V must be constructed so that $Z = Y(X) + V$ carries as little information about X as possible. Here, we follow an *information-theoretic approach* to privacy. We use the *mutual information* between private information X and distorted queries $Y(X)+V$, $I[X;Y(X)+V]$, as *privacy metric*. The design of the discrete additive vector is casted as an optimization problem where we minimize $I[X;Y(X)+V]$ using the probability mass function of V, $p_V(v)$, as optimization variables. That is, the optimal distribution, $p_V^*(v)$, is given by $p_V^*(v) := \arg\min_{p_V(v)} I[X;Y(X)+V]$, where $p_V(v)$ is taken over a class of probability mass functions. Contrary to related work [6]-[11], we do not consider any sort of privacy-distortion trade-off in our formulation. We actually aim at making $I[X;Y(X)+V]$ as small as possible regardless of the distortion between $Y(X)$ and $Y(X)+V$ induced by V. Distortion is not an issue because we seek to generate exactly the same realization of V at the remote station; then, we could recover the query by simply subtracting this realization from the one of $Z = Y(X) + V$. In order to accomplish this, we propose an algorithm to generate pseudorandom realizations from $p_V^*(v)$ at both sides of the channel using trajectories of two synchronized chaotic oscillators.

There are a number of requirements that the oscillators must satisfy for our algorithm to work: 1) trajectories of the oscillators must be *bounded* and *chaotic*; 2) they must be *synchronized*, i.e., we need them to generate exactly the same trajectories on both sides of the channel synchronously in time; and 3) the synchronous solution, regarded as a random process, must be *stationary*. Before giving the algorithm, we provide general guidelines for selecting the dynamics of the oscillators so that all the aforementioned requirements are satisfied. In particular, we use a range of well-known results in the literature to provide a synthesis procedure that allows to choose suitable oscillators. For boundedness, we use the notion of *Input-to-State-Stability* (ISS); for chaos, we employ standard *largest Lyapunov exponent methods* [12] and the (0-1) *test* [13]; for synchronization, we introduce the notion of *convergent systems* [14]; and for stationarity, we use *hyperbolicity* of the chaotic trajectories [15].

To generate equal realizations, our algorithm needs trajectories of the two chaotic oscillators (one at each side of the channel) to be synchronized. We force the oscillators into *exponential synchronization* using a driving signal. Exponential synchronization implies that trajectories of the oscillators converge to each other exponentially for all admissible initial conditions and are perfectly synchronized in the limit only. Therefore, in finite time, there is always a "small" difference between their trajectories. However, because oscillators synchronize exponentially fast, and it is often possible in practice to select initial conditions from a known compact set (known to both sides of the channel), it is safe to assume that the interconnected systems have been operating for sufficiently large time such that oscillators are *practically* synchronized, i.e., the synchronization error is so small that trajectories can be assumed to be equal. This is a standard assumption that is made in most, if not all, of the existing work on chaotic encryption based on synchronization [16]-[20]. Here, we give sufficient conditions for exponential synchronization to occur, provide tools for selecting the oscillators such that these conditions are satisfied, and assume that, after transients have settled down, trajectories are perfectly synchronized to some chaotic trajectory, say $\phi(t) \in \mathbb{R}^{n_\zeta}$, $\zeta \in \mathbb{N}$. If $n_\zeta > 1$, our algorithm uses any entry $\phi^s(t) \in \mathcal{S} \subset \mathbb{R}$ of $\phi(t)$ to generate realizations from $p_V^*(v)$, where $\mathcal{S}$ denotes some compact set that characterizes the support of $\phi^s(t)$. Because oscillators are selected such that $\phi(t)$, regarded as a random process, is stationary, samples from $\phi^s(t)$ follow a stationary probability density function. We obtain this density through Monte Carlo simulations [21] and divide its support $\mathcal{S}$ into a finite set of cells $C = \{c^1, \ldots, c^M\}$ such that the probability that $\phi^s(t)$ lies in these cells equals the optimal probability distribution $p_V^*(v)$. That is, we generate pseudorandom realizations from $p_V^*(v)$ by properly selecting C and evaluating if $\phi^s(t)$ lies in C at the sampling instants.

The use of additive noise to preserve privacy is common practice. There are mainly two classes of privacy metrics considered in the literature; namely, differential privacy [22]-[23] and information-theoretic metrics, e.g., mutual information, conditional entropy, Kullback-Leibler divergence, and Fisher information [24]-[28]. In differential privacy, because it provides certain privacy guarantees, Laplace noise is usually used [29]. However, when maximal privacy is desired, Laplace noise is generally not the optimal solution. This raises the fundamental question: what is the noise distribution achieving maximal privacy? This question has many possible answers depending on the particular privacy metric being considered and the system configuration, see, e.g., [6]-[8],[11], for differential privacy based results, and [24]-[28], for information theoretic results. In general, if the data to be kept private follows continuous distributions, the problem of finding the optimal additive noise to maximize privacy is hard to solve. If a close-form solution for the distribution is desired, the problem amounts to solving a set of nonlinear partial differential equations which, in general, might not have a solution, and even if they do have a solution, it is hard to find [24]. This problem has been addressed by imposing some particular structure on the considered distributions or assuming the data to be kept private is deterministic [24],[7],[8]. The authors in [7],[8] consider deterministic input data sets and treat optimal distributions as distributions that concentrate probability around zero as much as possible while

ensuring differential privacy. Under this framework, they obtain a family of piecewise constant probability density functions that achieve minimal distortion for a given level of privacy. In [24], the authors consider the problem of preserving the privacy of deterministic databases using additive continuous noise with constrained support. They use the Fisher information and the Cramer-Rao bound to construct a privacy metric between deterministic data and the one with the additive noise, and find the probability density function that minimizes it. Moreover, they prove that, in the unconstrained support case, the optimal noise distribution minimizing the Fisher information is Gaussian. This observation has been also made in [30] when using mutual information as a measure of privacy. We remark that most of the aforementioned papers consider privacy-distortion trade-offs when designing their distorting mechanisms. We do not consider this trade-off here because, at the end of the channel, we remove the distortion that we induce using our synchronization based formulation.

Existing work on chaotic encryption based on synchronization [16]-[20] directly uses the states of the chaotic oscillators to mask private information. That is, standard algorithms do not use chaotic trajectories to generate pseudorandom realization from probability distributions (as we do here); instead, they simply add the value of the sampled chaotic trajectory (or functions of it) to private messages. Although the latter succeeds in masking messages, it does not give any privacy guarantees (neither information-theoretic nor in a differential privacy sense) on the private information, and it is not optimal in any sense. Hence, the contributions of our scheme with respect to existing work on chaotic encryption [16]-[20] are the treatment of fully stochastic datasets, the information-theoretic privacy guarantees that our framework provides, and the optimal performance of the designed distorting additive vector (optimal in the sense of minimizing the mutual information $I[X; Y(X) + V]$). The work here is inspired by the experimental results presented in [31], where the authors propose a framework similar to ours for deterministic data using a electronic circuit implementation of the Mackey-Glass chaotic oscillator [32]. The contribution of our work with respect to [31] is threefold: 1) we consider fully stochastic data, which makes the privacy scheme fundamentally very different; 2) we provide a general formulation that encompasses a large class of chaotic systems, not only the electronic circuit implementation of the Mackey-Glass oscillator; and 3) we generate realizations from optimal distorting distributions, in [31], they consider uniform distributions only which is not optimal for stochastic data.

Next, we summarize the main contributions of the chapter.

Contributions:

1) We provide a general information-theoretic privacy framework based on optimal additive distorting random vectors and synchronization of chaotic oscillators; 2) We prove that the synthesis of the probability mass function $p_V(v)$ of the distorting random vector V can be posed as a convex program in $p_V(v)$ over a class of probability mass functions; 3) We provide an algorithm to generate pseudorandom realizations from this distribution using trajectories of chaotic oscillators; 4) Using off-the-shelf results in the literature, we provide a synthesis procedure for selecting the dynamics of the oscillators so that our algorithm is guaranteed to work.

The remainder of the paper is organized as follows. In Section 3, we present some preliminaries results needed for the subsequent sections. We introduce the notion of convergent systems and the concept of mutual information. The general formulation and the specific problems to be addressed are given in Section 4. In Section 5, we pose the synthesis of the probability distribution of the optimal distorting vector. General guidelines for selecting the chaotic oscillators are given in Section 6. The algorithm for generating pseudorandom realizations from the optimal distribution is presented in Section 7. Simulation results are given in Section 8 and concluding remarks in Section 9.

3 Notation and Preliminaries

The symbol $\mathbb{R}$ stands for the real numbers, $\mathbb{R}_{>0}(\mathbb{R}_{\geq 0})$ denotes the set of positive (non-negative) real numbers. The symbol $\mathbb{N}$ stands for the set of natural numbers. The Euclidian norm in $\mathbb{R}^n$ is denoted simply as $|\cdot|$, $|x|^2 = x^\top x$, where $^\top$ defines transposition. For a given measurable function $u(t)$, $t \in \mathbb{R}_{\geq 0}$, we denote its $\mathcal{L}_\infty$ norm as $||u||_\infty := \operatorname{ess\,sup}_{t\geq 0} |u(t)|$, where ess sup denotes essential supremum. Matrices composed of only ones and only zeros of dimension $n \times m$ are denoted by $\mathbf{1}_{n\times m}$ and $\mathbf{0}_{n\times m}$, respectively, or simply $\mathbf{1}$ and $\mathbf{0}$ when their dimensions are clear. For square matrices $A \in \mathbb{R}^{n\times n}$, $\rho[A]$ denotes the spectral radius of A. A continuous function $\gamma : [0, a) \to [0, \infty)$ is said to belong to class $\mathcal{K}$ if it strictly increasing and $\gamma(0) = 0$. Similarly, a continuous function $\beta : [0, a) \times [0, \infty) \to [0, \infty)$ belongs to class $\mathcal{KL}$ if, for fixed s, $\beta(r, s)$ belongs to class $\mathcal{K}$ with respect to r and, for fixed r, $\beta(r, s)$ is decreasing with respect to s and $\lim_{s\to\infty} \beta(r, s) = 0$. Consider a discrete random vector X with alphabet $\mathcal{X} = \{x_1, \ldots, x_N\}$, $x_i \in \mathbb{R}^m$, $m \in \mathbb{N}$, $i \in \{1, \ldots, N\}$, and probability mass function $p_X(x) = \Pr[X = x]$, $x \in \mathcal{X}$, where $\Pr[B]$ denotes probability of event B. Similarly, for two random vectors X and Y, taking values in the alphabets $\mathcal{X}$ and $\mathcal{Y}$, respectively, their joint probability

mass function is denoted by $p_{X,Y}(x,y)$, the marginal distribution of X is given by $p_X(x) = \sum_{y\in\mathcal{Y}} p_{X,Y}(x,y)$, and the conditional distribution of X given Y as $p_{Y|X}(y|x) = p_{X,Y}(x,y)/p_X(x)$. Analogously, for a continuous random vector Y, we denote their (multivariate) probability density function as $f_Y(y)$. The notation $X \sim f_X(x)$ ($X \sim p_X(x)$) stands for continuous (discrete) random vectors X following the probability density (mass) function $f_X(x)$ ($p_X(x)$). We denote by "Simplex" the probability simplex defined by $\sum_{x\in\mathcal{X}} p_X(x) = 1$, $p_X(x) \geq 0$ for all $x \in \mathcal{X}$. The notation $E[a]$ denotes the expected value of the random vector a. We denote independence between two random vectors, X and Y, as $X \perp\!\!\!\perp Y$.

3.1 Mutual Information

Definition 1 *Consider two random vectors, X and Y, with joint probability mass function $p_{X,Y}(x,y)$ and marginal probability mass functions, $p_X(x)$ and $p_Y(y)$, respectively. Their mutual information $I[X;Y]$ is defined as the relative entropy between the joint distribution and the product distribution $p_X(x)p_Y(y)$, i.e.,*

$$I[X;Y] := \sum_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} p_{X,Y}(x,y) \log \frac{p_{X,Y}(x,y)}{p_X(x)p_Y(y)}.$$

Mutual information $I[X;Y]$ between two jointly distributed vectors, X and Y, is a measure of the dependence between X and Y.

3.2 Convergent Systems

Consider the dynamical system:

$$\dot{x}(t) = r(x(t), u(t)), \tag{1}$$

with $t \in \mathbb{R}_{\geq 0}$, state $x \in \mathbb{R}^n$, input $u \in \mathcal{U} \subseteq \mathbb{R}^m$, and vector field $r : \mathbb{R}^n \times \mathcal{U} \to \mathbb{R}^n$. The vector field $r(x,u)$ is continuously differentiable in x, and $u(t)$ is piecewise continuous in t and takes values in some compact set $\mathcal{U} \subseteq \mathbb{R}^m$.

Definition 2 [33]. *System (1) is said to be globally asymptotically convergent if and only if for any bounded input $u(t)$, $t \in \mathbb{R}$, there is a unique bounded globally asymptotically stable solution $\bar{x}_u(t)$, $t \in \mathbb{R}$, such that $\lim_{t\to\infty} |x(t) - \bar{x}_u(t)| = 0$ for all initial conditions.*

For a *convergent system*, the limit solution is solely determined by the external excitation $u(t)$ and not by the initial conditions. A sufficient condition for convergence obtained by Demidovich [33] and later extended in [14] is presented in the following proposition.

Proposition 1 [33, 14]. *If there exists a positive definite matrix $P \in \mathbb{R}^{n\times n}$ such that all the eigenvalues $\lambda_i(Q)$ of the symmetric matrix*

$$Q(x,u) = \frac{1}{2}\left(P\left(\frac{\partial r}{\partial x}(x,u)\right) + \left(\frac{\partial r}{\partial x}(x,u)\right)^T P\right), \tag{2}$$

are negative and separated from zero, i.e., there exists a constant $c \in \mathbb{R}_{>0}$ such that $\lambda_i(Q) \leq -c < 0$, for all $i \in \{1, ..., n\}$, $u \in \mathcal{U}$, and $x \in \mathbb{R}^n$, then system (1) is globally exponentially convergent; and, for any pair of solutions $x_1(t), x_2(t) \in \mathbb{R}^n$ of (1), the following is satisfied:

$$\frac{d}{dt}\Big(\big(x_1(t) - x_2(t)\big)^\top P\big(x_1(t) - x_2(t)\big)\Big) \leq -\alpha \left|x_1(t) - x_2(t)\right|^2, \; t \in \mathbb{R}_{\geq 0},$$

with constant $\alpha := (c/\lambda_{\max}(P))$ and $\lambda_{\max}(P)$ being the largest eigenvalue of the symmetric matrix P.

Remark 1 *There are other methods to verify that trajectories of system (1) converge to a limit solution that is independent of the initial conditions and solely determined by the external excitation $u(t)$. For instance, contraction theory [34], Lyapunov function approach to incremental stability [35], the quadratic (QUAD) inequality approach (a Lipschitz-like condition) [36], and differential dissipativity [37], which are all concepts that are closely related to notion of convergent systems [14] that we use here.*

4 Problem Setup

Let X be a discrete random vector that must be kept private. The alphabet and probability mass function of X are denoted as $\mathcal{X} = \{x_1, \ldots, x_N\}$, $x_i \in \mathbb{R}^{n_x}$, $n_x \in \mathbb{N}$, $i \in \{1, \ldots, N\}$ and $p_X(x) = \Pr[X = x]$, $x \in \mathcal{X}$,

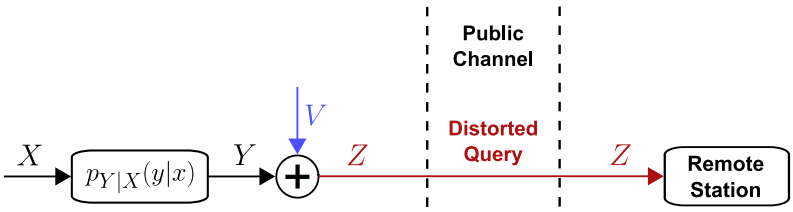

Figure 1: Configuration for Problem 1.

respectively. The n_x entries of X represent, for instance, private entries of n_x users within a dataset that is stored by a trusted server. The server admits queries of the form $Y = q(X)$, $Y \in \mathbb{R}^{n_y}$, for some (stochastic or deterministic) mapping $q : \mathbb{R}^{n_x} \to \mathbb{R}^{n_y}$ characterized by the transition probabilities $p_{Y|X}(y|x)$, $x \in \mathcal{X}$, $y \in \mathcal{Y}$, where $\mathcal{Y} = \{y_1, \ldots, y_M\}$, $y_i \in \mathbb{R}^{n_y}$, $n_y \in \mathbb{N}$. The aim of our privacy scheme is to respond to queries of the form $q(X)$ with distorted queries $Z = q(X) + V$, for some discrete random vector V (with $V \perp\!\!\!\perp Y$), such that, when releasing Z, the individual entries of X are "hidden". Realizations of the vector Z are transmitted over a public (unsecured) communication channel to a remote station, see Figure 1. Then, if we do not add V to $q(X)$ before transmission, information about X is directly accessible through the public channel. As a preliminary problem that we need to solve for the subsequent results, we address the design of the probability distribution of V to maximize privacy, i.e., the distribution of V must be constructed so that the sum, $Z = q(X) + V$, carries as little information about X as possible. In this manuscript, we use the *mutual information* between X and $Z = Y + V$, $I[X; Z]$, as *privacy metric*. We aim at finding the probability mass function of V, $p_V(v)$, that minimizes $I[X; Z]$ over a class of probability mass functions. That is, we cast the design of $p_V(v)$ as an optimization problem with cost function $I[X; Z]$, optimization variables $p_V(v)$, and subject to $V \perp\!\!\!\perp Y$ and the usual probability simplex constraints. Note that, contrary to related work [9]-[11],[27],[28], we do not consider any sort of privacy-distortion trade-off in our formulation. We minimize $I[X; Y + V]$ regardless of the distortion between Y and $Y + V$ induced by V. Distortion is not an issue because, we seek to generate exactly the same realization of V at the remote station and then recover the query by subtracting this realization from the one of $Z = Y + V$. This is addressed in Problem 2 and Problem 3 below.

We let V be a discrete random vector with alphabet $\mathcal{Y}$ and probability mass function $p_V(v) = \Pr[V = v]$, $v \in \mathcal{Y}$, i.e., the alphabet of V and the one of the query $Y = q(X)$ are equal. Having equal alphabets imposes a tractable convex structure on the cost $I[X; Z]$ and reduces the optimization variables to the probabilities of each element of the alphabet. The case with arbitrary alphabet leads to a combinatorial optimization problem where the objective changes its structure for different combinations. We do not address this case in this manuscript; it is left as a future work. In what follows, we formally present the optimization problem we seek to address.

Problem 1 [Optimal Distribution of the Additive Distorting Signal] *For given $p_X(x) = \Pr[X = x]$ and $p_{Y|X}(y|x) = \Pr[Y = y|X = x]$, $x \in \mathcal{X}$, $y \in \mathcal{Y}$, find the probability mass function $p_V(v) = \Pr[V = v]$, $v \in \mathcal{Y}$ solution of the optimization problem:*

$$\begin{cases} p_V^*(v) := \underset{p_V(v)}{\arg\min}\ I[X; V + Y], \\ \text{s.t. } V \perp\!\!\!\perp Y \text{ and } p_V(v) \in \text{ Simplex.} \end{cases} \tag{3}$$

Here, $p_V^*(v)$ denotes the optimal distribution solution to (3). To hide X, once we have obtained $p_V^*(v)$, we aim at generating realizations $v \in \mathcal{Y}$ from this distribution, add them to the required query ($Y = q(X)$), and send realizations of the sum $Z = Y + V$ to the remote station through the public channel. At the other end of the channel, we seek to *generate the exact same realizations from $p_V^*(v)$* so that we can recover the query by simply subtracting V from Z, see Figure 2. Note that, in Figure 2, we have a recovered $\hat{Y}$ at the remote station rather that the actual Y. This is because we want to remark that, due to practical errors in our algorithm–e.g., due to communication delays and transients–realizations of V that we generate at both ends of the channel might be slightly different in practice. To generate these realizations, we use trajectories, $\phi_{u,1}^{\zeta}(t, \zeta_1(0), u(t))$, $t \in \mathbb{R}_{\geq 0}$, $\zeta_1(0) \in \mathbb{R}^{n_\zeta}$, $u(t) \in \mathbb{R}^{n_u}$, of a chaotic dynamical system of the form:

$$\begin{cases} \dot{\zeta}_1(t) = r(\zeta_1(t), u(t)), \\ s_1(t) = h(\zeta_1(t)), \end{cases} \tag{4}$$

with state $\zeta_1(t) \in \mathbb{R}^{n_\zeta}$, output $s_1(t) \in \mathbb{R}$, continuous in t input $u(t) \in \mathcal{U} \subset \mathbb{R}^{n_u}$ taking values in some compact set $\mathcal{U}$, continuous function $h : \mathbb{R}^{n_\zeta} \to \mathbb{R}$, and vector field $r : \mathbb{R}^{n_\zeta} \times \mathcal{U} \to \mathbb{R}^{n_\zeta}$ continuously differentiable in

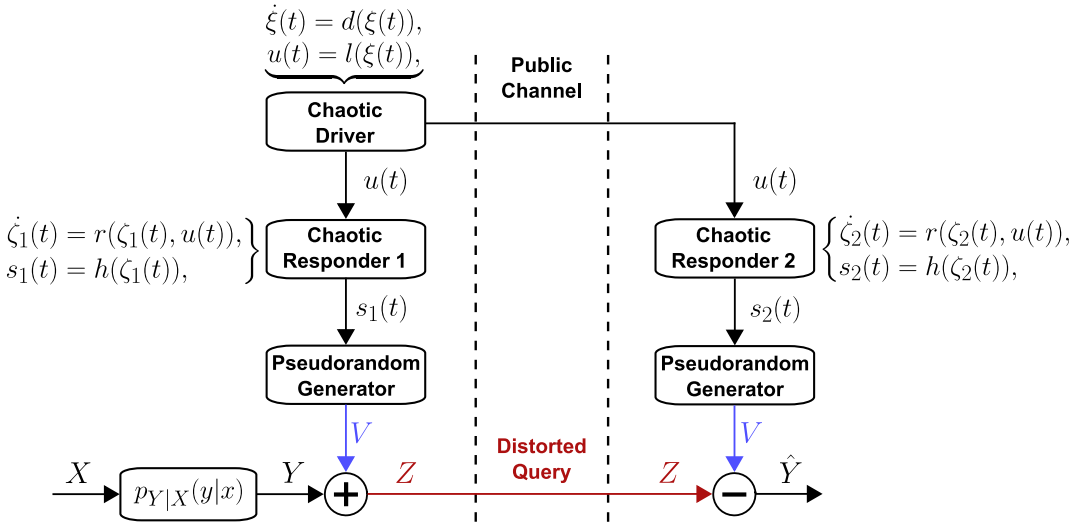

Figure 2: Complete System Configuration.

its first argument, uniformly in its second argument. Hereafter, system (4) is referred to as *responder* 1. Responder 1 is placed at the side of the trusted server, see Figure 2. The input signal $u(t)$ is generated by a chaotic autonomous exosystem:

$$\begin{cases} \dot{\xi}(t) = d(\xi(t)), \\ u(t) = l(\xi(t)), \end{cases} \tag{5}$$

with state $\xi(t) \in \mathbb{R}^{n_\xi}$, output $u(t) \in \mathcal{U} \subset \mathbb{R}^{n_u}$, and vector fields $d : \mathbb{R}^{n_\xi} \to \mathbb{R}^{n_\xi}$ and $l : \mathbb{R}^{n_\xi} \to \mathbb{R}^{n_u}$. The vector field $d(\xi)$ is locally Lipschitz in ξ and $l(\xi)$ is continuous. We refer to (5) as the *driver system*. We let $u(t)$ be connected to the remote station via the public channel, see Figure 2. At the other end of the channel, driven by the same input signal $u(t)$, we have a third chaotic oscillator with the same dynamics as (4) but with potentially different initial conditions, i.e., the second oscillator is given by

$$\begin{cases} \dot{\zeta}_2(t) = r(\zeta_2(t), u(t)), \\ s_2(t) = h(\zeta_2(t)), \end{cases} \tag{6}$$

with state $\zeta_2(t) \in \mathbb{R}^{n_\zeta}$ and output $s_2(t) \in \mathbb{R}$. We denote trajectories of (6) as $\phi^{\zeta}_{u,2}(t, \zeta_2(0), u(t))$ with $t \in \mathbb{R}_{\geq 0}$, $\zeta_2(0) \in \mathbb{R}^{n_\zeta}$, and $u(t) \in \mathcal{U} \subset \mathbb{R}^{n_\zeta}$. System (6) is referred to as *responder* 2. Note that if $\zeta_1(t) = \zeta_2(t)$, $t \in \mathbb{R}_{\geq 0}$, i.e., if systems (4) and (6) are synchronized, and we use the synchronous chaotic solution, say $\phi^{\zeta}_u(t, u(t))$, to generate realizations from $p^*_V(v)$, we could have the same realization of V at both sides of the channel.

Problem 2 [Boundedness, Chaos, and Synchronization] *State sufficient conditions on the vector fields $r(\cdot)$, $h(\cdot)$, $d(\cdot)$, and $l(\cdot)$ of the coupled system (4)-(6) such that: 1) trajectories of (4)-(6) exist and are bounded and chaotic; and 2) systems (4) and (6) exponentially synchronize, i.e., $\lim_{t\to\infty} |\zeta_1(t) - \zeta_2(t)| = 0$, exponentially fast.*

Remark 2 *Problem 2 seeks to enforce exponential synchronization by selecting the dynamics of the oscillators. Exponential synchronization implies that trajectories of the responders converge to each other exponentially for all initial conditions and are perfectly synchronized in the limit only. It follows that, in finite time, there is always a "small" difference between their trajectories. Nevertheless, because oscillators synchronize exponentially fast, and it is often possible in practice to select initial conditions from a known compact set (known to both the trusted server and the remote station), it is safe to assume that the interconnected systems have been operating for sufficiently large time such that oscillators are practically synchronized, i.e., the synchronization error is so small that trajectories can be assumed to be equal. This is a standard assumption that is made in most, if not all, of the existing work on chaotic encryption based on synchronization* [16]-[20].

Finally, once we have found functions solution to Problem 2, which guarantees exponential synchronization of the responders, and assuming that responders are synchronized (see Remark 2), we aim at designing a procedure to generate pseudorandom realizations from $p^*_V(v)$ using the synchronous chaotic solution $\phi^{\zeta}_u(t, u(t))$. Note that $\zeta_1(t) = \zeta_2(t) \Rightarrow s_1(t) = h(\zeta_1(t)) = s_2(t) = h(\zeta_2(t))$, for all $t \geq 0$. Moreover, because

$\zeta_1(t) = \zeta_2(t) = \phi_u^{\zeta}(t, u(t))$; then, $s_1(t) = s_2(t) = h(\phi_u^{\zeta}(t, u(t))) =: \phi_u^s(t, u(t)) \in \mathcal{S} \subset \mathbb{R}$ for some compact set $\mathcal{S}$. To reduce the complexity of the algorithm, we use the lower dimensional synchronous solution $\phi_u^s(t, u(t))$ to generate the realizations from $p_V^*(v)$.

Problem 3 [Generation of Optimal Pseudorandom Numbers] *Using the lower dimensional synchronous solution, $\phi_u^s(t, u(t))$, design an algorithm to generate pseudorandom realizations from the optimal distribution $p_V^*(v)$, $v \in \mathcal{Y}$.*

5 Optimal Distribution of the Additive Distorting Signal

In this section, we prove that Problem 1 can be posed as a convex program in the probabilities $p_V(v)$, $v \in \mathcal{Y}$. We derive an explicit expression for the cost function $I[X; Z]$, $Z = Y + V$, in terms of the given $p_X(x)$ and $p_{Y|X}(y|x)$ and the variables $p_V(v)$, restricted to satisfy the independence constraint $V \perp\!\!\!\perp Y$.

Lemma 1 *$I[X; Z]$ with $Z = Y + V$, $V \perp\!\!\!\perp Y$, is a convex function of $p_V(v)$, $v \in \mathcal{Y}$, for given $p_X(x)$ and $p_{Y|X}(y|x)$, $x \in \mathcal{X}$, $y \in \mathcal{Y}$; and can be written compactly in terms of $p_X(x)$, $p_{Y|X}(y|x)$, and $p_V(v)$, as follows:*

$$\begin{cases} I[X; Z] = \displaystyle\sum_{x \in \mathcal{X}} \sum_{z \in \mathcal{Z}} p_X(x) p_{Z|X}(z|x) \log \frac{p_{Z|X}(z|x)}{p_Z(z)}, & \text{(7a)} \\ p_{Z|X}(z|x) = \displaystyle\sum_{y \in \mathcal{Y}} p_{Y|X}(y|x) p_V(z - y), & \text{(7b)} \\ p_Z(z) = \displaystyle\sum_{y \in \mathcal{Y}} p_Y(y) p_V(z - y). & \text{(7c)} \end{cases}$$

Proof: The expression on the right-hand side of (7a) follows by inspection of Definition 1 and the fact that $p_{Z,X}(z, x) = p_X(x) p_{Z|X}(z|x)$. By [38, Theorem 2.7.4], cost (7a) is convex in $p_{Z|X}(z|x)$ for given $p_X(x)$. However, our optimization variables are $p_V(v)$ and not $p_{Z|X}(z|x)$. Note that X, Y, and Z form a Markov chain in that order [39]; therefore, $p_{X,Y,Z}(x, y, z) = p_X(x) p_{Y|X}(y|x) p_{Z|Y}(z|y)$. Marginalizing $p_{X,Y,Z}(x, y, z)$ with respect to $Y \in \mathcal{Y}$ and then conditioning with respect to X yields $p_{X,Z}(x, z) = \sum_{y \in \mathcal{Y}} p_X(x) p_{Y|X}(y|x) p_{Z|Y}(z|y)$ and $p_{Z|X}(z|x) = \sum_{y \in \mathcal{Y}} p_{Y|X}(y|x) p_{Z|Y}(z|y)$, respectively. Note that $p_{Z|X}(z|x)$ is just a linear transformation of $p_{Z|Y}(z|y)$. Hence, convexity with respect to $p_{Z|X}(z|x)$ implies convexity with respect to $p_{Z|Y}(z|y)$ because convexity is preserved under affine transformations [40]. Next, consider $p_{Z|Y}(z|y) = p_{Z,Y}(z, y)/p_Y(y)$. By definition, $p_{Z,Y}(z, y) = \Pr[Z = z, Y = y]$, $z \in \mathcal{Z}$, $y \in \mathcal{Y}$. Note that

$$\begin{aligned} \Pr[Z = z, Y = y] &= \Pr[Y + V = z, Y = y] = \Pr[V = z - y, Y = y] \\ &\overset{\text{(a)}}{=} \Pr[V = z - y] \Pr[Y = y] = p_V(z - y) p_Y(y), \end{aligned}$$

where (a) follows from independence between V and Y. Thus,

$$\begin{aligned} p_{Z|Y}(z|y) &= \frac{p_{Z,Y}(z, y)}{p_Y(y)} \\ &= \frac{p_V(z - y) p_Y(y)}{p_Y(y)} = p_V(z - y). \end{aligned}$$

We have concluded convexity of $I[X; Z]$ with respect to $p_{Z|Y}(z|y)$ above. Hence, because $p_{Z|Y}(z|y) = p_V(z-y)$ and $p_V(z-y)$ is a linear transformation of $p_V(v)$ ($p_V(z-y) = p_V(v)$ for $z-y = v$ and zero otherwise), the cost $I[X; Z]$ is convex in $p_V(v)$. Moreover, since $p_{Z|X}(z|x) = \sum_{y \in \mathcal{Y}} p_{Y|X}(y|x) p_{Z|Y}(z|y)$ and $p_{Z|Y}(z|y) = p_V(z-y)$, equality (7b) holds true. It remains to prove that $p_Z(z)$ can be written as (7c). Because $Z = Y + V$, $p_Z(z) = \Pr[Z = z]$, for a given $z \in \mathcal{Z}$, can be written as the sum of the probabilities of all $Y = y$ and $V = v$ that result in z, i.e.,

$$\begin{aligned} p_Z(z) &= \Pr[Z = z] = \Pr[Y + V = z] \\ &= \sum_{y \in \mathcal{Y}} \Pr[V = z - y, Y = y] \\ &\overset{\text{(b)}}{=} \sum_{y \in \mathcal{Y}} \Pr[Y = y] \Pr[V = z - y] = \sum_{y \in \mathcal{Y}} p_Y(y) p_V(z - y), \end{aligned}$$

where (b) follows from independence between V and Y. ■

By Lemma 1, the cost $I[X; Z]$, for $V \perp\!\!\!\perp Y$, is convex in $p(v)$ and parametrized by $p_X(x)$ and $p_{Y|X}(y|x)$. In

what follows, we cast the nonlinear program for solving Problem 1.

Theorem 1 *Given $p_X(x)$ and $p_{Y|X}(y|x)$, $x \in \mathcal{X}$, $y \in \mathcal{Y}$, the mapping $p_V(v)$, $v \in \mathcal{Y}$, that minimizes $I[X;Z]$, $Z = V + Y$, subject to $V \perp\!\!\!\perp Y$ can be found by solving the following convex program:*

$$\begin{cases} p_V^*(v) = \underset{p_V(v)}{\arg\min} \sum\limits_{x\in\mathcal{X}} \sum\limits_{y\in\mathcal{Y}} \sum\limits_{z\in\mathcal{Z}} p_X(x) p_{Y|X}(y|x) p_V(z-y) \log \dfrac{\sum_{y\in\mathcal{Y}} p_{Y|X}(y|x) p_V(z-y)}{\sum_{y\in\mathcal{Y}} p_Y(y) p_V(z-y)}, \\ \\ \text{s.t. } p_V(v) \in \text{ Simplex.} \end{cases} \tag{8}$$

Proof: Theorem 1 follows from Lemma 1.

6 Boundedness, Chaos, and Synchronization

6.1 Existence, Uniqueness, and Boundedness of Solutions

We start addressing existence, uniqueness, and boundedness of the solutions of the coupled systems (4)-(6). To be able to use synchronous solutions to generate realizations from $p_V^*(v)$, we first need these solutions to exist and be bounded. In the system description given above, we have assumed that $r(\zeta, u(t))$ is continuously differentiable in ζ uniformly in $u(t)$, $u(t)$ is continuous in t, and $d(\xi)$ is locally Lipschitz. These alone imply uniqueness and existence of solutions of (4)-(6) over some finite time interval $t \in [0, \tau]$, $\tau \in \mathbb{R}_{>0}$, [41, Theorem 2.2]. To conclude the latter for arbitrarily large τ, besides the locally Lipschitz assumption on the functions, we need boundedness of the solutions of (4)-(6) [41, Theorem 2.4]. Note that the coupled systems (4)-(6) have a cascade structure. The driver dynamics is independent of the responders states, and its output, $u(t)$, is the input of the responders. Then, an approach to conclude boundedness of the overall system is to conclude boundedness of the driver first, and then boundedness of the responders when driven by bounded inputs. In what follows, we formally introduce the notion of boundedness that we use here.

Definition 3 [41] *The solutions of* (5) *are bounded for a bounded set of initial conditions if there exists a positive constant c, independent of the initial time instant, and for every $a \in (0, c)$, there is $b = b(a) > 0$, independent of the initial time instant, such that $|\xi(0)| \leq a \Rightarrow |\xi(t)| \leq b$, $\forall\, t \geq 0$. If the latter holds for arbitrarily large a; then, the solutions of* (5) *are globally bounded.*

Remark 3 *Because $l(\xi)$ is continuous, by the extreme value theorem, boundedness of $\xi(t)$ implies boundedness of $u(t) = l(\xi(t))$.*

Remark 4 *We do not give conditions for boundedness of the solutions of* (5)*. It is assumed that the vector field $d(\xi)$ is such that the solutions of the driver are globally bounded. We refer the reader to, for instance,* [41, Theorem 4.18]*, where sufficient conditions for boundedness are given in terms of Lyapunov-like results.*

Next, for bounded solutions of the driver, we need the solutions of the responders to be bounded when driven by $u(t)$. To address this, we use the notion if Input-to-State-Stability (ISS) [42].

Definition 4 [42] *System* (4) *(and thus system* (5) *as well) is said to be Input-to-State-Stable if there exist a class $\mathcal{KL}$ function $\beta(\cdot)$ and a class $\mathcal{K}$ function $\gamma(\cdot)$ such that for any initial condition $\zeta_1(0)$ and any bounded input $u(t)$, the solution $\zeta_1(t)$ exists for all $t \in \mathbb{R}_{\geq 0}$ and satisfies: $|\zeta_1(t)| \leq \beta(\zeta_1(0), t) + \gamma\left(||u||_\infty\right)$.*

Remark 5 ISS *of the responders with respect to $u(t)$ guarantees that, for any bounded $u(t)$, the states $\zeta_1(t)$ and $\zeta_2(t)$ are bounded. Moreover, as t increases, $|\zeta_1(t)|$ and $|\zeta_2(t)|$ are ultimately bounded* [41] *by $\gamma\left(||u||_\infty\right)$, see* [42] *for further details.*

Remark 6 *Sufficient conditions for the responders to be ISS with input $u(t)$ are not provided here. We assume that the vector field $r(\zeta, u(t))$ is such that systems* (4) *and* (5) *are ISS with respect to $u(t)$. We refer the reader to, for instance,* [41, Theorem 4.19]*, where sufficient conditions for ISS are given in terms of ISS-Lyapunov functions.*

Remark 7 *The weaker property of integral Input-to-State-Stable* (iISS) [43] *could be used to conclude boundedness of the responder's trajectories when driven by "sufficiently small" inputs. We refer the reader to* [44]*, where sufficient conditions for* iISS *and related boundedness results are given.*

6.2 Synchronization

Next, we give sufficient conditions on $r(\zeta, u(t))$ such that $\lim_{t\to\infty} |\zeta_1(t) - \zeta_2(t)| = 0$, i.e., the responders exponentially synchronize. We assume that solutions of the coupled systems (4)-(6) exist and are bounded, i.e., vector fields $r(\cdot)$, $d(\cdot)$, and $l(\cdot)$ satisfy the conditions stated in the previous subsection. Then, for bounded $u(t)$, a sufficient condition for the responders to exponentially synchronize is that systems (4) and (6) are *convergent systems* in the sense of Definition 2. The latter implies that, because both responders are driven by the input $u(t)$ and their dynamics are described by the same set of differential equations, trajectories of (4) and (6) converge to the same the limit solution, $\phi_u^{\zeta}(t, u(t))$, and this solution is solely determined by $u(t)$ and not by the initial conditions. In the following corollary of Proposition 1, we give a sufficient condition for the responders to be exponentially convergent (and thus to exponentially synchronize).

Corollary 1 *Consider the responders* (4) *and* (6)*. If there exists a positive definite matrix* $P \in \mathbb{R}^{n_\zeta \times n_\zeta}$ *such that, for all* $u \in \mathbb{R}^{n_u}$ *and* $\zeta \in \mathbb{R}^{n_\zeta}$*, all the eigenvalues of the symmetric matrix:*

$$\frac{1}{2}\left(P\left(\frac{\partial r}{\partial \zeta}(\zeta, u)\right) + \left(\frac{\partial r}{\partial \zeta}(\zeta, u)\right)^T P \right), \tag{9}$$

are negative and separated from zero; then, responders (4) *and* (6) *are globally exponentially convergent, and thus* $\lim_{t\to\infty} |\zeta_1(t) - \zeta_2(t)| = 0$*, exponentially fast.*

Remark 8 *If the driver's output* $u(t)$ *is to be sent over a network and quantization (or some sort of coding) is required, we would need to drive responders by the same quantized* $u(t)$*, say* $u_Q(t)$*, to achieve exponential synchronization. That is, if we quantize* $u(t)$ *to obtain* $u_Q(t)$*, and we drive both responders by* $u_Q(t)$ *(with, e.g., a Zero-Order-Hold* (ZOH)*), they would also exponentially synchronize. They would synchronize to a different trajectory than when driven by* $u(t)$*, but they would synchronize exponentially fast.*

Besides the notion of convergent systems, there are other methods available in the literature that can be used to verify that trajectories of responders asymptotically synchronize to a limit solution that is independent of the initial conditions. See Remark 1 for details.

6.3 Chaotic Dynamics

There are mainly two branches of methods to identify chaotic dynamics; namely, standard largest Lyapunov exponent methods [12], and the more recent (0-1) test [13]. Both methods use trajectories (numerical or experimental) of the systems under study to decide whether they are chaotic or not. In general, there are no sufficient conditions directly on the differential equations (the vector fields $r(\cdot)$ and $d(\cdot)$) such that chaotic trajectories are guaranteed to occur. There are, however, many well known systems in the literature known to exhibit chaotic trajectories. For instance, the Lorenz system [45], Duffing [46] and van der Pol [47] oscillators, the Rössler [48] and Chua [49] systems, and neural oscillators [50] (e.g., the Hodgkin-Huxley, Morris-Lecar, Hindmarsh-Rose, and FitzHugh-Nagumo oscillators). We can use any of these chaotic systems (if they satisfy all the required extra conditions, see Section 6.4) as driver and then select a pair of responders with convergent dynamics. Indeed, we need to verify that the responders that we choose produce chaotic trajectories when driven by the chaotic driver. Moreover, to generate the pseudorandom realizations from $p_V^*(v)$ (this is addressed in the next section), we need the chaotic trajectories of the responders, regarded as a random process, to be *stationary*, i.e., after transients have settled down, trajectories must follow a stationary probability distribution [39] which is independent of the initial conditions. The latter is a strong condition that is not satisfied for all chaotic systems. The existence of stationary distributions for chaotic trajectories has been proven for hyperbolic and quasi-hyperbolic (also called singular-hyperbolic) chaotic systems [15]. The definition of (quasi) hyperbolic dynamical systems [15, 51] is technical and not needed for the subsequent results. It requires concepts from differential topology that we prefer to omit here for readability of the manuscript. It suffices to know that the chaotic system that we use for the driver must lead to stationary distributions of the responders. This can be tested numerically by Monte Carlo simulations [21]. Moreover, there are many well-known chaotic systems with (quasi) hyperbolic dynamics in the literature, e.g., the Lorenz and Chua systems [52], neural oscillators [53], the many predator-pray like systems given in [54, 55], and some mechanical nonlinear oscillators [56]. In the next subsection, we provide a synthesis procedure to choose the functions of the coupled systems (4)-(6) such that all the required conditions mentioned above are satisfied.

6.4 General Guidelines

Synthesis Procedure:

1) Select a driver dynamics (5) (i.e., the vector field $d(\xi)$) known to be chaotic and (quasi) hyperbolic (e.g., systems in [52]-[56]).

2) Verify that the corresponding $d(\xi)$ is locally Lipschitz and the trajectories of the driver are globally bounded, in the sense of Definition 3, using, e.g., [41, Theorem 4.18].

3) In (5), let $\xi = (\xi^1, \ldots, \xi^{n_\xi})^\top \in \mathbb{R}^{n_\xi}$, $\xi^i \in \mathbb{R}$, and $u(t) = l(\xi(t)) = \xi^j(t)$, $i, j \in \{1, \ldots, n_\xi\}$, i.e., fix the output of the driver to be any state of (5). In doing this, we ensure that $u(t)$ is continuous, bounded, chaotic, and (quasi) hyperbolic.

4) For the responders (4) and (6), select any continuously differentiable vector field $r(\zeta, u)$ (with respect to ζ) leading to ISS dynamics, see Remark 6, and satisfying the conditions for convergence in Corollary 1, e.g., $r(\zeta, u) = A\zeta + \psi(u)$, for any matrix $A \in \mathbb{R}^{n_\zeta \times n_\zeta}$ with spectral radius $\rho[A] < 1$ and differentiable vector field $\psi : \mathbb{R}^{n_u} \to \mathbb{R}^{n_\zeta}$. Then, we ensure that the responders have bounded trajectories and exponentially synchronize.

5) Verify that the trajectories of the responders, when driven by the chaotic driver, are chaotic (using Lyapunov exponents or the (0-1) test) and, after transients have settled down, lead to a stationary probability distribution independent of the initial conditions. See Section 6.3 for details.

6) In (4) (and respectively in (6)), let $\zeta_1 = (\zeta_1^1, \ldots, \zeta_1^{n_\zeta})^\top \in \mathbb{R}^{n_\zeta}$, $\zeta_1^i \in \mathbb{R}$, and $s_1(t) = l(\zeta_1(t)) = \zeta_1^j(t)$, $i, j \in \{1, \ldots, n_\xi\}$, i.e., fix the output of the responders to be any state of (4) and (6), respectively. Indeed, we need the same j for both responders, i.e., $s_1(t) = \zeta_1^j(t)$ and $s_2(t) = \zeta_2^j(t)$. In doing this, we ensure that $s_1(t)$ and $s_2(t)$ are continuous, bounded, chaotic, and lead to stationary probability distributions.

7 Generation of Optimal Pseudorandom Numbers

In this section, we assume that the driver and the responders dynamics have been designed following the general guidelines in Section 6.4. Then, for sufficiently large t, the chaotic trajectories of the responders are practically synchronized, i.e., for any finite $t^* \in \mathbb{R}_{>0}$, there is $\epsilon_{t^*} \in \mathbb{R}_{>0}$, such that $|s_1(t) - \phi_u^s(t, u(t))| \leq \epsilon_{t^*}$ and $|s_2(t) - \phi_u^s(t, u(t))| \leq \epsilon_{t^*}$, for all $t \geq t^*$, where $\phi_u^s(t, u(t)) \in \mathcal{S} \subset \mathbb{R}$ denotes the asymptotic synchronous solution for some compact set $\mathcal{S}$; and samples from $\phi_u^s(t, u(t))$ follow a stationary probability distribution. Here, we assume that the responders have been operating for sufficiently large time such that the synchronization error, $|s_1(t) - s_2(t)|$, is so small that trajectories of the responders can be assumed to be equal to $\phi_u^s(t, u(t))$ (see Remark 2), i.e., t^* is sufficiently large so that ϵ_{t^*} is practically zero. In Section 7.1, we quantify the worst-case distortion induced by assuming $s_1(t) = s_2(t) = \phi_u^s(t, u(t))$ in finite time. In particular, we give an upper bound on the mean squared error $E[|Y - \hat{Y}|^2]$, where $\hat{Y}$ denotes the estimate of realizations of Y using $s_1(t)$, $s_2(t)$, and the algorithm provided below. In the remainder of this section, we assume $s_1(t) = s_2(t) = \phi_u^s(t, u(t))$. Note that the sample space of $\phi_u^s(t, u(t))$, regarded as a random process, is some compact set $\mathcal{S} \subset \mathbb{R}$, i.e., the sample space is a subset of the real line and thus samples from $\phi_u^s(t, u(t))$ follow some stationary probability density function (pdf), say $f_S(s)$, for some virtual continuous random variable S. That is, for $s(t) := \phi_u^s(t, u(t))$, define the sampled sequence $s_k := s(t_k)$ for sampling time-instants $t_k \in \mathbb{R}_{>0}$, $t_k := \Delta k$, $k \in \mathbb{N}$, and sampling period $\Delta \in \mathbb{R}_{>0}$; then, $s_k \sim f(s)$ for all k. Because we know the dynamics (4)-(6), we can obtain $f_S(s)$ by Monte Carlo simulations [21]. If we know $f_S(s)$, we can always find a set of cells $C := \{c^1, \ldots, c^M\}$, $M \in \mathbb{N}$, $j \in \{1, \ldots, M\}$, such that $\bigcup_j c^j = \mathbb{R}$, $\bigcap_j c^j = \emptyset$, and $\Pr[s_k \in c] = \Pr[V = v] = p_V^*(v)$ for $v \in \mathcal{Y}$ and $c \in C$. In other words, using the pdf $f_S(s)$, we can select the cells C so that the probability that s_k lies in the cells equals the optimal probability distribution $p_V^*(v)$. It follows that we can generate pseudorandom realizations from $p_V^*(v)$ by properly selecting C. Note that, because realizations are being generated by a deterministic process, there would be high correlation between consecutive realizations for small sampling period Δ. However, because the s_k is a stationary process (see Section 6.3), the larger the Δ, the smaller the correlation between s_k and s_{k+1} for all $k \in \mathbb{N}$. Indeed, large Δ would introduce large time-delays for generating realizations. There is a trade-off between correlation and time-delay that should be taken into account in practice. One way to deal with this trade-off is to compute the normalized autocorrelation function [15, 20] of s_k. Then, we select the smallest time-delay $\tau \in \mathbb{N}$ that leads to a desired correlation between s_k and $s_{k+\tau}$, $k \in \mathbb{N}$, and use the delayed sequence $s^\tau(\cdot) := \{s_k, s_{k+\tau}, s_{k+2\tau}, \ldots\}$ to generate realizations from $p_V^*(v)$. In the following algorithm, we summarize the ideas introduced above.

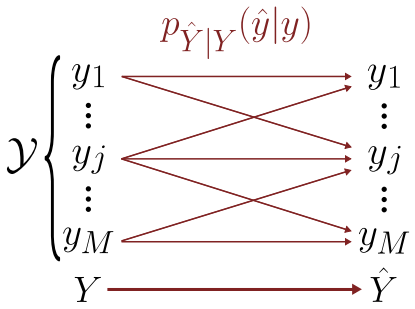

Figure 3: Transition probabilities $p_{\hat{Y}|Y}(\hat{y}|y)$.

Algorithm 1: Pseudorandom Number Generation:

1) Consider the probability mass function $p_V^*(v) = \Pr[V = v]$, $v \in \mathcal{Y} = \{y_1, \ldots, y_M\}$, solution to Problem 1; and the synchronous solution $s(t) = \phi_u^s(t, u(t))$ of the responders.

2) Fix the sampling period $\Delta \in \mathbb{R}_{>0}$ and obtain, by Monte Carlo simulations [21], the probability density function $f_S(s_k)$ of the sampled sequence $s_k = s(t_k)$, $t_k = \Delta k$, $k \in \mathbb{N}$.

3) Select a finite set of cells $C = \{c^1, \ldots, c^M\}$, $M \in \mathbb{N}$, $j \in \{1, \ldots, M\}$, such that $\bigcup_j c^j = \mathbb{R}$, $\bigcap_j c^j = \emptyset$, and $\Pr[s_k \in c^j] = \Pr[V = y_j]$ for all $y_j \in \mathcal{Y}$.

4) Generate realization from $p_V^*(v)$ using the piecewise function:

$$v_k = \psi(s_k) := \begin{cases} y_1 & \text{if } s_k \in c^1, \\ \vdots & \\ y_M & \text{if } s_k \in c^M. \end{cases} \tag{10}$$

7.1 Distortion Induced by Synchronization Errors

Algorithm 1 in Section 7 is constructed under the assumption that responders are perfectly synchronized. However, because we only have exponential synchronization, in finite time, there is always a "small" difference between $s_1(t)$ and $s_2(t)$ due to potentially different initial conditions. It follows that there is also a difference between realizations generated using $s_1(t_k)$, denoted as $v_k^1 \in \mathcal{Y}$, and realizations $v_k^2 \in \mathcal{Y}$ generated through $s_2(t_k)$, where $\mathcal{Y} = \{y_1, \ldots, y_M\}$. Exponential synchronization implies that for any finite $t^* \in \mathbb{R}_{>0}$, there is $\delta(t^*, |s_1(0) - s_2(0)|) \in \mathbb{R}_{>0}$ (denoted as δ_{t^*} for simplicity), parametrized by t^* and the initial synchronization error $|s_1(0) - s_2(0)|$, such that $|s_1(t_k) - s_2(t_k)| \leq \delta_{t^*}$ for all $t_k \geq t_k^*$, and $\lim_{k\to\infty} |s_1(t_k) - s_2(t_k)| = 0$. Consider the cell c^j, $c^j \in C$, with end points c_1^j and c_2^j, $c_1^j < c_2^j$, the length of c^j is defined as $l(c^j) := c_2^j - c_1^j$. If $c_1^j = \pm\infty$ (or $c_2^j = \pm\infty$), $l(c^j) = \infty$. Without loss of generality, let $l(c^2) \leq l(c^3) \leq \ldots \leq l(c^{M-1})$, $l(c^1) = \infty$, and $l(c^M) = \infty$. Note that, if $\delta_{t^*} \leq l(c^2)$, v_k^1 and v_k^2 are at most one level apart from each other, e.g., if $v_k^1 = y_1$, then either $v_k^2 = y_1$ or $v_k^2 = y_2$; and if $v_k^1 = y_3$, then $v_k^2 = y_2$, $v_k^2 = y_3$, or $v_k^2 = y_4$. It follows that $p_{\hat{Y}|Y}(\hat{y}|y)$, $y, \hat{y} \in \mathcal{Y}$, is of the form depicted in Figure 3, where $\hat{Y}$ denotes the estimate of realizations of Y using $s_1(t_k)$, $s_2(t_k)$, and Algorithm 1. Similarly, if $l(c^2) < \delta_{t^*} \leq l(c^3)$, v_k^1 and v_k^2 are at most two levels apart from each other and thus lead to a different structure of the transition probabilities. Here, we only consider the case where $\delta_{t^*} \leq l(c^2)$. Distortion induced by larger synchronization errors can be estimated following the same methods. Note that, because responders synchronize exponentially, as $\delta_{t^*} \to 0$ ($t^* \to \infty$), $p_{\hat{Y}|Y}(\hat{y}|y) \to 1$ for $\hat{y} = y$, and $p_{\hat{Y}|Y}(\hat{y}|y) \to 0$, for $\hat{y} \neq y$, for all $y, \hat{y} \in \mathcal{Y}$. That is, distortion due to synchronization errors disappears exponentially fast. The actual value of the transition probabilities depend on the responders and driver dynamics, the initial conditions, and the cells C. However, we do not need these probabilities, only the structure of $p_{\hat{Y}|Y}(\hat{y}|y)$ depicted in Figure 3 is used to derive an upper bound on the expected distortion. Let $\mathcal{V}_\delta \subseteq \mathcal{Y} \times \mathcal{Y}$ denote the set of pairs (y_j, y_i) for which there is a nonzero transition probability $p_{\hat{Y}|Y}(y_j|y_i)$ between $Y = y_j$ and $\hat{Y} = y_i$, $y_j, y_i \in \mathcal{Y}$, as depicted in Figure 3. The set $\mathcal{V}_\delta$ is parametrized by the upper bound on the synchronization error $|s_1(t_k) - s_2(t_k)| \leq \delta_{t^*} \leq l(c^2)$. Define the distortion function $d(Y, \hat{Y}) := |Y - \hat{Y}|^2$. The function $d(Y, \hat{Y})$ is a deterministic function of two jointly distributed random vectors, Y and $\hat{Y}$, with joint

distribution $p_{Y,\hat{Y}}(y,\hat{y}) = p_Y(y)p_{\hat{Y}|Y}(\hat{y}|y)$. Hence, see [39] for details, we can write the expected distortion as follows

$$\begin{aligned} E[d(Y,\hat{Y})] &= \sum_{y,\hat{y}\in\mathcal{Y}} p_{Y,\hat{Y}}(y,\hat{y})d(y,\hat{y}) = \sum_{y,\hat{y}\in\mathcal{Y}} p_Y(y)p_{\hat{Y}|Y}(\hat{y}|y)|y-\hat{y}|^2 \\ &= \sum_{(y,\hat{y})\in\mathcal{V}_\delta} p_Y(y)p_{\hat{Y}|Y}(\hat{y}|y)|y-\hat{y}|^2 \leq \sum_{(y,\hat{y})\in\mathcal{V}_\delta} p_Y(y)|y-\hat{y}|^2 =: \bar{d}_\delta, \end{aligned} \tag{11}$$

where the left-hand side of (11) follows from the definition of $\mathcal{V}_\delta$ above, and the last inequality from the fact that $p_{\hat{Y}|Y}(\hat{y}|y) \leq 1$ for all $y, \hat{y} \in \mathcal{Y}$. The constant $\bar{d}_\delta \in \mathbb{R}_{>0}$ provides an upper bound on the worst-case distortion induced by a δ_{t^*} synchronization error. Moreover, as $\delta_{t^*} \to 0$, $\mathcal{V}_\delta \to \{(y_1,y_1),(y_2,y_2),\ldots,(y_M,y_M)\}$; therefore, $\lim_{\delta_{t^*}\to 0} \bar{d}_\delta = 0$. That is, distortion due to synchronization errors is bounded by $\bar{d}_\delta$ and vanishes exponentially fast.

8 Simulation Results

We next present an evaluation of our algorithms on real data. We use the *adult-dataset*, available from the UCI Machine Learning Repository [57], which contains census data. Each attribute within the dataset has 3.9×10^4 entries. We use three of these attributes: race, sex, and income, which take values on finite discrete sets. We let *race* and *sex* be the private information, X, and use *income* as the information requested by the query, Y. The probability mass functions of X and Y, and part of the one of (X,Y) are given in Table 1. In Figure 4, we depict $p_X(x)$, $p_Y(y)$, and $p_{X,Y}(x,y)$ with mass points indexed in the order given in Table 1. We first compute the optimal distribution $p_V^*(v)$ of the distorting additive noise V. We solve the convex program (8) in Theorem 1. The optimal distribution is depicted in Figure 5 and the corresponding numerical values are given in Table 2. This $p_V^*(v)$ leads to $I[X;Y+V] = 0.0024$ while the mutual information without distortion is $I[X;Y] = 0.0251$, i.e., according to our metric, by optimally distorting the query, we leak about ten times less information. To generate realization from this distribution at both sides of the channel, we use trajectories of two chaotic responders as introduced in Section 2. We use the synthesis procedure in Section 6.4 to select suitable driver and responders. As driver (5), we use the Lorenz system:

$$\begin{cases} \dot{\xi}_1(t) = 10(\xi_2(t) - \xi_1(t)), \\ \dot{\xi}_2(t) = 28\xi_1(t) - \xi_2(t) - \xi_1(t)\xi_3(t), \\ \dot{\xi}_3(t) = -\frac{8}{3}\xi_3(t) + \xi_1(t)\xi_2(t), \\ u(t) = \xi_1(t), \end{cases} \tag{12}$$

with states $\xi_1, \xi_2, \xi_3 \in \mathbb{R}$ and driving signal $u \in \mathbb{R}$. The Lorenz system produces bounded trajectories [58], and is known to be chaotic and quasi-hyperbolic [52]. For the responders (4) and (6), we let $r(\zeta,u) = A\zeta + \psi(u)$, with $A = \text{diag}[-1,-2.5]$ and $\psi(u) = (-5u^2, 50\sin(u))^\top$. Because A is diagonal and has negative eigenvalues, responders satisfy the conditions of Corollary 1 with $P = I_2$; hence, they are convergent systems and thus exponentially synchronize when driven by the same input $u(t)$. Moreover, since responders are linear in ζ and A is Hurwitz, systems can be proved to be ISS with input $\psi(u)$ [42]. Because u is bounded and $\psi(u)$ is continuous, by the extreme value theorem, $\psi(u)$ is bounded, which, together with ISS, imply boundedness of the responders' trajectories [42]. We let the outputs of the responders be $s_1(t) = \zeta_1^2$ and $s_2(t) = \zeta_2^2$ (their second state). In Figure 6, we show traces of the chaotic driver and responders trajectories obtained by computer simulations (using Matlab from Mathworks), and in Figure 7, we plot the synchronization error between the outputs of the responders. We initialized the responders in antiphase $\zeta_1(0) = -\zeta_2(0) = (150,150)^\top$, and far from the limit trajectory. Note, in Figure 7, that responders synchronize exponentially and are practically synchronized for $t \geq 5$. Moreover, after $t \geq 14$, the synchronization error is within Matlab's precision (10^{-12}). Because the Lorenz system is quasi-hyperbolic, samples from the driving signal $u(t)$ follow a stationary distribution that is independent of the initial conditions of the driver, see Section 6.3. Then, according to the synthesis procedure in Section 6.4, we next verify, using Monte Carlo simulations, that samples $s_k = s(t_k)$ (see Section 7), from the synchronous trajectory, $s_1(t) = s_1(t) = s(t)$, are also stationary. To do so, we compute the probability density function $f_S(s)$, $s_k \sim f_S(s)$, for different initial conditions and verify that all of them lead to the same density. In Figure 8, we depict probability densities of s_k for twenty different initial conditions, sampling instants $t_k = \Delta k$, $\Delta = 0.001$, and $t \in [0, 4000]$. Note that they all lead to the same density $f_S(s)$. The support (obtained numerically) of $f_S(s)$ is given $\mathcal{S} = [-10.8585, 10.8683]$. Finally, we use the piecewise function (10) to generate realizations from $p_V^*(v)$ using samples, s_k, from the synchronous trajectory. Following the algorithm given in Section 7, we have to divide the support $\mathcal{S}$ of $f_S(s)$ into a set of partitions $C = \{c^1, \ldots, c^M\}$, such that the probability that s_k lies in the cells equals the optimal

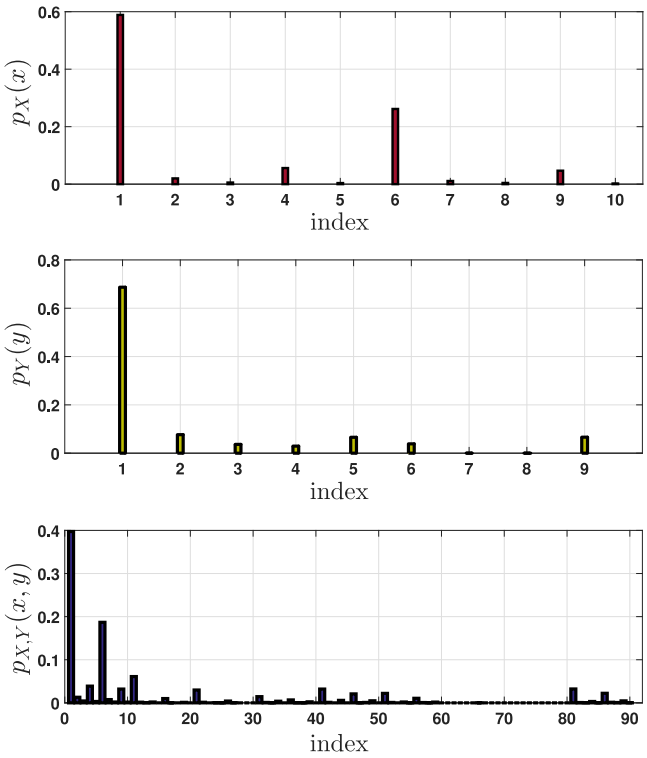

Figure 4: Probability mass functions of X, Y, and (X, Y).

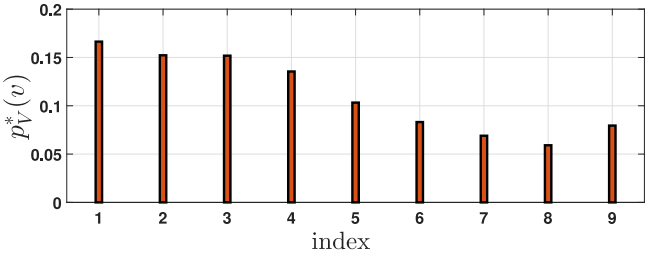

Figure 5: Optimal distribution $p_V^*(v)$ solution to (8) in Theorem 1.

probability distribution $p_V^*(v)$. This can be done using the empirical Cumulative Distribution Function (CDF), $F_S(s)$, corresponding to $f_S(s)$. We depict this CDF in Figure 9. Then, we simply select the cells C such that $p_V^*(y_i) = \Pr[V = y_i] = \Pr[c^i \leq S \leq c^{i+1}] = F_S(c^{i+1}) - F_S(c^i)$ for all $i \in \{1, \ldots, M-1\}$, $M = 9$ (the cardinality of the alphabet of Y). For this CDF and $p_V^*(v)$ in Table 2, we obtain the following cells:

$$C = \big\{[-\infty, -4.1739), [-4.1739, -2.0965), [-2.0965, -0.3658), [-0.3658, 1.1408), [1.1408, 2.3321) \quad (13)$$
$$[2.3321, 3.4341), [3.4341, 4.5985), [4.5985, 5.7743), [5.7743, \infty]\big\}.$$

In Figure 10, we show realizations generated by the piecewise function (10) at both sides of the channel, and the corresponding probability mass functions. To generate this realizations, at the trusted server, we use samples from $s_1(t)$ and, at the remote station, we sample $s_2(t)$. Note that, as expected, all samples are perfectly synchronized and their probability mass functions are equal to $p_V^*(v)$ in Figure 5.

9 Conclusions

Using an information-theoretic privacy metric (mutual information), we have provided a general privacy framework based on additive distorting random vectors and exponential synchronization of chaotic systems. The synthesis of the optimal probability distribution, $p_V^*(v)$, of the additive distorting vector V has been posed as a convex program in $p_V(v)$. We have provided an algorithm for generating pseudorandom realizations from this distribution using trajectories of chaotic oscillators. To generate equal realizations at both sides of the channel, we have induced exponential synchronization on two chaotic oscillators (one at each side of the

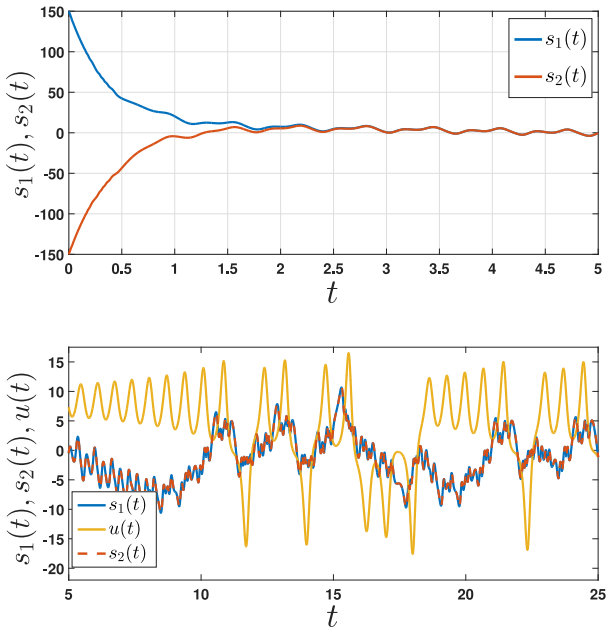

Figure 6: Traces of the chaotic driver and responders trajectories. Top: trajectories of the responders converging to each other. Bottom: traces of chaotic solutions of the driver and responders.

X	$\begin{bmatrix}0\\0\end{bmatrix}$	$\begin{bmatrix}0\\1\end{bmatrix}$	$\begin{bmatrix}0\\2\end{bmatrix}$	$\begin{bmatrix}0\\3\end{bmatrix}$	$\begin{bmatrix}0\\4\end{bmatrix}$	$\begin{bmatrix}1\\0\end{bmatrix}$	$\begin{bmatrix}1\\1\end{bmatrix}$	$\begin{bmatrix}1\\2\end{bmatrix}$	$\begin{bmatrix}1\\3\end{bmatrix}$	$\begin{bmatrix}1\\4\end{bmatrix}$
$p_X(x)$	0.5888	0.0200	0.0056	0.0560	0.0038	0.2616	0.0110	0.0042	0.0468	0.0022

Y	1	2	3	4	5	6	7	8	9
$p_Y(y)$	0.6870	0.0766	0.0364	0.0292	0.0658	0.0386	0.0002	0.0001	0.0662

(X,Y)	$\begin{bmatrix}0\\0\\1\end{bmatrix}$	$\begin{bmatrix}0\\1\\1\end{bmatrix}$	$\begin{bmatrix}0\\2\\1\end{bmatrix}$	$\begin{bmatrix}0\\3\\1\end{bmatrix}$	$\begin{bmatrix}0\\4\\1\end{bmatrix}$	$\cdots$	$\begin{bmatrix}1\\0\\9\end{bmatrix}$	$\begin{bmatrix}1\\1\\9\end{bmatrix}$	$\begin{bmatrix}1\\2\\9\end{bmatrix}$	$\begin{bmatrix}1\\3\\9\end{bmatrix}$	$\begin{bmatrix}1\\4\\9\end{bmatrix}$
$p_{X,Y}(x,y)$	0.3974	0.0130	0.0044	0.0388	0.0032	$\cdots$	0.0222	0.0014	0.0008	0.0046	0.0004

Table 1: Probability mass functions of X and Y, and part of the one of (X,Y).

channel), and use their trajectories and the proposed algorithm to generate realizations. However, exponential synchronization implies that, in finite time, there is always a small error between trajectories (and thus also between realizations). We have derived an upper bound on the worst-case distortion induced by finite-time synchronization errors and showed that this distortion disappears exponentially fast. Using off-the-shelf results in the literature, we have provided general guidelines for selecting the dynamics of the responders and driver so that our algorithm for generating synchronized realizations from $p_V^*(v)$ is guaranteed to work. We have presented simulation results to illustrate our results.

V	1	2	3	4	5	6	7	8	9
$p_V^*(v)$	0.1664	0.1522	0.1518	0.1355	0.1033	0.0832	0.0690	0.0591	0.0795

Table 2: Optimal distribution $p_V^*(v)$ of the distorting additive random variable V.

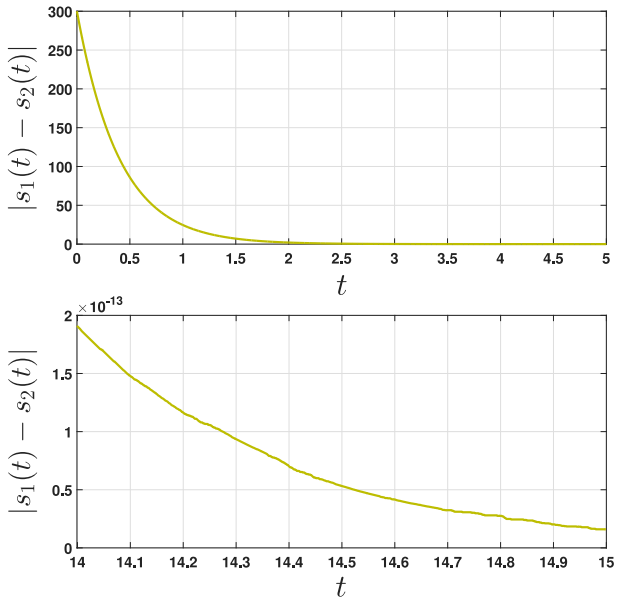

Figure 7: Synchronization error $|s_1(t) - s_2(t)|$. Responders are initialized in antiphase, i.e., $s_1(0) = -s_2(0)$.

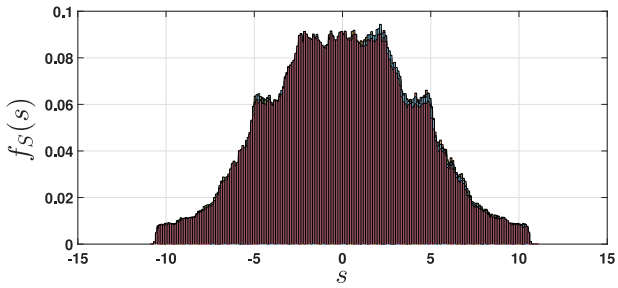

Figure 8: Empirical probability densities of samples, $s(t_k)$, from the synchronous solution $s_1(t) = s_1(t) = s(t)$, for twenty different, randomly selected, initial conditions.

References

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

[2] O. Tan, D. Gunduz, 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] Z. Huang, Y. Wang, S. Mitra, and G. E. Dullerud, "On the cost of differential privacy in distributed control systems," in *Proceedings of the 3rd International Conference on High Confidence Networked Systems*, 2014, pp. 105–114.

[4] and M. Gruteser, , and A. Alrabady, "Enhancing security and privacy in traffic-monitoring systems," *IEEE Pervasive Computing*, vol. 5, pp. 38–46, 2006.

[5] R. H. Weber, "Internet of things âĂŞ new security and privacy challenges," *Computer Law and Security Review*, vol. 26, pp. 23–30, 2010.

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

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

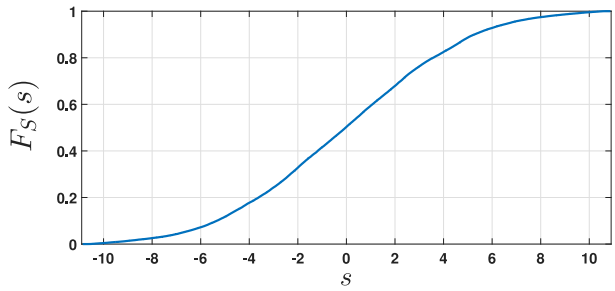

Figure 9: Empirical CDF corresponding to $f_S(s)$.

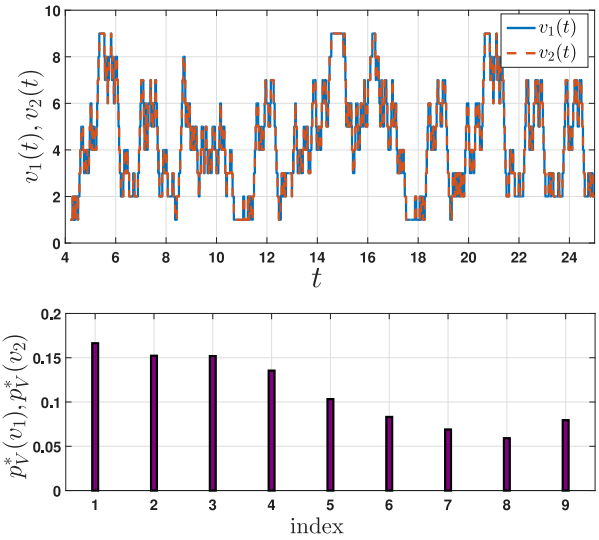

Figure 10: Top: realizations of $p_V^*(v)$ generated by the piecewise function (10) at both sides of the channel, $v_1(t)$ at the trusted server and $v_2(t)$ at the remote station. Bottom: corresponding probability mass functions.

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

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

[10] 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.

[11] Y. Wang, Z. Huang, S. Mitra, and G. E. Dullerud, "Entropy-minimizing mechanism for differential privacy of discrete-time linear feedback systems," in *53rd IEEE Conference on Decision and Control*, 2014, pp. 2130–2135.

[12] S. Wiggins, *Introduction to Applied Nonlinear Dynamical Systems and Chaos*, ser. Texts in Applied Mathematics. Springer New York, 2003.

[13] G. A. Gottwald and I. Melbourne, "A new test for chaos in deterministic systems," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 460, pp. 603–611, 2004.

[14] A. Pavlov, A. Pogromsky, N. van de Wouw, and H. Nijmeijer, "Convergent dynamics, a tribute to Boris Pavlovich Demidovich," *Syst. Control Lett.*, vol. 52, p. 257, 2004.

[15] V. S. Anishchenko, V. Astakhov, A. Neiman, T. Vadivasova, and L. Schimansky-Geier, *Nonlinear Dynamics of Chaotic and Stochastic Systems: Tutorial and Modern Developments (Springer Series in Synergetics)*. Berlin, Heidelberg: Springer-Verlag, 2007.

[16] T. Yang, C. Wu, and L. Chua, "Cryptography based on chaotic systems," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 44, pp. 469–472, 1997.

[17] J. Grzybowski, M. Rafikov, and J. Balthazar, "Synchronization of the unified chaotic system and application in secure communication," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, pp. 2793 – 2806, 2009.

[18] J. Lu, X. Wu, and J. Lu, "Synchronization of a unified chaotic system and the application in secure communication," *Physics Letters A*, vol. 305, pp. 365 – 370, 2002.

[19] G. ÃĄlvarez, S. Li, F. Montoya, G. Pastor, and M. Romera, "Breaking projective chaos synchronization secure communication using filtering and generalized synchronization," *Chaos, Solitons and Fractals*, vol. 24, pp. 775 – 783, 2005.

[20] L. Kocarev, K. Halle, K. Eckert, L. Chua, and U. Parlitz, "Experimental demonstration of secure communications via chaotic synchronization," *Chua's Circuit: A Paradigm for Chaos*, vol. 371-378, 1992.

[21] C. P. Robert and G. Casella, *Monte Carlo Statistical Methods (Springer Texts in Statistics)*. Berlin, Heidelberg: Springer-Verlag, 2005.

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

[23] 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.

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

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

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

[27] S. Salamatian, A. Zhang, F. du Pin Calmon, S. Bhamidipati, N. Fawaz, B. Kveton, P. Oliveira, and N. Taft, "Managing your private and public data: Bringing down inference attacks against your privacy," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, pp. 1240–1255, 2015.

[28] O. Tan, D. Gunduz, 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.

[29] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, pp. 211–407, 2014.

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

[31] L. Keuninckx, M. Soriano, I. Fischer, C. Mirasso, R. Nguimdo, and G. van der Sande, "Encryption key distribution via chaos synchronization," *Scientific Reports*, vol. 7, pp. 1–15, 2017.

[32] M. Mackey and L. Glass, "Oscillation and chaos in physiological control systems," *Science*, vol. 197, pp. 287–289, 1977.

[33] B. Demidovich, *Lectures on Stability Theory*, Moscow. In Russian, 1967.

[34] W. Lohmiller and J. Slotine, "On contraction analysis for nonlinear systems." *Automatica*, vol. 34, pp. 683–695, 1998.

[35] D. Angeli, "A Lyapunov approach to incremental stability properties." *IEEE Trans. Automat. Contr*, vol. 47, pp. 410–421, 2000.

[36] X. Liu and T. Chen, "Boundedness and synchronization of y-coupled lorenz systems with or without controllers," *Physica D*, vol. 237, pp. 630–639, 2008.

[37] L. Scardovi and R. Sepulchre, "Synchronization in networks of identical linear systems," *IEEE Trans. Automat. Contr*, vol. 57, pp. 2132–2143, 2010.

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

[39] M. Ross, *Introduction to Probability Models, Ninth Edition.* Orlando, FL, USA: Academic Press, Inc., 2006.

[40] S. Boyd and L. Vandenberghe, *Convex optimization.* New York, NY, USA: Cambridge University Press, 2004.

[41] H. K. Khalil, *Nonlinear Systems*, 3rd ed. Englewood Cliffs, NJ: Prentice-Hall, 2002.

[42] E. Sontag and Y. Wang, "On characterizations of the input-to-state stability property," *Systems and Control Letters*, vol. 24, pp. 351 – 359, 1995.

[43] M. Arcak, D. Angeli, and E. Sontag, "A unifying integral iss framework for stability of nonlinear cascades," *SIAM J. Control Optim*, vol. 40, pp. 1888–1904, 2002.

[44] A. Chaillet, D. Angeli, and H. Ito, "Combining iiss and iss with respect to small inputs: The strong iiss property," *IEEE Transactions on Automatic Control*, vol. 59, pp. 2518–2524, 2014.

[45] S. H. Strogatz, *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry and Engineering*, 2000.

[46] I. Kovacic and M. Brennan, *The Duffing Equation: Nonlinear Oscillators and their Behaviour.* Wiley, 2011.

[47] B. Van der Pol and V. der Mark, "Frequency demultiplication," *Nature*, vol. 120, pp. 363–364, 1927.

[48] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, pp. 821–824, 1990.

[49] C. Wu and L. Chua, "Synchronization in an array of linearly coupled dynamical systems," *IEEE Transactions on Circuit and Systems-I*, vol. 42, pp. 430–447, 1995.

[50] E. Steur, I. Tyukin, and H. Nijmeijer, "Semi-passivity and synchronization of diffusively coupled neuronal oscillators," *Physica D*, vol. 238, pp. 2119–2128, 2009.

[51] S. Kuznetsov, *Hyperbolic Chaos: A PhysicistâĂŹs View.* Springer Berlin Heidelberg, 2012.

[52] T. Kapitaniak, J. Wojewoda, and J. Brindley, "Synchronization and desynchronization in quasi-hyperbolic chaotic systems." *Physics Letters A*, vol. 210, pp. 283–289, 2000.

[53] V. N. Belykh, I. Belykh, and E. Mosekilde, "Hyperbolic plykin attractor can exist in neuron models," *I. J. Bifurcation and Chaos*, vol. 15, pp. 3567–3578, 2005.

[54] S. P. Kuznetsov and A. Pikovsky, "Autonomous coupled oscillators with hyperbolic strange attractors," *Physica D*, vol. 232, pp. 87–102, 2007.

[55] L. Turukina and A. Pikovsky, "Hyperbolic chaos in a system of resonantly coupled weakly nonlinear oscillators," *Physics Letters A*, vol. 11, pp. 1407 – 1411, 2011.

[56] S. P. Kuznetsov and V. P. Kruglov, "On some simple examples of mechanical systems with hyperbolic chaos," *Proceedings of the Steklov Institute of Mathematics*, vol. 297, 2017.

[57] C. Blake and C. Merz, "UCI machine learning repository databases," 1998. [Online]. Available: http://archive.ics.uci.edu/ml

[58] A. Pogromsky, "Passivity based design of synchronizing systems," *International Journal of Bifurcation and Chaos*, vol. 8, pp. 295–319, 1998.

Author/s:
Murguia, C; Shames, I; Farokhi, F; Neši, D

Title:
Information-theoretic privacy through chaos synchronization and optimal additive noise

Date:
2020

Citation:
Murguia, C., Shames, I., Farokhi, F. & Neši, D. (2020). Information-theoretic privacy through chaos synchronization and optimal additive noise. Farokhi, F (Ed.). Privacy in Dynamical Systems, Privacy in Dynamical Systems, (1), pp.103-129. Springer.

Persistent Link:
http://hdl.handle.net/11343/295002

File Description:
Accepted version