# Privacy-Aware MMSE Estimation

Shahab Asoodeh, Fady Alajaji, and Tamás Linder
Department of Mathematics and Statistics, Queen's University
{asoodehshahab, fady, linder}@mast.queensu.ca

***Abstract*—We investigate the problem of the predictability of random variable $Y$ under a privacy constraint dictated by random variable $X$, correlated with $Y$, where both predictability and privacy are assessed in terms of the minimum mean-squared error (MMSE). Given that $X$ and $Y$ are connected via a binary-input symmetric-output (BISO) channel, we derive the *optimal* random mapping $P_{Z|Y}$ such that the MMSE of $Y$ given $Z$ is minimized while the MMSE of $X$ given $Z$ is greater than $(1-\varepsilon)\mathsf{var}(X)$ for a given $\varepsilon \geq 0$. We also consider the case where $(X, Y)$ are continuous and $P_{Z|Y}$ is restricted to be an additive-noise channel.**

## I. Introduction and Preliminaries

Given private information, represented by $X$, nature usually generates non-private observable information, say $Y$, via a fixed channel $P_{Y|X}$. Consider two communicating agents Alice and Bob, where Alice observes $Y$ and wants to reveal it to Bob in order to receive a payoff. Alice, therefore, wishes to disclose $Y$ to Bob as accurately as possible, but in such a way that $X$ is kept almost private from him. For instance, $Y$ may represent the information that a social network (Alice) obtains from its users and $X$ may represent political preferences of the users. Alice wants to disclose $Y$ as accurately as possible to an advertising company and, simultaneously, wishes to protect the privacy of its users. Given a fixed joint distribution $P_{XY}$, Alice, hence, needs to choose a random mapping $P_{Z|Y}$, the so-called *privacy filter*, to release a new random variable $Z$, called the *displayed data*, such that $X$ and $Z$ satisfy a privacy constraint and $Z$ maximizes a utility function (corresponding to the predictability of $Y$).

This problem has been addressed from an information-theoretic viewpoint in [1]–[7] where both utility and privacy are measured in terms of information-theoretic quantities. In particular, in [4] *non-trivial perfect privacy* for discrete $X$ and $Y$, where $Z$ is required to be statistically independent of $X$ and dependent on $Y$, is studied. It is shown that non-trivial perfect privacy is possible if and only if $X$ is *weakly independent* of $Y$, that is, if the set of vectors $\{P_{X|Y}(\cdot) : y \in \mathcal{Y}\}$ is linearly dependent. An equivalent result is obtained by Calmon et al. [5] in terms of the singular values of the operator $f \mapsto \mathbb{E}[f(X)|Y]$.

Although, a connection between the information-theoretic privacy measure and a coding theorem is established in [3], the use of mutual information as a privacy measure is not satisfactorily motivated in an *operational* sense. To have an operational measure of privacy, in this paper we take an estimation-theoretic approach and define both the privacy and utility functions in terms of the minimum mean-squared error (MMSE). For a given pair of random variables $(U, V)$, the MMSE of estimating $U$ given $V$ is

$$\mathsf{mmse}(U|V) := \mathbb{E}[(U - \mathbb{E}[U|V])^2] = \mathbb{E}[\mathsf{var}(U|V)],$$

where $\mathsf{var}(\cdot|\cdot)$ denotes the conditional variance. The privacy filter $P_{Z|Y}$ is said to satisfy the *$\varepsilon$-strong estimation privacy* condition for some $\varepsilon \geq 0$ if $\mathsf{mmse}(f(X)|Y) \geq (1-\varepsilon)\mathsf{var}(f(X))$ for any Borel function[1] $f$ of $X$ and similarly, it is said to satisfy the *$\varepsilon$-weak estimation privacy* condition if $\mathsf{mmse}(X|Y) \geq (1-\varepsilon)\mathsf{var}(X)$. The parameter $\varepsilon$ determines the level of desired privacy; in particular, $\varepsilon = 0$ corresponds to perfect privacy. We propose to use the estimation noise to signal ratio (ENSR), defined by $\frac{\mathsf{mmse}(Y|Z)}{\mathsf{var}(Y)}$, as the loss function associated with $Y$ and $Z$. The goal is to choose $P_{Z|Y}$ which satisfies the strong (resp., weak) estimation privacy condition and *minimizes* the ENSR (or equivalently maximizes $\frac{\mathsf{var}(Y)}{\mathsf{mmse}(Y|Z)}$ as the utility function), which ensures the best predictability of $Y$ given a privacy-preserving $Z$. The function $\mathsf{sENSR}_\varepsilon(X;Y)$ (resp., $\mathsf{wENSR}_\varepsilon(X;Y)$) is introduced as this minimum to quantify the above goal.

To evaluate $\mathsf{sENSR}_\varepsilon(X;Y)$, we first obtain an equivalent characterization of the $\varepsilon$-strong estimation privacy condition. We then show that $\mathsf{sENSR}_\varepsilon(X;Y)$ and $\mathsf{wENSR}_\varepsilon(X;Y)$ admit closed-form expressions when $P_{X|Y}$ is a BISO channel. Moreover, when $X$ is discrete, we develop a bound characterizing the privacy-constrained error probability, $\Pr(\hat{Y}(Z) \neq Y)$, for all estimators $\hat{Y}(Z)$ given a privacy-preserving $Z$, thus generalizing the results of [9]. In particular, we show that the fundamental bound on privacy-constrained error probability decreases *linearly* as $\varepsilon$ increases, analogously to [9, Corollaries 3,5]. We also study $\mathsf{sENSR}_\varepsilon(X^n;Y^n)$ when $n$ independent identically distributed (i.i.d.) copies $(X^n, Y^n)$ of $(X, Y)$ are available. We demonstrate that if the class of privacy filters is constrained to be memoryless, then $\mathsf{sENSR}_\varepsilon(X^n;Y^n)$ remains the same for any $n$. This is reminiscent of the tensorization property for maximal correlation [10].

In addition, $\mathsf{sENSR}_\varepsilon(X;Y)$ is considered for the case where $(X, Y)$ has a joint probability density function by studying the problem where the displayed data $Z$ is obtained

[1] This is reminiscent of *semantic security* [8] in the cryptography community. An encryption mechanism is said to be semantically secure if the adversary's advantage for correctly guessing *any function* of the privata data given an observation of the mechanism's output (i.e., the ciphertext) is required to be negligible.

This work was supported in part by NSERC of Canada.

by passing $Y$ through an additive noise channel. In this case, we show that for a Gaussian noise process, jointly Gaussian $(X_{\mathsf{G}}, Y_{\mathsf{G}})$ is the worst case (i.e., has the largest ENSR). We also show that if only $Y_{\mathsf{G}}$ is Gaussian then the ENSR of $(X, Y_{\mathsf{G}})$ is very close to the Gaussian ENSR if the maximal correlation between $X$ and $Y_{\mathsf{G}}$ is close to the correlation coefficient between $X$ and $Y_{\mathsf{G}}$.

We omit the proof of most of the paper's results due to space limitation. The proofs are available in [11].

## II. Strong Estimation Privacy Guarantee

Consider the scenario where Alice observes $Y$ which is correlated with a private random variable $X$, drawn from a given joint distribution $P_{XY}$, and wishes to transmit the random variable $Z$ to Bob to receive some utility from him. Her goal is to maximize the utility while making sure that Bob cannot efficiently estimate any non-trivial function of $X$ given $Z$. To formalize this privacy guarantee, we give the following definition. In what follows random variables $X$, $Y$, and $Z$ have alphabets $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$, respectively, which are either finite subsets of $\mathbb{R}$ or they are all equal to $\mathbb{R}$.

**Definition 1.** *Given a joint distribution $P_{XY}$ and $\varepsilon \ge 0$, $Z$ is said to satisfy* $\varepsilon$-strong estimation privacy, *denoted as $Z \in \Gamma_\varepsilon(P_{XY})$, if there exists a random mapping (channel) $P_{Z|Y}$ that induces a joint distribution $P_X \times P_{Z|X}$ on $\mathcal{X} \times \mathcal{Z}$, via the Markov condition $X -\!\circ\!- Y -\!\circ\!- Z$, satisfying*

$$\mathsf{mmse}(f(X)|Z) \ge (1-\varepsilon)\mathsf{var}(f(X)), \tag{1}$$

*for any non-constant Borel functions $f$ on $\mathcal{X}$. Similarly, $Z$ is said to satisfy* $\varepsilon$-weak estimation privacy, *denoted as $Z \in \partial\Gamma_\varepsilon(P_{XY})$, if (1) is satisfied only for the identity function $f(x) = x$.*

In the sequel, we drop in the notation the dependence of $\Gamma_\varepsilon(P_{XY})$ (resp., $\partial\Gamma_\varepsilon(P_{XY})$) on $P_{XY}$ and simply write $\Gamma_\varepsilon$ (resp., $\partial\Gamma_\varepsilon$).

Suppose the utility Alice receives from Bob is $\frac{\mathsf{var}(Y)}{\mathsf{mmse}(Y|Z)}$. The utility is maximized (and is equal to $\infty$) when $Z = Y$ with probability one and is minimized (and is equal to one) when $Z$ is independent of $Y$. In order to quantify the tradeoff between privacy guarantee (introduced above) and the utility, we propose the following function, which we call the strong privacy-aware *estimation noise to signal ratio* (ENSR):

$$\mathsf{sENSR}_\varepsilon(X;Y) := \inf_{Z \in \Gamma_\varepsilon} \frac{\mathsf{mmse}(Y|Z)}{\mathsf{var}(Y)}. \tag{2}$$

Similarly, we can use weak estimation privacy to define the weak privacy-aware ENSR as follows:

$$\mathsf{wENSR}_\varepsilon(X;Y) := \inf_{Z \in \partial\Gamma_\varepsilon} \frac{\mathsf{mmse}(Y|Z)}{\mathsf{var}(Y)}. \tag{3}$$

*Remark* 1. Rényi [12] defined the *correlation ratio* of $Y$ on $Z$, denoted by $\eta_Z(Y)$, as $\eta_Z^2(Y) := \dfrac{\mathsf{var}(\mathbb{E}[Y|Z])}{\mathsf{var}(Y)}$ which can be shown to be equal to $\sup_g \rho^2(Y; g(Z))$, where $\rho$ is the standard correlation coefficient. It is clear from the law of total variance that $\dfrac{\mathsf{mmse}(Y|Z)}{\mathsf{var}(Y)} = 1 - \eta_Z^2(Y)$.

In the sequel, we obtain an equivalent characterization for the random mapping $P_{Z|X}$ which generates $Z \in \Gamma_\varepsilon$. To this goal, we need the following definition.

**Definition 2** ([12]). *Given random variables $U$ and $V$ taking values over arbitrary alphabets $\mathcal{U}$ and $\mathcal{V}$, respectively, the* maximal correlation *$\rho_m(U;V)$ is defined as*

$$\begin{aligned}\rho_m^2(U;V) &:= \sup_{f,g} \rho^2(f(U), g(V)) \\ &= \sup_{(f(U),g(V)) \in \mathcal{S}^0} \frac{\mathbb{E}^2[f(U)g(V)]}{\mathsf{var}(f(U))\mathsf{var}(g(V))},\end{aligned}$$

*where $\mathcal{S}^0$ is the collection of all pairs of real-valued measurable functions $f$ and $g$ of $U$ and $V$, respectively, such that $\mathbb{E}[f(U)] = \mathbb{E}[g(V)] = 0$ and $0 < \mathsf{var}(f(U)), \mathsf{var}(g(V)) < \infty$.*

Rényi [12] derived an equivalent characterization of maximal correlation as

$$\rho_m^2(U;V) = \sup_{f \in \mathcal{S}_{\mathcal{U}}^0} \frac{\mathbb{E}\left[\mathbb{E}^2[f(U)|V]\right]}{\mathsf{var}(f(U))}, \tag{4}$$

where $\mathcal{S}_{\mathcal{U}}^0$ is the collection of real-valued measurable functions $f$ of $U$ such that $\mathbb{E}[f(U)] = 0$ and $0 < \mathsf{var}(f(U)) < \infty$.

**Theorem 1.** *For a given $P_{XY}$, $Z \in \Gamma_\varepsilon$ if and only if there exists $P_{Z|Y}$ which induces $P_{Z|X}$ via $X -\!\circ\!- Y -\!\circ\!- Z$ satisfying $\rho_m^2(X;Z) \le \varepsilon$ for any $\varepsilon \ge 0$.*

In light of Theorem 1 and Remark 1, we can alternatively write $\mathsf{sENSR}_\varepsilon(X;Z)$ and $\mathsf{wENSR}_\varepsilon(X;Z)$ as

$$\mathsf{sENSR}_\varepsilon(X;Y) = 1 - \sup_{\substack{P_{Z|Y}: \rho_m^2(X;Z) \le \varepsilon, \\ X -\circ- Y -\circ- Z}} \eta_Z^2(Y), \tag{5}$$

and

$$\mathsf{sENSR}_\varepsilon(X;Y) = 1 - \sup_{\substack{P_{Z|Y}: \eta_Z^2(X) \le \varepsilon, \\ X -\circ- Y -\circ- Z}} \eta_Z^2(Y), \tag{6}$$

for any $\varepsilon \ge 0$. We note that, using the Support Lemma [13], one can show that the set $\Gamma_\varepsilon$ can be described by considering $Z \in \mathcal{Z}$ with $|\mathcal{Z}| \le |\mathcal{Y}| + 1$ in case $\mathcal{Y}$ is finite. We also note that since both maximal correlation and correlation ratio satisfy the data processing inequality [3], [9], i.e. $\rho_m^2(X;Z) \le \eta_m^2(X;Y)$ and $\eta_Z^2(X) \le \eta_Y^2(X)$ if $X -\!\circ\!- Y -\!\circ\!- Z$, we can restrict our attention to $0 \le \varepsilon \le \rho_m^2(X;Y)$ and $0 \le \varepsilon \le \eta_Y^2(X)$ in (5) and (6), respectively.

## III. Characterization of $\mathsf{sENSR}_\varepsilon(X;Y)$ and $\mathsf{wENSR}_\varepsilon(X;Y)$ For Discrete $X$ and $Y$

We first derive some properties of $\mathsf{sENSR}_\varepsilon(X;Y)$ and $\mathsf{wENSR}_\varepsilon(X;Y)$ when both $X$ and $Y$ are discrete. For a given $P_{XY}$ and $0 \le \varepsilon \le \rho_m^2(X;Y)$, we have the following trivial bounds:

$$0 \le \mathsf{wENSR}_\varepsilon(X;Y) \le \mathsf{sENSR}_\varepsilon(X;Y) \le 1 - \varepsilon, \tag{7}$$

where the last inequality can be proved by noticing that $\mathsf{sENSR}_\varepsilon(X;Y) \le \mathsf{sENSR}_\varepsilon(Y;Y)$ and

$$\mathsf{mmse}(Y|Z) \quad = \quad \mathsf{var}(Y)(1 - \eta_Z^2(Y))$$

$$\geq \quad \mathsf{var}(Y)(1-\rho_m^2(Y;Z)), \tag{8}$$

where (8) follows from the definition of maximal correlation. The lower bound $0 \leq \mathsf{sENSR}_\varepsilon(X;Y)$ in (7) is achieved if and only if $\rho_m^2(X;Y) = \varepsilon$. On the other hand, when $\varepsilon = 0$, the upper bound $\mathsf{sENSR}_0(X;Y) \leq 1$ is tight if and only if all $Z \in \Gamma_0$ are independent of $Y$. Hence, from [3, Lemma 6], $\mathsf{sENSR}_0(X;Y) = 1$ if and only if $X$ is not *weakly independent* of $Y$. In particular, if $|\mathcal{Y}| > |\mathcal{X}|$ then $\mathsf{sENSR}_0(X;Y) < 1$, and if $|\mathcal{Y}| = 2$, then $\mathsf{sENSR}_0(X;Y) = 1$.

The map $\varepsilon \mapsto \mathsf{sENSR}_\varepsilon(X;Y)$ is clearly non-increasing. The following lemma states that this map is indeed convex and thus strictly decreasing. As another consequence of this convexity, we obtain an upper bound on $\mathsf{sENSR}_\varepsilon(X;Y)$ which strictly strengthens (7).

**Lemma 1.** *For any joint distribution $P_{XY}$, the maps $\varepsilon \mapsto \mathsf{sENSR}_\varepsilon(X;Y)$ and $\varepsilon \mapsto \mathsf{wENSR}_\varepsilon(X;Y)$ are convex.*

In light of the convexity of $\varepsilon \mapsto \mathsf{sENSR}_\varepsilon(X;Y)$, the following corollaries are immediate.

**Corollary 1.** *For a given $P_{XY}$, the maps $\varepsilon \mapsto \frac{1-\mathsf{sENSR}_\varepsilon(X;Y)}{\varepsilon}$ and $\varepsilon \mapsto \frac{1-\mathsf{wENSR}_\varepsilon(X;Y)}{\varepsilon}$ are non-increasing over $(0,1)$.*

**Corollary 2.** *For a given $P_{XY}$ and $0 \leq \varepsilon \leq \rho_m^2(X;Y)$,*

$$\mathsf{sENSR}_\varepsilon(X;Y) \leq 1 - \frac{\varepsilon}{\rho_m^2(X;Y)}.$$

*Remark* 2. Note that simple calculations reveal that the upper bound in Corollary 2 is achieved by the erasure channel:

$$P_{Z|Y}(z|y) = \begin{cases} 1-\tilde{\delta}, & \text{if } z = y \\ \tilde{\delta}, & \text{if } z = \mathrm{e}, \end{cases}$$

for all $y \in \mathcal{Y}$ and the erasure probability $\tilde{\delta} = 1 - \frac{\varepsilon}{\rho_m^2(X;Y)}$ for $0 \leq \varepsilon \leq \rho_m^2(X;Y)$.

### A. Binary Input Symmetric Output $P_{X|Y}$

We now turn our attention to the special case where the backward channel from $Y$ to $X$, $P_{X|Y}$, belongs to a family of channels called binary input symmetric output (BISO) channels, see e.g., [14]. For $Y \sim \mathsf{Bernoulli}(p)$, $P_{X|Y}$ is BISO if, for any $x \in \mathcal{X} = \{0, \pm1, \pm2, \ldots, \pm k\}$, we have $P_{X|Y}(x|1) = P_{X|Y}(-x|0)$. As pointed out in [14], one can always assume that the output alphabet $\mathcal{X} = \{\pm1, \pm2, \ldots, \pm k\}$ has even number of elements by splitting the symbol 0 into two symbols and assigning them equal probabilities. Binary symmetric channels and binary erasure channels are both BISO. In the following theorem, we show that $\mathsf{wENSR}_\varepsilon(X;Y)$ can be calculated in closed-form when $P_{X|Y}$ is a BISO channel.

**Theorem 2.** *Let $Y \sim \mathsf{Bernoulli}(p)$ and $P_{X|Y}$ be a BISO channel. Then for $0 \leq \varepsilon \leq \rho_m^2(X;Y)$, we have*

$$\mathsf{wENSR}_\varepsilon(X;Y) = 1 - \varepsilon\frac{\mathsf{var}(X)}{4\mathsf{var}(Y)\mathbb{E}^2[X|Y=1]},$$

*and*

$$1-\varepsilon\frac{\mathsf{var}(X)}{4\mathsf{var}(Y)\mathbb{E}^2[X|Y=1]} \leq \mathsf{sENSR}_\varepsilon(X;Y) \leq 1-\frac{\varepsilon}{\rho_m^2(X;Y)}.$$

Similar to [9], we also consider the tradeoff between strong estimation privacy and the probability of correctly guessing $Y$. To quantify this, let $\hat{Y}: \mathcal{Z} \to \mathcal{Y}$ be the Bayes decoding map. The resulting (minimum) error probability is $\Pr(\hat{Y}(Z) \neq Y)$. Let

$$\mathsf{P}^{\mathsf{e}}_\varepsilon(X;Y) \coloneqq \min_{Z \in \partial\Gamma_\varepsilon} \Pr(\hat{Y}(Z) \neq Y). \tag{9}$$

Note that when $Z$ is independent of $Y$, the optimal Bayes decoding map yields $\Pr(\hat{Y}(Z) \neq Y) = 1-p$, if $p = P_Y(1) \geq \frac{1}{2}$. Using a similar argument as in [15, Appendix A], we establish the following connection between $\mathsf{P}^{\mathsf{e}}_\varepsilon(X;Y)$ and $\mathsf{wENSR}_\varepsilon(X;Y)$.

**Proposition 1.** *Let $Y \sim \mathsf{Bernoulli}(p)$ with $p \geq \frac{1}{2}$. Then we have*

$$\mathsf{wENSR}_\varepsilon(X;Y) \leq \frac{\mathsf{P}^{\mathsf{e}}_\varepsilon(X;Y)}{\mathsf{var}(Y)} \leq 2\mathsf{wENSR}_\varepsilon(X;Y)$$

Calmon et al. [9] considered the same problem for $X = Y$, i.e., minimizing $\Pr(\hat{X}(Z) \neq X)$ over all $P_{Z|X}$ such that $\rho_m^2(X;Z) \leq \varepsilon$ and showed that the best privacy-constrained error probability is lower bounded by a straight line of $\varepsilon$ with negative slope. Combining Theorem 2 and Proposition 1, we can lower bound $\mathsf{P}^{\mathsf{e}}_\varepsilon(X;Y)$ for all BISO $P_{X|Y}$ by a straight line in $\varepsilon$ as follows:

$$\mathsf{P}^{\mathsf{e}}_\varepsilon(X;Y) \geq \mathsf{var}(Y) - \varepsilon\frac{\mathsf{var}(X)}{4\mathbb{E}^2[X|Y=1]},$$

which generalizes [9, Corollaries 3,5].

In the following, we consider two examples of BISO channels for which the bounds in Theorem 2 coincide. First consider $P_{X|Y}$ being a binary symmetric channel with crossover probability $\alpha$, denoted as $\mathrm{BSC}(\alpha)$.

**Lemma 2.** *For $Y \sim \mathsf{Bernoulli}(p)$ and $P_{X|Y} = BSC(\alpha)$ for $\alpha \in [0, \frac{1}{2})$, we have for $0 \leq \varepsilon \leq \rho_m^2(X;Y)$,*

$$1 - \frac{\varepsilon\mathsf{var}(X)}{4(1-2\alpha)^2\mathsf{var}(Y)} \leq \mathsf{sENSR}_\varepsilon(X;Y) \leq 1 - \frac{\varepsilon}{\rho_m^2(X;Y)},$$

*and*

$$\mathsf{var}(Y) - \frac{\varepsilon\mathsf{var}(X)}{4(1-2\alpha)^2} \leq \mathsf{P}^{\mathsf{e}}_\varepsilon(X;Y) \leq 2\left[\mathsf{var}(Y) - \frac{\varepsilon\mathsf{var}(X)}{4(1-2\alpha)^2}\right].$$

*Moreover, if $p = 0.5$,*

$$\mathsf{sENSR}_\varepsilon(X;Y) = \mathsf{wENSR}_\varepsilon(X;Y) = 1 - \frac{\varepsilon}{(1-2\alpha)^2},$$

*and the optimal channel is $BEC(\tilde{\delta})$ (see Fig. 1) where*

$$\tilde{\delta} = 1 - \frac{\varepsilon}{(1-2\alpha)^2}. \tag{10}$$

We next consider $P_{X|Y}$ being a binary erasure channel with erasure probability $\delta$, denoted as $\mathrm{BEC}(\delta)$.

**Lemma 3.** *For $Y \sim \mathsf{Bernoulli}(p)$ and $P_{X|Y} = BEC(\delta)$ for $\delta \in [0,1)$, we have for $0 \leq \varepsilon \leq \rho_m^2(X;Y)$,*

$$1 - \frac{\varepsilon\mathsf{var}(X)}{4\mathsf{var}(Y)(1-\delta)^2} \leq \mathsf{sENSR}_\varepsilon(X;Y) \leq 1 - \frac{\varepsilon}{1-\delta},$$

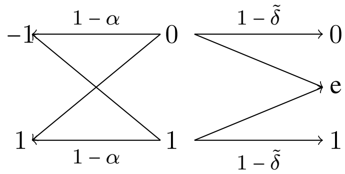


Fig. 1. Optimal privacy filter where $P_{Y|X}$ = BSC($\alpha$) with $Y \sim$ Bernoulli(0.5) where $\tilde{\delta}$ is specified in (10).

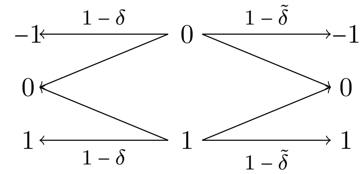


Fig. 2. Optimal privacy filter where $P_{X|Y}$ = BEC($\delta$) with $Y \sim$ Bernoulli(0.5) where $\tilde{\delta}$ is specified in (11).

*and*

$$\mathsf{var}(Y) - \frac{\varepsilon \mathsf{var}(X)}{4(1-\delta)^2} \le \mathsf{P}^{\mathsf{e}}_{\varepsilon}(X;Y) \le 2\left[\mathsf{var}(Y) - \frac{\varepsilon \mathsf{var}(X)}{4(1-\delta)^2}\right].$$

*Moreover, if* $p = 0.5$,

$$\mathsf{sENSR}_{\varepsilon}(X;Y) = 1 - \frac{\varepsilon}{1-\delta},$$

*and the optimal channel is BEC*($\tilde{\delta}$) *(see Fig. 2) where*

$$\tilde{\delta} = 1 - \frac{\varepsilon}{1-\delta}. \tag{11}$$

We conclude this section by connecting the above results to *initial efficiency*[2]. For BISO channels, we define the initial efficiency of $f_{\varepsilon}(X;Y) := \mathsf{var}(Y) - \mathsf{var}(Y)\mathsf{wENSR}_{\varepsilon}(X;Y)$ with respect to $\varepsilon$ as the derivative $f'_0(X;Y)$ of $\varepsilon \mapsto f_{\varepsilon}(X;Y)$ at $\varepsilon = 0$. In fact, $f'_0(X;Y)$ quantifies the decrease of $\mathsf{mmse}(Y|Z)$ when $\varepsilon$ slightly increases from 0. Then since for any BISO $P_{X|Y}$, $f_0(X;Y) = 0$, using Corollary 1 and the convexity of $\varepsilon \mapsto \mathsf{wENSR}_{\varepsilon}(X;Y)$, we can write

$$\begin{aligned} f'_0(X;Y) &= \lim_{\varepsilon \downarrow 0} \frac{f_{\varepsilon}(X;Y)}{\varepsilon} = \sup_{\varepsilon > 0} \frac{f_{\varepsilon}(X;Y)}{\varepsilon} \\ &= \mathsf{var}(X) \max_{\substack{P_{Z|Y}: \\ X - Y - Z}} \frac{\mathsf{var}(Y) - \mathsf{mmse}(Y|Z)}{\mathsf{var}(X) - \mathsf{mmse}(X|Z)} \end{aligned}$$

We can, therefore, conclude from Theorem 2 that for a given pair of random variables $(X,Y)$ with BISO $P_{X|Y}$, we have

$$\max_{\substack{P_{Z|Y}: \\ X - Y - Z}} \frac{\mathsf{var}(Y) - \mathsf{mmse}(Y|Z)}{\mathsf{var}(X) - \mathsf{mmse}(X|Z)} = \frac{1}{4\mathbb{E}^2[X|Y=1]}.$$

### *B.* $\mathsf{sENSR}_{\varepsilon}(X;Y)$ *and* $\mathsf{wENSR}_{\varepsilon}(X;Y)$ *with* $n$ *i.i.d. observations*

Let $(X^n, Y^n)$ be $n$ i.i.d. copies of $(X,Y)$ with a given distribution $P_{XY}$. Similar to (2) and (3), we can define

$$\mathsf{sENSR}_{\varepsilon}(X^n;Y^n) := 1 - \frac{1}{n} \sup_{Z \in \Gamma_{\varepsilon}^{\otimes n}} \sum_{i=1}^{n} \eta^2_{Z^n}(Y_i),$$

and

$$\mathsf{wENSR}_{\varepsilon}(X^n;Y^n) := 1 - \frac{1}{n} \sup_{Z \in \partial\Gamma_{\varepsilon}^{\otimes n}} \sum_{i=1}^{n} \eta^2_{Z^n}(Y_i),$$

where $\Gamma_{\varepsilon}^{\otimes n} := \{P_{Z^n|Y^n} : \rho_m^2(X^n;Z^n) \le \varepsilon\}$, and $\partial\Gamma_{\varepsilon}^{\otimes n} := \{P_{Z^n|Y^n} : \sum_{i=1}^{n} \eta^2_{Z^n}(X_i) \le n\varepsilon\}$.

As shown in [5], $\mathsf{sENSR}_0(X;Y) < 1$ if and only if the smallest singular value, $\sigma_{\mathsf{min}}$, of the operator $f(X) \mapsto \mathbb{E}[f(X)|Y]$ is zero. It is also shown in [5, Proposition 1] that the smallest singular value of the operator $f(X^n) \mapsto \mathbb{E}[f(X^n)|Y^n]$ for i.i.d. $(X^n, Y^n)$, is $\sigma^n_{\mathsf{min}}$ and it hence follows that unless $\sigma_{\mathsf{min}} = 1$, $\lim_{n\to\infty} \mathsf{sENSR}_0(X^n;Y^n) < 1$ for any distribution $P_{XY}$ and hence non-trivial perfect privacy is possible. The following result implies that the optimal privacy filter $P_{Z^n|Y^n}$ which achieves non-trivial perfect privacy cannot be a memoryless channel.

**Proposition 2.** *Let* $(X^n, Y^n)$ *be an i.i.d. copies of* $(X,Y)$ *with distribution* $P_{XY}$. *If the family of feasible random mapping in the optimizations* (5) *and* (6) *is constrained to be of the form* $P_{Z^n|Y^n}(z^n|y^n) = \prod_{i=1}^n P_i(z_i|y_i)$, *then*

$$\mathsf{sENSR}_{\varepsilon}(X^n;Y^n) = \mathsf{sENSR}_{\varepsilon}(X;Y),$$

$$\mathsf{wENSR}_{\varepsilon}(X^n;Y^n) = \mathsf{wENSR}_{\varepsilon}(X;Y).$$

## IV. Continuous $(X,Y)$, Additive Gaussian Noise As Privacy Filter

In this section, we assume that $X$ and $Y$ are both absolutely continuous random variables and the channel $P_{Z|Y}$ is modelled by a scaled additive stable[3] noise variable $N_f$ which is independent of $(X,Y)$ and has density $f$ with zero mean and unit variance, i.e.,

$$Z_{\gamma} = Y + \gamma N_f,$$

for some $\gamma \ge 0$. We then define

$$\mathsf{sENSR}^f_{\varepsilon}(X;Y) := 1 - \sup_{\gamma \in \mathcal{C}_{\varepsilon}(P_{XY})} \eta^2_{Z_{\gamma}}(Y),$$

and

$$\mathsf{wENSR}^f_{\varepsilon}(X;Y) := 1 - \sup_{\gamma \in \partial\mathcal{C}_{\varepsilon}(P_{XY})} \eta^2_{Z_{\gamma}}(Y),$$

where $\mathcal{C}_{\varepsilon}(P_{XY}) := \{\gamma \ge 0 : \rho_m^2(X;Z_{\gamma}) \le \varepsilon\}$ and $\partial\mathcal{C}_{\varepsilon}(P_{XY}) := \{\gamma \ge 0 : \eta^2_{Z_{\gamma}}(X) \le \varepsilon\}$. If the noise process is Gaussian $N(0,1)$, we denote $N_f$, $\mathsf{sENSR}^f_{\varepsilon}(X;Y)$, and $\mathsf{wENSR}^f_{\varepsilon}(X;Y)$ by $N_{\mathsf{G}}$, $\mathsf{sENSR}_{\varepsilon}(X;Y)$, and $\mathsf{wENSR}_{\varepsilon}(X;Y)$, respectively.

[2] Initial efficiency was previously defined for the common randomness problem in [16], for secret key generation in [17], for incremental growth rate in a stock market [18], and for information extraction under privacy constraint in [3].

[3] A random variable $X$ with distribution $P$ is called stable if for $X_1$, $X_2$ i.i.d. according to $P$, for any constants $a$, $b$, the random variable $aX_1 + bX_2$ has the same distribution as $cX + d$ for some constants $c$ and $d$ [19, Chapter 1].

The bounds for $\mathsf{wENSR}_\varepsilon(X;Y)$ obtained in (7) clearly hold: $0 \le \mathsf{wENSR}^f_\varepsilon(X;Y) \le \mathsf{sENSR}^f_\varepsilon(X;Y) \le 1-\varepsilon$, and in particular, $\mathsf{sENSR}^f_0(X;Y) \le 1$. In the following, we show that this last inequality is in fact an equality.

**Proposition 3.** *For a given absolutely continuous $(X,Y)$, the map $\varepsilon \mapsto \mathsf{sENSR}^f_\varepsilon(X;Y)$ is non-negative, strictly decreasing and satisfies*

$$\mathsf{sENSR}^f_0(X;Y) = 1.$$

*Example 1.* Let $(X_\mathsf{G}, Y_\mathsf{G})$ be jointly Gaussian with correlation coefficient $\rho$ and let $N_f = N_\mathsf{G}$. Without loss of generality, we can assume that $\mathbb{E}[X_\mathsf{G}] = \mathbb{E}[Y_\mathsf{G}] = 0$. It is known [12] that $\rho_m^2(X_\mathsf{G}; Z_\gamma) = \rho^2(X_\mathsf{G}; Z_\gamma)$ and hence

$$\rho_m^2(X_\mathsf{G}; Z_\gamma) = \rho^2 \frac{\mathsf{var}(Y_\mathsf{G})}{\mathsf{var}(Y_\mathsf{G}) + \gamma^2},$$

which implies that $\gamma \mapsto \rho_m^2(X_\mathsf{G}; Z_\gamma)$ is strictly decreasing and hence $\rho_m^2(X_\mathsf{G}; Z_\gamma) = \varepsilon$ for $0 \le \varepsilon \le \rho_m^2(X_\mathsf{G}; Y_\mathsf{G}) = \rho^2$ has a unique solution

$$\gamma_\varepsilon^2 := \mathsf{var}(Y_\mathsf{G})\left(\frac{\rho^2}{\varepsilon} - 1\right)$$

and $Z_\gamma \in \Gamma_\varepsilon$ for any $\gamma \ge \gamma_\varepsilon$. On the other hand, $\mathsf{mmse}(Y_\mathsf{G}|Z_\gamma) = \mathsf{var}(Y_\mathsf{G})\frac{\gamma^2}{\mathsf{var}(Y_\mathsf{G})+\gamma^2}$ which shows that the map $\gamma \mapsto \mathsf{mmse}(Y_\mathsf{G}|Z_\gamma)$ is strictly increasing and hence

$$\mathsf{sENSR}_\varepsilon(X_\mathsf{G}; Y_\mathsf{G}) = \frac{\mathsf{mmse}(Y_\mathsf{G}|Z_{\gamma_\varepsilon})}{\mathsf{var}(Y_\mathsf{G})} = 1 - \frac{\varepsilon}{\rho^2}. \tag{12}$$

It is easy to check that that $\eta^2_{Z_\varepsilon}(X_\mathsf{G}) = \rho_m^2(X_\mathsf{G}; Z_\varepsilon) = \varepsilon$ This then implies that for the jointly Gaussian $(X_\mathsf{G}, Y_\mathsf{G})$, $\mathcal{C}_\varepsilon(P_{X_\mathsf{G}Y_\mathsf{G}}) = \partial\mathcal{C}_\varepsilon(P_{X_\mathsf{G}Y_\mathsf{G}})$. Hence, for $0 \le \varepsilon \le \rho^2$,

$$\mathsf{sENSR}_\varepsilon(X_\mathsf{G}; Y_\mathsf{G}) = \mathsf{wENSR}_\varepsilon(X_\mathsf{G}; Y_\mathsf{G}) = 1 - \frac{\varepsilon}{\rho^2}. \tag{13}$$

This example suggests that the bound in Corollary 2 still holds for absolutely continuous $(X,Y)$ in this model. We prove this observation in the following lemma with the assumption that $N = N_\mathsf{G}$.

**Lemma 4.** *For a given absolutely continuous $(X,Y)$, we have for $0 \le \varepsilon \le \rho_m^2(X;Y)$*

$$\mathsf{wENSR}_\varepsilon(X;Y) \le \mathsf{sENSR}_\varepsilon(X;Y) \le 1 - \frac{\varepsilon}{\rho_m^2(X;Y)}.$$

Combined with (13), this lemma also shows that among all $(X,Y)$ with identical maximal correlation, the jointly Gaussian $(X_\mathsf{G}, Y_\mathsf{G})$ yields the largest $\mathsf{sENSR}_\varepsilon(X;Y)$ when the noise process is Gaussian. This observation is similar to [20, Theorem 12] which states that for Gaussian noise, the Gaussian input is the worst with no privacy constraint imposed; i.e., $\mathsf{mmse}(Y|Y+N_\mathsf{G}) \le \mathsf{mmse}(Y_\mathsf{G}|Y_\mathsf{G}+N_\mathsf{G})$ where $Y_\mathsf{G}$ is Gaussian having the same variance as $Y$.

We finally obtain a lower bound on $\mathsf{sENSR}_\varepsilon(X;Y)$ when only $Y$ is Gaussian.

**Lemma 5.** *Let $X$ be jointly distributed with Gaussian $Y_\mathsf{G}$. Then,*

$$1 - \frac{\varepsilon}{\rho^2(X;Y_\mathsf{G})} \le \mathsf{sENSR}_\varepsilon(X;Y_\mathsf{G}) \le 1 - \frac{\varepsilon}{\rho_m^2(X;Y_\mathsf{G})},$$

This lemma, together with Example 1, implies that

$$\mathsf{sENSR}_\varepsilon(X_\mathsf{G}, Y_\mathsf{G}) - \mathsf{sENSR}_\varepsilon(X;Y_\mathsf{G}) \le \varepsilon\left[\frac{1}{\rho^2(X;Y_\mathsf{G})} - \frac{1}{\rho_m^2(X;Y_\mathsf{G})}\right]$$

for Gaussian $X_\mathsf{G}$ which satisfies $\rho_m^2(X_\mathsf{G};Y_\mathsf{G}) = \rho_m^2(X;Y_\mathsf{G})$. This demonstrates that if the difference $\rho_m^2(X;Y_\mathsf{G}) - \rho^2(X;Y_\mathsf{G})$ is small, then $\mathsf{sENSR}_\varepsilon(X;Y_\mathsf{G})$ is very close to $\mathsf{sENSR}_\varepsilon(X_\mathsf{G};Y_\mathsf{G})$.

## REFERENCES


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

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

[3] S. Asoodeh, M. Diaz, F. Alajaji, and T. Linder, "Information extraction under privacy constraints," *Information*, vol. 7, 2016. [Online]. Available: http://www.mdpi.com/2078-2489/7/1/15

[4] S. Asoodeh, F. Alajaji, and T. Linder, "Notes on information-theoretic privacy," in *Proc. 52nd Annual Allerton Conference on Communication, Control, and Computing*, Sept. 2014, pp. 1272–1278.

[5] F. P. Calmon, A. Makhdoumi, and M. Médard, "Fundamental limits of perfect privacy," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2015, pp. 1796–1800.

[6] D. Rebollo-Monedero, J. Forne, and J. Domingo-Ferrer, "From t-closeness-like privacy to postrandomization via information theory," *IEEE Trans. Knowl. Data Eng.*, vol. 22, no. 11, pp. 1623–1636, Nov 2010.

[7] A. Makhdoumi, S. Salamatian, N. Fawaz, and M. Médard, "From the information bottleneck to the privacy funnel," in *Proc. IEEE Inf. Theory Workshop (ITW)*, 2014, pp. 501–505.

[8] S. Goldwasser and S. Micali, "Probabilistic encryption," *Journal of Computer and System Sciences*, vol. 28, no. 2, pp. 270 – 299, 1984.

[9] F. P. Calmon, M. Varia, M. Médard, M. M. Christiansen, K. R. Duffy, and S. Tessaro, "Bounds on inference," in *Proc. 51st Annual Allerton Conference on Communication, Control, and Computing*, Oct 2013, pp. 567–574.

[10] H. S. Witsenhausen, "On sequence of pairs of dependent random variables," *SIAM Journal on Applied Mathematics*, vol. 28, no. 2, pp. 100–113, 1975.

[11] S. Asoodeh, F. Alajaji, and T. Linder, "Privacy-aware MMSE estimation," *arXiv:1601.07417v1*, 2016.

[12] A. Rényi, "On measures of dependence," *Acta Mathematica Academiae Scientiarum Hungarica*, vol. 10, no. 3, pp. 441–451, 1959.

[13] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press, 2011.

[14] I. Sutskover, S. Shamai, and J. Ziv, "Extremes of information combining," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1313–1325, April 2005.

[15] N. Chayat and S. Shamai, "Bounds on the capacity of a binary input AWGN channel with intertransition duration restrictions," in *Proc. 17th Convention of Electrical and Electronics Engineers in Israel,*, March 1991, pp. 227–229.

[16] L. Zhao, "Common randomness, efficiency, and actions," Ph.D. dissertation, Stanford University, 2011.

[17] J. Liu, P. Cuff, and S. Verdú, "Key capacity for product sources with application to stationary Gaussian processes," *arXiv:1409.5844*, 2014.

[18] E. Erkip and T. Cover, ""the efficiency of investment information"," *IEEE Trans. Inf. Theory*, vol. 44, no. 3, pp. 1026–1040, May 1998.

[19] J. P. Nolan, *Stable Distributions-Models for Heavy Tailed Data*. Boston: Birkhauser, in progress, Chapter 1 online at, academic2.american.edu/~jpnolan, 2010.

[20] Y. Wu and S. Verdú, "Functional properties of minimum mean-square error and mutual information," *IEEE Trans. Inf. Theory,*, vol. 58, no. 3, pp. 1289–1301, March 2012.