Estimation Efficiency Under Privacy Constraints

Shahab Asoodeh, Mario Diaz, Fady Alajaji, *Senior Member, IEEE,* and Tamás Linder, *Fellow, IEEE*

***Abstract*—We investigate the problem of estimating a random variable Y under a privacy constraint dictated by another correlated random variable X. When X and Y are discrete, we express the underlying privacy-utility tradeoff in terms of the privacy-constrained guessing probability $\hbar(P_{XY},\varepsilon)$, the maximum probability $\mathsf{P_c}(Y|Z)$ of correctly guessing Y given an auxiliary random variable Z, where the maximization is taken over all $P_{Z|Y}$ ensuring that $\mathsf{P_c}(X|Z)\leq\varepsilon$ for a given privacy threshold $\varepsilon\geq 0$. We prove that $\hbar(P_{XY},\cdot)$ is concave and piecewise linear, which allows us to derive its expression in closed form for any ε when X and Y are binary. In the non-binary case, we derive $\hbar(P_{XY},\varepsilon)$ in the high utility regime (i.e., for sufficiently large, but nontrivial, values of ε) under the assumption that Y and Z have the same alphabets. We also analyze the privacy-constrained guessing probability for two scenarios in which X,Y and Z are binary vectors. When X and Y are continuous random variables, we formulate the corresponding privacy-utility tradeoff in terms of $\mathsf{sENSR}(P_{XY},\varepsilon)$, the smallest normalized minimum mean squared-error (mmse) incurred in estimating Y from a Gaussian perturbation Z. Here the minimization is taken over a family of Gaussian perturbations Z for which the mmse of $f(X)$ given Z is within a factor $1-\varepsilon$ from the variance of $f(X)$ for any non-constant real-valued function f. We derive tight upper and lower bounds for sENSR when Y is Gaussian. For general absolutely continuous random variables, we obtain a tight lower bound for $\mathsf{sENSR}(P_{XY},\varepsilon)$ in the high privacy regime, i.e., for small ε.**

***Index Terms*—Data privacy, privacy-utility tradeoff, guessing probability, Rényi's entropy, minimum mean-squared error, maximal correlation, Gaussian additive privacy mechanism.**

I. Introduction

We consider the following constrained estimation problem: given two correlated random variables X and Y, how accurately can Y be estimated from another correlated random variable Z, while ensuring that the "information leakage" about X is limited? More precisely, we seek to design a randomized mechanism $\mathcal{M}$ which maps Y to an auxiliary random variable Z such that the information leakage from X to Z is limited, and the "estimation efficiency" of Y given Z is maximal. This basic question arises often in data privacy problems, where Alice wishes to disclose *non-private information* Y to Bob as accurately as possible in order to receive a payoff, but in such a way that her *private information* X cannot be effectively inferred by Bob. For instance, her browsing history might constitute the non-private information which a social media website collects in order to provide personalized recommendations. In an ideal world, her browser should sanitize Y before its release in order to avoid compromising her private information X (which may for example include her political leanings). In this context, her browser has access only to Y, but the potential correlation between X and Y makes the sanitization of Y critical. Motivated by this type of applications, we assume throughout the paper that X, Y, and Z form a Markov chain in that order, denoted by $X \multimap Y \multimap Z$.

Given the joint distribution P_{XY}, Alice chooses a random mapping $\mathcal{M}$ to generate the *displayed data* Z in such a way that Bob can guess Y from Z as accurately as possible while being unable to use Z to efficiently guess X. Note that $\mathcal{M}$, the so-called *privacy filter*, is completely determined by $P_{Z|Y}$. The system block diagram of this model is depicted in Fig. 1.

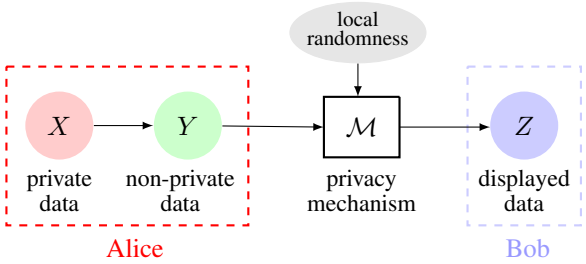


Fig. 1. The system block diagram.

A quantitative answer to this problem requires: (i) an appropriate measure $\mathcal{L}(X\to Z)$ of information leakage from X to Z; and (ii) an appropriate measure $\mathcal{S}(Y|Z)$ of the estimation efficiency of Y given Z. A quantitative and operationally well-justified measure of information leakage has been long sought to assess the performance of different mechanisms used in practice. In this paper, we set $\mathcal{S}(Y|Z)=\mathcal{L}(Y\to Z)$ and propose two measures of information leakage depending on the support of X and Y.

Discrete case: When $X\in\mathcal{X}$ and $Y\in\mathcal{Y}$ are both discrete, it is natural to define information leakage as Bob's efficiency in guessing X. Hence, we propose $\mathcal{L}(X\to Z)$ to be $\frac{\mathsf{P_c}(X|Z)}{\mathsf{P_c}(X)}$, where $\mathsf{P_c}(X):=\max_{x\in\mathcal{X}}P_X(x)$ is the *probability of correctly guessing* X and

$$\begin{aligned}\mathsf{P_c}(X|Z)&:=\sum_{z\in\mathcal{Z}}P_Z(z)\max_{x\in\mathcal{X}}P_{X|Z}(x|z)\\&=\sum_{z\in\mathcal{Z}}\max_{x\in\mathcal{X}}P_X(x)P_{Z|X}(z|x),\end{aligned}\tag{1}$$

is the *probability of correctly guessing* X given Z. Note that a large value of $\mathcal{L}(X\to Z)$ corresponds to a small probability of error in guessing X upon observing Z.

This work was supported by the Natural Sciences and Engineering Research Council of Canada. This paper was presented in part at the IEEE International Symposium on Information Theory 2016 and 2017 [1], [2].

S. Asoodeh is with the Computation Institute, The University of Chicago, Chicago, IL 60637 USA (e-mail: shahab@uchicago.edu).

M. Diaz is with the School of Electrical, Computer and Energy Engineering, Arizona State University, Tempe, AZ 85287-5706 USA and the School of Engineering and Applied Sciences, Harvard University, Cambridge, MA 02138 USA (emails: mdiaztor@{asu,g.harvard}.edu).

F. Alajaji and T. Linder are with the Department of Mathematics and Statistics, Queen's University, Kingston, ON K7L3N6 Canada (e-mails: fa@queensu.ca; tamas.linder@queensu.ca).

Although we only assume that $\mathcal{Z}$, the alphabet of Z, has finite cardinality, we will show that any $\mathcal{Z}$ with cardinality $|\mathcal{Y}|+1$ is sufficient for our purpose.

Continuous case: When X and Y are continuous random variables with $\mathcal{X}=\mathcal{Y}=\mathbb{R}$, we associate information leakage with Bob's efficiency in estimating X given Z. Consequently, we define $\mathcal{L}(X\to Z)$ to be $\frac{\mathsf{var}(X)}{\mathsf{mmse}(X|Z)}$, where $\mathsf{var}(X)\coloneqq\mathbb{E}[(X-\mathbb{E}[X])^2]$ is the variance of X and $\mathsf{mmse}(X|Z)\coloneqq\mathbb{E}[(X-\mathbb{E}[X|Z])^2]$ is the minimum mean squared-error of X given Z.

Returning to the setup of Fig. 1, recall that in order to receive a utility, Alice wishes to disclose her non-private information Y to Bob. However, Y might be correlated with her private information, represented by X. In order to quantify the tradeoff between information display and privacy leakage, we investigate the quantity

$$\sup_{\substack{P_{Z|Y}:X-\circ-Y-\circ-Z\\ \mathcal{L}(X\to Z)\le\varepsilon}}\mathcal{L}(Y\to Z). \tag{2}$$

We seek to characterize this constrained optimization problem in both the discrete and the continuous cases. It is worth mentioning that the chosen information leakage functions are special cases of leakage functions based on a large family of general loss functions, see the discussion in [3, Section 6.2] and references therein. For example, Hamming and squared-error loss functions give rise to the proposed leakage functions in the discrete and continuous cases, respectively.

In the discrete case, the optimization problem in (2) gives rise to the following definition.

Definition 1. *Let (X,Y) be a pair of discrete random variables with joint distribution P_{XY}. We define the* privacy-constrained guessing *function,*

$$\hbar(P_{XY},\cdot):[\mathsf{P_c}(X),1]\to[0,1],$$

by

$$\hbar(P_{XY},\varepsilon)\coloneqq\sup_{\substack{P_{Z|Y}:X-\circ-Y-\circ-Z\\ \mathsf{P_c}(X|Z)\le\varepsilon}}\mathsf{P_c}(Y|Z). \tag{3}$$

We write $\hbar(\varepsilon)$ whenever P_{XY} is clear from the context.

Let $H_\infty(X)\coloneqq-\log\mathsf{P_c}(X)$ be the Rényi entropy of order ∞ and $H_\infty(X|Z)\coloneqq-\log\mathsf{P_c}(X|Z)$ be its conditional version [4]. It follows that $\mathsf{P_c}(X|Z)=2^{-H_\infty(X|Z)}$ and $\mathsf{P_c}(X)=2^{-H_\infty(X)}$. Then, $\hbar$ is in correspondance with the function $g^\infty(P_{XY},\cdot):\mathbb{R}^+\to\mathbb{R}^+$ defined by

$$g^\infty(P_{XY},\varepsilon)\coloneqq\sup_{\substack{P_{Z|Y}:X-\circ-Y-\circ-Z\\ I_\infty(X;Z)\le\varepsilon}}I_\infty(Y;Z), \tag{4}$$

where $I_\infty(X;Z)\coloneqq H_\infty(X)-H_\infty(X|Z)$ is Arimoto's mutual information of order ∞ [5]–[7]. Indeed, it is straightforward to show that

$$g^\infty(P_{XY},\varepsilon)=\log\frac{\hbar(P_{XY},2^\varepsilon\mathsf{P_c}(X))}{\mathsf{P_c}(Y)}. \tag{5}$$

The above functional relationship allows us to translate results for $\hbar$ into results for g^∞. Two functions closely related to g^∞ are the "rate-privacy function" [8], defined as in (4) with I_∞ replaced by Shannon's mutual information, and the "privacy funnel" [9] which is the dual representation of the rate-privacy function. Consequently, g^∞ can be thought of as the *rate-privacy function of order* ∞.

In the machine learning literature, the *information bottleneck* (IB) method has been proposed by Tishby et al. [10] to quantify a fundamental relevance-compression tradeoff. Specifically, the IB method minimizes the "compression rate" $I(Y;Z)$ subject to a relevance constraint given by $I(X;Z)\ge R$ for some $R\ge 0$. Thus, the IB problem is conceptually the dual of the privacy funnel problem. Recently, the privacy funnel and the IB function were unified in a single geometric framework [11] which also encompasses the privacy funnel of order ∞ (or equivalently g^∞) and its dual which may be called the *IB function of order* ∞. The relation between the different properties of IB function (of order ∞) and the privacy funnel (of order ∞) within this framework is the subject of ongoing research.

It is important to note that Arimoto's mutual information of order ∞ differs from other notions of information leakage, for example the ones studied in [8], [12]–[14], in the fact that $I_\infty(X;Z)=0$ is not necessarily equivalent to X and Z being independent. Indeed, if $X\sim\mathsf{Bernoulli}(p)$ with $p\in[\frac{1}{2},1]$ and $P_{Z|X}=\mathsf{BSC}(\alpha)$ with $\alpha\in[0,\frac{1}{2}]$ (the binary symmetric channel with crossover probability α), then $\mathsf{P_c}(X)=p$ and $\mathsf{P_c}(X|Z)=p\bar\alpha+\max\{\bar p\bar\alpha,\alpha p\}$, where $\bar a=1-a$. In this case, it is straightforward to verify that $\mathsf{P_c}(X|Z)=\mathsf{P_c}(X)$ if and only if $p\ge\bar\alpha$. Therefore, for $\frac{1}{2}<\bar\alpha\le p<1$, $I_\infty(X;Z)=0$ despite the fact that X and Z are not independent.

For continuous real-valued random variables X, Y, and Z, the optimization problem in (2) is hard and seems intractable in general. In order to have a tractable model, we assume that the displayed data Z is a Gaussian perturbation of Y, i.e., $Z=Z_\gamma\coloneqq\sqrt{\gamma}Y+N_\mathsf{G}$, where $\gamma\ge0$ and $N_\mathsf{G}\sim\mathcal{N}(0,1)$ is independent of (X,Y). We thus consider the following privacy-utility tradeoff, which is a dual representation of (2) with the privacy constraint strengthened.

Definition 2. *Let (X,Y) be a pair of real-valued random variables with joint density P_{XY}. We define the strong estimation noise-to-signal ratio* $\mathsf{sENSR}(P_{XY},\cdot):\mathbb{R}^+\to\mathbb{R}^+$ *by*

$$\mathsf{sENSR}(P_{XY},\varepsilon)\coloneqq\inf_{\gamma\ge0}\frac{\mathsf{mmse}(Y|Z_\gamma)}{\mathsf{var}(Y)},$$

where the infimum is taken over all $\gamma\ge0$ such that

$$\mathsf{mmse}(f(X)|Z_\gamma)\ge(1-\varepsilon)\mathsf{var}(f(X))$$

whenever $f:\mathbb{R}\to\mathbb{R}$ is measurable and $\mathsf{var}(f(X))<\infty$.

A. Main Contributions

We begin in Section II by investigating the salient properties of $\hbar$. In Theorem 1, we show that the map $\hbar(P_{XY},\cdot)$ is piecewise linear (Fig. 2). The proof relies on a geometric reformulation of $\hbar$ and a careful study of the directional derivatives in the space of stochastic matrices. As a byproduct of Theorem 1, a formula for the derivative of $\hbar$ at $\mathsf{P_c}(X|Y)$ is established in (30). This formula, along with the concavity of $\hbar$, permits us to obtain a tight upper bound for $\hbar$. In particular, when $|\mathcal{X}|=|\mathcal{Y}|=2$, this upper bound and the chord lower

bound for concave functions allow us to derive a closed form expression for $\hbar$ in Theorem 2. Moreover, it is also shown that, depending on the backward channel $P_{X|Y}$, either a Z-channel or a *reverse* Z-channel (Fig. 3) achieves $\hbar(P_{XY}, \varepsilon)$ for each ε.

We next consider a variant quantity $\underline{\hbar}$ which we define analogously to $\hbar$ except that Z is required to be supported over $\mathcal{Y}$. By definition, $\underline{\hbar}$ captures the fundamental trade-off between privacy and utility in situations where enlarging the alphabet is not possible. This is particularly relevant when the displayed data might be used by parties not aware of the implemented privatization scheme. The function $\underline{\hbar}$ may not be concave and consequently the techniques developed to study $\hbar$ do not apply. Nevertheless, we can still study the functional properties of $\underline{\hbar}$ in the *high utility regime* (i.e., for sufficiently large privacy threshold ε), deriving a closed form expression in Theorem 3.

We then specialize Theorem 3 to the binary vector case. Here, Z^n is revealed publicly and the goal is to guess Y^n under the privacy constraint $\mathsf{P_c}(X^n|Z^n) \leq \varepsilon^n$. We consider two models for the pair of random vectors (X^n, Y^n). In the first model (Theorem 4), we assume that X^n consists of n independent and identically distributed (i.i.d.) $\mathsf{Bernoulli}(p)$ samples with $p \in [\frac{1}{2}, 1)$. In the second model (Theorem 5), we assume that X^n comprises the first n samples of a first-order homogeneous Markov process having a simple symmetric transition matrix. We assume that in both cases Y_k, $k = 1, \ldots, n$, is the output of a $\mathsf{BSC}(\alpha)$, $\alpha \in [0, \frac{1}{2})$, whose input is X_k. We also study in detail the problem of *learning from a private distribution*, which corresponds to the special case $X_1 = \cdots = X_n$ of the second model (Proposition 3).

In the continuous case, we first show that the strong privacy constraint in Definition 2 is equivalent to a condition on the maximal correlation (also referred to as the Hirschfeld-Gebelein-Rényi maximal correlation [15]–[17]) between X and Z. We then derive the value of sENSR for the Gaussian case (Example 1) and obtain sharp lower and upper bounds for general X and Gaussian Y in Theorem 7. Finally, we establish in Lemma 2 a tight lower bound for $\mathsf{sENSR}(P_{XY}, \varepsilon)$ for general (X, Y) in the high privacy regime (i.e., sufficiently small ε).

B. Related Work

There have been several choices proposed for an appropriate measure $\mathcal{L}$ of information leakage in the information theory and computer science literature. Shannon's mutual information $I(X;Z)$ (or equivalently the conditional entropy $H(X|Z)$), while an intuitively reasonable choice, does not lead to an arguably "operational" privacy guarantee and thus may not satisfactorily serve as an appropriate information leakage function, see [18] and [19]. Smith [18] discussed that the guessing entropy [20] (defined as the expected number of guesses required to guess X from Z) cannot be adopted as an information leakage function and then proposed Arimoto's mutual information of order ∞ as an appropriate notion of information leakage. Operationally, $I_\infty(X;Z) \leq \varepsilon$ for sufficiently small ε implies that it is nearly as hard for an adversary observing Z to guess X as it is without Z. Braun et al. [21] proposed the information leakage measures $\mathsf{P_c}(X|Z) - \mathsf{P_c}(X)$ and $\max I_\infty(X;Z)$, where the maximization is taken over all priors P_X. In [22], Barthe and Köpf studied the latter quantity in the context of differential privacy [23].

Issa et al. [12] recently found an interesting operational interpretation for $I^{\mathsf{s}}_\infty(X;Z)$, Sibson's mutual information of order ∞ [7], [24]. Specifically, they showed that the requirement $I^{\mathsf{s}}_\infty(X;Z) \leq \varepsilon$ is equivalent to $I_\infty(U;Z) \leq \varepsilon$ for *all* auxiliary random variables U satisfying $U \multimap X \multimap Z$. Consequently, this constraint guarantees that no *randomized* function of X can be efficiently estimated from Z, which leads to a strong privacy guarantee. In contrast, the privacy requirement $I_\infty(X;Z) \leq \varepsilon$ only guarantees to keep X itself private. Nonetheless, the latter requirement comes at a lower utility cost, as illustrated by the following example. Suppose that X and Y are binary and that Alice wishes to reveal absolutely no information about X (i.e., perfect privacy) when disclosing a sanitized version of Y. According to the privacy constraint dictated by Sibson's mutual information, perfect privacy leads to the independence of X and Z. It can be shown that for binary Y and $X \multimap Y \multimap Z$, independence of X and Z implies independence of Y and Z (cf [8, Corollary 11]). Hence, perfect privacy under Sibson's mutual information results in trivial utility. However, as shown in Theorem 2, a non-trivial utility might be achieved for the perfect privacy requirement $I_\infty(X;Z) = 0$.

There exist other estimation-theoretic measures of information leakage in the literature. For example, Makhdoumi and Fawaz [25] proposed to use maximal correlation ρ_m as a measure of information leakage. Later, Calmon et al. [26, Theorem 9] showed that if X and Z are discrete random variables, then $\mathsf{P_c}(f(X)|Z) - \mathsf{P_c}(f(X)) \leq \rho_m(X,Z)$ for every function f, thus providing an interesting operational interpretation for maximal correlation as a measure of information leakage. Similarly, we show that

$$\mathsf{mmse}(f(X)|Z) \geq (1 - \rho_m^2(X,Z))\mathsf{var}(f(X))$$

for every measurable real-valued function f. This then provides an operational interpretation for the privacy guarantee $\rho_m^2(X,Z) \leq \varepsilon$ that we study in Section IV for X and Y absolutely continuous random variables. We refer the readers to [27] for a fairly comprehensive list of existing information leakage measures.

The study of the privacy-utility tradeoff from an information theoretic point of view was initiated by Yamamoto [28] and further extended by several authors, see, e.g., [8], [9], [13], [29]–[33]. In relation with the present work, as already noted the rate-privacy function $g(P_{XY}, \varepsilon)$ was introduced in [8] as the maximum $I(Y;Z)$ over all privacy filters $P_{Z|Y}$ such that $I(X;Z) \leq \varepsilon$ (the privacy funnel [9] is a dual representation of $g(P_{XY}, \varepsilon)$). Motivated by [14], a more operational privacy-rate function $\tilde{g}(P_{XY}, \varepsilon)$ was introduced also in [8] by replacing the privacy guarantee $I(X;Z) \leq \varepsilon$ with $\rho_m^2(X,Z) \leq \varepsilon$. It was also shown that $g(P_{XY}, \varepsilon)$ can bound $\tilde{g}(P_{XY}, \varepsilon)$ from above.

C. Notation

Throughout, we use capital letters, e.g., X, to denote random variables and lowercase letters, e.g., x, to denote their realizations. We use X^n to denote the vector $(X_1, X_2, \ldots, X_n)$. We let $\mathsf{Z}(\beta)$ denote the Z-channel with crossover probability β. For any $a \in [0,1]$, we write $\bar{a}$ for $1-a$. As already mentioned, we let $\mathsf{BSC}(\alpha)$ denote the binary symmetric channel with crossover probability α; we also use $X \perp\!\!\!\perp Z$ to indicate the independence of random variables X and Z and we write $X \multimap Y \multimap Z$ when X and Z are conditionally independent given Y (i.e., when X, Y, and Z form a Markov chain in this order). Finally, for real-valued random variables X and Z, the conditional variance of X given Z is given by $\mathsf{var}(X|Z) \coloneqq \mathbb{E}[(X - \mathbb{E}(X|Z))^2|Z]$.

D. Organization

The rest of the paper is organized as follows. We study the discrete case in Section II. In particular, we determine $\hbar$ in the binary case and obtain a tight lower bound for $\hbar$ for general discrete alphabets in the high utility regime by studying $\underline{\hbar}$. In Section III, we specialize our results to study $\underline{\hbar}$ when X^n, Y^n, and Z^n are binary random vectors. In Section IV, we focus on the continuous case and obtain sharp bounds on sENSR. We summarize our findings in Section V. Finally, we point out that all proofs in the paper are deferred to the appendix.

II. Discrete Scalar Case

In this section, we assume that X and Y are finite-alphabet random variables taking values in $\mathcal{X} = \{1, \ldots, M\}$ and $\mathcal{Y} = \{1, \ldots, N\}$, respectively. Let $P(x,y)$ with $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ be their joint distribution and p_X and q_Y the marginal distributions of X and Y, respectively. The goal here is to maximize the information leakage from Y to Z (i.e., utility) while ensuring that the information leakage from X to Z (i.e., privacy leakage) remains bounded. As stated earlier, we quantify the tradeoff between privacy and utility by means of $\hbar$, as defined in (3).

A. Geometric Properties of $\hbar$

First, note that $\mathsf{P_c}(X|Y,Z) \geq \mathsf{P_c}(X|Z) \geq \mathsf{P_c}(X)$ for jointly distributed random variables X, Y and Z. Therefore, from (3) we have that $\mathsf{P_c}(Y) \leq \hbar(\varepsilon) \leq 1$ and that $\hbar(\varepsilon) = 1$ if and only if $\varepsilon \geq \mathsf{P_c}(X|Y)$. Thus it is enough to study $\hbar$ on the interval $[\mathsf{P_c}(X), \mathsf{P_c}(X|Y)]$.

An application of the Support Lemma [34, Lemma 15.4] shows that it is enough to consider random variables Z supported on $\mathcal{Z} = \{1, \ldots, N+1\}$. Thus, the privacy filter $P_{Z|Y}$ can be realized by an $N \times (N+1)$ stochastic matrix $F \in \mathcal{M}_{N\times(N+1)}$, where $\mathcal{M}_{N\times M}$ denotes the set of all real-valued $N \times M$ matrices. Let $\mathcal{F}$ be the set of all such matrices F. Then both privacy $\mathcal{P}(P,F) = \mathsf{P_c}(X|Z)$ and utility $\mathcal{U}(P,F) = \mathsf{P_c}(Y|Z)$ are functions of $F \in \mathcal{F}$ and can be written as

$$\begin{aligned} \mathcal{P}(P,F) &\coloneqq \sum_{z=1}^{N+1} \max_{1\leq x\leq M} \sum_{y=1}^{N} P(x,y)F(y,z), \\ \mathcal{U}(P,F) &\coloneqq \sum_{z=1}^{N+1} \max_{1\leq y\leq N} q(y)F(y,z). \end{aligned} \tag{6}$$

In particular, we can express $\hbar(\varepsilon)$ as

$$\hbar(\varepsilon) = \sup_{\substack{F\in\mathcal{F},\\ \mathcal{P}(P,F)\leq\varepsilon}} \mathcal{U}(P,F). \tag{7}$$

As before, we omit P in $\mathcal{P}(P,F)$ and $\mathcal{U}(P,F)$ when there is no risk of confusion.

It is straightforward to verify that $\mathcal{P}$ and $\mathcal{U}$ are continuous and convex on $\mathcal{F}$. As a consequence, for every $\varepsilon \in [\mathsf{P_c}(X), \mathsf{P_c}(X|Y)]$, there exists $G \in \mathcal{F}$ such that $\mathcal{P}(G) = \varepsilon$ and $\mathcal{U}(G) = \hbar(\varepsilon)$. It is then direct to show that $\hbar$ is continuous on $[\mathsf{P_c}(X), \mathsf{P_c}(X|Y)]$. Using a proof technique similar to [35, Theorem 2.3], it can also be shown[1] that the graph of $\hbar$ is the upper boundary of the two-dimensional convex set $\{(\mathcal{P}(F), \mathcal{U}(F)) : F \in \mathcal{F}\}$ and thus $\hbar$ is concave and strictly increasing. The following theorem, which is the most important and technically difficult result of this paper, states that $\hbar$ is a piecewise linear function, as illustrated in Fig. 2.

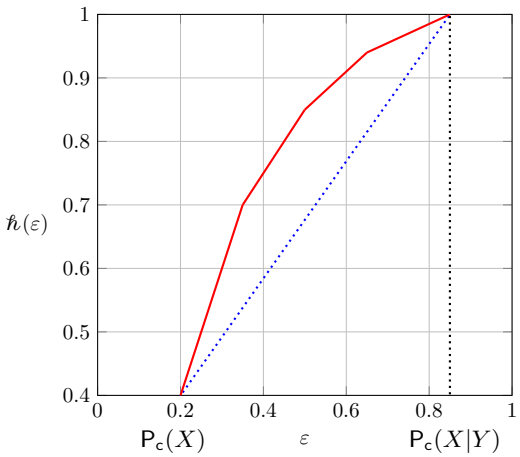


Fig. 2. Typical $\hbar$ and its trivial lower bound, the chord connecting $(\mathsf{P_c}(X), \hbar(\mathsf{P_c}(X)))$ and $(\mathsf{P_c}(X|Y), 1)$.

Theorem 1. *The function $\hbar : [\mathsf{P_c}(X), \mathsf{P_c}(X|Y)] \to \mathbb{R}^+$ is piecewise linear, i.e., there exist $K \geq 1$ and thresholds $\mathsf{P_c}(X) = \varepsilon_0 \leq \varepsilon_1 \leq \ldots \leq \varepsilon_K = \mathsf{P_c}(X|Y)$ such that $\hbar$ is linear on $[\varepsilon_{i-1}, \varepsilon_i]$ for all $i = 1, \ldots, K$.*

The proof of this theorem, which is given in Appendix A, relies on the geometrical formulation of $\hbar$. In particular, it

[1] Note that [35, Theorem 2.3] deals with a similar problem where $\mathsf{P_c}(X|Z)$ and $\mathsf{P_c}(Y|Z)$ are replaced by $H(X|Z)$ and $H(Y|Z)$, respectively. Just as $(H(X|Z), H(Y|Z))$, the pair $(\mathsf{P_c}(X|Z), \mathsf{P_c}(Y|Z))$ can be written as a convex combination of points in a two-dimensional set. In our setting, this set turns out to be $\{(\mathsf{P_c}(X'), \mathsf{P_c}(Y')) : Y' \sim q' \in \mathcal{P}(\mathcal{Y})$ and $X' \sim p'$, where $p'(x) = \sum_y P_{X|Y}(x|y)q'(y)\}$. See [11] for a generalization of this argument.

is proved that $\mathcal{P}$ and $\mathcal{U}$, are piecewise linear functions on $\mathcal{F}$. Using this fact, we establish the existence of a piecewise linear path of *optimal filters* in $\mathcal{F}$. The proof technique allows us to derive the slope of $\hbar$ on $[\varepsilon_{i-1}, \varepsilon_i]$, given the family of optimal filters at a single point $\varepsilon \in [\varepsilon_{i-1}, \varepsilon_i]$. For example, since the family of optimal filters at $\varepsilon = \mathsf{P_c}(X|Y)$ is easily obtainable, it is possible to compute $\hbar$ on the last interval. We utilize this observation in Section II-C to prove that in the binary case $\hbar$ is indeed linear.

B. Perfect Privacy

When $\varepsilon = \mathsf{P_c}(X)$, observing Z does not increase the probability of guessing X. In this case we say that perfect privacy holds. An interesting problem is to characterize when non-trivial utility can be obtained under perfect privacy, that is, to characterize when $\hbar(\mathsf{P_c}(X)) > \mathsf{P_c}(Y)$ holds. To the best of our knowledge, a general necessary and sufficient condition for this requirement is unknown.

Note that $\hbar(\mathsf{P_c}(X)) > \mathsf{P_c}(Y)$ is equivalent to $g^\infty(0) > 0$. As opposed to the Shannon mutual information, $I_\infty(X;Z) = 0$ does not necessarily imply that $X \perp\!\!\!\perp Z$. In particular, the *weak independence*[2] argument from [8, Lemma 10] (see also [13]) cannot be applied for g^∞. However, we have the following result whose proof is given in Appendix B.

Proposition 1. *Let (X, Z) be a pair of random variables with X uniformly distributed. If $I_\infty(X;Z) = 0$, then $X \perp\!\!\!\perp Z$.*

As a consequence of Proposition 1, when X and Y are uniformly distributed, one can apply the weak independence arguments from [8, Lemma 10] to obtain the following.

Corollary 1. *If X and Y are uniformly distributed, then $g^\infty(0) > 0$ if and only if X is weakly independent of Y.*

When X is uniform, the privacy requirement $I_\infty(X;Z) \le \varepsilon$ guarantees that an adversary observing Z cannot efficiently estimate any arbitrary *randomized function* of X. To see this, consider a random variable U satisfying $U \multimap X \multimap Z$. Then we have

$$\begin{aligned}\mathsf{P_c}(U|Z) &= \sum_{z\in\mathcal{Z}} \max_{u\in\mathcal{U}} \sum_{x\in\mathcal{X}} P_{UX}(u,x) P_{Z|X}(z|x) \\ &\le \sum_{z\in\mathcal{Z}} \left[\max_{x\in\mathcal{X}} P_{Z|X}(z|x)\right] \left[\max_{u\in\mathcal{U}} \sum_{x\in\mathcal{X}} P_{UX}(u,x)\right] \\ &= \frac{\mathsf{P_c}(X|Z)\mathsf{P_c}(U)}{\mathsf{P_c}(X)},\end{aligned}$$

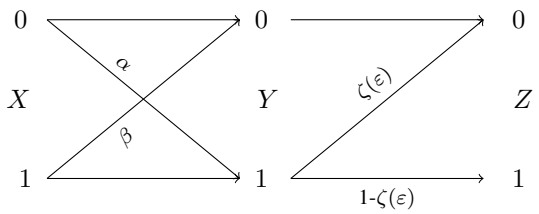
which can be rearranged to yield $I_\infty(U;Z) \le I_\infty(X;Z)$. It is worth mentioning that the data processing inequality for I_∞ [4] states that $I_\infty(Z;U) \le I_\infty(Z;X)$. However, $I_\infty(Z;U)$ is not necessarily equal to $I_\infty(U;Z)$.

C. Binary Case

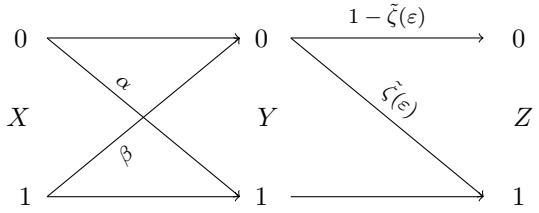
A channel W is called a binary input binary output channel with crossover probabilities α and β, denoted by $\mathsf{BIBO}(\alpha,\beta)$, if $\mathsf{W}(\cdot|0) = (\bar\alpha, \alpha)$ and $\mathsf{W}(\cdot|1) = (\beta, \bar\beta)$. Note that if $X \sim \mathsf{Bernoulli}(p)$ with $p \in [\frac{1}{2}, 1)$ and $P_{Y|X} = \mathsf{BIBO}(\alpha,\beta)$ with $\alpha, \beta \in [0, \frac{1}{2})$, then $\mathsf{P_c}(X) = p$ and

$$\mathsf{P_c}(X|Y) = \max\{\bar\alpha\bar p, \beta p\} + \bar\beta p.$$

In this case, if $\bar\alpha\bar p \le \beta p$ then $\mathsf{P_c}(X|Y) = p = \mathsf{P_c}(X)$ and hence $\hbar(p) = 1$. The following theorem, whose proof is given in Appendix C, establishes the linear behavior of $\hbar$ in the non-trivial case $\bar\alpha\bar p > \beta p$.



(a) $\alpha\bar\alpha\bar p^2 < \beta\bar\beta p^2$.



(b) $\alpha\bar\alpha\bar p^2 \ge \beta\bar\beta p^2$.

Fig. 3. Optimal privacy mechanisms in Theorem 2.

Theorem 2. *Let $X \sim \mathsf{Bernoulli}(p)$ with $p \in [\frac{1}{2}, 1)$ and $P_{Y|X} = \mathsf{BIBO}(\alpha,\beta)$ with $\alpha, \beta \in [0, \frac{1}{2})$ such that $\bar\alpha\bar p > \beta p$. Then, for any $\varepsilon \in [p, \bar\alpha\bar p + \bar\beta p] = [\mathsf{P_c}(X), \mathsf{P_c}(X|Y)]$,*

$$\hbar(\varepsilon) = \begin{cases} 1 - \zeta(\varepsilon) q, & \alpha\bar\alpha\bar p^2 < \beta\bar\beta p^2, \\ 1 - \tilde\zeta(\varepsilon)\bar q, & \alpha\bar\alpha\bar p^2 \ge \beta\bar\beta p^2, \end{cases}$$

where $q \coloneqq q_Y(1) = \alpha\bar p + \bar\beta p$,

$$\zeta(\varepsilon) \coloneqq \frac{\bar\alpha\bar p + \bar\beta p - \varepsilon}{\bar\beta p - \alpha\bar p}, \quad \text{and} \quad \tilde\zeta(\varepsilon) \coloneqq \frac{\bar\alpha\bar p + \bar\beta p - \varepsilon}{\bar\alpha\bar p - \beta p}. \tag{8}$$

Furthermore, the Z-channel $\mathsf{Z}(\zeta(\varepsilon))$ and the reverse Z-channel $\tilde{\mathsf{Z}}(\tilde\zeta(\varepsilon))$ achieve $\hbar(\varepsilon)$ when $\alpha\bar\alpha\bar p^2 < \beta\bar\beta p^2$ and $\alpha\bar\alpha\bar p^2 \ge \beta\bar\beta p^2$, respectively. The optimal privacy filters are depicted in Fig. 3.

Note that the condition $\alpha\bar\alpha\bar p^2 < \beta\bar\beta p^2$ is equivalent to

$$P_{X|Y}(1|1) > P_{X|Y}(0|0),$$

and that $P_{X|Y}(0|0) > \frac{1}{2}$ whenever $\bar\alpha\bar p > \beta p$. Hence, intuitively speaking, the event $Y = 1$ reveals more information about X than the event $Y = 0$. Consequently, an optimal privacy mechanism $\mathcal{M}$ needs to distort the event $Y = 1$.

Under the hypotheses of Theorem 2, there exists a Z-channel for every $\varepsilon \in [\mathsf{P_c}(X), \mathsf{P_c}(X|Y)]$ that achieves $\hbar(\varepsilon)$. A minor modification to the proof of Theorem 2 shows that the Z-channel is the only binary privacy filter with this optimality property for $p \in (\frac{1}{2}, 1)$. It is worth mentioning that in the

[2] X is said to be weakly independent of Z if the vectors $\{P_{X|Z}(\cdot|z) : z \in \mathcal{Z}\}$ are linearly dependent [36].

symmetric case ($\alpha = \beta$) with uniform input ($p = \frac{1}{2}$), the channel $\mathsf{BSC}(0.5\zeta(\varepsilon))$ can be shown to also achieve $\hbar(\varepsilon)$.

It is straightforward to show that $1-\zeta(p)q > \bar{q}$ if and only if $p \in (\frac{1}{2}, 1)$, and $1-\zeta(p)q > q$ if and only if $\alpha\bar{\alpha}\bar{p}^2 < \beta\bar{\beta}p^2$. Also, note that $\hbar(p) = q$ when $\alpha\bar{\alpha}\bar{p}^2 \geq \beta\bar{\beta}p^2$. In particular, we have the following necessary and sufficient condition for the non-trivial utility under perfect privacy.

Corollary 2. *Let $X \sim \mathsf{Bernoulli}(p)$ with $p \in [\frac{1}{2}, 1)$ and $P_{Y|X} = \mathsf{BIBO}(\alpha, \beta)$ with $\alpha, \beta \in [0, \frac{1}{2})$ such that $\bar{\alpha}\bar{p} > \beta p$. Then $g^{\infty}(0) > 0$ if and only if $\alpha\bar{\alpha}\bar{p}^2 < \beta\bar{\beta}p^2$ and $p \in (\frac{1}{2}, 1)$.*

D. A variant of $\hbar$

Thus far, we studied the privacy-constrained guessing probability $\hbar(\varepsilon)$ where no constraint on the cardinality of the alphabet of the displayed data Z is imposed (other than being finite). Nevertheless, we know that it is sufficient to consider $\mathcal{Z}$ with cardinality $|\mathcal{Y}| + 1$. However, as mentioned in the introduction, it may be desirable to generate the displayed data on the same alphabet as that of Y. In this section, we consider the case where $\mathcal{Z}$ is constrained to satisfy $|\mathcal{Z}| = |\mathcal{Y}|$, which leads to the following variant of $\hbar$, denoted by $\underline{\hbar}$.

Definition 3. *For arbitrary discrete random variables X and Y supported on $\mathcal{X}$ and $\mathcal{Y}$ respectively, we define the function $\underline{\hbar} : [\mathsf{P_c}(X), \mathsf{P_c}(X|Y)] \to \mathbb{R}^+$ by*

$$\underline{\hbar}(\varepsilon) \coloneqq \sup_{P_{Z|Y} \in \underline{\mathfrak{D}}_{\varepsilon}} \mathsf{P_c}(Y|Z),$$

where

$$\underline{\mathfrak{D}}_{\varepsilon} \coloneqq \left\{P_{Z|Y} : \mathcal{Z} = \mathcal{Y}, X \multimap Y \multimap Z, \mathsf{P_c}(X|Z) \leq \varepsilon\right\}.$$

Unlike $\hbar$, the definition of $\underline{\hbar}$ requires $\mathcal{Z} = \mathcal{Y}$. This difference makes the tools from [35] unavailable. In particular, the concavity and hence the piecewise linearity of $\hbar$ do not carry over to $\underline{\hbar}$. However, we have the following theorem for $\underline{\hbar}$ whose proof is given in Appendix D. For notational convenience, we adopt the convention $\frac{x}{0} = +\infty$ for $x > 0$. For $(y_0, z_0) \in \mathcal{Y} \times \mathcal{Y}$, a channel W is said to be an N-ary Z-channel with crossover probability γ from y_0 to z_0, denoted by $\mathsf{Z}^{y_0,z_0}(\gamma)$, if the input and output alphabets are $\mathcal{Y}$ and $\mathsf{W}(y|y) = 1$ for $y \neq y_0$, $\mathsf{W}(z_0|y_0) = \gamma$, and $\mathsf{W}(y_0|y_0) = \bar{\gamma}$. We also let $\underline{\hbar}'(\mathsf{P_c}(X|Y))$ denote the left derivative of $\underline{\hbar}(\cdot)$ evaluated at $\varepsilon = \mathsf{P_c}(X|Y)$.

Theorem 3. *Let X and Y be discrete random variables. If $\mathsf{P_c}(X) < \mathsf{P_c}(X|Y)$, then there exists $\varepsilon_{\mathsf{L}} \in (\mathsf{P_c}(X), \mathsf{P_c}(X|Y))$ such that $\underline{\hbar}$ is linear on $[\varepsilon_{\mathsf{L}}, \mathsf{P_c}(X|Y)]$. In particular, for every $\varepsilon \in [\varepsilon_{\mathsf{L}}, \mathsf{P_c}(X|Y)]$,*

$$\underline{\hbar}(\varepsilon) = 1 - (\mathsf{P_c}(X|Y) - \varepsilon)\underline{\hbar}'(\mathsf{P_c}(X|Y)). \tag{9}$$

Moreover, if $q_Y(y) > 0$ for all $y \in \mathcal{Y}$ and for each $y \in \mathcal{Y}$ there exists (a unique) $x_y \in \mathcal{X}$ such that $P_{X|Y}(x_y|y) > P_{X|Y}(x|y)$ for all $x \neq x_y$, then

$$\underline{\hbar}'(\mathsf{P_c}(X|Y)) = \min_{(y,z)\in\mathcal{Y}\times\mathcal{Y}} \frac{q_Y(y)}{P_{XY}(x_y, y) - P_{XY}(x_z, y)}. \tag{10}$$

In addition, if $(y_0, z_0) \in \mathcal{Y} \times \mathcal{Y}$ attains the minimum in (10), then there exists $\varepsilon_{\mathsf{L}}^{y_0,z_0} < \mathsf{P_c}(X|Y)$ such that $\mathsf{Z}^{y_0,z_0}(\zeta^{y_0,z_0}(\varepsilon))$ achieves $\underline{\hbar}(\varepsilon)$ for every $\varepsilon \in [\varepsilon_{\mathsf{L}}^{y_0,z_0}, \mathsf{P_c}(X|Y)]$, where

$$\zeta^{y_0,z_0}(\varepsilon) = \frac{\mathsf{P_c}(X|Y) - \varepsilon}{P_{XY}(x_{y_0}, y_0) - P_{XY}(x_{z_0}, y_0)}.$$

It is clear, from Definition 3, that $\underline{\hbar}(\varepsilon) \leq \hbar(\varepsilon)$ for all $\varepsilon \in [\mathsf{P_c}(X), \mathsf{P_c}(X|Y)]$. Hence, Theorem 3 provides a lower bound for $\hbar$ in the high utility regime.

Although (9) establishes the linear behavior of $\underline{\hbar}$ over $[\varepsilon_{\mathsf{L}}, \mathsf{P_c}(X|Y)]$ for general X and Y, a priori it is not clear how to obtain $\underline{\hbar}'(\mathsf{P_c}(X|Y))$. Under the assumptions of Theorem 3, (10) expresses $\underline{\hbar}'(\mathsf{P_c}(X|Y))$ as the minimum of *finitely* many numbers, and a suitable Z-channel achieves $\underline{\hbar}$ for ε close to $\mathsf{P_c}(X|Y)$. As we will see in the following section, these assumptions are rather general and allow us to derive a closed form expression for $\underline{\hbar}$ in the high utility regime for some pairs of binary random *vectors* (X^n, Y^n) with $X^n, Y^n \in \{0,1\}^n$.

III. Binary Vector Case

We next study privacy aware guessing for a pair of binary random vectors (X^n, Y^n). First note that since having more side information only improves the probability of correct guessing, one can write

$$\mathsf{P_c}(X^n) \leq \mathsf{P_c}(X^n|Z^n) \leq \mathsf{P_c}(X^n|Y^n, Z^n) = \mathsf{P_c}(X^n|Y^n)$$

for $X^n \multimap Y^n \multimap Z^n$ and thus, we can restrict ε^n in the following definition to $[\mathsf{P_c}(X^n), \mathsf{P_c}(X^n|Y^n))]$.

Definition 4. *For a given pair of binary random vectors (X^n, Y^n), let $\underline{\hbar}_n : [\mathsf{P_c}^{1/n}(X^n), \mathsf{P_c}^{1/n}(X^n|Y^n)] \to \mathbb{R}^+$ be the function defined by*

$$\underline{\hbar}_n(\varepsilon) \coloneqq \sup_{P_{Z^n|Y^n} \in \underline{\mathfrak{D}}_{n,\varepsilon}} \mathsf{P_c}^{1/n}(Y^n|Z^n), \tag{11}$$

where $\underline{\mathfrak{D}}_{n,\varepsilon} \coloneqq \{P_{Z^n|Y^n} : \mathcal{Z}^n = \{0,1\}^n, X^n \multimap Y^n \multimap Z^n, \mathsf{P_c}^{1/n}(X^n|Z^n) \leq \varepsilon\}$.

Note that this definition does not make any assumption about the privacy filters $P_{Z^n|Y^n}$ apart from $\mathcal{Z}^n = \{0,1\}^n$. Nonetheless, this restriction makes the functional properties of $\underline{\hbar}_n$ different from those of $\hbar$.

We study $\underline{\hbar}_n$ in the following two scenarios for (X^n, Y^n):

- (a_1) $X_1, \ldots, X_n$ are i.i.d. samples drawn from $\mathsf{Bernoulli}(p)$,
- (a_2) $X_1 \sim \mathsf{Bernoulli}(p)$ and $X_k = X_{k-1} \oplus U_k$ for $k = 2, \ldots, n$, where $U_2, \ldots, U_n$ are i.i.d. samples drawn from $\mathsf{Bernoulli}(r)$ and independent of X_1, and $\oplus$ denotes mod 2 addition,

and in both cases, we assume that

- (b) $Y_k = X_k \oplus V_k$ for $k = 1, \ldots, n$, where $V_1, \ldots, V_n$ are i.i.d. samples drawn from $\mathsf{Bernoulli}(\alpha)$ and independent of X^n.

We study $\underline{\hbar}_n$ for (X^n, Y^n) satisfying the assumptions (a_1) and (b) in Section III-A and for (X^n, Y^n) satisfying the assumptions (a_2) and (b) in Section III-B. In the latter section, we also study $\underline{\hbar}_n$ in the special case $r = 0$ in more detail.

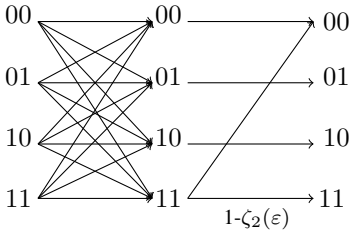


Fig. 4. The optimal mechanism for $\underline{\hbar}_2(\varepsilon)$ for $\varepsilon \in [\varepsilon_{\mathsf{L}}, \bar{\alpha}]$.

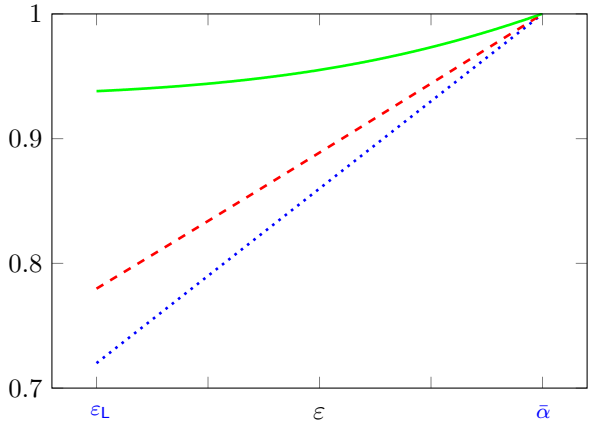


Fig. 5. The graphs of $\underline{\hbar}_{10}(\varepsilon)$ (green solid curve), $\underline{\hbar}_2(\varepsilon)$ (red dashed curve), and $\hbar^{\mathsf{i}}_2(\varepsilon) = \hbar^{\mathsf{i}}_{10}(\varepsilon)$ (blue dotted line) given in Proposition 2 and Theorem 4 for i.i.d. (X^n, Y^n) with $X \sim \mathsf{Bernoulli}(0.6)$ and $P_{Y|X} = \mathsf{BSC}(0.2)$.

A. I.I.D. Case

Here, we assume that (X^n, Y^n) satisfy (a_1) and (b) and apply Theorem 3 to derive a closed form expression for $\underline{\hbar}_n(\varepsilon)$ for ε close to $\mathsf{P_c}(X^n|Y^n)$. Additionally, we determine an optimal filter in the same regime.

We begin by identifying the domain $[\mathsf{P_c}(X^n), \mathsf{P_c}(X^n|Y^n)]$ of $\underline{\hbar}_n$ in the following lemma, whose proof follows directly from the definition of $\mathsf{P_c}$.

Lemma 1. *Assume that $(X_1, Z_1), \ldots, (X_n, Z_n)$ are independent pairs of random variables. Then*

$$\mathsf{P_c}(X^n|Z^n) = \prod_{k=1}^{n} \mathsf{P_c}(X_k|Z_k).$$

Thus, according to this lemma, if $p \in [\frac{1}{2}, 1)$ and $\alpha \in [0, \bar{p})$ then $\mathsf{P_c}(X^n) = p^n$ and $\mathsf{P_c}(X^n|Y^n) = \bar{\alpha}^n$. The following theorem, whose proof is given in Appendix E, is a straightforward consequence of Theorem 3. A channel W is said to be a 2^n-ary Z-channel with crossover probability γ, denoted by $\mathsf{Z}_n(\gamma)$, if its input and output alphabets are $\{0,1\}^n$ and it is $\mathsf{Z}^{\mathbf{1},\mathbf{0}}(\gamma)$, where $\mathbf{0} = (0, 0, \ldots, 0)$ and $\mathbf{1} = (1, 1, \ldots, 1)$.

Theorem 4. *Assume that (X^n, Y^n) satisfy (a_1) and (b) with $p \in [\frac{1}{2}, 1)$ and $\alpha \in [0, \frac{1}{2})$ such that $\bar{\alpha} > p$. Then there exists $\varepsilon_{\mathsf{L}} < \bar{\alpha}$ such that, for all $\varepsilon \in [\varepsilon_{\mathsf{L}}, \bar{\alpha}]$,*

$$\underline{\hbar}^n_n(\varepsilon) = 1 - \zeta_n(\varepsilon) q^n$$

where $q \coloneqq \alpha\bar{p} + \bar{\alpha}p$ and

$$\zeta_n(\varepsilon) \coloneqq \frac{\bar{\alpha}^n - \varepsilon^n}{(\bar{\alpha}p)^n - (\alpha\bar{p})^n}.$$

Moreover, the 2^n-ary Z-channel $\mathsf{Z}_n(\zeta_n(\varepsilon))$ achieves $\underline{\hbar}_n(\varepsilon)$ in this interval.

The optimal privacy mechanism achieving $\underline{\hbar}_2(\varepsilon)$ is depicted in Fig. 4. From an implementation point of view, the simplest family of privacy mechanisms consists of those mechanisms for which Z_k is a noisy version of Y_k for each $k = 1, \ldots, n$. Specifically, the family of mechanisms that generate Z_k, given Y_k, using a *single* BIBO channel W, and thus

$$P_{Z^n|Y^n}(z^n|y^n) = \prod_{k=1}^{n} \mathsf{W}(z_k|y_k), \tag{12}$$

for all $y^n, z^n \in \{0,1\}^n$. Now, let $\hbar^{\mathsf{i}}_n(\varepsilon) = \sup \mathsf{P_c}^{1/n}(Y^n|Z^n)$, where the supremum is taken over all $P_{Z^n|Y^n}$ satisfying (12) and $\mathsf{P_c}^{1/n}(X^n|Z^n) \le \varepsilon$. It is clear that $\hbar^{\mathsf{i}}_n(\varepsilon) \le \underline{\hbar}_n(\varepsilon)$ for all $\varepsilon \in [\mathsf{P_c}^{1/n}(X^n), \mathsf{P_c}^{1/n}(X^n|Y^n)]$. The following proposition, whose proof is given in Appendix F, shows that if we restrict the privacy filter $P_{Z^n|Y^n}$ to be memoryless, then the optimal filter coincides with the optimal filter in the scalar case, which in this case is $\mathsf{Z}(\zeta(\varepsilon))$ as defined in Theorem 2.

Proposition 2. *Assume that (X^n, Y^n) satisfy (a_1) and (b) with $p \in [\frac{1}{2}, 1)$ and $\alpha \in [0, \frac{1}{2})$ such that $\bar{\alpha} > p$. Then, for all $\varepsilon \in [p, \bar{\alpha}]$,*

$$\hbar^{\mathsf{i}}_n(\varepsilon) = 1 - \zeta(\varepsilon) q,$$

where $q \coloneqq \alpha\bar{p} + \bar{\alpha}p$ and $\zeta(\varepsilon) \coloneqq \dfrac{\bar{\alpha}\bar{p} + \bar{\alpha}p - \varepsilon}{\bar{\alpha}p - \alpha\bar{p}}$.

It must be noted that, despite the fact that (X^n, Y^n) is i.i.d., the memoryless privacy filter associated to $\hbar^{\mathsf{i}}_n(\varepsilon)$ is not optimal, as $\underline{\hbar}_n(\varepsilon)$ is a function of n while $\hbar^{\mathsf{i}}_n(\varepsilon)$ is not. The following corollary, whose proof is given in Appendix G, bounds the loss resulting from using a memoryless filter instead of an optimal one for $\varepsilon \in [\varepsilon_{\mathsf{L}}, \bar{\alpha}]$. Clearly, for $n = 1$, there is no gap as $\underline{\hbar}_1(\varepsilon) = \hbar(\varepsilon) = \hbar^{\mathsf{i}}_1(\varepsilon)$.

Corollary 3. *Let (X^n, Y^n) satisfy (a_1) and (b) with $p \in [\frac{1}{2}, 1)$ and $\alpha \in [0, \frac{1}{2})$ such that $\bar{\alpha} > p$. Let ε_{L} be as in Theorem 4. If $p > \frac{1}{2}$ and $\alpha > 0$, then for $\varepsilon \in [\varepsilon_{\mathsf{L}}, \bar{\alpha}]$ and sufficiently large n*

$$\underline{\hbar}_n(\varepsilon) - \hbar^{\mathsf{i}}_n(\varepsilon) \ge (\bar{\alpha} - \varepsilon)[\Phi(1) - \Phi(n)], \tag{13}$$

where $q = \alpha\bar{p} + \bar{\alpha}p$ and

$$\Phi(n) \coloneqq \frac{q^n \bar{\alpha}^{n-1}}{(\bar{\alpha}p)^n - (\alpha\bar{p})^n}.$$

If $p = \frac{1}{2}$, then

$$\hbar^{\mathsf{i}}_n(\varepsilon) \le \underline{\hbar}_n(\varepsilon) \le \hbar^{\mathsf{i}}_n(\varepsilon) + \frac{\alpha}{2\bar{\alpha}}, \tag{14}$$

for every $n \ge 1$ and $\varepsilon \in [\varepsilon_{\mathsf{L}}, \bar{\alpha}]$.

Note that $\Phi(n) \downarrow 0$ as $n \to \infty$. Thus (13) implies that, as expected, the gap between the performance of the optimal

privacy filter and that of the optimal memoryless privacy filter increases as n increases. This observation is numerically illustrated in Fig. 5, where $\underline{\hbar}_n(\varepsilon)$ is plotted as a function of ε for $n = 2$ and $n = 10$. Moreover, (14) implies that when $p = \frac{1}{2}$ and α is small, $\underline{\hbar}_n(\varepsilon)$ can be approximated by $\hbar^{\mathsf{i}}_n(\varepsilon)$. Thus, we can approximate the optimal filter $\mathsf{Z}_n(\zeta_n(\varepsilon))$ with a simple memoryless filter given by $Z_k = Y_k \oplus W_k$, where $W_1, \dots, W_n$ are i.i.d. $\mathsf{Bernoulli}(0.5\zeta(\varepsilon))$ random variables that are independent of (X^n, Y^n).

B. Markov Private Data

In this section, we assume that X^n comprises the first n samples of a homogeneous first-order Markov process having a symmetric transition matrix; i.e., (X^n, Y^n) satisfy (a_2) and (b). In practice, this may account for data that follows a pattern, such as a password.

It is easy to see that under assumptions (a_2) and (b),

$$\Pr(X^n = x^n) = \bar{p}\bar{r}^{n-1}\left(\frac{p}{\bar{p}}\right)^{x_1}\prod_{k=2}^{n}\left(\frac{r}{\bar{r}}\right)^{x_k \oplus x_{k-1}}.$$

In particular, if $r < \frac{1}{2} \le p$, then a direct computation shows that $\mathsf{P_c}(X^n) = p\bar{r}^{n-1}$. The values of $\mathsf{P_c}(X^n|Y^n)$ for odd and even n are slightly different. For simplicity, in what follows we assume that n is odd. In this case, as shown in equation (64) in Appendix H,

$$\mathsf{P_c}(X^n|Y^n) = \bar{\alpha}^n\bar{r}^{n-1}\sum_{k=0}^{(n-1)/2}\binom{n}{k}\left(\frac{\alpha}{\bar{\alpha}}\right)^k. \tag{15}$$

Theorem 3 established the optimality of a Z-channel Z^{y_0,z_0} for some $y_0, z_0 \in \{0,1\}^n$. In order to find a closed form expression for $\underline{\hbar}_n$, it is necessary to find (y_0, z_0) which in principle depends on the parameters (p, α, r). The following theorem, whose proof is given in Appendix H, bounds $\underline{\hbar}_n$ for different values of (p, α, r).

Theorem 5. *Assume that $n \in \mathbb{N}$ is odd and (X^n, Y^n) satisfy (a_2) and (b) with $p \in [\frac{1}{2}, 1)$, $\alpha \in (0, \frac{1}{2})$, and $\bar{\alpha}\bar{p} > \alpha p$. If $\frac{r}{\bar{r}} < \left(\frac{\alpha}{\bar{\alpha}}\right)^{n-1}$, then there exists $\varepsilon_{\mathsf{L}} < \mathsf{P_c}(X^n|Y^n)$ such that*

$$1 - \zeta_n(\varepsilon)\Pr(Y^n = \mathbf{1}) \le \underline{\hbar}^n_n(\varepsilon) \le 1 - \zeta_n(\varepsilon)\alpha^n,$$

for every $\varepsilon \in [\varepsilon_{\mathsf{L}}, \mathsf{P_c}(X^n|Y^n)]$, where

$$\zeta_n(\varepsilon) := \bar{r}\frac{\mathsf{P_c}(X^n|Y^n) - \varepsilon^n}{p(\bar{\alpha}\bar{r})^n - \bar{p}(\alpha\bar{r})^n}.$$

Furthermore, the 2^n-ary Z-channel $\mathsf{Z}_n(\zeta_n(\varepsilon))$ achieves the lower bound in this interval.

The special case of $r = 0$ is of particular interest. Note that when $r = 0$, then (a_2) corresponds to $X_1 = \cdots = X_n = \theta \in \{0,1\}$. Here, $Y^n \in \{0,1\}^n$ are i.i.d. copies drawn from $P_{Y|\theta} = \mathsf{Bernoulli}(\bar{\alpha}^\theta\alpha^{\bar{\theta}})$. The prior distribution of the parameter θ is $\mathsf{Bernoulli}(p)$. The parameter θ is considered to be private and Y^n must be guessed as accurately as possible. This problem can be viewed as a reverse version of *privacy-aware learning* studied in [37]. The following proposition, whose proof is given in Appendix I, provides a closed form expression for $\underline{\hbar}_n$ in the low privacy regime. Note that in this case, $\mathsf{P_c}(\theta) = p$ and the value of $\mathsf{P_c}(\theta|Y^n)$ is obtained from (15) by setting $r = 0$.

Proposition 3. *Assume that n is odd. Let $\theta \sim \mathsf{Bernoulli}(p)$ with $p \in [\frac{1}{2}, 1)$ and Y^n be n i.i.d. $\mathsf{Bernoulli}(\bar{\alpha}^\theta\alpha^{\bar{\theta}})$ samples with $\alpha \in (0, \frac{1}{2})$, $\bar{\alpha}\bar{p} > \alpha p$ and $p < \mathsf{P_c}(\theta|Y^n)$. Then, there exists $\varepsilon_{\mathsf{L}} < \mathsf{P_c}(\theta|Y^n)$ such that*

$$\max_{\substack{P_{Z^n|Y^n}: Z^n = \{0,1\}^n, \\ \mathsf{P_c}(\theta|Z^n) \le \varepsilon^n}} \mathsf{P_c}(Y^n|Z^n) = 1 - \zeta_n(\varepsilon)(p\bar{\alpha}^n + \bar{p}\alpha^n),$$

for every $\varepsilon \in [\varepsilon_{\mathsf{L}}, \mathsf{P_c}(\theta|Y^n)]$ where

$$\zeta_n(\varepsilon) = \frac{\mathsf{P_c}(\theta|Y^n) - \varepsilon^n}{p\bar{\alpha}^n - \bar{p}\alpha^n}.$$

Moreover, the 2^n-ary Z-channel $\mathsf{Z}_n(\zeta_n(\varepsilon))$ achieves $\underline{\hbar}_n(\varepsilon)$ in this interval.

IV. Continuous Case

In this section, we assume that X and Y are real-valued random variables having a joint density P_{XY} and the filter $P_{Z|Y}$ is realized by an independent additive Gaussian noise random variable. In particular, the privacy filter's output is

$$Z_\gamma = \sqrt{\gamma}Y + N_{\mathsf{G}},$$

for some $\gamma \ge 0$, where $N_{\mathsf{G}} \sim \mathcal{N}(0,1)$ is independent of (X, Y). The choice of additive Guassian mechanisms is due to their implementation simplicity and mathematical tractability. Nonetheless, additive non-Gaussian and more general non-linear mechanisms might be natural in specific applications; their investigation is left as a future work. The goal of this section is to study sENSR, defined in Definition 2. To make the notation simpler, we define the following.

Definition 5. *Given a pair of absolutely continuous random variables (X, Y) with distribution P_{XY} and $\varepsilon \ge 0$, we say that Z_γ satisfies ε-*strong estimation privacy*, denoted as $Z_\gamma \in \Gamma(P_{XY}, \varepsilon)$, if*

$$1 - \varepsilon \le \frac{\mathsf{mmse}(f(X)|Z_\gamma)}{\mathsf{var}(f(X))} \le 1, \tag{16}$$

*holds for every measurable function $f : \mathbb{R} \to \mathbb{R}$ with $0 < \mathsf{var}(f(X)) < \infty$. Similarly, Z_γ is said to satisfy ε-*weak estimation privacy*, denoted by $Z_\gamma \in \partial\Gamma(P_{XY}, \varepsilon)$, if (16) holds for identity function, i.e., $f(x) = x$.*

Similar to privacy, the utility between Y and Z_γ will be measured in terms of $\mathsf{mmse}(Y|Z_\gamma)$, and hence sENSR (Definition 2) quantifies the tradeoff between utility and privacy. In fact, sENSR can be equivalently written as

$$\mathsf{sENSR}(P_{XY}, \varepsilon) = \inf_{\gamma \ge 0 : Z_\gamma \in \Gamma(P_{XY}, \varepsilon)} \frac{\mathsf{mmse}(Y|Z_\gamma)}{\mathsf{var}(Y)}.$$

We can analogously define the *weak estimation noise-to-signal ratio* as

$$\mathsf{wENSR}(P_{XY}, \varepsilon) := \inf_{\gamma \ge 0 : Z_\gamma \in \partial\Gamma(P_{XY}, \varepsilon)} \frac{\mathsf{mmse}(Y|Z_\gamma)}{\mathsf{var}(Y)}.$$

Note that sENSR and wENSR are non-increasing since $\Gamma(P_{XY}, \varepsilon) \subseteq \Gamma(P_{XY}, \varepsilon')$ and $\partial\Gamma(P_{XY}, \varepsilon) \subseteq \partial\Gamma(P_{XY}, \varepsilon')$ if $\varepsilon \le \varepsilon'$. For the sake of brevity, we omit P_{XY} in $\Gamma(P_{XY}, \varepsilon)$,

$\partial\Gamma(P_{XY},\varepsilon)$, $\mathsf{sENSR}(P_{XY},\varepsilon)$, and $\mathsf{wENSR}(P,\varepsilon)$ when there is no risk of confusion.

In what follows we derive equivalent conditions for $Z_\gamma \in \Gamma(\varepsilon)$ and $Z_\gamma \in \partial\Gamma(\varepsilon)$, respectively. Recall that the (Pearson) correlation coefficient of the random variables U and V is defined as

$$\rho(U,V) = \frac{\mathsf{cov}(U,V)}{\sqrt{\mathsf{var}(U)\mathsf{var}(V)}}$$

provided that $0 < \mathsf{var}(U), \mathsf{var}(V) < \infty$. For a random variable U, let $\mathcal{S}_U$ be the set of all measurable functions $f : \mathbb{R} \to \mathbb{R}$ such that $0 < \mathsf{var}(f(U)) < \infty$. Consider the following.

Definition 6 ([17], [38]). *Let U and V be a pair of random variables.*

i) The maximal correlation *of U and V, denoted by $\rho_m(U,V)$, is defined as*

$$\rho_m(U,V) \;\coloneqq\; \sup_{(f,g)\in\mathcal{S}_U\times\mathcal{S}_V} \rho(f(U),g(V)),$$

provided that $0 < \mathsf{var}(U), \mathsf{var}(V) < \infty$. If either $\mathcal{S}_U \times \mathcal{S}_V$ is empty (which happens precisely when either U or V is constant almost surely), then we set $\rho_m(U,V) = 0$.

ii) The one-sided maximal correlation[3] *between U and V, denoted by $\eta_V(U)$, is defined as*

$$\eta_V(U) \coloneqq \sup_{g\in\mathcal{S}_V} \rho(U,g(V)),$$

provided that $0 < \mathsf{var}(U) < \infty$. If $\mathcal{S}_V$ is empty, then we set $\eta_V(U) = 0$.

Rényi [17] showed that $\eta_V^2(U) = \frac{\mathsf{var}(\mathbb{E}[U|V])}{\mathsf{var}(U)}$. Therefore, the law of total variance implies

$$\frac{\mathsf{mmse}(U|V)}{\mathsf{var}(U)} = \frac{\mathbb{E}[\mathsf{var}(U|V)]}{\mathsf{var}(U)} = 1 - \frac{\mathsf{var}(\mathbb{E}[U|V])}{\mathsf{var}(U)} = 1 - \eta_V^2(U). \tag{17}$$

It can also be shown that $0 \le \rho_m(U,V) \le 1$, where the lower bound is achieved if and only if U and V are independent, and the upper bound is achieved if and only if there exists a pair of functions $(f,g) \in \mathcal{S}_U \times \mathcal{S}_V$ such that $f(U) = g(V)$ almost surely [17]. It is well known that if $(X_\mathsf{G}, Y_\mathsf{G})$ is a pair of jointly Gaussian random variables with correlation coefficient ρ, then $\rho_m^2(X_\mathsf{G}, Y_\mathsf{G}) = \rho^2(X_\mathsf{G}, Y_\mathsf{G})$, see [16] or [40] for a more recent proof. Rényi [17] derived an equivalent characterization of maximal correlation as

$$\rho_m^2(U;V) = \sup_{f\in\mathcal{S}_U} \eta_V^2(f(U)). \tag{18}$$

The following theorem, whose proof is given in Appendix J, provides an equivalent characterization of ε-strong estimation privacy $Z_\gamma \in \Gamma(\varepsilon)$.

Theorem 6. *Let U and V be non-degenerate random variables and $\varepsilon \in [0,1]$. Then*

$$\mathsf{mmse}(f(U)|V) \ge (1-\varepsilon)\mathsf{var}(f(U)),$$

for all $f \in \mathcal{S}_U$ if and only if $\rho_m^2(U,V) \le \varepsilon$. In particular, $Z_\gamma \in \Gamma(\varepsilon)$ if and only if $\rho_m^2(X,Z_\gamma) \le \varepsilon$.

[3]This name is taken from [39, Def. 7.4]. Originally, Rényi named this quantity as the "correlation ratio" of U on V [17, eq. (6)].

From this theorem and (17), we can equivalently express $\mathsf{sENSR}(\varepsilon)$ and $\mathsf{wENSR}(\varepsilon)$ as

$$\mathsf{sENSR}(\varepsilon) = 1 - \sup_{\gamma\ge 0:\ \rho_m^2(X,Z_\gamma)\le\varepsilon} \eta_{Z_\gamma}^2(Y),$$
$$\mathsf{wENSR}(\varepsilon) = 1 - \sup_{\gamma\ge 0:\ \eta_{Z_\gamma}^2(X)\le\varepsilon} \eta_{Z_\gamma}^2(Y).$$

It is known that both η and ρ_m satisfy the data processing inequality (see e.g., [14] and [41]) and hence $\eta_{Z_\gamma}(X) \le \eta_Y(X)$ and $\rho_m(X,Z_\gamma) \le \rho_m(X,Y)$. Therefore, we can restrict ε in the definition of $\mathsf{wENSR}(\varepsilon)$ and $\mathsf{sENSR}(\varepsilon)$ to the intervals $[0,\eta_Y^2(X)]$ and $[0,\rho_m^2(X,Y)]$, respectively. Unlike the discrete case, it is clear that perfect privacy $\varepsilon = 0$ implies $\gamma = 0$. Thus perfect privacy yields trivial utility; i.e., $\mathsf{sENSR}(0) = 1$ and $\mathsf{wENSR}(0) = 1$.

Note that $\gamma \mapsto \mathsf{mmse}(Y|Z_\gamma)$ is continuous and decreasing on $(0,\infty)$ [42] and $\gamma \mapsto \rho_m^2(X,Z_\gamma)$ is left-continuous and increasing on $(0,\infty)$ [43, Theorem 2]. Thus we can define $\gamma_\varepsilon^* \coloneqq \max\{\gamma \ge 0 : \rho_m^2(X,Z_\gamma) \le \varepsilon\}$ for which we have $\mathsf{sENSR}(\varepsilon) = \frac{\mathsf{mmse}(Y|Z_{\gamma_\varepsilon^*})}{\mathsf{var}(Y)}$. The left-continuity of $\gamma \mapsto \rho_m^2(X,Z_\gamma)$ implies that $\varepsilon \mapsto \gamma_\varepsilon^*$ is right-continuous, and thus $\varepsilon \mapsto \mathsf{sENSR}(\varepsilon)$ is right-continuous on $(0,\rho_m^2(X,Y))$.

Example 1. Let $(X_\mathsf{G}, Y_\mathsf{G})$ be jointly Gaussian random variables with mean zero and correlation coefficient ρ and let $Z_\gamma = \sqrt{\gamma}Y_\mathsf{G} + N_\mathsf{G}$. Since $\rho_m^2(X_\mathsf{G},Z_\gamma) = \rho^2(X_\mathsf{G},Z_\gamma)$, we have that

$$\rho_m^2(X_\mathsf{G},Z_\gamma) = \rho^2\frac{\gamma\mathsf{var}(Y_\mathsf{G})}{1+\gamma\mathsf{var}(Y_\mathsf{G})},$$

and hence the mapping $\gamma \mapsto \rho_m^2(X_\mathsf{G},Z_\gamma)$ is strictly increasing. As a consequence, for $0 \le \varepsilon \le \rho^2$, the equation $\rho_m^2(X_\mathsf{G},Z_\gamma) = \varepsilon$ has a unique solution

$$\gamma_\varepsilon \coloneqq \frac{\varepsilon}{\mathsf{var}(Y_\mathsf{G})(\rho^2-\varepsilon)},$$

and $\rho_m^2(X_\mathsf{G},Z_\gamma) \le \varepsilon$ if and only if $\gamma \le \gamma_\varepsilon$. On the other hand,

$$\mathsf{mmse}(Y_\mathsf{G}|Z_\gamma) = \frac{\mathsf{var}(Y_\mathsf{G})}{1+\gamma\mathsf{var}(Y_\mathsf{G})},$$

which shows that the map $\gamma \mapsto \mathsf{mmse}(Y_\mathsf{G}|Z_\gamma)$ is strictly decreasing. Therefore,

$$\mathsf{sENSR}(\varepsilon) = \frac{\mathsf{mmse}(Y_\mathsf{G}|Z_{\gamma_\varepsilon})}{\mathsf{var}(Y_\mathsf{G})} = 1 - \frac{\varepsilon}{\rho^2}. \tag{19}$$

Clearly, for jointly Gaussian X_G and Y_G, we have $\eta_{Z_\gamma}^2(X_\mathsf{G}) = \rho_m^2(X_\mathsf{G},Z_\gamma)$ for any $\gamma \ge 0$. Consequently, $\Gamma(\varepsilon) = \partial\Gamma(\varepsilon)$ and, for $0 \le \varepsilon \le \rho^2$,

$$\mathsf{sENSR}(\varepsilon) = \mathsf{wENSR}(\varepsilon) = 1 - \frac{\varepsilon}{\rho^2}. \tag{20}$$

Next, we obtain bounds on $\mathsf{sENSR}(\varepsilon)$ for the special case of Gaussian non-private data Y_G. The proof of the following result is given in Appendix K.

Theorem 7. *Let X be jointly distributed with Gaussian Y_G. Then,*

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

Combined with (20), this theorem shows that for a Gaussian Y, a Gaussian X_{G} minimizes $\mathsf{sENSR}(\varepsilon)$ among all continuous random variables X having identical $\rho(X,Y_{\mathsf{G}})$ and maximizes $\mathsf{sENSR}(\varepsilon)$ among all continuous random variables X having identical $\rho_m(X,Y_{\mathsf{G}})$. These observations establish another extremal property of Gaussian distribution over AWGN channels, see e.g., [44, Theorem 12] for another example. This theorem also implies that

$$\mathsf{sENSR}(P_{X_{\mathsf{G}}Y_{\mathsf{G}}},\varepsilon)-\mathsf{sENSR}(P_{XY_{\mathsf{G}}},\varepsilon) \leq \frac{\varepsilon}{\rho^2(X,Y_{\mathsf{G}})} - \frac{\varepsilon}{\rho_m^2(X,Y_{\mathsf{G}})},$$

for Gaussian X_{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 $\mathsf{sENSR}(P_{XY_{\mathsf{G}}},\varepsilon)$ is very close to $\mathsf{sENSR}(P_{X_{\mathsf{G}}Y_{\mathsf{G}}},\varepsilon)$.

As stated before, for any given joint density P_{XY}, perfect privacy results in trivial utility, i.e., $\mathsf{sENSR}(0)=1$. Therefore, it is interesting to study the approximation of $\mathsf{sENSR}(\varepsilon)$ for sufficiently small ε, i.e., in the almost perfect privacy regime. The next result, whose proof is given in Appendix L, provides such an approximation and also shows that the lower bound in Theorem 7 holds for general Y for ε in the almost perfect privacy regime.

Lemma 2. *We have that*

$$\limsup_{\varepsilon\to 0}\frac{1-\mathsf{sENSR}(\varepsilon)}{\varepsilon}\leq\frac{1}{\rho^2(X,Y)}.$$

V. Conclusion

We studied the problem of displaying Y under a privacy constraint with respect to another correlated random variable X, where utility and privacy are measured in terms of the probability of correctly guessing and minimum mean-squared error in the discrete and continuous cases, respectively.

In the discrete case, we introduced the privacy-constrained guessing function $\hbar$ to quantify the fundamental tradeoff between privacy and utility. We proved that $\hbar$ is piecewise linear for every X and Y. When X and Y are binary, this result allowed us to obtain $\hbar$ in closed form and to establish the optimility of the Z-channel. We then defined $\underline{\hbar}$ analogously to $\hbar$ with the additional assumption that Z is supported over the alphabet of Y, thereby providing a lower bound for $\hbar$. For arbitrary X and Y, we derived $\underline{\hbar}$ in closed form in the high utility regime and established the optimality of a generalized Z-channel in this regime. Finally, we specialized our results about $\underline{\hbar}$ to the vector case, where X^n, Y^n, and Z^n are assumed to be binary random vectors. Overall, these results provide tangible answers for the estimation theoretic privacy-utility tradeoff problem and the performance of Z-channels in the high utility regime.

In the continuous case, we proposed the estimation-noise-to-signal ratio function sENSR to capture the fundamental privacy-utility tradeoff with an intrinsic operational meaning. In the special case of additive Gaussian privacy filters, we showed that if Y is Gaussian, then a Gaussian X minimizes sENSR among all (X,Y) with identical correlation coefficients and maximizes sENSR among all (X,Y) with identical maximal correlations. We also obtained a tight lower bound for sENSR for general absolutely continuous random variables when ε is sufficiently small.

Appendix A
Proof of Theorem 1

Before proving Theorem 1, we need to establish some technical facts.

Consider the map $\mathcal{H}:\mathcal{F}\to[0,1]\times[0,1]$ given by

$$\mathcal{H}(F)=(\mathcal{P}(F),\mathcal{U}(F)),$$

with $\mathcal{P}(F)$ and $\mathcal{U}(F)$ defined in (6). For ease of notation, let $\mathcal{D}=\left\{D\in\mathcal{M}_{N\times(N+1)}:\|D\|=1\right\}$ where $||\cdot||$ denotes the Euclidean norm in $\mathcal{M}_{N\times(N+1)}\equiv\mathbb{R}^{N(N+1)}$. For $G\in\mathcal{F}$, let

$$\mathcal{D}(G)=\left\{D\in\mathcal{D}:G+tD\in\mathcal{F}\text{ for some }t>0\right\}.$$

In graphical terms, $\mathcal{D}$ is the set of all possible directions in $\mathcal{M}_{N\times(N+1)}$ and $\mathcal{D}(G)$ is the set of directions that make $t\mapsto G+tD$ $(t\geq 0)$ stay locally in $\mathcal{F}$.

Lemma 3. *For every $G\in\mathcal{F}$, the set $\mathcal{D}(G)$ is compact.*

Proof. Let $A=\{(y,z):G_{y,z}=0\}$ and $B=\{(y,z):G_{y,z}=1\}$. It is straightforward to verify that

$$\mathcal{D}(G)=\mathcal{A}\cap\mathcal{B}\cap\mathcal{C}\cap\mathcal{D},$$

where

$$\mathcal{A}=\bigcap_{(y,z)\in A}\left\{D\in\mathcal{M}_{N,(N+1)}:D_{y,z}\geq 0\right\},$$

$$\mathcal{B}=\bigcap_{(y,z)\in B}\left\{D\in\mathcal{M}_{N,(N+1)}:D_{y,z}\leq 0\right\},$$

$$\mathcal{C}=\left\{D\in\mathcal{M}_{N,(N+1)}:\sum_{z=1}^{N+1}D_{y,z}=0,\ y=1,\dots,N\right\}.$$

Observe that since sets $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ and $\mathcal{D}$ are closed, so is $\mathcal{D}(G)$. Since $\mathcal{D}$ is bounded, we have that $\mathcal{D}(G)$ is bounded as well. In particular, $\mathcal{D}(G)$ is closed and bounded and thus compact. ∎

Lemma 4. *Let $G\in\mathcal{F}$ be given and define $\tau:\mathcal{D}(G)\to\mathbb{R}$ by*

$$\tau(D):=\sup\{t\geq 0\mid G+tD\in\mathcal{F}\}.$$

The function τ is continuous on $\mathcal{D}(G)$.

Proof. Let $\mathrm{ri}(\mathcal{F})$ and $\mathrm{rb}(\mathcal{F})$ denote the relative interior and relative boundary of $\mathcal{F}$, respectively. In what follows, we assume that $G\in\mathrm{rb}(\mathcal{F})$. The proof for $G\in\mathrm{ri}(\mathcal{F})$ follows the same steps and the details are left to the reader. The proof of the lemma is by contradiction. Assume that there exists a sequence $(D_n)_{n\geq 0}\subset\mathcal{D}(G)$ such that $D_n\to D_0$ but $\tau(D_n)\not\to\tau(D_0)$ as $n\to\infty$. Since $\mathcal{F}$ is bounded, the sequence $(\tau(D_n))_{n\geq 1}$ is necessarily bounded. Therefore, there must exist a subsequence $(D_{n_k})_{k\geq 1}$ such that

$$\lim_{k\to\infty}\tau(D_{n_k})=r\neq\tau(D_0). \tag{21}$$

By the maximality of $\tau(D)$, we have that $G+\tau(D)D\in\mathrm{rb}(\mathcal{F})$ for all $D\in\mathcal{D}(G)$. Notice that $\mathcal{F}$ is a convex polytope defined by the intersection of finitely many hyperplanes. In particular,

$G + \tau(D)D$ belongs to one of the supporting hyperplanes of $\mathcal{F}$. Furthermore, the maximality of $\tau(D)$ can be used once again to show that $G + \tau(D)D$ belongs to a supporting hyperplane of $\mathcal{F}$ that does not contain G. Since there are finitely many supporting hyperplanes of $\mathcal{F}$, there exists a further subsequence $(D_{n'_k})_{k\geq 1}$ and a hyperplane H such that $G+\tau(D_{n'_k})D_{n'_k} \in H$ for all $k \geq 1$ and $G \notin H$. Since H and $\mathcal{F}$ are closed sets, we conclude that

$$\lim_{k\to\infty} G + \tau(D_{n'_k})D_{n'_k} = G + rD_0 \in H \cap \mathcal{F}.$$

By the maximality of $\tau(D_0)$ and (21), we have $\tau(D_0) > r$. Since H is a hyperplane and $G \notin H$, it is easy to verify that

$$\{G + tD_0 : t \in [0, \tau(D_0)]\} \cap H = \{G + rD_0\}. \tag{22}$$

In particular, (22) implies that G and $G + \tau(D_0)D_0$ are on opposite sides of H. Since $G \in \mathcal{F}$ and H is a supporting hyperplane of $\mathcal{F}$, we conclude that $G + \tau(D_0)D_0 \notin \mathcal{F}$. This contradicts the fact that $G + \tau(D)D \in \text{rb}(\mathcal{F}) \subset \mathcal{F}$ for all $D \in \mathcal{D}(G)$. ∎

The following lemma shows the local linear nature of the mapping $\mathcal{H}$. Let $[G_1, G_2] = \{\lambda G_1 + (1-\lambda)G_2 : \lambda \in [0,1]\}$.

Lemma 5. *For every $G \in \mathcal{F}$, there exists $\delta > 0$ such that $F \mapsto \mathcal{H}(F)$ is linear on $[G, G + \delta D]$ for every $D \in \mathcal{D}(G)$.*

Proof. Let $P = [P(x,y)]_{x\in\mathcal{X},y\in\mathcal{Y}}$ be the joint probability matrix of X and Y, and Q the diagonal matrix with $q_1, \ldots, q_N$ as diagonal entries where $q_y = \Pr(Y = y)$ for $y \in \mathcal{Y}$. For $G \in \mathcal{F}$ let $\tau : \mathcal{D}(G) \to \mathbb{R}$ be as defined in Lemma 4. The definition of $\mathcal{D}(G)$ clearly implies that $\tau(D) > 0$ for all $D \in \mathcal{D}(G)$. For $x \in \mathcal{X}$, $z \in \mathcal{Z}$, and $D \in \mathcal{D}(G)$, consider the function $f^{(D)}_{x,z} : \mathbb{R} \to \mathbb{R}$ given by

$$f^{(D)}_{x,z}(t) \coloneqq [PG](x,z) + t[PD](x,z), \tag{23}$$

where PG (resp., PD) is the product of matrices P and G (resp., P and D). Note that $\mathcal{P}(G + tD) = \sum_{z\in\mathcal{Z}} \max_{x\in\mathcal{X}} f^{(D)}_{x,z}(t)$ for all $t \in [0, \tau(D)]$ (see (6)). Let

$$\begin{aligned} a_z &= \max_{x\in\mathcal{X}} [PG](x,z), \\ \mathcal{M}_z &= \{x \in \mathcal{X} : [PG](x,z) = a_z\}, \text{ and} \\ b^{(D)}_z &= \max_{x\in\mathcal{M}_z} [PD](x,z). \end{aligned} \tag{24}$$

Let $t^{(D)}_{x,z} \coloneqq -\dfrac{a_z - [PG](x,z)}{b^{(D)}_z - [PD](x,z)}$ whenever $[PD](x,z) \neq b^{(D)}_z$, and $t^{(D)}_{x,z} = \infty$ otherwise. Notice that $f^{(D)}_{x,z}(t^{(D)}_{x,z}) = a_z + t^{(D)}_{x,z} b^{(D)}_z$. Since $t^{(D)}_{x,z} \neq 0$ for all $x \notin \mathcal{M}_z$,

$$t^{(D)} \coloneqq \min_{z\in\mathcal{Z}} \min_{x\notin\mathcal{M}_z} \min\{|t^{(D)}_{x,z}|, \tau(D)\} > 0.$$

It is easy to see that $a_z + tb^{(D)}_z = \max_{x\in\mathcal{X}} f^{(D)}_{x,z}(t)$ for all $t \in [0, t^{(D)}]$. In particular,

$$\begin{aligned} \mathcal{P}(G + tD) &= \sum_{z=1}^{N+1} \max_{x\in\mathcal{X}} f^{(D)}_{x,z}(t) = \sum_{z=1}^{N+1} a_z + t\sum_{z=1}^{N+1} b^{(D)}_z \\ &= \mathcal{P}(G) + tb^{(D)}, \end{aligned} \tag{25}$$

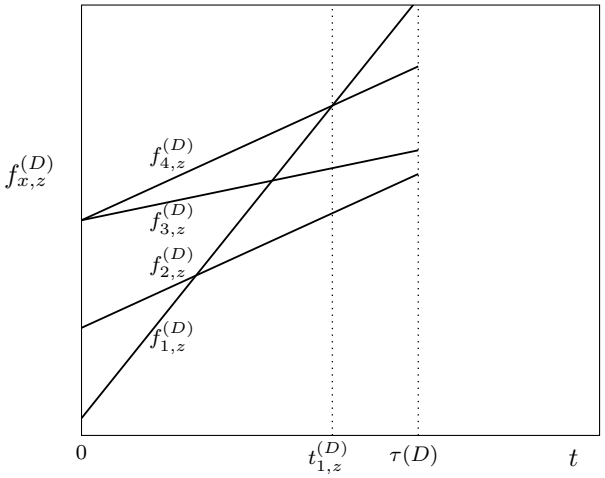


Fig. 6. Typical functions $f^{(D)}_{x,z}$ ($x = \{1,2,3,4\}$) for a given $z \in \mathcal{Z}$ and $D \in \mathcal{D}(G)$. In this example, we have $\mathcal{M}_z = \{3,4\}$ and $a_z + tb^{(D)}_z = f^{(D)}_{4,z}(t)$. Notice that $t^{(D)}_{2,z} = \infty$ and $t^{(D)}_{3,z} = t^{(D)}_{4,z} = 0$.

for every $D \in \mathcal{D}(G)$ and $t \in [0, t^{(D)}]$, where $b^{(D)} \coloneqq \sum_{z=1}^{N+1} b^{(D)}_z$. Consequently, $\mathcal{P}$ is linear on $[G, G + t^{(D)}D]$. By Lemma 4, $\tau : \mathcal{D}(G) \to \mathbb{R}$ is continuous and bounded. Hence, the map $D \mapsto \min\{|t^{(D)}_{x,z}|, \tau(D)\}$ ($x \notin \mathcal{M}_z$) is also continuous. In particular, the map $D \mapsto t^{(D)}$ is continuous. By compactness of $\mathcal{D}(G)$ established in Lemma 3, we conclude that $\delta_{\mathcal{P}} \coloneqq \min_{D\in\mathcal{D}(G)} t^{(D)} > 0$. Thus, $\mathcal{P}$ is linear on $[G, G+\delta_{\mathcal{P}}D]$ for every $D \in \mathcal{D}(G)$.

For $y \in \mathcal{Y}$, $z \in \mathcal{Z}$, and $D \in \mathcal{D}(G)$, consider the function $g^{(D)}_{y,z} : \mathbb{R} \to \mathbb{R}$ given by

$$g^{(D)}_{y,z}(t) = [QG](y,z) + t[QD](y,z).$$

Observe that $\mathcal{U}(G + tD) = \sum_{z\in\mathcal{Z}} \max_{y\in\mathcal{Y}} g^{(D)}_{y,z}(t)$ for all $t \in [0, \tau(D)]$ (see (6)). Similarly to (24), let

$$\begin{aligned} \alpha_z &= \max_{y\in\mathcal{Y}} [QG](y,z), \\ \mathcal{N}_z &= \{y \in \mathcal{Y} : [QG](y,z) = \alpha_z\}, \text{ and} \\ \beta^{(D)}_z &= \max_{y\in\mathcal{N}_z} [QD](y,z). \end{aligned}$$

Using a similar argument that resulted in (25), it can be shown that there exists $\delta_U > 0$ such that

$$\begin{aligned} \mathcal{U}(G + tD) &= \sum_{z=1}^{N+1} g^{(D)}_{y_z,z}(t) = \sum_{z=1}^{N+1} \alpha_z + t\sum_{z=1}^{N+1} \beta^{(D)}_z \\ &= \mathcal{U}(G) + t\beta^{(D)}, \end{aligned} \tag{26}$$

for every $D \in \mathcal{D}(G)$ and $t \in [0, \delta_{\mathcal{U}}]$, where $\beta^{(D)} \coloneqq \sum_{z=1}^{N+1} \beta^{(D)}_z$. Consequently, $\mathcal{U}$ is linear on $[G, G + \delta_{\mathcal{U}}D]$ for every $D \in \mathcal{D}(G)$. Therefore, $F \mapsto \mathcal{H}(F) = (\mathcal{P}(F), \mathcal{U}(F))$ is linear on $[G, G + \delta D]$ for every $D \in \mathcal{D}(G)$, where $\delta = \min(\delta_{\mathcal{P}}, \delta_{\mathcal{U}})$. ∎

We say that a filter $F \in \mathcal{F}$ is optimal if $\mathcal{U}(F) = \hbar(\mathcal{P}(F))$. If F is an optimal filter and $\mathcal{P}(F) = \varepsilon$, we say that F is optimal at ε. The following result is a straightforward application of the concavity of $\hbar$, and thus its proof is omitted.

Lemma 6. *For $G \in \mathcal{F}$, let $\delta > 0$ be as in Lemma 5. If there exist $D \in \mathcal{D}(G)$ and $0 < t_1 < t_2 \leq \delta$ such that G, $G + t_1 D$ and $G + t_2 D$ are optimal filters, then $G + tD$ is an optimal filter for each $t \in [0, \delta]$.*

A function $[\mathsf{P_c}(X), \mathsf{P_c}(X|Y)] \ni \varepsilon \mapsto F_\varepsilon \in \mathcal{F}$ is called a *path* of optimal filters if $\mathcal{P}(F_\varepsilon) = \varepsilon$ and $\mathcal{U}(F_\varepsilon) = \hbar(\varepsilon)$ for every $\varepsilon \in [\mathsf{P_c}(X), \mathsf{P_c}(X|Y)]$. As mentioned in Section II-A, for every ε there exists F_ε such that $\mathcal{P}(F_\varepsilon) = \varepsilon$ and $\mathcal{U}(F_\varepsilon) = \hbar(\varepsilon)$, i.e., a path of optimal filters always exists. In the rest of this section we establish the existence of a *piecewise* linear path of optimal filters.

Lemma 7. *For every $\varepsilon \in [\mathsf{P_c}(X), \mathsf{P_c}(X|Y))$, there exists $F_\varepsilon \in \mathcal{F}$ and $D \in \mathcal{D}(F_\varepsilon)$ such that F_ε is an optimal filter at ε, $\mathcal{P}(F_\varepsilon + \delta D) > \varepsilon$, and $F_\varepsilon + tD$ is an optimal filter for each $t \in [0, \delta]$ with $\delta > 0$ as in Lemma 5 for F_ε.*

Proof. Let $K = 2(\mathsf{P_c}(X|Y) - \varepsilon)^{-1}$. For every $n, m > K$, let $G_{n,m}$ be an optimal filter at $\varepsilon + \frac{1}{n} + \frac{1}{m}$. For every $n > K$, the set $\{G_{n,m} : m > K\}$ is an infinite set. Since $\mathcal{F}$ is compact, $\{G_{n,m} : m > K\}$ has at least one accumulation point, say G_n. Let $(G_{n,m_k})_{k \geq 1} \subset \{G_{n,m} : m > K\}$ be a subsequence with $\lim_k G_{n,m_k} = G_n$. By continuity of $\mathcal{P}$, $\mathcal{U}$, and $\hbar$, we have that

$$\mathcal{P}(G_n) = \lim_{k\to\infty} \mathcal{P}(G_{n,m_k}) = \varepsilon + \frac{1}{n},$$
$$\mathcal{U}(G_n) = \lim_{k\to\infty} \mathcal{U}(G_{n,m_k}) = \lim_{k\to\infty} \hbar(\mathcal{P}(G_{n,m_k})) = \hbar(\mathcal{P}(G_n)),$$

i.e., G_n is an optimal filter at $\varepsilon + \frac{1}{n}$. By the same arguments as before, the set $\{G_n : n > K\}$ has at least one accumulation point, say F_ε, and this accumulation point is an optimal filter at ε. Let $\delta > 0$ be as in Lemma 5 for F_ε. By construction of F_ε, there exists $n_1 > K$ such that $\|G_{n_1} - F_\varepsilon\| < \frac{\delta}{2}$. The filter G_{n_1} can be written as $G_{n_1} = F_\varepsilon + t_1 D_1$ with $t_1 \in (0, \frac{\delta}{2})$ and $D_1 \in \mathcal{D}(F_\varepsilon)$. Recall that, by (25) and (26), for every $D \in \mathcal{D}(F_\varepsilon)$ and $t \in [0, \delta]$,

$$\mathcal{P}(F_\varepsilon + tD) = \varepsilon + tb^{(D)} \quad \text{and} \quad \mathcal{U}(F_\varepsilon + tD) = \hbar(\varepsilon) + t\beta^{(D)}.$$

Notice that the maps $D \mapsto b^{(D)}$ and $D \mapsto \beta^{(D)}$ are continuous. Since $\mathcal{P}(G_{n_1}) = \varepsilon + \frac{1}{n_1} > \varepsilon$, we conclude that $b^{(D_1)} > 0$ and, in particular, $\mathcal{P}(F_\varepsilon + \delta D_1) > \varepsilon$.

Let $(G_{n_1,m_k})_{k \geq 1} \subset \{G_{n_1,m} : m > K\}$ be such that $\lim_k G_{n_1,m_k} = G_{n_1}$. For k large enough, we can write $G_{n_1,m_k} = F_\varepsilon + \theta_k E_k$ with $\theta_k \in [0, \delta]$ and $E_k \in \mathcal{D}(F_\varepsilon)$. Since $\theta_k \to t_1$ and $E_k \to D_1$ as $k \to \infty$, there exists $n_2 > K$ such that $\theta_{n_2} < \frac{\delta}{2}$ and $|b^{(E_{n_2})} - b^{(D_1)}| < \frac{b^{(D_1)}}{2}$. Let $t_2 \coloneqq \theta_{n_2}$ and $D_2 \coloneqq E_{n_2}$. Clearly, $t_2 < \frac{\delta}{2}$ and $\frac{1}{2} b^{(D_1)} < b^{(D_2)} < 2b^{(D_1)}$. These inequalities yield $\mathcal{P}(F_\varepsilon + \delta D_1) > \mathcal{P}(F_\varepsilon + t_2 D_2)$ and $\mathcal{P}(F_\varepsilon + \delta D_2) > \mathcal{P}(F_\varepsilon + t_1 D_1)$. Thus, there exist $s_1, s_2 \in [0, \delta]$ such that $\mathcal{P}(F_\varepsilon + t_2 D_2) = \mathcal{P}(F_\varepsilon + s_1 D_1)$ and $\mathcal{P}(F_\varepsilon + t_1 D_1) = \mathcal{P}(F_\varepsilon + s_2 D_2)$. In particular,

$$\varepsilon + t_2 b^{(D_2)} = \varepsilon + s_1 b^{(D_1)} \quad \text{and} \quad \varepsilon + t_1 b^{(D_1)} = \varepsilon + s_2 b^{(D_2)}. \tag{27}$$

By the optimality of $G_{n_1} = F_\varepsilon + t_1 D_1$ and $G_{n_1,m_{n_2}} = F_\varepsilon + t_2 D_2$,

$$\begin{aligned} \mathcal{U}(F_\varepsilon + t_2 D_2) &= \hbar(\varepsilon) + t_2 \beta^{(D_2)} \\ &\geq \hbar(\varepsilon) + s_1 \beta^{(D_1)} = \mathcal{U}(F_\varepsilon + s_1 D_1), \end{aligned}$$

and

$$\begin{aligned} \mathcal{U}(F_\varepsilon + t_1 D_1) &= \hbar(\varepsilon) + t_1 \beta^{(D_1)} \\ &\geq \hbar(\varepsilon) + s_2 \beta^{(D_2)} = \mathcal{U}(F_\varepsilon + s_2 D_2). \end{aligned}$$

By the equations in (27), the above inequalities are in fact equalities. In particular, F_ε, $F_\varepsilon + t_1 D_1$ and $F_\varepsilon + s_1 D_1$ are optimal filters. Invoking Lemma 6, we conclude that $F_\varepsilon + tD_1$ is an optimal filter for all $t \in [0, \delta]$. ∎

Using an analogous proof, we can also prove the following lemma.

Lemma 8. *For every $\varepsilon \in (\mathsf{P_c}(X), \mathsf{P_c}(X|Y)]$, there exists $F_\varepsilon \in \mathcal{F}$ and $D \in \mathcal{D}(F_\varepsilon)$ such that F_ε is an optimal filter at ε, $\mathcal{P}(F_\varepsilon + \delta D) < \varepsilon$, and $F_\varepsilon + tD$ is an optimal filter for each $t \in [0, \delta]$ with $\delta > 0$ as in Lemma 5 for F_ε.*

We are in position to prove Theorem 1.

Proof of Theorem 1. For notational simplicity, we define $S \coloneqq \mathsf{P_c}(X)$ and $T \coloneqq \mathsf{P_c}(X|Y)$. In light of Lemmas 7 and 8, for every $\varepsilon \in (S, T)$ there exist optimal filters F_ε and G_ε at ε, $\delta_\varepsilon > 0$, $D_\varepsilon \in \mathcal{D}(F_\varepsilon)$, and $E_\varepsilon \in \mathcal{D}(G_\varepsilon)$ such that $F_\varepsilon + tD_\varepsilon$ and $G_\varepsilon + tE_\varepsilon$ are optimal filters for each $t \in [0, \delta_\varepsilon]$, and $\mathcal{P}(G_\varepsilon + \delta_\varepsilon E_\varepsilon) < \varepsilon < \mathcal{P}(F_\varepsilon + \delta_\varepsilon D_\varepsilon)$. Note that $\delta_\varepsilon = \min\{\delta_{F_\varepsilon}, \delta_{G_\varepsilon}\}$, where δ_{F_ε} and δ_{G_ε} are the constants obtained in Lemma 5 for filters F_ε and G_ε, respectively. For every $\varepsilon \in (S, T)$, let $V_\varepsilon = (\mathcal{P}(F_\varepsilon + \delta_\varepsilon E_\varepsilon), \mathcal{P}(G_\varepsilon + \delta_\varepsilon D_\varepsilon))$. Similarly, there exist

a) an optimal filter F_S at S, $\delta_S > 0$, and $D_S \in \mathcal{D}(F_S)$ such that $F_S + tD_S$ is an optimal filter for each $t \in [0, \delta_S]$ and $\mathcal{P}(F_S + \delta_S D_S) > S$;
b) an optimal filter G_T at T, $\delta_T > 0$, and $E_T \in \mathcal{D}(G_T)$ such that $G_T + tE_T$ is an optimal filter for each $t \in [0, \delta_T]$ and $\mathcal{P}(G_T + \delta_T E_T) < T$.

Let $V_S = [S, \mathcal{P}(F_S + \delta_S D_S))$ and $V_T = (\mathcal{P}(G_T + \delta_T E_T), T]$. The family $\{V_\varepsilon : \varepsilon \in [S, T]\}$ forms an open cover of $[S, T]$ (in the subspace topology). By compactness, there exist $S = \varepsilon_0 < \cdots < \varepsilon_l = T$ such that $\{V_{\varepsilon_0}, \ldots, V_{\varepsilon_l}\}$ forms an open cover for $[S, T]$. For each $i \in \{0, \ldots, l-1\}$, the mapping

$$[\varepsilon_i, \mathcal{P}(F_{\varepsilon_i} + \delta_{\varepsilon_i} D_{\varepsilon_i})) \ni \varepsilon \mapsto F_{\varepsilon_i} + \frac{\varepsilon - \varepsilon_i}{b^{(D_{\varepsilon_i})}} D_{\varepsilon_i} \in \mathcal{F}, \tag{28}$$

is clearly linear. Similarly, for each $i \in \{1, \ldots, l\}$, the mapping

$$(\mathcal{P}(G_{\varepsilon_i} + \delta_{\varepsilon_i} E_{\varepsilon_i}), \varepsilon_i] \ni \varepsilon \mapsto G_{\varepsilon_i} + \frac{\varepsilon - \varepsilon_i}{b^{(E_{\varepsilon_i})}} E_{\varepsilon_i} \in \mathcal{F}, \tag{29}$$

is also linear. Notice that $\mathcal{P}\left(F_{\varepsilon_i} + \frac{\varepsilon - \varepsilon_i}{b^{(D_{\varepsilon_i})}} D_{\varepsilon_i}\right) = \varepsilon = \mathcal{P}\left(G_{\varepsilon_i} + \frac{\varepsilon - \varepsilon_i}{b^{(E_{\varepsilon_i})}} E_{\varepsilon_i}\right)$. Since $\{V_{\varepsilon_0}, \ldots, V_{\varepsilon_l}\}$ forms an open cover for $[S, T]$, the mappings in (28) and (29) implement a piecewise linear path of optimal filters. ∎

The proof provided in this appendix establishes the existence of $\delta_* > 0$, an optimal filter F_* at $T \coloneqq \mathsf{P_c}(X|Y)$, and $D_* \in \mathcal{D}(F_*)$ such that $\mathcal{P}(F_* + \delta_* D_*) < T$ (or equivalently $b^{(D_*)} < 0$) and

$$\hbar(\varepsilon) = 1 + (\varepsilon - T)\frac{\beta^{(D_*)}}{b^{(D_*)}},$$

for every $\varepsilon \in [T+\delta_* b^{(D_*)}, T]$. This then implies that

$$\hbar'(T) = \min_{\substack{F\in\mathcal{F}\\ \mathcal{P}(F)=T}} \min_{\substack{D\in\mathcal{D}(F)\\ b^{(D)}<0}} \frac{\beta^{(D)}}{b^{(D)}}. \tag{30}$$

Appendix B
Proof of Proposition 1

Since X is uniformly distributed in $\{1,\dots,M\}$,

$$-\log \mathsf{P_c}(X) = \log M = H(X).$$

By the definition of $I_\infty(X;Z)$, we have that

$$\begin{aligned} I_\infty(X;Z) &= \log\left(\frac{\mathsf{P_c}(X|Z)}{\mathsf{P_c}(X)}\right) \\ &= H(X) + \log\left(\sum_{z\in\mathcal{Z}} P_Z(z) \max_{x\in\mathcal{X}} P_{X|Z}(x|z)\right) \\ &\geq H(X) + \sum_{z\in\mathcal{Z}} P_Z(z) \max_{x\in\mathcal{X}} \log P_{X|Z}(x|z), \end{aligned}$$

where the inequality follows from Jensen's inequality. Clearly, for each $z\in\mathcal{Z}$,

$$\begin{aligned} \max_{x\in\mathcal{X}} \log P_{X|Z}(x|z) &\geq \sum_{x\in\mathcal{X}} P_{X|Z}(x|z)\log P_{X|Z}(x|z) \\ &= -H(X|Z=z). \end{aligned}$$

Therefore,

$$I_\infty(X;Z) \geq H(X) - \sum_{z\in\mathcal{Z}} P_Z(z) H(X|Z=z) = I(X;Z).$$

Since $I_\infty(X;Z)=0$, we conclude that $I(X;Z)=0$ and thus $X \perp\!\!\!\perp Z$.

Appendix C
Proof of Theorem 2

We first note that since $\hbar$ is concave on $[\mathsf{P_c}(X), \mathsf{P_c}(X|Y)]$, its right derivative exists at $\varepsilon = \mathsf{P_c}(X|Y)$. Therefore, we have by concavity

$$\hbar(\varepsilon) \leq 1 - (\mathsf{P_c}(X|Y) - \varepsilon)\hbar'(\mathsf{P_c}(X|Y)), \tag{31}$$

for all $\varepsilon \in [p, \mathsf{P_c}(X|Y)]$. In Lemma 9 below, we show that

$$\begin{aligned} \hbar'(\mathsf{P_c}(X|Y)) &= \frac{q}{\bar\beta p - \alpha\bar p} 1_{\{\alpha\bar\alpha\bar p^2 < \beta\bar\beta p^2\}} \\ &\quad + \frac{\bar q}{\bar\alpha\bar p - \beta p} 1_{\{\alpha\bar\alpha\bar p^2 \geq \beta\bar\beta p^2\}}. \end{aligned}$$

Thus, (31) becomes

$$\hbar(\varepsilon) \leq \begin{cases} 1-\zeta(\varepsilon)q, & \alpha\bar\alpha\bar p^2 < \beta\bar\beta p^2, \\ 1-\tilde\zeta(\varepsilon)\bar q, & \alpha\bar\alpha\bar p^2 \geq \beta\bar\beta p^2. \end{cases} \tag{32}$$

To finish the proof of Theorem 2 we show that the Z-channel $\mathsf{Z}(\zeta(\varepsilon))$ and the reverse Z-channel $\tilde{\mathsf{Z}}(\tilde\zeta(\varepsilon))$ achieve (31) and (32), when $\alpha\bar\alpha\bar p^2 < \beta\bar\beta p^2$ and $\alpha\bar\alpha\bar p^2 \geq \beta\bar\beta p^2$, respectively.

For $\alpha\bar\alpha\bar p^2 < \beta\bar\beta p^2$, consider the filter $P_{Z|Y} = \begin{bmatrix} 1 & 0 \\ \zeta(\varepsilon) & 1-\zeta(\varepsilon)\end{bmatrix}$. Notice that

$$\begin{aligned} P_{XZ} &= \begin{bmatrix} \bar p(\bar\alpha + \alpha\zeta(\varepsilon)) & \bar p\alpha(1-\zeta(\varepsilon)) \\ p(\beta + \bar\beta\zeta(\varepsilon)) & p\bar\beta(1-\zeta(\varepsilon))\end{bmatrix}, \text{ and} \\ P_{YZ} &= \begin{bmatrix} \bar q & 0 \\ q\zeta(\varepsilon) & q(1-\zeta(\varepsilon))\end{bmatrix}. \end{aligned} \tag{33}$$

It is straightforward to verify that $\bar p(\bar\alpha + \alpha\zeta(\varepsilon)) \geq p(\beta + \bar\beta\zeta(\varepsilon))$. As a consequence, $\mathsf{P_c}(X|Z) = \varepsilon$. Since $\alpha\bar\alpha\bar p^2 < \beta\bar\beta p^2$, we have that $\frac{q}{\bar q} > \zeta(\varepsilon)$. Thus, $\mathsf{P_c}(Y|Z) = 1-\zeta(\varepsilon)q$.

For $\alpha\bar\alpha\bar p^2 \geq \beta\bar\beta p^2$, consider the filter $P_{Z|Y} = \begin{bmatrix} 1-\tilde\zeta(\varepsilon) & \tilde\zeta(\varepsilon) \\ 0 & 1\end{bmatrix}$. Notice that

$$\begin{aligned} P_{XZ} &= \begin{bmatrix} \bar p\bar\alpha(1-\tilde\zeta(\varepsilon)) & \bar p(\alpha + \bar\alpha\tilde\zeta(\varepsilon)) \\ p\beta(1-\tilde\zeta(\varepsilon)) & p(\bar\beta + \beta\tilde\zeta(\varepsilon))\end{bmatrix}, \text{ and} \\ P_{YZ} &= \begin{bmatrix} \bar q(1-\tilde\zeta(\varepsilon)) & \bar q\tilde\zeta(\varepsilon) \\ 0 & q\end{bmatrix}. \end{aligned} \tag{34}$$

Recall that $\bar\alpha\bar p > \beta p$ and also observe that $p(\bar\beta + \beta\tilde\zeta(\varepsilon)) \geq \bar p(\alpha + \bar\alpha\tilde\zeta(\varepsilon))$. As a consequence, $\mathsf{P_c}(X|Z) = \varepsilon$. The fact that $\alpha\bar\alpha\bar p^2 \geq \beta\bar\beta p^2$ implies $q \geq \bar q\tilde\zeta(\varepsilon)$. Therefore, $\mathsf{P_c}(Y|Z) = 1-\tilde\zeta(\varepsilon)\bar q$.

Lemma 9. *Let $X \sim \mathsf{Bernoulli}(p)$ with $p \in [\frac12, 1)$ and $P_{Y|X} \sim \mathsf{BIBO}(\alpha,\beta)$ with $\alpha,\beta \in [0,\frac12)$ such that $\bar\alpha\bar p > \beta p$. Then $\hbar'(\mathsf{P_c}(X|Y)) = \frac{q}{\bar\beta p - \alpha\bar p} 1_{\{\alpha\bar\alpha\bar p^2 < \beta\bar\beta p^2\}} + \frac{\bar q}{\bar\alpha\bar p - \beta p} 1_{\{\alpha\bar\alpha\bar p^2 \geq \beta\bar\beta p^2\}}$.*

Proof. As before, let $T \coloneqq \mathsf{P_c}(X|Y)$. We begin the proof by noticing that the Z-channels defined in (33) and (34) provide a lower bound on $\hbar(\varepsilon)$ as follows:

$$\hbar(\varepsilon) \geq 1 - \zeta(\varepsilon)q 1_{\{\alpha\bar\alpha\bar p^2 < \beta\bar\beta p^2\}} - \tilde\zeta(\varepsilon)\bar q 1_{\{\alpha\bar\alpha\bar p^2 \geq \beta\bar\beta p^2\}}. \tag{35}$$

By concavity of $\hbar$, this inequality implies

$$\hbar'(T) \leq \frac{q}{\bar\beta p - \alpha\bar p} 1_{\alpha\bar\alpha\bar p^2 < \beta\bar\beta p^2} + \frac{\bar q}{\bar\alpha\bar p - \beta p} 1_{\alpha\bar\alpha\bar p^2 \geq \beta\bar\beta p^2}.$$

The rest of the proof is devoted to establishing the reverse inequality. To this end, we use the variational formula for $\hbar'(T)$ given in (30). Let $P = [P(x,y)]_{x,y\in\{0,1\}}$ be the joint probability matrix of X and Y. Without loss of generality we can assume $\mathcal{Z} = \{z_1,z_2,z_3\}$. It follows from (25) and (26) that for every $F \in \mathcal{F} \subset \mathcal{M}_{2\times 3}$ there exists $\delta > 0$ such that

$$\mathcal{P}(F+tD) = \mathcal{P}(F) + tb^{(D)}, \text{ and } \mathcal{U}(F+tD) = \mathcal{U}(F) + t\beta^{(D)}, \tag{36}$$

for every $t \in [0,\delta]$ and $D \in \mathcal{D}(F)$, where $b^{(D)} = \sum_{i=1}^{3} \max_{x\in\mathcal{M}_{z_i}} [PD](x,z_i)$ and $\beta^{(D)} = \sum_{i=1}^{3} \max_{y\in\mathcal{N}_{z_i}} q(y)D(y,z_i)$ with

$$\mathcal{M}_{z_i} = \Big\{x\in\{0,1\} : (PF)(x,z_i) = \max_{x'\in\{0,1\}} (PF)(x',z_i)\Big\},$$
$$\mathcal{N}_{z_i} = \Big\{y\in\{0,1\} : q(y)F(y,z_i) = \max_{y'\in\{0,1\}} q(y')F(y',z_i)\Big\}.$$

Up to permutation of columns, which corresponds to permuting the elements of $\mathcal{Z}$, the set of filters $F \in \mathcal{F}$ such that $\mathcal{P}(F) = T$ equals

$$\left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & u & v \end{bmatrix} : \begin{array}{c} 0 < v \leq u \\ u+v=1 \end{array} \right\} \bigcup \left\{ \begin{bmatrix} 0 & u & v \\ 1 & 0 & 0 \end{bmatrix} : \begin{array}{c} 0 < v \leq u \\ u+v=1 \end{array} \right\} \bigcup \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \right\}. \tag{37}$$

To compute $\hbar'(T)$ using formula (30) we need to compute $\beta^{(D)}$ and $b^{(D)}$ for each $D \in \mathcal{D}(F)$ with F of the form described in (37).

Let $F = \begin{bmatrix} 1 & 0 & 0 \\ 0 & u & v \end{bmatrix}$ for some $0 < v \leq u$ and $u + v = 1$. A direct computation shows that

$$PF = \begin{bmatrix} \bar{\alpha}\bar{p} & u\alpha\bar{p} & v\alpha\bar{p} \\ \beta p & u\bar{\beta}p & v\bar{\beta}p \end{bmatrix}. \tag{38}$$

In particular, $\mathcal{M}_{z_1} = \{0\}$, $\mathcal{M}_{z_2} = \{1\}$, and $\mathcal{M}_{z_3} = \{1\}$. For every $D \in \mathcal{D}(F)$, the matrix PD is equal to

$$\begin{bmatrix} \bar{\alpha}\bar{p}D_{11} + \alpha\bar{p}D_{21} & \bar{\alpha}\bar{p}D_{12} + \alpha\bar{p}D_{22} & \bar{\alpha}\bar{p}D_{13} + \alpha\bar{p}D_{23} \\ \beta p D_{11} + \bar{\beta}pD_{21} & \beta p D_{12} + \bar{\beta}pD_{22} & \beta p D_{13} + \bar{\beta}pD_{23} \end{bmatrix},$$

and hence $b^{(D)} = \bar{\alpha}\bar{p}D_{11} + \alpha\bar{p}D_{21} + \beta p D_{12} + \bar{\beta}pD_{22} + \beta p D_{13} + \bar{\beta}pD_{23}$. Notice that, for $1 \leq i \leq 3$, we have that $D_{i1} + D_{i2} + D_{i3} = 0$. In particular, $b^{(D)} = (\bar{\alpha}\bar{p} - \beta p)D_{11} + (\alpha\bar{p} - \bar{\beta}p)D_{21}$. Consider the matrices,

$$\begin{bmatrix} \bar{q} & 0 \\ 0 & q \end{bmatrix} F = \begin{bmatrix} \bar{q} & 0 & 0 \\ 0 & qu & qv \end{bmatrix},$$

and

$$\begin{bmatrix} \bar{q} & 0 \\ 0 & q \end{bmatrix} D = \begin{bmatrix} \bar{q}D_{11} & \bar{q}D_{12} & \bar{q}D_{13} \\ qD_{21} & qD_{22} & qD_{33} \end{bmatrix},$$

from which we obtain $\mathcal{N}_{z_1} = \{0\}$, $\mathcal{N}_{z_2} = \{1\}$, $\mathcal{N}_{z_3} = \{1\}$, and therefore, $\beta^{(D)} = \bar{q}D_{11} + qD_{22} + qD_{23} = \bar{q}D_{11} - qD_{21}$. In what follows we use the simple fact that $\frac{ax+y}{bx+y} \geq \min\left\{\frac{a}{b}, 1\right\}$ for $a, b > 0$ and $x, y \geq 0$ with $x + y > 0$. For notational simplicity, let $\eta := \frac{\bar{q}}{q}$ and $\zeta := \zeta(p)$, where $\zeta(\cdot)$ is defined in (8).

From the form of F, it is clear that $-D_{11} \geq 0$ and $D_{21} \geq 0$. If $b^{(D)} < 0$, then D_{11} and D_{21} cannot be simultaneously zero, and hence

$$\begin{aligned} \frac{\beta^{(D)}}{b^{(D)}} &= \frac{q}{\bar{\beta}p - \alpha\bar{p}} \frac{-\eta D_{11} + D_{21}}{-\zeta D_{11} + D_{21}} \\ &\geq \frac{q}{\bar{\beta}p - \alpha\bar{p}} \min\left\{\frac{\eta}{\zeta}, 1\right\} \\ &= \begin{cases} \frac{q}{\bar{\beta}p - \alpha\bar{p}}, & \alpha\bar{\alpha}\bar{p}^2 < \beta\bar{\beta}p^2, \\ \frac{\bar{q}}{\bar{\alpha}\bar{p} - \beta p}, & \alpha\bar{\alpha}\bar{p}^2 \geq \beta\bar{\beta}p^2. \end{cases} \end{aligned}$$

In particular, we obtain that

$$\min_{\substack{D \in \mathcal{D}(F) \\ b^{(D)} < 0}} \frac{\beta^{(D)}}{b^{(D)}} \geq \begin{cases} \frac{q}{\bar{\beta}p - \alpha\bar{p}}, & \alpha\bar{\alpha}\bar{p}^2 < \beta\bar{\beta}p^2, \\ \frac{\bar{q}}{\bar{\alpha}\bar{p} - \beta p}, & \alpha\bar{\alpha}\bar{p}^2 \geq \beta\bar{\beta}p^2. \end{cases} \tag{39}$$

The case $F = \begin{bmatrix} 0 & u & v \\ 1 & 0 & 0 \end{bmatrix}$ for $0 < v \leq u$ and $u + v = 1$ is analogous.

Now, let $F = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$. By (38) with $u = 1$ and $v = 0$, we obtain that $\mathcal{M}_{z_1} = \{0\}$, $\mathcal{M}_{z_2} = \{1\}$, and $\mathcal{M}_{z_3} = \{0, 1\}$. In a similar way, $\mathcal{N}_{z_1} = \{0\}$, $\mathcal{N}_{z_2} = \{1\}$, and $\mathcal{N}_{z_3} = \{0, 1\}$. Hence

$$\begin{aligned} b^{(D)} &= \bar{\alpha}\bar{p}D_{11} + \alpha\bar{p}D_{21} + \beta p D_{12} + \bar{\beta}pD_{22} \\ &\quad + \max\{\bar{\alpha}\bar{p}D_{13} + \alpha\bar{p}D_{23}, \beta p D_{13} + \bar{\beta}pD_{23}\}, \\ \beta^{(D)} &= \bar{q}D_{11} + qD_{22} + \max\{\bar{q}D_{13}, qD_{23}\}. \end{aligned}$$

We therefore need to consider the following cases:

Case I: $\bar{\alpha}\bar{p}D_{13} + \alpha\bar{p}D_{23} \leq \beta p D_{13} + \bar{\beta}pD_{23}$ and $\bar{q}D_{13} \leq qD_{23}$. The computation in this case reduces to the computation for $F = \begin{bmatrix} 1 & 0 & 0 \\ 0 & u & v \end{bmatrix}$.

Case II: $\bar{\alpha}\bar{p}D_{13} + \alpha\bar{p}D_{23} \leq \beta p D_{13} + \bar{\beta}pD_{23}$ and $\bar{q}D_{13} > qD_{23}$. Notice that these conditions imply that $\zeta D_{13} \leq D_{23} < \eta D_{13}$, and therefore this case requires $\zeta < \eta$ (or equivalently, $\alpha\bar{\alpha}\bar{p}^2 < \beta\bar{\beta}p^2$). This yields

$$b^{(D)} = (\bar{\alpha}\bar{p} - \beta p)D_{11} + (\alpha\bar{p} - \bar{\beta}p)D_{21},$$

and

$$\beta^{(D)} = qD_{22} - \bar{q}D_{12}.$$

Hence, we have

$$\frac{\beta^{(D)}}{b^{(D)}} = \frac{q}{\bar{\beta}p - \alpha\bar{p}} \frac{D_{22} - \eta D_{12}}{\zeta D_{11} - D_{21}}.$$

By the form of F, we have that $-D_{11}, D_{12}, D_{21} \geq 0$. The inequalities $\zeta < \eta$ and $\zeta D_{13} \leq D_{23}$ imply that $\frac{D_{22} - \eta D_{12}}{\zeta D_{11} - D_{21}} \geq 1$, and hence

$$\frac{\beta^{(D)}}{b^{(D)}} \geq \frac{q}{\bar{\beta}p - \alpha\bar{p}} 1_{\{\alpha\bar{\alpha}\bar{p}^2 < \beta\bar{\beta}p^2\}}. \tag{40}$$

Case III: $\bar{\alpha}\bar{p}D_{13} + \alpha\bar{p}D_{23} > \beta p D_{13} + \bar{\beta}pD_{23}$ and $\bar{q}D_{13} \leq qD_{23}$. Notice that these conditions imply that $\eta D_{13} \leq D_{23} < \zeta D_{13}$, and hence this case requires $\zeta > \eta$ (or equivalently, $\alpha\bar{\alpha}\bar{p}^2 > \beta\bar{\beta}p^2$). In this case, we have

$$b^{(D)} = (\beta p - \bar{\alpha}\bar{p})D_{12} + (\bar{\beta}p - \alpha\bar{p})D_{22},$$

and

$$\beta^{(D)} = \bar{q}D_{11} - qD_{21}.$$

Therefore,

$$\frac{\beta^{(D)}}{b^{(D)}} = \frac{\bar{q}}{\bar{\alpha}\bar{p} - \beta p} \frac{D_{11} - \eta^{-1}D_{21}}{-D_{12} + \zeta^{-1}D_{22}}.$$

By the form of F, we have that $-D_{22}, D_{12}, D_{21} \geq 0$. The inequalities $\zeta^{-1} < \eta^{-1}$ and $\zeta D_{13} > D_{23}$ imply that $\frac{D_{11} - \eta^{-1}D_{21}}{-D_{12} + \zeta^{-1}D_{22}} > 1$, and hence

$$\frac{\beta^{(D)}}{b^{(D)}} > \frac{\bar{q}}{\bar{\alpha}\bar{p} - \beta p} 1_{\{\alpha\bar{\alpha}\bar{p}^2 > \beta\bar{\beta}p^2\}}. \tag{41}$$

Case IV: $\bar{\alpha}\bar{p}D_{13} + \alpha\bar{p}D_{23} > \beta p D_{13} + \bar{\beta}pD_{23}$ and $\bar{q}D_{13} > qD_{23}$. Notice that these two inequalities imply that $D_{23} < \min\{\zeta, \eta\}D_{13}$. For this case we have that

$$b^{(D)} = (\beta p - \bar{\alpha}\bar{p})D_{12} + (\bar{\beta}p - \alpha\bar{p})D_{22},$$

and

$$\beta^{(D)} = qD_{22} - \bar{q}D_{12}.$$

Hence, we have

$$\frac{\beta^{(D)}}{b^{(D)}} = \frac{q}{\bar{\beta}p - \alpha\bar{p}} \frac{\eta D_{12} - D_{22}}{\zeta D_{12} - D_{22}}.$$

By the form of F, we have that $-D_{22}, D_{12} \geq 0$. As before, we conclude that

$$\begin{aligned} \frac{\beta^{(D)}}{b^{(D)}} &\geq \frac{q}{\bar{\beta}p - \alpha\bar{p}} \min\left\{\frac{\eta}{\zeta}, 1\right\} \\ &= \begin{cases} \frac{q}{\bar{\beta}p - \alpha\bar{p}}, & \alpha\bar{\alpha}\bar{p}^2 < \beta\bar{\beta}p^2, \\ \frac{\bar{q}}{\bar{\alpha}\bar{p} - \beta p}, & \alpha\bar{\alpha}\bar{p}^2 \geq \beta\bar{\beta}p^2. \end{cases} \end{aligned} \tag{42}$$

Combining (39), (40), (41), and (42), we obtain

$$\min_{\substack{F\in\underline{\mathcal{F}} \\ \mathcal{P}(F)=T}} \min_{\substack{D\in\underline{\mathcal{D}}(F) \\ b^{(D)}<0}} \frac{\beta^{(D)}}{b^{(D)}} \geq \begin{cases} \frac{q}{\bar{\beta}p - \alpha\bar{p}}, & \alpha\bar{\alpha}\bar{p}^2 < \beta\bar{\beta}p^2, \\ \frac{\bar{q}}{\bar{\alpha}\bar{p} - \beta p}, & \alpha\bar{\alpha}\bar{p}^2 \geq \beta\bar{\beta}p^2, \end{cases}$$

as desired. ∎

Appendix D
Proof of Theorem 3

Recall that $\mathcal{X} = \{1, \ldots, M\}$ and $\mathcal{Y} = \mathcal{Z} = \{1, \ldots, N\}$, $P = [P(x,y)]_{(x,y)\in\mathcal{X}\times\mathcal{Y}}$ is the joint probability matrix of X and Y, and the marginals are $p_X(x) = \Pr(X = x)$ and $q_Y(y) = \Pr(Y = y)$ for every $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. Similar to $\hbar$, the function $\underline{\hbar}$ admits the alternative formulation

$$\underline{\hbar}(\varepsilon) = \sup_{F\in\underline{\mathcal{F}}:\ \underline{\mathcal{P}}(F)\leq\varepsilon} \underline{\mathcal{U}}(F),$$

where $\underline{\mathcal{F}}$ is the set of all stochastic matrices $F \in \mathcal{M}_{N\times N}$,

$$\underline{\mathcal{P}}(F) = \sum_{z\in\mathcal{Z}} \max_{x\in\mathcal{X}} (PF)(x,z),$$

and

$$\underline{\mathcal{U}}(F) = \sum_{z\in\mathcal{Z}} \max_{y\in\mathcal{Y}} q_Y(y)F(y,z).$$

We let $\underline{\mathcal{D}} = \{D \in \mathcal{M}_{N\times N} : \|D\| = 1\}$ and, for each $F \in \underline{\mathcal{F}}$, we define

$$\underline{\mathcal{D}}(F) \coloneqq \{D \in \underline{\mathcal{D}} : F + tD \in \underline{\mathcal{F}} \text{ for some } t > 0\}.$$

Before proving Theorem 3, we need to establish some technical lemmas. Notice that the proofs of Lemmas 3 and 5 do not depend on the alphabets $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$. Therefore, $\underline{\mathcal{D}}(F)$ is compact for any $F \in \underline{\mathcal{F}}$ and also we obtain the following lemma.

Lemma 10. *Let $\underline{\mathcal{H}} : \underline{\mathcal{F}} \to [0,1] \times [0,1]$ be the mapping given by $\underline{\mathcal{H}}(F) = (\underline{\mathcal{P}}(F), \underline{\mathcal{U}}(F))$. For every $F \in \underline{\mathcal{F}}$, there exists $\delta > 0$ such that $\underline{\mathcal{H}}$ is linear on $[F, F + \delta D]$ for every $D \in \underline{\mathcal{D}}(F)$.*

The convex analysis tools used to study $\hbar$ heavily rely on the fact that $|\mathcal{Z}| = |\mathcal{Y}| + 1$. Hence, they are unavailable in this case, and thus we need an alternative approach to establish the desired functional properties of $\underline{\hbar}$.

Lemma 11. *If $\mathsf{P_c}(X) < \mathsf{P_c}(X|Y)$, then $\underline{\hbar}$ is continuous at $\mathsf{P_c}(X|Y)$.*

Proof. Without loss of generality, we will assume that $q_Y(1) > 0$. Let $D_* \in \underline{\mathcal{D}}(\mathrm{I}_N)$ be given by

$$D_* = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ \lambda & -\lambda & 0 & \cdots & 0 \\ \lambda & 0 & -\lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & 0 & 0 & \cdots & -\lambda \end{bmatrix},$$

where $\lambda = (2(N-1))^{-1/2}$. As in the proof of Lemma 5, one can show that there exist $\delta_1 > 0$ and $(x_z)_{z\in\mathcal{Z}} \subset \mathcal{X}$ such that for every $t \in [0, \delta_1]$,

$$\begin{aligned} \underline{\mathcal{P}}(\mathrm{I}_N + tD_*) &= \sum_{z\in\mathcal{Z}} \max_{x\in\mathcal{X}} (P(\mathrm{I}_N + tD_*))(x,z) \\ &= \sum_{z\in\mathcal{Z}} (P(\mathrm{I}_N + tD_*))(x_z, z). \end{aligned} \tag{43}$$

In this case, we have that

$$\begin{aligned} \underline{\mathcal{P}}(\mathrm{I}_N + tD_*) &= P(x_1,1) + t\lambda \sum_{z=2}^{N} P(x_1,z) \\ &\quad + (1 - t\lambda) \sum_{z=2}^{N} P(x_z,z) \\ &= \sum_{z\in\mathcal{Z}} P(x_z,z) \\ &\quad - t\lambda \left(\sum_{z\in\mathcal{Z}} P(x_z,z) - P(x_1,z) \right). \end{aligned}$$

Note that $\mathsf{P_c}(X|Y) = \underline{\mathcal{P}}(\mathrm{I}_N) = \sum_{z\in\mathcal{Z}} P(x_z,z)$. Hence,

$$\underline{\mathcal{P}}(\mathrm{I}_N + tD_*) = \mathsf{P_c}(X|Y) - t\lambda\sigma, \tag{44}$$

where $\sigma = \sum_{z\in\mathcal{Z}} (P(x_z,z) - P(x_1,z))$. Setting $t = 0$ in (43), we have that $P(x_z,z) \geq P(x,z)$ for all $(x,z) \in \mathcal{X}\times\mathcal{Z}$. If $P(x_z,z) = P(x_1,z)$ for all $z \geq 1$, then

$$\mathsf{P_c}(X|Y) = \sum_{z\in\mathcal{Z}} P(x_1,z) = p_X(x_1) \leq \mathsf{P_c}(X),$$

which contradicts the hypothesis of the lemma. Therefore, there exists $z \in \mathcal{Z}$ such that $P(x_z,z) > P(x_1,z)$ and hence $\sigma > 0$. Similarly, there exists $\delta_2 > 0$ such that for every $t \in [0, \delta_2]$,

$$\underline{\mathcal{U}}(\mathrm{I}_N + tD_*) = q_Y(1) + (1 - t\lambda) \sum_{z=2}^{N} q_Y(z) = 1 - t\lambda(1 - q_Y(1)). \tag{45}$$

Let $\delta = \min(\delta_1, \delta_2)$. From (44) and (45), we have for every $t \in [0, \delta]$

$$1 - t\lambda(1 - q_Y(1)) \leq \underline{\hbar}(\mathsf{P_c}(X|Y) - t\lambda\sigma) \leq 1. \tag{46}$$

In particular,

$$\lim_{\varepsilon\to\mathsf{P_c}(X|Y)} \underline{\hbar}(\varepsilon) = \lim_{t\to 0} \underline{\hbar}(\mathsf{P_c}(X|Y) - t\lambda\sigma) = 1 = \underline{\hbar}(\mathsf{P_c}(X|Y)),$$

i.e., $\underline{\hbar}$ is continuous at $\mathsf{P_c}(X|Y)$. ∎

We say that $F \in \underline{\mathcal{F}}$ is an optimal filter at ε if $\underline{\mathcal{U}}(F) = \underline{\hbar}(\varepsilon)$ and $\underline{\mathcal{P}}(F) \leq \varepsilon$. As opposed to $\hbar$, the concavity of $\underline{\hbar}$ is unknown and hence the existence of an optimal filter at ε

with $\underline{\mathcal{P}}(F) = \varepsilon$ is not immediate. Nonetheless, since $\underline{\mathcal{P}}$ and $\underline{\mathcal{U}}$ are continuous functions, there exists an optimal filter F at ε (with $\underline{\mathcal{P}}(F) \le \varepsilon$) for every $\varepsilon \in [\mathsf{P_c}(X), \mathsf{P_c}(X|Y)]$. For any $F \in \underline{\mathcal{F}}$ and $\delta > 0$, let $B(F,\delta) = \{G \in \underline{\mathcal{F}} : \|G - F\| < \delta\}$.

Lemma 12. *Let $\delta > 0$ be as in Lemma 10 for I_N, i.e., $\underline{\mathcal{U}}$ and $\underline{\mathcal{P}}$ are linear on $[\mathrm{I}_N, \mathrm{I}_N + \delta D]$ for every $D \in \underline{\mathcal{D}}(\mathrm{I}_N)$. If $\mathsf{P_c}(X) < \mathsf{P_c}(X|Y)$ and $q_Y(y) > 0$ for all $y \in \mathcal{Y}$, then there exists $\varepsilon_{\mathsf{L}} < \mathsf{P_c}(X|Y)$ such that for every $\varepsilon \in [\varepsilon_{\mathsf{L}}, \mathsf{P_c}(X|Y)]$ there exists an optimal filter F_ε at ε with $F_\varepsilon \in B(\mathrm{I}_N, \delta)$.*

Proof. Let $\underline{\mathcal{F}}^1 = \{F \in \underline{\mathcal{F}} : \underline{\mathcal{U}}(F) = 1\}$ and let $\mathcal{B} = \bigcup_{F \in \underline{\mathcal{F}}^1} B(F,\delta)$. The proof is based on the following claim.

Claim. There exists $\varepsilon_{\mathsf{L}} < \mathsf{P_c}(X|Y)$ such that if F is an optimal filter at ε with $\varepsilon \ge \varepsilon_{\mathsf{L}}$, then $F \in \mathcal{B}$.

Proof of the claim. The proof is by contradiction. Assume that for every $\varepsilon < \mathsf{P_c}(X|Y)$ there exists an optimal filter $G_{\varepsilon'}$ at $\varepsilon' \in [\varepsilon, \mathsf{P_c}(X|Y))$ with $G_{\varepsilon'} \notin \mathcal{B}$. Since $\underline{\hbar}$ is a non-decreasing function, we have that $\underline{\mathcal{U}}(G_{\varepsilon'}) = \underline{\hbar}(\varepsilon') \ge \underline{\hbar}(\varepsilon)$. Let $K := (\mathsf{P_c}(X|Y) - \mathsf{P_c}(X))^{-1}$. For each $n > K$, let $F_n = G_{\mathsf{P_c}(X|Y)-1/n} \notin \mathcal{B}$. Since $\mathcal{F}\backslash\mathcal{B}$ is compact, there exist $\{n_1 < n_2 < \cdots\}$ and $F \in \mathcal{F}\backslash\mathcal{B}$ such that $F_{n_k} \to F$ as $k \to \infty$. By continuity of $\underline{\mathcal{U}}$ and $\underline{\hbar}$ at $\mathsf{P_c}(X|Y)$, established in Lemma 11, we have

$$\begin{aligned} 1 \;&\ge\; \underline{\mathcal{U}}(F) = \lim_{k\to\infty} \underline{\mathcal{U}}(F_{n_k}) \\ &\ge\; \lim_{k\to\infty} \underline{\hbar}(\mathsf{P_c}(X|Y) - n_k^{-1}) = \underline{\hbar}(\mathsf{P_c}(X|Y)) = 1. \end{aligned}$$

In particular, we have that $F \in \underline{\mathcal{F}}^1 \subset \mathcal{B}$, which contradicts the fact that $F \in \mathcal{F}\backslash\mathcal{B}$. ∎

The assumption $q_Y(y) > 0$ for every $y \in \mathcal{Y}$ implies that $F \in \underline{\mathcal{F}}^1$ if and only if F is a permutation matrix, i.e., F can be obtained by permuting the columns of I_N. In particular, the mapping $G \mapsto GF^{-1}$ is a bijection between $B(F,\delta)$ and $B(\mathrm{I}_N,\delta)$ which preserves $\underline{\mathcal{P}}$ and $\underline{\mathcal{U}}$, i.e., $\underline{\mathcal{P}}(G) = \underline{\mathcal{P}}(GF^{-1})$ and $\underline{\mathcal{U}}(G) = \underline{\mathcal{U}}(GF^{-1})$ for every $G \in B(F,\delta)$. As mentioned earlier, there exists an optimal filter F_ε at ε for every $\varepsilon \in [\mathsf{P_c}(X), \mathsf{P_c}(X|Y)]$. By the claim, F_ε, for $\varepsilon \ge \varepsilon_{\mathsf{L}}$, belongs to $\mathcal{B}$ and, in particular, $F_\varepsilon \in B(F,\delta)$ for some $F \in \underline{\mathcal{F}}^1$. By the aforementioned properties of the bijection $G \mapsto GF^{-1}$, the filter $F_\varepsilon F^{-1}$ is an optimal filter at ε with $F_\varepsilon F^{-1} \in B(\mathrm{I}_N,\delta)$. ∎

Now we are in position to prove Theorem 3.

Proof of Theorem 3. If $q_Y(y) = 0$ for some $y \in \mathcal{Y}$, the effective cardinality of the alphabet of Y is $|\mathcal{Y}| - 1$ and thus $\underline{\hbar}(\varepsilon)$ equals $\hbar(\varepsilon)$ for every $\varepsilon \in [\mathsf{P_c}(X), \mathsf{P_c}(X|Y)]$. In this case, $\underline{\hbar}$ is piecewise linear and (9) follows trivially by Theorem 1. In what follows, we assume that $q_Y(y) > 0$ for all $y \in \mathcal{Y}$.

Let $\delta > 0$ and $\varepsilon'_{\mathsf{L}} < \mathsf{P_c}(X|Y)$ be as in Lemma 12. For each $\varepsilon \in [\varepsilon'_{\mathsf{L}}, \mathsf{P_c}(X|Y))$, let G_ε be an optimal filter at ε with $G_\varepsilon \in B(\mathrm{I}_N,\delta)$ whose existence was established in Lemma 12. Let $t_\varepsilon \in [0,\delta]$ and $D_\varepsilon \in \underline{\mathcal{D}}(\mathrm{I}_N)$ be such that $G_\varepsilon = \mathrm{I}_N + t_\varepsilon D_\varepsilon$ for every $\varepsilon \in [\varepsilon'_{\mathsf{L}}, \mathsf{P_c}(X|Y))$. As in (25) and (26) in the proof of Lemma 5, for every $t \in [0,\delta]$ and $D \in \underline{\mathcal{D}}(\mathrm{I}_N)$,

$$\begin{aligned} \underline{\mathcal{P}}(\mathrm{I}_N + tD) &= \mathsf{P_c}(X|Y) + tb^{(D)} \\ \underline{\mathcal{U}}(\mathrm{I}_N + tD) &= 1 + t\beta^{(D)}, \end{aligned} \tag{47}$$

where

$$\begin{aligned} b^{(D)} &= \sum_{z\in\mathcal{Z}} \max_{x\in\mathcal{M}_z} (PD)(x,z) \\ \beta^{(D)} &= \sum_{z\in\mathcal{Z}} q(z) D(z,z), \end{aligned} \tag{48}$$

where $\mathcal{M}_z = \{x \in \mathcal{X} : P(x,z) \ge P(x',z) \text{ for all } x' \in \mathcal{X}\}$. Since $\underline{\mathcal{P}}(F) \le \mathsf{P_c}(X|Y)$ for all $F \in \underline{\mathcal{F}}$, it is immediate that $b^{(D)} \le 0$ for every $D \in \underline{\mathcal{D}}(\mathrm{I}_N)$. Moreover, since $\underline{\mathcal{P}}(G_\varepsilon) \le \varepsilon$, we have that $b^{(D_\varepsilon)} < 0$ for all $\varepsilon \in [\varepsilon'_{\mathsf{L}}, \mathsf{P_c}(X|Y))$. By definition of $\underline{\mathcal{D}}(\mathrm{I}_N)$, it is clear that if $D \in \underline{\mathcal{D}}(\mathrm{I}_N)$, then we have $D(y,y) \le 0$ for all $y \in \mathcal{Y}$, which together with the fact that $\|D\| = 1$ for all $D \in \underline{\mathcal{D}}(\mathrm{I}_N)$, implies that $\beta^{(D)} < 0$ for all $D \in \underline{\mathcal{D}}(\mathrm{I}_N)$. We first establish the following intuitive claim.

Claim. Let $\varepsilon'_{\mathsf{L}} < \mathsf{P_c}(X|Y)$ be as defined in Lemma 12. Then, there exists an optimal filter G_ε at ε for each $\varepsilon \in [\varepsilon'_{\mathsf{L}}, \mathsf{P_c}(X|Y)]$ such that $\underline{\mathcal{P}}(G_\varepsilon) = \varepsilon$ and $\underline{\mathcal{U}}(G_\varepsilon) = \underline{\hbar}(\varepsilon)$.

Proof of Claim. The filter $G_\varepsilon = \mathrm{I}_N + t_\varepsilon D_\varepsilon$ is optimal at ε for every $\varepsilon \in [\varepsilon'_{\mathsf{L}}, \mathsf{P_c}(X|Y))$. To reach contradiction, assume that there exists $\varepsilon_0 < \varepsilon$ such that $\underline{\mathcal{P}}(G_\varepsilon) = \varepsilon_0$. According to (47), we obtain $\mathsf{P_c}(X|Y) + t_\varepsilon b^{(D_\varepsilon)} = \varepsilon_0 < \varepsilon$ and hence

$$t_\varepsilon > \frac{\mathsf{P_c}(X|Y) - \varepsilon}{-b^{(D_\varepsilon)}} =: t'.$$

Now consider the filter $\mathrm{I}_N + t'D_\varepsilon$. Since $t' \le \delta$, we have from (47) that $\underline{\mathcal{P}}(\mathrm{I}_N + t'D_\varepsilon) = \varepsilon$ and

$$\underline{\hbar}(\varepsilon) \overset{(a)}{=} 1 + t_\varepsilon \beta^{(D_\varepsilon)} \overset{(b)}{<} \underline{\mathcal{U}}(\mathrm{I}_N + t'D_\varepsilon) = 1 + t'\beta^{(D_\varepsilon)},$$

where (a) is due to the optimality of G_ε and (b) follows from the negativity of $\beta^{(D_\varepsilon)}$. The above inequality contradicts the maximality of $\underline{\hbar}(\varepsilon)$. This implies that $\underline{\mathcal{P}}(G_\varepsilon) = \varepsilon$ which, according to (47), yields

$$\underline{\hbar}(\varepsilon) = 1 - (\mathsf{P_c}(X|Y) - \varepsilon)\frac{\beta^{(D_\varepsilon)}}{b^{(D_\varepsilon)}}, \tag{49}$$

for all $\varepsilon \in [\varepsilon'_{\mathsf{L}}, \mathsf{P_c}(X|Y))$. ∎

Now fix $\varepsilon' \in [\varepsilon'_{\mathsf{L}}, \mathsf{P_c}(X|Y)]$ with $\varepsilon \le \varepsilon'$. On the one hand, according to (49), we know that

$$\underline{\hbar}(\varepsilon') = 1 - (\mathsf{P_c}(X|Y) - \varepsilon')\frac{\beta^{(D_{\varepsilon'})}}{b^{(D_{\varepsilon'})}}. \tag{50}$$

On the other hand, we obtain from (47) that $0 \le \frac{\mathsf{P_c}(X|Y)-\varepsilon'}{-b^{(D_\varepsilon)}} \le t_\varepsilon$ and hence

$$\underline{\mathcal{P}}\left(\mathrm{I}_N + \frac{\mathsf{P_c}(X|Y) - \varepsilon'}{-b^{(D_\varepsilon)}} D_\varepsilon\right) = \varepsilon', \tag{51}$$

$$\underline{\mathcal{U}}\left(\mathrm{I}_N + \frac{\mathsf{P_c}(X|Y) - \varepsilon'}{-b^{(D_\varepsilon)}} D_\varepsilon\right) = 1 - (\mathsf{P_c}(X|Y) - \varepsilon')\frac{\beta^{(D_\varepsilon)}}{b^{(D_\varepsilon)}}. \tag{52}$$

Comparing (50) and (52), we conclude that

$$1 - (\mathsf{P_c}(X|Y) - \varepsilon')\frac{\beta^{(D_{\varepsilon'})}}{b^{(D_{\varepsilon'})}} = \underline{\hbar}(\varepsilon') \ge 1 - (\mathsf{P_c}(X|Y) - \varepsilon')\frac{\beta^{(D_\varepsilon)}}{b^{(D_\varepsilon)}},$$

and hence the function $\varepsilon \mapsto \frac{\beta^{(D_\varepsilon)}}{b^{(D_\varepsilon)}}$ is non-increasing over $[\varepsilon'_{\mathsf{L}}, \mathsf{P_c}(X|Y))$. Therefore, since $\frac{\beta^{(D_\varepsilon)}}{b^{(D_\varepsilon)}} > 0$, the limit $\lim_{\varepsilon \to \mathsf{P_c}(X|Y)^-} \frac{\beta^{(D_\varepsilon)}}{b^{(D_\varepsilon)}} =: A$ exists.

Let $K = (\mathsf{P_c}(X|Y) - \varepsilon'_{\mathsf{L}})^{-1}$. For each $n > K$, let $F_n = G_{\mathsf{P_c}(X|Y)-\frac{1}{n}}$. Write $F_n = \mathrm{I}_N + t_n D_n$ with $t_n \in [0, \delta]$ and $D_n \in \underline{\mathcal{D}}(\mathrm{I}_N)$. Since $\underline{\mathcal{D}}(\mathrm{I}_N)$ is compact, there exist $\{n_1 < n_2 < \cdots\}$ and $D^* \in \underline{\mathcal{D}}(\mathrm{I}_N)$ such that $D_{n_k} \to D^*$ as $k \to \infty$. By continuity of the mappings $D \mapsto b^{(D)}$ and $D \mapsto \beta^{(D)}$, we have that $b^{(D_{n_k})} \to b^{(D^*)}$ and $\beta^{(D_{n_k})} \to \beta^{(D^*)}$ as $k \to \infty$.

Claim. We have that $b^{(D^*)} < 0$ and, in particular, $A = \frac{\beta^{(D^*)}}{b^{(D^*)}}$.

Proof of Claim. Recall that $F \in \underline{\mathcal{F}}^1$ if and only if F is a permutation matrix. In particular, $\underline{\mathcal{F}}^1$ is finite with $|\underline{\mathcal{F}}^1| = N!$. Recall that $b^{(D^*)} \le 0$. Assume that $b^{(D^*)} = 0$. Since $\frac{\beta^{(D_{n_k})}}{b^{(D_{n_k})}} \to A \in [0, \infty)$ and $b^{(D_{n_k})} \to b^{(D^*)} = 0$ as $k \to \infty$, we have that $\beta^{(D_{n_k})} \to 0$ and hence $\beta^{(D^*)} = 0$. This implies that $\underline{\mathcal{U}}(\mathrm{I}_N + tD^*) = 1$ for all $t \in [0, \delta]$, i.e., $\mathrm{I}_N + tD^* \in \underline{\mathcal{F}}^1$ for all $t \in [0, \delta]$. This contradicts the fact that $\underline{\mathcal{F}}^1$ is finite. ∎

The claim implies that for $\varepsilon \in [\mathsf{P_c}(X|Y) + \delta b^{(D^*)}, \mathsf{P_c}(X|Y)]$,

$$\underline{\mathcal{P}}\left(\mathrm{I}_N + \frac{\mathsf{P_c}(X|Y) - \varepsilon}{-b^{(D^*)}} D^*\right) = \varepsilon,$$
$$\underline{\mathcal{U}}\left(\mathrm{I}_N + \frac{\mathsf{P_c}(X|Y) - \varepsilon}{-b^{(D^*)}} D^*\right) = 1 - (\mathsf{P_c}(X|Y) - \varepsilon)A.$$

Recall that $\frac{\beta^{(D^*)}}{b^{(D^*)}} = A \le \frac{\beta^{(D_\varepsilon)}}{b^{(D_\varepsilon)}}$ for all $\varepsilon \in [\varepsilon'_{\mathsf{L}}, \mathsf{P_c}(X|Y))$. Let $\varepsilon_{\mathsf{L}} := \max\{\varepsilon'_{\mathsf{L}}, \mathsf{P_c}(X|Y) + \delta b^{(D^*)}\}$. Then for all $\varepsilon \in [\varepsilon_{\mathsf{L}}, \mathsf{P_c}(X|Y)]$

$$\begin{aligned} \underline{\hbar}(\varepsilon) &\ge 1 - (\mathsf{P_c}(X|Y) - \varepsilon)\frac{\beta^{(D^*)}}{b^{(D^*)}} \\ &\ge 1 - (\mathsf{P_c}(X|Y) - \varepsilon)\frac{\beta^{(D_\varepsilon)}}{b^{(D_\varepsilon)}} = \underline{\hbar}(\varepsilon), \end{aligned} \tag{53}$$

where the equality follows from (49). This proves that $\underline{\hbar}$ is linear on $\varepsilon \in [\varepsilon_{\mathsf{L}}, \mathsf{P_c}(X|Y)]$.

Recall that $\beta^{(D)} < 0$ for all $D \in \underline{\mathcal{D}}(\mathrm{I}_N)$. Clearly, (53) implies that

$$\underline{\hbar}'(\mathsf{P_c}(X|Y)) = \min_{D \in \underline{\mathcal{D}}(\mathrm{I}_N)} \frac{\beta^{(D)}}{b^{(D)}}. \tag{54}$$

If $b^{(D)} = 0$ for some $D \in \underline{\mathcal{D}}(\mathrm{I}_N)$, the term $\frac{\beta^{(D)}}{b^{(D)}}$ is defined to be $+\infty$. Notice that this convention agrees with the fact that if $b^{(D)} = 0$ then D cannot be an *optimal direction*. Furthermore, for every $D' \in \underline{\mathcal{D}}(\mathrm{I}_N)$ such that $\underline{\hbar}'(\mathsf{P_c}(X|Y)) = \frac{\beta^{(D')}}{b^{(D')}}$, there exists $\varepsilon_{\mathsf{L}} < \mathsf{P_c}(X|Y)$ (depending on D') such that

$$\mathrm{I}_N + \frac{\mathsf{P_c}(X|Y) - \varepsilon}{-b^{(D')}} D' \tag{55}$$

achieves $\underline{\hbar}(\varepsilon)$ for every $\varepsilon \in [\varepsilon_{\mathsf{L}}, \mathsf{P_c}(X|Y)]$. In addition, assume that for each $y \in \mathcal{Y}$ there exists (a unique) $x_y \in \mathcal{X}$ such that $P_{X|Y}(x_y|y) > P_{X|Y}(x|y)$, for all $x \ne x_y$. In particular, $\mathcal{M}_z = \{x_z\}$ for every $z \in \mathcal{Z}$ and hence (48) becomes

$$b^{(D)} = \sum_{z \in \mathcal{Z}} (PD)(x_z, z) \quad \text{and} \quad \beta^{(D)} = \sum_{z \in \mathcal{Z}} q_Y(z) D(z, z),$$

for every $D \in \underline{\mathcal{D}}(\mathrm{I}_N)$. Using the fact that $\sum_{z \in \mathcal{Z}} D(y, z) = 0$ for all $y \in \mathcal{Y}$, we obtain

$$b^{(D)} = -\sum_{y \in \mathcal{Y}} \sum_{z \ne y} (P(x_y, y) - P(x_z, y)) D(y, z),$$

and

$$\beta^{(D)} = -\sum_{y \in \mathcal{Y}} \sum_{z \ne y} q_Y(y) D(y, z).$$

Therefore, for every $D \in \underline{\mathcal{D}}(\mathrm{I}_N)$,

$$\frac{\beta^{(D)}}{b^{(D)}} = \frac{\sum_{y \in \mathcal{Y}} \sum_{z \ne y} q_Y(y) D(y, z)}{\sum_{y \in \mathcal{Y}} \sum_{z \ne y} (P(x_y, y) - P(x_z, y)) D(y, z)}. \tag{56}$$

Since $\frac{\sum_k a_k x_k}{\sum_k b_k x_k} \ge \min_k \frac{a_k}{b_k}$ for $a_k > 0$ and $b_k, x_k \ge 0$ with $\sum_k x_k > 0$, we obtain from (56) that for every $D \in \underline{\mathcal{D}}(\mathrm{I}_N)$

$$\frac{\beta^{(D)}}{b^{(D)}} \ge \min_{(y,z) \in \mathcal{Y} \times \mathcal{Z}} \frac{q_Y(y)}{P(x_y, y) - P(x_z, y)}.$$

Equation (54) implies that

$$\underline{\hbar}'(\mathsf{P_c}(X|Y)) \ge \min_{(y,z) \in \mathcal{Y} \times \mathcal{Z}} \frac{q_Y(y)}{P(x_y, y) - P(x_z, y)}.$$

Assume that (y_0, z_0) attains the above minimum. We note that one can easily show from (46) that $0 \le \underline{\hbar}'(\varepsilon) \le \frac{1 - q_Y(1)}{\sigma} < \infty$, for some $\sigma > 0$. Hence, we have $y_0 \ne z_0$. Now, consider the direction D_* such that

$$D_*(y, z) = \begin{cases} \lambda, & y = y_0, z = z_0 \\ -\lambda, & y = z = y_0 \\ 0, & \text{otherwise}, \end{cases}$$

where $\lambda = 2^{-1/2}$. Equation (56) implies then that

$$\frac{\beta^{(D_*)}}{b^{(D_*)}} = \frac{q_Y(y_0)}{P(x_{y_0}, y_0) - P(x_{z_0}, y_0)},$$

and hence

$$\begin{aligned} \underline{\hbar}'(\mathsf{P_c}(X|Y)) &\le \frac{q_Y(y_0)}{P(x_{y_0}, y_0) - P(x_{z_0}, y_0)} \\ &= \min_{(y,z) \in \mathcal{Y} \times \mathcal{Z}} \frac{q_Y(y)}{P(x_y, y) - P(x_z, y)}. \end{aligned}$$

As a consequence,

$$\underline{\hbar}'(\mathsf{P_c}(X|Y)) = \min_{(y,z) \in \mathcal{Y} \times \mathcal{Z}} \frac{q_Y(y)}{P(x_y, y) - P(x_z, y)}.$$

Moreover, (55) implies that there exists $\varepsilon_{\mathsf{L}}^{y_0, z_0} < \mathsf{P_c}(X|Y)$ such that $\mathrm{I}_N + \frac{\mathsf{P_c}(X|Y) - \varepsilon}{-b^{(D_*)}} D_*$ achieves $\underline{\hbar}(\varepsilon)$ for every $\varepsilon \in [\varepsilon_{\mathsf{L}}^{y_0, z_0}, \mathsf{P_c}(X|Y)]$. Note that

$$\mathrm{I}_N + \frac{\mathsf{P_c}(X|Y) - \varepsilon}{-b^{(D_*)}} D_* = \mathsf{Z}^{y_0, z_0}(\zeta^{y_0, z_0}(\varepsilon)),$$

where $\zeta^{y_0, z_0}(\varepsilon) = \frac{\mathsf{P_c}(X|Y) - \varepsilon}{P(x_{y_0}, y_0) - P(x_{z_0}, y_0)}$. ∎

Appendix E
Proof of Theorem 4

Let $P = [P(x^n, y^n)]_{x^n, y^n \in \{0,1\}^n}$ denotes the joint probability matrix of X^n and Y^n and $q(y^n) = \Pr(Y^n = y^n)$ for $y^n \in \{0,1\}^n$. Let $\mathbf{0} = (0, 0, \ldots, 0)$ and $\mathbf{1} = (1, 1, \ldots, 1)$. We will show that (X^n, Y^n) satisfies the hypotheses of Theorem 3 with $y_0 = \mathbf{1}$ and $z_0 = \mathbf{0}$.

Under the assumptions (a_1) and (b), it is straightforward to verify that

$$P(x^n, y^n) = (\bar{\alpha}\bar{p})^n \prod_{k=1}^{n} \left(\frac{p}{\bar{p}}\right)^{x_k} \left(\frac{\alpha}{\bar{\alpha}}\right)^{x_k \oplus y_k}, \tag{57}$$

for every $x^n, y^n \in \{0,1\}^n$. By assumption, $\mathsf{P_c}(X^n) = p^n < \bar{\alpha}^n = \mathsf{P_c}(X^n|Y^n)$. It is also straightforward to verify that $q(y^n) > 0$ for all $y \in \{0,1\}^n$. Since $\bar{\alpha}\bar{p} > \alpha p$, we have from (57) that

$$\Pr(X^n = z^n, Y^n = z^n) > \Pr(X^n = x^n, Y^n = z^n),$$

for all $x^n \neq z^n$. In the notation of Theorem 3, $x^n_{z^n} = z^n$ for all $z^n \in \{0,1\}^n$. Note that

$$\begin{aligned} &\min_{y^n, z^n \in \{0,1\}^n} \frac{q(y^n)}{P(x^n_{y^n}, y^n) - P(x^n_{z^n}, y^n)} \\ &= \min_{y^n \in \{0,1\}^n} \frac{q(y^n)}{P(y^n, y^n) - \min\limits_{z^n \neq y^n} P(z^n, y^n)}. \end{aligned}$$

It is easy to show that $\min\limits_{z^n \neq y^n} P(z^n, y^n) = (\alpha p)^n \prod\limits_{k=1}^{n} \left(\frac{p}{\bar{p}}\right)^{-y_k}$ and that the minimum is attained by $z^n = (\bar{y}_1, \bar{y}_2, \ldots, \bar{y}_n)$. As a consequence,

$$\begin{aligned} &\min_{y^n, z^n \in \{0,1\}^n} \frac{q(y^n)}{P(x^n_{y^n}, y^n) - P(x^n_{z^n}, y^n)} \\ &= \min_{y^n \in \{0,1\}^n} \frac{\sum\limits_{x^n \in \{0,1\}^n} \prod\limits_{k=1}^{n} \left(\frac{p}{\bar{p}}\right)^{x_k - y_k} \left(\frac{\alpha}{\bar{\alpha}}\right)^{x_k \oplus y_k}}{1 - \left(\frac{p\alpha}{\bar{p}\bar{\alpha}}\right)^n \Pi_{y^n}^{-2}} \\ &= \min_{y^n \in \{0,1\}^n} \frac{\prod\limits_{k=1}^{n} \left[\left(\frac{p}{\bar{p}}\right)^{-y_k} \left(\frac{\alpha}{\bar{\alpha}}\right)^{y_k} + \left(\frac{p}{\bar{p}}\right)^{1-y_k} \left(\frac{\alpha}{\bar{\alpha}}\right)^{1-y_k}\right]}{1 - \left(\frac{p\alpha}{\bar{p}\bar{\alpha}}\right)^n \Pi_{y^n}^{-2}}, \end{aligned}$$

where $\Pi_{y^n} = \prod\limits_{k=1}^{n} \left(\frac{p}{\bar{p}}\right)^{y_k}$. Observe that the denominator is maximized when $y^n = \mathbf{1}$. Using the fact that $p \geq \frac{1}{2} \geq \bar{p}$, one can show that the numerator is minimized when $y^n = \mathbf{1}$. In particular,

$$\min_{y^n, z^n \in \{0,1\}^n} \frac{q(y^n)}{P(x^n_{y^n}, y^n) - P(x^n_{z^n}, y^n)} = \frac{(\alpha\bar{p} + \bar{\alpha}p)^n}{(\bar{\alpha}p)^n - (\alpha\bar{p})^n},$$

and the minimum is attained by $(y_0^n, z_0^n) = (\mathbf{1}, \mathbf{0})$.

Therefore (X^n, Y^n) satisfies the hypotheses of Theorem 3 with $(y_0^n, z_0^n) = (\mathbf{1}, \mathbf{0})$. Thus, there exists $\varepsilon'_{\mathsf{L}} < \bar{\alpha}^n$ such that for every $\varepsilon \in [\varepsilon'_{\mathsf{L}}, \bar{\alpha}^n]$

$$\underline{\hbar}(\varepsilon) = 1 - \frac{\bar{\alpha}^n - \varepsilon}{(\bar{\alpha}p)^n - (\alpha\bar{p})^n} q^n.$$

Moreover, $\mathsf{Z}^{\mathbf{1},\mathbf{0}}(\zeta^{y_0,z_0}(\varepsilon))$ achieves $\underline{\hbar}(\varepsilon)$ for every $\varepsilon \in [\varepsilon'_{\mathsf{L}}, \bar{\alpha}^n]$, where

$$\zeta^{y_0,z_0}(\varepsilon) = \frac{\bar{\alpha}^n - \varepsilon}{(\bar{\alpha}p)^n - (\alpha\bar{p})^n}.$$

Recall that $\underline{\hbar}(\varepsilon) = \underline{\hbar}_n^n(\varepsilon^{1/n})$ and let $\varepsilon_{\mathsf{L}} = (\varepsilon'_{\mathsf{L}})^{1/n}$. Therefore, $\underline{\hbar}_n^n(\varepsilon) = 1 - \zeta_n(\varepsilon) q^n$ for all $\varepsilon \in [\varepsilon_{\mathsf{L}}, \bar{\alpha}]$ which is attained by the Z-channel $\mathsf{Z}_n(\zeta_n(\varepsilon))$, where $\zeta_n(\varepsilon) \coloneqq \zeta^{y_0,z_0}(\varepsilon^n)$.

Appendix F
Proof of Proposition 2

For any privacy filter satisfying (12), (X^n, Z^n) and (Y^n, Z^n) are i.i.d. By Lemma 1, we have $\mathsf{P_c}(X^n|Z^n) = (\mathsf{P_c}(X|Z))^n$ and $\mathsf{P_c}(Y^n|Z^n) = (\mathsf{P_c}(Y|Z))^n$ where (X, Y, Z) has the common distribution of $\{(X_k, Y_k, Z_k)\}_{k=1}^n$. In particular,

$$\hbar_n^{\mathsf{i}}(\varepsilon) = \sup_{\mathsf{P_c}^{1/n}(X^n|Z^n) \leq \varepsilon} \mathsf{P_c}^{1/n}(Y^n|Z^n) = \sup_{\mathsf{P_c}(X|Z) \leq \varepsilon} \mathsf{P_c}(Y|Z),$$

where the first supremum assumes (12) and the second supremum is implicitly constrained to $\mathcal{Z} = \{0,1\}$. The result then follows from Theorem 2.

Appendix G
Proof of Corollary 3

Assume that $p > \frac{1}{2}$. By Theorem 4, for every $\varepsilon \in [\varepsilon_{\mathsf{L}}, \bar{\alpha}]$ we have $\underline{\hbar}_n(\varepsilon) = [A_n \varepsilon^n + B_n]^{1/n}$, where $A_n = \frac{q^n}{(\bar{\alpha}p)^n - (\alpha\bar{p})^n}$ and $B_n = 1 - \frac{\bar{\alpha}^n q^n}{(\bar{\alpha}p)^n - (\alpha\bar{p})^n}$. In particular,

$$\begin{aligned} \underline{\hbar}'_n(\varepsilon) &= A_n \left(\frac{\varepsilon}{\underline{\hbar}_n(\varepsilon)}\right)^{n-1}, \\ \underline{\hbar}''_n(\varepsilon) &= (n-1) \frac{A_n B_n}{\underline{\hbar}_n^{n+1}(\varepsilon)} \left(\frac{\varepsilon}{\underline{\hbar}_n(\varepsilon)}\right)^{n-2}. \end{aligned} \tag{58}$$

Since $p > \frac{1}{2}$ and $\alpha > 0$, we have $B_n \to 1$ as $n \to \infty$. Let $N_0 \geq 1$ be such that $B_n \geq 0$ for all $n \geq N_0$. In this case, we have that $\underline{\hbar}''_n(\varepsilon) \geq 0$ for all $\varepsilon \in [\varepsilon_{\mathsf{L}}, \bar{\alpha}]$ and $n \geq N_0$. In particular, $\underline{\hbar}_n$ is convex on $[\varepsilon_{\mathsf{L}}, \bar{\alpha}]$. As a consequence, for all $\varepsilon \in [\varepsilon_{\mathsf{L}}, \bar{\alpha}]$ and $n \geq N_0$

$$\underline{\hbar}_n(\varepsilon) \geq 1 - (\bar{\alpha} - \varepsilon)\underline{\hbar}'_n(\bar{\alpha}).$$

Since $\hbar_n^{\mathsf{i}}(\varepsilon) = \underline{\hbar}_1(\varepsilon) = 1 - (\bar{\alpha} - \varepsilon)\underline{\hbar}'_1(\bar{\alpha})$ for all $\varepsilon \in [p, \bar{\alpha}]$, the above inequality implies that

$$\underline{\hbar}_n(\varepsilon) - \hbar_n^{\mathsf{i}}(\varepsilon) \geq (\bar{\alpha} - \varepsilon)(\underline{\hbar}'_1(\bar{\alpha}) - \underline{\hbar}'_n(\bar{\alpha}))$$

for all $\varepsilon \in [\varepsilon_{\mathsf{L}}, \bar{\alpha}]$ and $n \geq N_0$. The result follows from (58).

Now, assume that $p = \frac{1}{2}$. In this case, we have for all $\varepsilon \in [\varepsilon_{\mathsf{L}}, \bar{\alpha}]$

$$\underline{\hbar}_n(\varepsilon) = \left(\frac{\varepsilon^n - \alpha^n}{\bar{\alpha}^n - \alpha^n}\right)^{1/n} \quad \text{and} \quad \hbar_n^{\mathsf{i}}(\varepsilon) = \frac{\varepsilon - \alpha}{\bar{\alpha} - \alpha}.$$

Let $\Xi_n : [\frac{1}{2}, \bar{\alpha}] \to \mathbb{R}$ be given by $\Xi_n(\varepsilon) = \underline{\hbar}_n(\varepsilon) - \hbar_n^{\mathsf{i}}(\varepsilon)$.

Claim. The function Ξ_n is decreasing on $[\frac{1}{2}, \bar{\alpha}]$.

Proof of Claim. We shall show that $\Xi_n'(\varepsilon) \le 0$ for all $\varepsilon \in [\frac{1}{2}, \bar{\alpha}]$. A straightforward computation shows that

$$\Xi_n'(\varepsilon) = \frac{1}{\left[1-\left(\frac{\alpha}{\varepsilon}\right)^n\right]^{(n-1)/n}} \frac{1}{[\bar{\alpha}^n - \alpha^n]^{1/n}} - \frac{1}{\bar{\alpha}-\alpha}.$$

This function is clearly decreasing, and so it is enough to show that $\Xi_n'(\frac{1}{2}) \le 0$. Note that $\Xi_n'(\frac{1}{2}) \le 0$ if and only if

$$\frac{\left(1-\frac{\alpha}{\bar{\alpha}}\right)^n}{1-\left(\frac{\alpha}{\bar{\alpha}}\right)^n} \le [1-(2\alpha)^n]^{n-1}. \tag{59}$$

Observe that $\frac{\left(1-\frac{\alpha}{\bar{\alpha}}\right)^n}{1-\left(\frac{\alpha}{\bar{\alpha}}\right)^n} \le \left(1-\frac{\alpha}{\bar{\alpha}}\right)^{n-1}$. Using the fact that $4\alpha\bar{\alpha} \le 1$, it is straightforward to verify that (59) holds. ∎

Since Ξ_n is decreasing over $[\frac{1}{2}, \bar{\alpha}]$, we obtain for all $\varepsilon \in [\varepsilon_{\mathsf{L}}, \bar{\alpha}]$

$$0 \le \underline{\hbar}_n(\varepsilon) - \hbar_n^{\mathsf{i}}(\varepsilon) \le \Xi_n\left(\frac{1}{2}\right) = \frac{1}{2}\left[\left(\frac{1-(2\alpha)^n}{\bar{\alpha}^n-\alpha^n}\right)^{1/n} - 1\right].$$

Since $1-(2\alpha)^n \le 1-\left(\frac{\alpha}{\bar{\alpha}}\right)^n$, it is straightforward to show that $\Xi_n\left(\frac{1}{2}\right) \le \frac{\alpha}{2\bar{\alpha}}$, which completes the proof.

Appendix H
Proof of Theorem 5

As before, let $P = [P(x^n, y^n)]_{x^n, y^n \in \{0,1\}^n}$ denote the joint probability matrix of X^n and Y^n and let $q(y^n) = \Pr(Y^n = y^n)$ for $y^n \in \{0,1\}^n$. We first show that (X^n, Y^n) satisfies the hypotheses of Theorem 3, and thus we can use (10) to obtain bounds on $\underline{\hbar}'(\mathsf{P_c}(X^n|Y^n))$. ((Note that $\mathsf{P_c}(X^n) < \mathsf{P_c}(X^n|Y^n)$ by the assumption.))

Assumptions (a_2) and (b) imply that, for all $x^n, y^n \in \{0,1\}^n$

$$P(x^n, y^n) = (\bar{\alpha}\bar{r})^n \frac{\bar{p}}{\bar{r}} \left(\frac{p}{\bar{p}}\right)^{x_1} \left(\frac{\alpha}{\bar{\alpha}}\right)^{x_1 \oplus y_1} \Upsilon(x^n, y^n), \tag{60}$$

where $\Upsilon(x^n, y^n) = \prod_{k=2}^{n} \left(\frac{r}{\bar{r}}\right)^{x_k \oplus x_{k-1}} \left(\frac{\alpha}{\bar{\alpha}}\right)^{x_k \oplus y_k}$ and the product equals one if $n = 1$. Since $\alpha > 0$, it is clear that $q(y^n) > 0$ for all $y^n \in \{0,1\}^n$. Let $N_0(z^n) = |\{1 \le k \le n : z_k = 0\}|$ and $N_1(z^n) = |\{1 \le k \le n : z_k = 1\}|$ for any binary vector $z^n \in \{0,1\}^n$. Recall that n is odd, so either $N_0(z^n) < N_1(z^n)$ or $N_0(z^n) > N_1(z^n)$. The following lemma shows that for every $y^n \in \{0,1\}^n$ there exists (a unique) $x^n_{y^n} \in \{0,1\}^n$ such that $P(x^n_{y^n}, y^n) > P(x^n, y^n)$ for all $x^n \ne x^n_{y^n}$.

Lemma 13. *Let (X^n, Y^n) be as in the hypothesis of Theorem 5. Then, we have for any $y^n \in \{0,1\}^n$*

$$P(x^n, y^n) \le \begin{cases} (\bar{\alpha}\bar{r})^n \frac{\bar{p}}{\bar{r}} \left(\frac{\alpha}{\bar{\alpha}}\right)^{N_1(y^n)}, & \text{if } N_0(y^n) > N_1(y^n), \\ (\bar{\alpha}\bar{r})^n \frac{p}{\bar{r}} \left(\frac{\alpha}{\bar{\alpha}}\right)^{N_0(y^n)}, & \text{if } N_0(y^n) < N_1(y^n), \end{cases}$$

for all $x^n \in \{0,1\}^n$ with equality if and only if $x^n = \mathbf{0}$ or $x^n = \mathbf{1}$, respectively.

To prove this lemma, we will make use of the following fact.

Claim. Let $y^n \in \{0,1\}^n$ be given. If $x^n \in \{0,1\}^n$ maximizes $P(x^n, y^n)$, then $x_1 = x_2 = \cdots = x_n$.

Proof of Claim. We prove the result using backward induction. To do so, we assume that the maximizer x^n satisfies $x_n = x_{n-1} = \cdots = x_l$ for $2 \le l \le n$. It is sufficient to show that $x_n = \cdots = x_l = x_{l-1}$. In light of (60), we have

$$P(x^n, y^n) = A_{l-1} \left(\frac{r}{\bar{r}}\right)^{x_l \oplus x_{l-1}} \prod_{k=l}^{n} \left(\frac{\alpha}{\bar{\alpha}}\right)^{x_l \oplus y_k}, \tag{61}$$

where[4]

$$A_{l-1} = (\bar{\alpha}\bar{r})^n \frac{\bar{p}}{\bar{r}} \left(\frac{p}{\bar{p}}\right)^{x_1} \left(\frac{\alpha}{\bar{\alpha}}\right)^{x_1 \oplus y_1} \Upsilon(x^{\ell-1}, y^{\ell-1}).$$

Notice that A_{l-1} depends only on $x_1, \ldots, x_{l-1}$. By the induction hypothesis, we have $x_l = \cdots = x_n$. In particular, x^n equals either

$$\tilde{x}^n := \{x_1, \ldots, x_{l-1}, \underbrace{\bar{x}_{l-1}, \ldots, \bar{x}_{l-1}}_{n-l+1}\},$$

or

$$\hat{x}^n := \{x_1, \ldots, x_{l-1}, \underbrace{x_{l-1}, \ldots, x_{l-1}}_{n-l+1}\}.$$

By (61), we have that

$$P(\tilde{x}^n, y^n) = A_{l-1} \frac{r}{\bar{r}} \prod_{k=l}^{n} \left(\frac{\alpha}{\bar{\alpha}}\right)^{1-x_{l-1} \oplus y_k},$$

and

$$P(\hat{x}^n, y^n) = A_{l-1} \prod_{k=l}^{n} \left(\frac{\alpha}{\bar{\alpha}}\right)^{x_{l-1} \oplus y_k}.$$

By the assumptions on r and α, we have

$$\begin{aligned} \frac{r}{\bar{r}} \prod_{k=l}^{n} \left(\frac{\alpha}{\bar{\alpha}}\right)^{1-x_{l-1} \oplus y_k} &\le \frac{r}{\bar{r}} < \left(\frac{\alpha}{\bar{\alpha}}\right)^{n-1} \\ &\le \left(\frac{\alpha}{\bar{\alpha}}\right)^{n-l+1} \le \prod_{k=l}^{n} \left(\frac{\alpha}{\bar{\alpha}}\right)^{x_{l-1} \oplus y_k}, \end{aligned}$$

which shows that $P(\tilde{x}^n, y^n) < P(\hat{x}^n, y^n)$ and hence $x^n = \hat{x}^n$. In other words, $x_{l-1} = x_l = \cdots = x_n$. This completes the induction step. ∎

Proof of Lemma 13. By the above claim, for any given $y^n \in \{0,1\}^n$, the maximizer $x^n \in \{0,1\}^n$ of $P(x^n, y^n)$ is either $x^n = \mathbf{0}$ or $x^n = \mathbf{1}$, for which we have

$$P(\mathbf{0}, y^n) = (\bar{\alpha}\bar{r})^n \frac{\bar{p}}{\bar{r}} \left(\frac{\alpha}{\bar{\alpha}}\right)^{N_1(y^n)}, \tag{62}$$

$$P(\mathbf{1}, y^n) = (\bar{\alpha}\bar{r})^n \frac{p}{\bar{r}} \left(\frac{\alpha}{\bar{\alpha}}\right)^{N_0(y^n)}. \tag{63}$$

Assume $N_0(y^n) > N_1(y^n)$ and recall that $\alpha p < \bar{\alpha}\bar{p}$. In this case,

$$p \left(\frac{\alpha}{\bar{\alpha}}\right)^{N_0(y^n)} \le \frac{\alpha p}{\bar{\alpha}} \left(\frac{\alpha}{\bar{\alpha}}\right)^{N_1(y^n)} < \bar{p} \left(\frac{\alpha}{\bar{\alpha}}\right)^{N_1(y^n)},$$

[4]When $l \le 3$, we use the convention that $\prod_{k=2}^{l-1} \left(\frac{r}{\bar{r}}\right)^{x_k \oplus x_{k-1}} \left(\frac{\alpha}{\bar{\alpha}}\right)^{x_k \oplus y_k} = 1$.

which implies $P(\mathbf{0},y^n) > P(\mathbf{1},y^n)$, and hence $x^n=\mathbf{0}$ is the only maximizer. If $N_0(y^n)<N_1(y^n)$, then $\left(\frac{\alpha}{\bar\alpha}\right)^{N_0(y^n)} > \left(\frac{\alpha}{\bar\alpha}\right)^{N_1(y^n)}$. Since $p\geq\bar p$, we conclude that

$$p\left(\frac{\alpha}{\bar\alpha}\right)^{N_0(y^n)} > \bar p\left(\frac{\alpha}{\bar\alpha}\right)^{N_1(y^n)}.$$

Consequently, $P(\mathbf{1},y^n) > P(\mathbf{0},y^n)$ and hence $x^n=\mathbf{1}$ is the only maximizer. ∎

Note that

$$\begin{aligned}\mathsf{P_c}(X^n|Y^n) &= \sum_{y^n\in\{0,1\}^n}\max_{x^n\in\{0,1\}^n} P(x^n,y^n)\\ &\overset{(a)}{=} \sum_{y^n:N_0(y^n)>N_1(y^n)} P(\mathbf{0},y^n)\\ &\quad+\sum_{y^n:N_0(y^n)<N_1(y^n)} P(\mathbf{1},y^n)\\ &\overset{(b)}{=} \bar\alpha^n\bar r^{n-1}\sum_{k=0}^{(n-1)/2}\binom{n}{k}\left(\frac{\alpha}{\bar\alpha}\right)^k, \end{aligned}\tag{64}$$

where (a) is due to Lemma 13 and (b) comes from (62) and (63).

In order to be able to use Theorem 3, we first need to show that $\mathsf{P_c}(X^n)<\mathsf{P_c}(X^n|Y^n)$. Note that $1=\sum_{k=0}^n\binom{n}{k}\alpha^n\bar\alpha^{n-k}$ and hence $\bar\alpha^n\sum_{k=0}^n\binom{n}{k}\left(\frac{\alpha}{\bar\alpha}\right)^k=1$. We can therefore write

$$\begin{aligned}\frac{1}{\bar\alpha^n} &= \sum_{k=0}^n\binom{n}{k}\left(\frac{\alpha}{\bar\alpha}\right)^k\\ &= \sum_{k=0}^{(n-1)/2}\binom{n}{k}\left(\frac{\alpha}{\bar\alpha}\right)^k\left(1+\left(\frac{\alpha}{\bar\alpha}\right)^{n-2k}\right)\\ &\leq \sum_{k=0}^{(n-1)/2}\binom{n}{k}\left(\frac{\alpha}{\bar\alpha}\right)^k\left(1+\frac{\alpha}{\bar\alpha}\right)\\ &< \sum_{k=0}^{(n-1)/2}\binom{n}{k}\left(\frac{\alpha}{\bar\alpha}\right)^k\left(1+\frac{\bar p}{p}\right)\\ &= \frac{1}{p}\sum_{k=0}^{(n-1)/2}\binom{n}{k}\left(\frac{\alpha}{\bar\alpha}\right)^k,\end{aligned}\tag{65}$$

which implies that $\mathsf{P_c}(X^n)<\mathsf{P_c}(X^n|Y^n)$.

Now that all the hypotheses of Theorem 3 are shown to be satisfied, we can use (10) to study $\underline{\hbar}'(\mathsf{P_c}(X^n|Y^n))$. The following lemma is important in bounding $\underline{\hbar}'(\mathsf{P_c}(X^n|Y^n))$.

Lemma 14. *Let (X^n,Y^n) be as in the hypothesis of Theorem 5. Then, for all $y^n\in\{0,1\}^n$,*

$$q(y^n)\geq\alpha^n.$$

Proof. From (60), we have

$$\begin{aligned}P(x^n,y^n) &= (\bar\alpha\bar r)^n\frac{\bar p}{\bar r}\left(\frac{p}{\bar p}\right)^{x_1}\left(\frac{\alpha}{\bar\alpha}\right)^{x_1\oplus y_1}\Upsilon_n(x^n,y^n)\\ &\geq \left(\frac{\alpha}{\bar\alpha}\right)^n(\bar\alpha\bar r)^n\frac{\bar p}{\bar r}\left(\frac{p}{\bar p}\right)^{x_1}\prod_{k=2}^n\left(\frac{r}{\bar r}\right)^{x_k\oplus x_{k-1}}\\ &= \alpha^n\bar r^n\frac{\bar p}{\bar r}\left(\frac{p}{\bar p}\right)^{x_1}\prod_{k=2}^n\left(\frac{r}{\bar r}\right)^{x_k\oplus x_{k-1}}.\end{aligned}$$

Summing over all $x^n\in\{0,1\}^n$, we obtain

$$q(y^n)\geq\alpha^n\bar r^{n-1}\bar p\sum_{x^n\in\{0,1\}^n}\left(\frac{p}{\bar p}\right)^{x_1}\prod_{k=2}^n\left(\frac{r}{\bar r}\right)^{x_k\oplus x_{k-1}}.\tag{66}$$

On the other hand, it is straightforward to verify that

$$\begin{aligned}1&=\sum_{x\in\{0,1\}^n}\Pr(X^n=x^n)\\ &=\bar r^{n-1}\bar p\sum_{x^n\in\{0,1\}^n}\left(\frac{p}{\bar p}\right)^{x_1}\prod_{k=2}^n\left(\frac{r}{\bar r}\right)^{x_k\oplus x_{k-1}}.\end{aligned}\tag{67}$$

Plugging (67) into (66), the result follows. ∎

By (10) and the previous lemma,

$$\underline{\hbar}'(\mathsf{P_c}(X^n|Y^n))\geq\min_{y^n,z^n\in\{0,1\}^n}\frac{\alpha^n}{P(x^n_{y^n},y^n)-P(x^n_{z^n},y^n)}.$$

Since both $x^n_{y^n}$ and $x^n_{z^n}$ are either $\mathbf{0}$ or $\mathbf{1}$, we have to maximize

$$\vartheta:=\begin{cases}(\bar\alpha\bar r)^n\frac{\bar p}{\bar r}\left(\frac{\alpha}{\bar\alpha}\right)^{N_1(y^n)}-(\bar\alpha\bar r)^n\frac{p}{\bar r}\left(\frac{\alpha}{\bar\alpha}\right)^{N_0(y^n)}, & \text{if } y^n\in\mathcal{R}_0,\\ (\bar\alpha\bar r)^n\frac{p}{\bar r}\left(\frac{\alpha}{\bar\alpha}\right)^{N_0(y^n)}-(\bar\alpha\bar r)^n\frac{\bar p}{\bar r}\left(\frac{\alpha}{\bar\alpha}\right)^{N_1(y^n)}, & \text{if } y^n\notin\mathcal{R}_0,\end{cases}$$

where $\mathcal{R}_0=\{y^n\in\{0,1\}^n: N_0(y^n)>N_1(y^n)\}$. Clearly, ϑ is maximized when $y^n=\mathbf{1}$ and thus

$$\underline{\hbar}'(\mathsf{P_c}(X^n|Y^n))\geq\frac{\bar r\alpha^n}{p(\bar\alpha\bar r)^n-\bar p(\alpha\bar r)^n}.$$

By (9) and the fact that $\underline{\hbar}^n_n(\varepsilon)=\underline{\hbar}(\varepsilon^n)$,

$$\underline{\hbar}^n_n(\varepsilon)\leq 1-\bar r\frac{\mathsf{P_c}(X^n|Y^n)-\varepsilon^n}{p(\bar\alpha\bar r)^n-\bar p(\alpha\bar r)^n}\alpha^n,$$

where $\mathsf{P_c}(X^n|Y^n)$ is computed in (64).

The lower bound follows from considering the direction $\tilde D\in\underline{\mathcal{D}}(\mathrm{I}_{2^n})$, whose entries are all zero except $\tilde D(\mathbf{1},\mathbf{0})=\lambda$ and $\tilde D(\mathbf{1},\mathbf{1})=-\lambda$ for $\lambda=2^{-1/2}$. In particular, plugging $\tilde D$ into (56), we obtain an upper bound for $\underline{\hbar}'(\mathsf{P_c}(X^n|Y^n))$ and thus a lower bound for $\underline{\hbar}(\varepsilon)$ for the desired range of ε. Note that the filter $\mathrm{I}_{2^n}+\zeta_n(\varepsilon)\tilde{\mathrm{D}}$ corresponds to the 2^n-ary Z-channel $\mathsf{Z}_n(\zeta_n(\varepsilon))$.

Appendix I
Proof of Proposition 3

Since $r=0$, the joint distribution $P_{\theta Y^n}$ can be equivalently written as the joint probability matrix $P=[P(x^n,y^n)]_{x^n,y^n\in\{0,1\}^n}$ with $x_1=x_2=\cdots=x_n=\theta$. As in the proof of Theorem 5, the hypotheses of Theorem 3 are fulfilled. In particular,

$$\underline{\hbar}'(\mathsf{P_c}(\theta|Y^n))=\min_{y^n,z^n\in\{0,1\}^n}\frac{q(y^n)}{P(x^n_{y^n},y^n)-P(x^n_{z^n},y^n)}.\tag{68}$$

In this case, (60) becomes

$$P(\mathbf{0},y^n)=\bar p\bar\alpha^n\left(\frac{\alpha}{\bar\alpha}\right)^{N_1(y^n)},$$

and

$$P(\mathbf{1},y^n)=p\bar\alpha^n\left(\frac{\alpha}{\bar\alpha}\right)^{N_0(y^n)}.$$

In particular,

$$\underline{\hbar}'(\mathsf{P_c}(\theta|Y^n)) = \min_{y^n,z^n\in\{0,1\}^n} \frac{p\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_0(y^n)} + \bar{p}\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_1(y^n)}}{P(x^n_{y^n},y^n) - P(x^n_{z^n},y^n)}.$$

Lemma 13 implies that both $x^n_{y^n}$ and $x^n_{z^n}$ are either $\mathbf{0}$ or $\mathbf{1}$. If $N_0(y^n) > N_1(y^n)$, then

$$\frac{p\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_0(y^n)} + \bar{p}\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_1(y^n)}}{P(x^n_{y^n},y^n) - P(x^n_{z^n},y^n)} \geq \frac{p\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_0(y^n)} + \bar{p}\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_1(y^n)}}{\bar{p}\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_1(y^n)} - p\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_0(y^n)}},$$

with equality if and only if $N_1(z^n) > N_0(z^n)$. It is not hard to show that

$$\frac{p\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_0(y^n)} + \bar{p}\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_1(y^n)}}{\bar{p}\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_1(y^n)} - p\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_0(y^n)}} \geq \frac{\bar{p}+p\left(\frac{\alpha}{\bar{\alpha}}\right)^n}{\bar{p}-p\left(\frac{\alpha}{\bar{\alpha}}\right)^n}, \tag{69}$$

with equality if and only if $y^n = \mathbf{0}$. Similarly, if $N_1(y^n) > N_0(y^n)$, then

$$\frac{p\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_0(y^n)} + \bar{p}\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_1(y^n)}}{P(x^n_{y^n},y^n) - P(x^n_{z^n},y^n)} \geq \frac{p\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_0(y^n)} + \bar{p}\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_1(y^n)}}{p\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_0(y^n)} - \bar{p}\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_1(y^n)}},$$

with equality if and only if $N_0(z^n) > N_1(z^n)$. As before,

$$\frac{p\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_0(y^n)} + \bar{p}\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_1(y^n)}}{\bar{p}\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_1(y^n)} - p\bar{\alpha}^n\left(\frac{\alpha}{\bar{\alpha}}\right)^{N_0(y^n)}} \geq \frac{p+\bar{p}\left(\frac{\alpha}{\bar{\alpha}}\right)^n}{p-\bar{p}\left(\frac{\alpha}{\bar{\alpha}}\right)^n}, \tag{70}$$

with equality if and only if $y^n = \mathbf{1}$. From (69) and (70), we conclude that

$$\underline{\hbar}'(\mathsf{P_c}(\theta|Y^n)) = \frac{p+\bar{p}\left(\frac{\alpha}{\bar{\alpha}}\right)^n}{p-\bar{p}\left(\frac{\alpha}{\bar{\alpha}}\right)^n} = \frac{p\bar{\alpha}^n+\bar{p}\alpha^n}{p\bar{\alpha}^n-\bar{p}\alpha^n},$$

and $y_0 = \mathbf{1}$ and $z_0 = \mathbf{0}$ achieve the minimum in (68). From the last part of Theorem 3 the optimality of the 2^n-ary Z-channel $\mathsf{Z}_n(\zeta_n(\varepsilon))$ is evident.

Appendix J
Proof of Theorem 6

From (17) and (18) we obtain that

$$\inf_{f\in\mathcal{S}_U} \frac{\mathsf{mmse}(f(U)|V)}{\mathsf{var}(f(U))} = 1 - \sup_{f\in\mathcal{S}_U} \eta_V^2(f(U)) = 1-\rho_m^2(U,V).$$

From the previous equation it is clear that $\rho_m^2(U,V) \leq \varepsilon$ if and only if

$$\mathsf{mmse}(f(U)|V) \geq (1-\varepsilon)\mathsf{var}(f(U)),$$

for all $f \in \mathcal{S}_U$. By (16), we obtain $Z_\gamma \in \Gamma(\varepsilon)$ if and only if $\rho_m^2(X,Z_\gamma) \leq \varepsilon$.

Appendix K
Proof of Theorem 7

Without loss of generality, assume $\mathbb{E}(X) = \mathbb{E}(Y_\mathsf{G}) = 0$. Since Y_G is Gaussian, (17) implies that

$$\begin{aligned}\mathsf{sENSR}(\varepsilon) &= \inf_{\gamma:\rho_m^2(X,Z_\gamma)\leq\varepsilon} \frac{\mathsf{mmse}(Y_\mathsf{G}|Z_\gamma)}{\mathsf{var}(Y_\mathsf{G})} \\ &= 1 - \sup_{\gamma:\rho_m^2(X,Z_\gamma)\leq\varepsilon} \rho_m^2(Y_\mathsf{G};Z_\gamma). \end{aligned} \tag{71}$$

A straightforward computation leads to

$$\begin{aligned}\rho_m^2(Y_\mathsf{G},Z_\gamma) = \rho^2(Y_\mathsf{G},Z_\gamma) &= \frac{\gamma\mathsf{var}(Y_\mathsf{G})}{1+\gamma\mathsf{var}(Y_\mathsf{G})}, \\ \rho_m^2(X,Z_\gamma) \geq \rho^2(X,Z_\gamma) &= \rho^2(X,Y_\mathsf{G})\rho_m^2(Y_\mathsf{G},Z_\gamma).\end{aligned} \tag{72}$$

The preceding inequality and (71) imply

$$\mathsf{sENSR}(\varepsilon) \geq 1 - \sup_{\gamma:\rho_m^2(X,Z_\gamma)\leq\varepsilon} \frac{\rho_m^2(X,Z_\gamma)}{\rho^2(X,Y_\mathsf{G})} \geq 1 - \frac{\varepsilon}{\rho^2(X,Y_\mathsf{G})},$$

which proves the lower bound.

The strong data processing inequality for maximal correlation [8, Lemma 6] states that $\rho_m^2(X,Z_\gamma) \leq \rho_m^2(X,Y_\mathsf{G})\rho_m^2(Y_\mathsf{G},Z_\gamma)$. In particular, if $\rho_m^2(Y_\mathsf{G},Z_\gamma) \leq \frac{\varepsilon}{\rho_m^2(X,Y)}$, then $\rho_m^2(X,Z_\gamma) \leq \varepsilon$. Therefore, (71) implies

$$\begin{aligned}\mathsf{sENSR}(\varepsilon) &\leq 1 - \sup_{\gamma:\rho_m^2(Y_\mathsf{G},Z_\gamma)\leq\frac{\varepsilon}{\rho_m^2(X,Y_\mathsf{G})}} \rho_m^2(Y_\mathsf{G};Z_\gamma) \\ &= 1 - \frac{\varepsilon}{\rho_m^2(X,Y_\mathsf{G})},\end{aligned}$$

where the last equality follows from the continuity of $\gamma \mapsto \rho_m^2(Y_\mathsf{G},Z_\gamma)$, established in (72), finishing the proof of the upper bound.

Appendix L
Proof of Lemma 2

Let

$$\gamma_\varepsilon^* := \max\{\gamma \geq 0 : \rho_m^2(X_\mathsf{G},Z_\gamma) \leq \varepsilon\}. \tag{73}$$

Recall that

$$\rho_m^2(X,Z_\gamma) \geq \rho^2(X,Z_\gamma) = \frac{\gamma\rho^2(X,Y)\mathsf{var}(Y)}{1+\gamma\mathsf{var}(Y)}. \tag{74}$$

Since $\varepsilon \to 0$, we can assume that $\varepsilon < \rho^2(X,Y)$. Thus, from (74) we obtain

$$\gamma_\varepsilon^* \leq \frac{\varepsilon}{\mathsf{var}(Y)(\rho^2(X,Y)-\varepsilon)}. \tag{75}$$

In particular, $\gamma_\varepsilon^* \to 0$ as $\varepsilon \to 0$. Since $\gamma \mapsto \mathsf{mmse}(Y|Z_\gamma)$ is decreasing, we have that $\mathsf{sENSR}(\varepsilon) = \mathsf{mmse}(Y|Z_{\gamma_\varepsilon^*})$. Therefore, the first-order approximation of $\mathsf{sENSR}(\cdot)$ around zero yields

$$\begin{aligned}\mathsf{sENSR}(\varepsilon) &= 1 + \frac{\gamma_\varepsilon^*}{\mathsf{var}(Y)}\frac{\mathrm{d}}{\mathrm{d}\gamma_\varepsilon^*}\mathsf{mmse}(Y|Z_{\gamma_\varepsilon^*})\Big|_{\varepsilon=0} + o(\gamma_\varepsilon^*) \\ &\overset{(a)}{=} 1 - \mathsf{var}(Y)\gamma_\varepsilon^* + o(\gamma_\varepsilon^*) \\ &\overset{(b)}{\geq} 1 - \frac{\varepsilon}{\rho^2(X,Y)} + o(\varepsilon)\end{aligned}$$

where (a) follows from the fact that $\frac{\mathrm{d}}{\mathrm{d}\gamma}\mathsf{mmse}(Y|Z_\gamma) = -\mathbb{E}[\mathsf{var}^2(Y|Z_\gamma)]$ [42, Prop. 9] and (b) follows from (75).

ACKNOWLEDGMENT

The authors would like to acknowledge two anonymous reviewers for their insightful comments and, in particular, one of them for the derivation in (65). Furthermore, the first author acknowledges useful discussions with M. Médard and F. P. Calmon.

REFERENCES

[1] S. Asoodeh, F. Alajaji, and T. Linder, "Privacy-aware MMSE estimation," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, July 2016, pp. 1989–1993.

[2] S. Asoodeh, M. Diaz, F. Alajaji, and T. Linder, "Privacy-aware guessing efficiency," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, June 2017.

[3] S. Asoodeh, "Information and estimation theoretic approaches to data privacy," Ph.D. dissertation, Queen's University, May 2017.

[4] S. Fehr and S. Berens, "On the conditional Rényi entropy," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6801–6810, Nov. 2014.

[5] S. Arimoto, "Information measures and capacity of order α for discrete memoryless channels," in *Topics in Information Theory, Coll. Math. Soc. J. Bolyai (I. Csiszár and P. Elias Eds.)*, vol. 16. North-Holland, Amsterdam, 1977, pp. 41–52.

[6] I. Csiszár, "Generalized cutoff rates and Rényi's information measures," *IEEE Trans. Inf. Theory*, vol. 41, no. 1, pp. 26–34, Jan. 1995.

[7] S. Verdú, "α-mutual information," in *Proc. Information Theory and Applications Workshop (ITA), 2015*, Feb. 2015, pp. 1–6.

[8] 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

[9] 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.

[10] N. Tishby, F. C. Pereira, and W. Bialek, "The information bottleneck method," in *Proc. of Allerton Conf. Comm. Control and Compiting*, 1999, pp. 368–377.

[11] H. Hsu, S. Asoodeh, S. Salamatian, and F. P. Calmon, "Generalizing bottleneck problems," 2018. [Online]. Available: arXiv:1802.05861v1

[12] I. Issa, S. Kamath, and A. B. Wagner, "An operational measure of information leakage," in *Proc. Annual Conference on Information Science and Systems (CISS)*, March 2016, pp. 234–239.

[13] 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.

[14] 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.

[15] H. O. Hirschfeld, "A connection between correlation and contingency," *Cambridge Philosophical Soc.*, vol. 31, pp. 520–524, 1935.

[16] H. Gebelein, "Das statistische problem der korrelation als variations- und eigenwert-problem und sein zusammenhang mit der ausgleichungsrechnung," *Zeitschrift f ur angew. Math. und Mech.*, no. 21, pp. 364–379, 1941.

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

[18] G. Smith, "On the foundations of quantitative information flow," in *Proc. of the 12th Int. Conf. on Foundations of Software Science and Computational Structures*, ser. FOSSACS '09. Berlin, Heidelberg: Springer-Verlag, 2009.

[19] A. V. Evfimievski, J. Gehrke, and R. Srikant, "Limiting privacy breaches in privacy preserving data mining," in *Proc. of the Twenty-Second Symposium on Principles of Database Systems*, 2003, pp. 211–222.

[20] J. L. Massey, "Guessing and entropy," in *Proc. IEEE Int. Symp. Inf. Theory*, June 1994, pp. 204–205.

[21] C. Braun, K. Chatzikokolakis, and C. Palamidessi, "Quantitative notions of leakage for one-try attacks," *Electronic Notes in Theoretical Computer Science*, vol. 249, pp. 75 – 91, 2009.

[22] G. Barthe and B. Kopf, "Information-theoretic bounds for differentially private mechanisms," in *Proc. IEEE 24th Computer Security Foundations Symposium*, June 2011, pp. 191–204.

[23] C. Dwork, "Differential privacy: a survey of results," *Lecture Notes in Computer Science, Theory and Applications of Models of Computation,*, no. 4978, pp. 1–19, 2008.

[24] R. Sibson, "Information radius," *Z. Wahrscheinlichkeitsth. Verw. Geb.*, vol. 14, pp. 149–161, 1969.

[25] A. Makhdoumi and N. Fawaz, "Privacy-utility tradeoff under statistical uncertainty," in *Proc. 51st Allerton Conference on Communication, Control, and Computing*, Oct 2013, pp. 1627–1634.

[26] F. P. Calmon, A. Makhdoumi, M. Médard, M. Varia, M. Christiansen, and K. R. Duffy, "Principal inertia components and applications," *IEEE Trans. Inf. Theory*, vol. 63, no. 8, pp. 5011–5038, May 2017.

[27] I. Wagner and D. Eckhoff, "Technical Privacy Metrics: a Systematic Survey," *ArXiv e-prints*, Dec. 2015. [Online]. Available: http://arxiv.org/abs/1512.00327

[28] 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.

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

[30] 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.

[31] L. Sankar, S. R. Rajagopalan, and S. Mohajer, "Smart meter privacy: A theoretical framework," *IEEE Trans. on Smart Grid*, vol. 4, no. 2, pp. 837–846, June 2013.

[32] J. Liao, L. Sankar, F. P. Calmon, and V. Y. Tan, "Hypothesis testing under maximal leakage privacy constraints," in *Proc. IEEE Int. Sym. on Inf. Theory (ISIT)*, June 2017.

[33] J. Liao, L. Sankar, V. Y. Tan, and F. P. Calmon, "Hypothesis testing under mutual information privacy constraints in the high privacy regime," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 4, pp. 1058–1071, April 2018.

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

[35] H. Witsenhausen and A. Wyner, "A conditional entropy bound for a pair of discrete random variables," *IEEE Trans. Inf. Theory*, vol. 21, no. 5, pp. 493–501, Sep. 1975.

[36] T. Berger and R. Yeung, "Multiterminal source encoding with encoder breakdown," *IEEE Trans. Inf. Theory*, vol. 35, no. 2, pp. 237–244, March 1989.

[37] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, "Privacy aware learning," *Journal of the Association for Computing Machinery (ACM)*, vol. 61, no. 6, Dec. 2014.

[38] O. Sarmanov, "The maximum correlation coefficient (nonsymmetric case)," *Dokl. Akad. Nauk SSSR*, vol. 120, no. 4, pp. 715–718, 1958.

[39] F. P. Calmon, "Information-theoretic metrics for security and privacy," Ph.D. dissertation, MIT, Sep. 2015.

[40] N. Papadatos and T. Xifara, "A simple method for obtaining the maximal correlation coefficient and related characterizations," *Journal of Multivariate Analysis*, vol. 118, pp. 102–114, 2013.

[41] W. Kang and S. Ulukus, "A new data processing inequality and its applications in distributed source and channel coding," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 56–69, Jan. 2011.

[42] D. Guo, Y. Wu, S. Shamai, and S. Verdú, "Estimation in Gaussian noise: properties of the minimum mean-square error," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2371–2385, April 2011.

[43] W. Bryc, A. Dembo, and A. Kagan, "On the maximum correlation coefficient," *Theory Probab. Appl.*, vol. 49, no. 1, pp. 132–138, Mar. 2005.

[44] 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.