Guessing Attacks on Distributed-Storage Systems

Annina Bracher, Eran Hof, and Amos Lapidoth, *Fellow, IEEE*

***Abstract*— The secrecy of a distributed-storage system for passwords is studied. The encoder, Alice, observes a length-n password and describes it using two hints, which she stores in different locations. The legitimate receiver, Bob, observes both hints and the eavesdropper, Eve, only one. In one scenario—the "guessing version"—we require that the expected number of guesses it takes Bob to guess the password approach one as n tends to infinity, and in the second—the "listsize version"—that the expected size of the shortest list that Bob must form to guarantee that it contain the password approach one. Assuming that Alice cannot control which hint Eve observes, the largest normalized (by n) exponent that can be guaranteed for the expected number of guesses it takes Eve to guess the password is characterized for each scenario. Key to the proof are new results on Massey–Arikan guessing, Bunte–Lapidoth task-encoding, and the close relation between them. A generalization that allows for Alice to produce δ (not necessarily two) hints, for Bob to observe ν (not necessarily two) of the hints, and for Eve to observe η (not necessarily one) of the hints is also discussed. This models scenarios where hints are stored on fail-prone disks.**

***Index Terms*— Secure storage, distributed storage, Rényi entropy, guessing, task-encoding.**

I. Introduction

SUPPOSE that some sensitive information X (e.g., a secret task or a password)[1] is drawn from a finite set $\mathcal{X}$ according to some probability mass function (PMF) P_X. A (stochastic) encoder, Alice, maps (possibly using randomization) X to two hints M_1 and M_2 and stores them on different storage systems (e.g., on two disks in two different locations). The hints are intended for a legitimate receiver, Bob, who knows where they are stored and sees both. An eavesdropper, Eve, sees one of the hints but not both; we do not know which. We adopt a conservative approach to the question of which hint is revealed to Eve and assume that, after observing X, an adversarial "genie" reveals to Eve the hint that minimizes her ambiguity. Not allowing the genie to observe X would lead to a weaker form of secrecy (Example 18). Given some notion of ambiguity, we would ideally like Bob's ambiguity about X to be small and Eve's large. Here we study the security gain from the distribution of the sensitive information to two hints in terms of this ambiguity.

There are several ways to define ambiguity. One approach is to require that Bob be able to reconstruct X whenever X is "typical" and that the conditional entropy of X given Eve's observation be large. Such an approach might be unsuitable in some scenarios. First, it may not properly address Bob's needs when X is "atypical." For example, if Bob must guess X, this approach does not guarantee that the expected number of guesses be small: It only guarantees that the probability of success after one guess be large. It does not indicate the number of guesses that Bob might need when X is atypical. Second, conditional entropy need not be an adequate measure of Eve's ambiguity. For example, if X is some password that Eve wishes to uncover, then we may care more about the number of guesses that Eve needs to uncover X than about its conditional entropy [3].

In this paper, we assume that Eve wants to guess X with the minimal number of guesses of the form "Is X = x?". We quantify Eve's ambiguity about X by the expected number of guesses she needs to uncover X. In this sense, Eve faces an instance of the Massey–Arikan guessing problem [4], [5]: When faced with the problem of guessing X after observing that $Z = z$, where Z denotes her observation, Eve must come up with a guessing order for the elements of $\mathcal{X}$. Such an order can be specified using a "guessing function"—a bijective function $G(\cdot|z)$ from $\mathcal{X}$ onto the set $\{1, \ldots, |\mathcal{X}|\}$—with the understanding that if Eve observes z, then the question "Is $X = x$?" will be her $G(x|z)$-th question. Eve's expected number of guesses is then $\mathbb{E}\big[G(X|Z)\big]$. This expectation is minimized if for each $z \in \mathcal{Z}$ the guessing function $G(\cdot|z)$ orders the elements of $\mathcal{X}$ in decreasing order of their posterior probabilities given $Z = z$.

As to Bob, we will consider two different criteria: In the "guessing version" the criterion is the expected number of guesses it takes Bob to guess X, and in the "list version" the criterion is the expected size of the list that Bob must form to guarantee that it contain X.

The former criterion is natural when Bob can check whether a guess is correct: If X is some password, then Bob can stop guessing as soon as he has gained access to the account that is secured by X. The latter criterion is appropriate if Bob does not know whether a guess is correct. For example, if X is a task that Bob must perform, then the only way for Bob to make sure that he performs X is to perform all the tasks in the list $\mathcal{L}_{M_1,M_2}$ comprising the tasks having positive posterior probability given his observation. In this scenario, a good

Manuscript received December 11, 2016; revised July 2, 2019; accepted July 7, 2019. Date of publication August 5, 2019; date of current version October 18, 2019. This article was presented in part at the 2014 IEEE Information Theory Workshop (ITW), and in part at the 2015 IEEE International Symposium on Information Theory (ISIT).

A. Bracher was with the Department of Information Technology and Electrical Engineering, ETH Zurich, 8092 Zürich, Switzerland. She is now with Swiss Re, 8002 Zürich, Switzerland (e-mail: annina.bracher@gmail.com).

E. Hof was with the R&D Center, Ramat-Gan 5251003, Israel. He is now with Qualcomm Israel, Haifa 39210, Israel (e-mail: eran.hof@gmail.com).

A. Lapidoth is with the Department of Information Technology and Electrical Engineering, ETH Zurich, 8092 Zürich, Switzerland (e-mail: lapidoth@isi.ee.ethz.ch).

Communicated by M. R. Bloch, Associate Editor for Shannon Theory.

Digital Object Identifier 10.1109/TIT.2019.2933000

[1]Though password is just an example of a sensitive information, secure management of passwords as some publications suggest, may be far from trivial, see e.g. [1], [2].

measure for Bob's ambiguity about X is the expected number of tasks that he must perform, i.e., $\mathbb{E}\big[|\mathcal{L}_{M_1,M_2}|\big]$, and this will be small whenever Alice is a good task-encoder for Bob [6].[2]

Alternatively, the list-size criterion can also be viewed as a worst-case version of the guessing criterion: Even if Bob is incognizant of the PMF of X, the number of guesses he needs to guess X cannot exceed the size of the smallest list that is guaranteed to contain X.

The guessing and the list-size criterion for Bob lead to similar results in the following sense: Every guessing function $G(\cdot|M_1, M_2)$ for X that guesses the elements of $\mathcal{X}$ of zero posterior probability only after those of positive posterior probabilities satisfies $\mathbb{E}\big[G(X|M_1, M_2)\big] \leq \mathbb{E}\big[|\mathcal{L}_{M_1,M_2}|\big]$. Conversely, one can prove that every pair of ambiguities for Bob and Eve that is achievable in the guessing version is—up to polylogarithmic factors of $|\mathcal{X}|$—also achievable in the list version (Remark 17). These polylogarithmic factors wash out in the asymptotic regime where the sensitive information is an n-tuple and n tends to infinity.

Things are different for Eve: Applying the list-size criterion for Eve would lead to results that differ markedly from those that apply under the guessing criterion; see Theorem 19 and the subsequent discussion.

To derive our results, we establish new results on guessing and task-encoding: We relate task-encoders to guessing functions (Theorem 8), and we quantify how additional side information can help guessing (Lemma 5). These results may be of interest in their own right. For example, the former result leads to alternative proofs of Bunte and Lapidoth's asymptotic task-encoding results [6, Theorems I.2 and VI.2] as well as the direct part of [10, Theorem I.1], which states that, in the presence of feedback, the listsize capacity of a discrete-memoryless channel (DMC) with positive zero-error capacity equals the cutoff rate with feedback (which is in fact equal to that without feedback [10, Corollary I.4]). The latter result on how additional side information can help guessing is related to [11]: To quantify how additional side information can help guessing, we establish how an encoder must describe X to minimize the expected number of guesses that a decoder needs to guess X. The list-size analog is Lapidoth and Pfister's optimal task-encoder [11], which describes X to minimize the expected size of the decoder's list. Despite the close relation between task-encoding and guessing, an optimal encoder for a guessing decoder is typically quite different from an optimal task-encoder.

We also generalize our problem in two different directions. The first, along the lines of [6], [12], is a rate-distortion version of the model in which Bob and Eve are content with reconstructing the sensitive information to within some given allowed distortion. This generalization is presented in [13], where we also extend the results on guessing and task-encoding of Section III accordingly. The second considers the case in which Alice produces δ s-bit hints, Bob sees $\nu \leq \delta$ hints, and Eve sees $\eta < \nu$ hints (not necessarily a subset of those that Bob sees). This may model a scenario in which the hints are stored on different disks and we want to guarantee robustness against the failure of $\delta - \nu$ disks and the compromise of η disks. We adopt again a conservative approach and assume that, after observing X, an adversarial genie reveals to Bob the ν hints that maximize his ambiguity and to Eve the η hints that minimize her ambiguity. This guarantees that—no matter which disks fail—the model be robust against the failure of $\delta - \nu$ disks and the compromise of η disks. The generalized problem models a distributed-storage system, which is static in that failed disks are not replaced.

The case where X is drawn uniformly, Bob must reconstruct X, and Eve's observation must satisfy some information-theoretic security criterion (e.g., that the mutual information between Eve's observation and X must be null) corresponds to the erasure-erasure wiretap channel studied in [14] and is a special case of the wiretap networks in [15], [16]. In the literature, this setting is also known as "secret sharing." In traditional secret sharing, each set of hints either reveals X or reveals no information about X [17], [18]. More general are ramp schemes, in which any ν hints reveal X and the amount of information that fewer-than-ν hints reveal is controlled (see e.g. [19]). Our setting is different in that we assume $X \sim P_X$ and in that, using some notion of ambiguity, we quantify how difficult it is for Bob and Eve to reconstruct X.

To better bring out the role of Rényi entropy, we generalize the models and replace expectations with ρ-th moments. (The generalization comes with no extra effort.) For an arbitrary $\rho > 0$, we thus study the ρ-th (instead of the first) moment of the list-size and of the number of guesses. Moreover, we shall allow some side information Y that is available to all parties.

The connection between Rényi entropy and the asymptotics of the ρ-th moment of the minimal number of guesses has been studied extensively in the literature [5], [12], [20]–[25]. These moments are related to the moment-generating function of the logarithm of the minimal number of required guesses, and one would therefore expect that they be related to the large-deviations behavior of this logarithm. Since the Rényi entropy is only related to the *asymptotics* of these moments, establishing the large-deviations behavior requires some work. This program was carried out in [23], where, subject to some technical assumptions, the large-deviations principle for the guessing problem was established. This large-deviation result suggests asymptotic approximations for the tail behavior of the logarithm of the number of guesses.

Carrying out this program for our problem is tricky. The large-deviations result of [23] hinges on the guessing being performed in decreasing order of probabilities. It is not clear what is the "canonical" scheme one would wish to analyze for our setting. (For task-encoding the optimal scheme was described in [11], and for guessing with side information it is described in Figure 1 ahead.) Moreover, the conservative ambiguity measure that we adopt for Eve (54) allows the hint that is revealed to Eve to depend on the realization of X. This ambiguity measure is therefore not a simple ρ-th moment. As such it does not translate to the moment-generating function of a quantity that is natural to the problem.

[2]The connection between the Massey–Arikan guessing problem and the task-encoding problem is studied in [7]. There it is clarified why the answers are so similar. However, as noted in [8] and [9], the problems have completely different answers in the distributed setting.

The idea to quantify Eve's ambiguity by the ρ-th moment of the number of guesses she needs to uncover X is due to Merhav and Arikan, who studied the Shannon cipher system with a guessing wiretapper [3]. Their approach was later adopted in [26], [27]. The current setting differs from the ones in [3], [26], [27] in the following sense: Instead of mapping X to a public message using a secret key, which is available to Bob but not to Eve, here Alice produces two hints and stores them so that Bob sees both but Eve sees only one. Moreover, unlike [3], [26], [27] we do not measure Bob's ambiguity in terms of the probability that X is not his first guess.

The rest of this paper is structured as follows. Section II briefly describes our notation and summarizes some notions and results pertaining to the guessing problem and the problem of encoding tasks. In Section III, we quantify how additional side information can help guessing and relate task-encoders to guessing functions, thereby establishing the prerequisites for the proofs of our main results. Section IV contains the problem statement and the main results (both finite-blocklength and asymptotic). The results are discussed in Section V and proved in Section VI. Section VII generalizes the model to allow for a limited number of disk failures. Section VIII concludes the paper.

II. Notation and Preliminaries

In this paper (X, Y) is a pair of chance variables that is drawn from the finite set $\mathcal{X} \times \mathcal{Y}$ according to the PMF $P_{X,Y}$, and $\rho > 0$ is fixed. We denote by P_X the marginal PMF of X and by P_Y the marginal PMF of Y, e.g.,

$$P_X(x) = \sum_{y \in \mathcal{Y}} P_{X,Y}(x, y), \quad \forall\, x \in \mathcal{X}. \tag{1}$$

For every positive integer $n \in \mathbb{N}$ we denote by $P_{X,Y}^n$ the n-fold product of $P_{X,Y}$, i.e.,

$$P_{X,Y}^n(\mathbf{x}, \mathbf{y}) = \prod_{i=1}^{n} P_{X,Y}(x_i, y_i), \quad \forall\, (\mathbf{x}, \mathbf{y}) \in \mathcal{X}^n \times \mathcal{Y}^n. \tag{2}$$

A generic probability measure on a measurable space $(\Omega, \mathcal{F})$ is denoted $\mathbb{P}$, i.e., whenever we introduce a set of chance variables (e.g., X and Y), we denote by $\mathbb{P}$ the probability measure associated with the probability space $(\Omega, \mathcal{F}, \mathbb{P})$ on which the chance variables live.

We denote the set of positive integers $\mathbb{N}$, the integers $\mathbb{Z}$, and the reals $\mathbb{R}$. The nonnegative reals are denoted $\mathbb{R}_0^+$. Addition modulo k (for $k \in \mathbb{N}$) is denoted $\oplus_k$: If α and β are integers, then $\alpha \oplus_k \beta$ is the unique element $\gamma \in \{0, \ldots, k-1\}$ satisfying

$$\gamma \equiv \alpha + \beta \mod k. \tag{3}$$

We denote the Galois field with q elements by $\mathbb{F}_q$. By default $\log(\cdot)$ denotes base-2 logarithm, and $\ln(\cdot)$ denotes natural logarithm. We denote by $\alpha \vee \beta$ the maximum of two real numbers α and β and by $\alpha \wedge \beta$ their minimum. For any $\alpha \in \mathbb{R}$, we use $[\alpha]^+$ for the maximum of α and zero,

$$[\alpha]^+ = \alpha \vee 0 \tag{4}$$

$\lceil \alpha \rceil$ for the smallest integer that is at least as large as α, and $\lfloor \alpha \rfloor$ for the largest integer that is at most as large as α. We sometimes use the identity

$$\lceil \xi \rceil^\rho < 1 + 2^\rho \xi^\rho, \quad \xi \in \mathbb{R}_0^+ \tag{5}$$

which can be verified by considering the cases $0 \le \xi \le 1$ and $\xi > 1$ separately [6].

A. The Conditional Rényi Entropy

To describe our results, we shall need the conditional version of Rényi entropy (originally proposed by Arimoto [28] and also studied in [6], [29])

$$H_\alpha(X|Y) = \frac{\alpha}{1-\alpha} \log \sum_{y \in \mathcal{Y}} \left(\sum_{x \in \mathcal{X}} P_{X,Y}(x, y)^\alpha \right)^{1/\alpha} \tag{6}$$

where $\alpha \in [0, \infty]$ is the order and where the cases where α is 0, 1, or ∞ are treated by a limiting argument. Let $\{(X_i, Y_i)\}_{i \in \mathbb{N}}$ be a discrete-time stochastic process with finite alphabet $\mathcal{X} \times \mathcal{Y}$. Whenever the limit as n tends to infinity of $H_\alpha(X^n|Y^n)/n$ exists, we denote it by $H_\alpha(\boldsymbol{X}|\boldsymbol{Y})$ and call it conditional Rényi entropy-rate. In this paper α will equal $1/(1+\rho)$, and thus, since $\rho > 0$, will take values in the set $(0, 1)$. To simplify notation, we henceforth write $\tilde{\rho}$ for $1/(1+\rho)$

$$\tilde{\rho} \triangleq \frac{1}{1+\rho}. \tag{7}$$

The conditional Rényi entropy satisfies the following properties (see, e.g. [29, Theorem 2]).

Lemma 1: Let (X, Y, Z) be a triple of chance variables taking values in the finite set $\mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ according to the joint PMF $P_{X,Y,Z}$. For every $\alpha \in [0, \infty]$

$$H_\alpha(X|Y) \le H_\alpha(X, Z|Y). \tag{8}$$

Lemma 2 ([29, Theorem 3]): Let (X, Y, Z) be a triple of chance variables taking values in the finite set $\mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ according to the joint PMF $P_{X,Y,Z}$. For every $\alpha \in [0, \infty]$

$$H_\alpha(X|Y, Z) \ge H_\alpha(X, Z|Y) - \log|\mathcal{Z}|. \tag{9}$$

B. Optimal Guessing Functions and Task-Encoders

Suppose we want to guess X with guesses of the form "Is $X = x$?". Following the notation of [5], we call a bijection $G\colon \mathcal{X} \to \{1, \ldots, |\mathcal{X}|\}$ a *guessing function* for X. The guessing function determines the guessing order: If we use $G(\cdot)$ to guess X, then the question "Is $X = x$?" will be our $G(x)$-th question. With a slight abuse of the term "function," we call $G(\cdot|Y)$ a guessing function for X given Y if the mapping $G(\cdot|y)\colon \mathcal{X} \to \{1, \ldots, |\mathcal{X}|\}$ is for every $y \in \mathcal{Y}$ a guessing function for X. If we use $G(\cdot|Y)$ to guess X from the observation Y and observe that $Y = y$, then the question "Is $X = x$?" will be our $G(x|y)$-th question.

In the following we shall consider guessing functions for X given Y. Since every guessing function for X can be viewed as a guessing function for X given Y for the case where Y is null, the results also apply to guessing functions for X.

The performance of a guessing function is studied in terms of the ρ-th moment of the number of guesses that we need to guess X when we use that function. That is, the expectation $\mathbb{E}\big[G(X|Y)^\rho\big]$ is the performance of $G(\cdot|Y)$. We can use Arikan's results on guessing [5] (see also subsequent work in [23], [24]) to bound the performance of optimal guessing functions.

Theorem 3 (On the Performance of Optimal Guessing Functions [5, Theorem 1 and Proposition 4]): There exists some guessing function $G(\cdot|Y)$ for which

$$\mathbb{E}\big[G(X|Y)^\rho\big] \le 2^{\rho H_{\tilde{p}}(X|Y)}. \tag{10}$$

Conversely, for every guessing function $G(\cdot|Y)$

$$\mathbb{E}\big[G(X|Y)^\rho\big] \ge \big(1+\ln|\mathcal{X}|\big)^{-\rho} 2^{\rho H_{\tilde{p}}(X|Y)} \vee 1. \tag{11}$$

For task-encoders we adopt the terminology of [6]. Given some finite set of descriptions $\mathcal{Z}$, we call a mapping $f\colon \mathcal{X} \to \mathcal{Z}$ a *task-encoder* for X. We associate every task-encoder with a decoder of the form

$$\begin{aligned} f^{-1}\colon \mathcal{Z} &\to 2^{\mathcal{X}} \\ z &\mapsto \big\{x \in \mathcal{X}\colon P_X(x) > 0 \text{ and } f(x) = z\big\}. \end{aligned} \tag{12}$$

If the encoder describes X by $Z \triangleq f(X)$, then the list $\mathcal{L}_Z \triangleq f^{-1}(Z)$ produced by the decoder is the list containing all the realizations of X of positive a priori probability that the encoder could have described by Z. (This is the shortest list that is almost-surely guaranteed to contain X given its description Z.)

Consider now the scenario where some side information Y is revealed to the encoder and decoder [6, Section VI]. In this scenario we call $f(\cdot|Y)$ a task-encoder for X given Y if the mapping $f(\cdot|y)\colon \mathcal{X} \to \mathcal{Z}$ is for every $y \in \mathcal{Y}$ a task-encoder for X. We associate every task-encoder with a decoder $f^{-1}(\cdot|Y)$ satisfying for every $y \in \mathcal{Y}$ that $f^{-1}(\cdot|y)$ is of the form (12), i.e., that

$$\begin{aligned} f^{-1}(\cdot|y)\colon \mathcal{Z} &\to 2^{\mathcal{X}} \\ z &\mapsto \big\{x \in \mathcal{X}\colon P_{X|Y}(x|y) > 0 \text{ and } f(x|y) = z\big\}. \end{aligned} \tag{13}$$

If, upon observing Y, the encoder describes X by $Z \triangleq f(X|Y)$, then the list $\mathcal{L}_Z^Y \triangleq f^{-1}(Z|Y)$ produced by the decoder is the list containing all the realizations of X that—given the side information Y—have a positive posterior probability under $P_{X|Y}$ and that the encoder could have described by Z.

In the following we shall consider task-encoders for X given Y. Since every task-encoder for X can be viewed as a task-encoder for X given Y for the case where Y is null, the results also apply to task-encoders for X.

We shall also need the notion of a *stochastic task-encoder*. Such an encoder associates with every possible realization $(x, y) \in \mathcal{X} \times \mathcal{Y}$ of the pair (X, Y) a PMF on $\mathcal{Z}$ and, upon observing the side information y, describes x by drawing Z from $\mathcal{Z}$ according to the PMF associated with (x, y). The conditional probability that $Z = z$ given $(X, Y) = (x, y)$ is thus determined by the stochastic encoder, and we denote it by

$$\mathbb{P}[Z = z|X = x, Y = y], \quad (x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}. \tag{14}$$

Based on (Y, Z) the decoder associated with the encoder (14) produces the smallest list $\mathcal{L}_Z^Y$ that is guaranteed to contain X, i.e., if $(Y, Z) = (y, z)$, then the decoder produces the list

$$\mathcal{L}_z^y = \big\{x \in \mathcal{X}\colon \mathbb{P}[X = x|Y = y, Z = z] > 0\big\}, \quad (y, z) \in \mathcal{Y} \times \mathcal{Z} \tag{15}$$

of all the possible realizations $x \in \mathcal{X}$ of X of positive posterior probability

$$\begin{aligned} &\mathbb{P}[X = x|Y = y, Z = z] \\ &\quad = \frac{P_{X,Y}(x, y)\,\mathbb{P}[Z = z|X = x, Y = y]}{\sum_{\tilde{x}\in\mathcal{X}} P_{X,Y}(\tilde{x}, y)\,\mathbb{P}[Z = z|X = \tilde{x}, Y = y]}. \end{aligned} \tag{16}$$

We assess the performance of a task-encoder in terms of the ρ-th moment $\mathbb{E}\big[|\mathcal{L}_Z^Y|^\rho\big]$ of the size of the list that the associated decoder must form. As we argue shortly, deterministic task-encoders are optimal in the sense that for every stochastic task-encoder there exists a deterministic task-encoder that performs at least as well. Therefore, we can use Bunte and Lapidoth's results on deterministic task-encoders [6] to bound the performance of optimal stochastic task-encoders.

Theorem 4 (On the Performance of the Optimal Task-Encoders [6, Theorem VI.1]): Let $\mathcal{Z}$ be a finite set. If $|\mathcal{Z}| > \log|\mathcal{X}| + 2$, then there exists a deterministic task-encoder $f(\cdot|Y)$ for which

$$\mathbb{E}\Big[\big|\mathcal{L}_Z^Y\big|^\rho\Big] = \mathbb{E}\Big[\big|f^{-1}\big(f(X|Y)\big|Y\big)\big|^\rho\Big] \tag{17}$$

$$< 1 + 2^{\rho(H_{\tilde{p}}(X|Y) - \log(|\mathcal{Z}| - \log|\mathcal{X}| - 2) + 2)}. \tag{18}$$

Conversely, given any stochastic task-encoder (14), the associated decoding lists $\{\mathcal{L}_z^y\}$ (15) satisfy

$$\mathbb{E}\Big[\big|\mathcal{L}_Z^Y\big|^\rho\Big] \ge 2^{\rho(H_{\tilde{p}}(X|Y) - \log|\mathcal{Z}|)} \vee 1. \tag{19}$$

We conclude this section by showing that for every stochastic task-encoder there exists a deterministic task-encoder that performs at least as well. Given a stochastic task-encoder (14) with associated decoding lists (15), we can construct a deterministic task-encoder $f(\cdot|Y)$ as follows. If $(x, y) \in \mathcal{X}\times\mathcal{Y}$ satisfies $P_{X|Y}(x|y) > 0$, then we choose $f(x|y)$ as one that—among all elements of $\{z \in \mathcal{Z}\colon x \in \mathcal{L}_z^y\}$—minimizes $|\mathcal{L}_z^y|$, so

$$f(x|y) \in \operatorname*{argmin}_{z\in\mathcal{Z}\colon x\in\mathcal{L}_z^y} |\mathcal{L}_z^y|. \tag{20}$$

Otherwise, we choose $f(x|y)$ to be an arbitrary element of $\mathcal{Z}$. It then follows from (13) that the deterministic task-encoder performs at least as well as the stochastic task-encoder:

$$\begin{aligned} &\mathbb{E}\Big[\big|\mathcal{L}_Z^Y\big|^\rho\Big] \\ &= \sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}} \sum_{z\in\mathcal{Z}} P_{X,Y}(x, y)\,\mathbb{P}[Z = z|X = x, Y = y]|\mathcal{L}_z^y|^\rho \end{aligned} \tag{21}$$

$$\begin{aligned} &\ge \sum_{\substack{(x,y)\in\mathcal{X}\times\mathcal{Y}\colon \\ P_{X,Y}(x,y)>0}} \sum_{z\in\mathcal{Z}} P_{X,Y}(x, y)\,\mathbb{P}[Z = z|X = x, Y = y] \\ &\qquad \cdot \min_{z'\in\mathcal{Z}\colon x\in\mathcal{L}_{z'}^y} |\mathcal{L}_{z'}^y|^\rho \end{aligned} \tag{22}$$

$$= \sum_{\substack{(x,y)\in\mathcal{X}\times\mathcal{Y}\colon \\ P_{X,Y}(x,y)>0}} P_{X,Y}(x, y) \min_{z'\in\mathcal{Z}\colon x\in\mathcal{L}_{z'}^y} |\mathcal{L}_{z'}^y|^\rho \tag{23}$$

$$= \sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}} P_{X,Y}(x,y)\left|\mathcal{L}^y_{f(x|y)}\right|^\rho \tag{24}$$

$$\overset{(a)}{\geq} \sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}} P_{X,Y}(x,y)\left|f^{-1}\big(f(x|y)\big|y\big)\right|^\rho \tag{25}$$

$$= \mathbb{E}\Big[\left|f^{-1}\big(f(X|Y)\big|Y\big)\right|^\rho\Big] \tag{26}$$

where (a) holds because (13) and (20) imply that $f^{-1}\big(f(x|y)|y\big) \subseteq \mathcal{L}^y_{f(x|y)}$.

III. Lists and Guesses

In this section we relate task-encoders to guessing functions and explain why the performance guarantees for optimal guessing functions (Theorem 3) and task-encoders (Theorem 4) are remarkably similar. Moreover, we quantify how additional side information can help guessing. We shall need these results to characterize the secrecy of the distributed-storage systems we study in the present paper, but they may also be of independent interest.

We start by quantifying how some additional information Z (e.g., some description produced by an encoder) can help guessing. As the following lemma shows, Z can reduce the ρ-th moment of the number of guesses by at most a factor of $\left|\mathcal{Z}^{-\rho}\right|$.

Lemma 5 [7]: Given a finite set $\mathcal{Z}$, draw Z from $\mathcal{Z}$ according to some conditional PMF $P_{Z|X,Y}$, so $(X,Y,Z) \sim P_{X,Y}\cdot P_{Z|X,Y}$. For optimal guessing functions $G^\star(\cdot|Y,Z)$ and $G^\star(\cdot|Y)$ (which minimize $\mathbb{E}\big[G(X|Y,Z)^\rho\big]$ and $\mathbb{E}\big[G(X|Y)^\rho\big]$, respectively)

$$\mathbb{E}\big[G^\star(X|Y,Z)^\rho\big] \geq \mathbb{E}\Big[\Big\lceil G^\star(X|Y)/\left|\mathcal{Z}\right|\Big\rceil^\rho\Big]. \tag{27}$$

Equality holds whenever $Z = f(X,Y)$ for some mapping $f\colon \mathcal{X}\times\mathcal{Y}\to\mathcal{Z}$ for which $f(x,y) = f(\tilde{x},y)$ for $x \neq \tilde{x}$ implies that $\big\lceil G^\star(x|y)/|\mathcal{Z}|\big\rceil \neq \big\lceil G^\star(\tilde{x}|y)/|\mathcal{Z}|\big\rceil$. Such a mapping always exists, because for all $\ell\in\mathbb{N}$ at most $|\mathcal{Z}|$ different $x\in\mathcal{X}$ satisfy $\big\lceil G^\star(x|y)/|\mathcal{Z}|\big\rceil = \ell$.

One can infer from Lemma 5 how to construct an optimal encoder $f\colon \mathcal{X}\times\mathcal{Y}\to\mathcal{Z}$ for a guessing decoder, i.e., an encoder $Z = f(X,Y)$ that achieves $\min_{G(\cdot|Y,Z)}\mathbb{E}\big[G(X|Y,Z)^\rho\big]$ among all the possible descriptions Z that are drawn from $\mathcal{Z}$ according to some conditional PMF $P_{Z|X,Y}$. To that end recall that a guessing function $G(\cdot|Y)$ is optimal, i.e., minimizes $\mathbb{E}\big[G(X|Y)^\rho\big]$, if, and only if, for every $y\in\mathcal{Y}$ $G(\cdot|y)$ orders the possible realizations of X in decreasing order of their posterior probabilities given $Y=y$. An optimal encoder $f\colon\mathcal{X}\times\mathcal{Y}\to\mathcal{Z}$ for a guessing decoder can be constructed as follows: For every $y\in\mathcal{Y}$ we first order the possible realizations of X in decreasing order of $P_{X,Y}(x,y)$ or, equivalently, in decreasing order of their posterior probabilities given $Y=y$, and we let x^y_j denote the j-th element. (Ties are resolved at will.) We then choose some mapping $f\colon\mathcal{X}\times\mathcal{Y}\to\mathcal{Z}$ for which $f(x^y_j,y) = f(x^y_{j'},y)$ implies either $\big\lceil j/|\mathcal{Z}|\big\rceil \neq \big\lceil j'/|\mathcal{Z}|\big\rceil$ or $j=j'$, e.g., by indexing the elements of $\mathcal{Z}$ by the elements of $\big\{0,\dots,|\mathcal{Z}|-1\big\}$ and choosing $f(x^y_j,y)$ as the element of $\mathcal{Z}$ indexed by the remainder of the Euclidean division of $j-1$ by $|\mathcal{Z}|$ (see Figure 1).

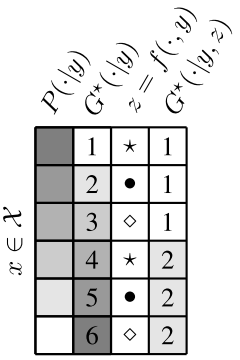

Fig. 1. How to construct an optimal encoder $f\colon\mathcal{X}\times\mathcal{Y}\to\mathcal{Z}$ for a guessing decoder when $\mathcal{Z}=\{\star,\bullet,\diamond\}$. Light background tones indicate small values of $P(\cdot|y)$ or $G^\star(\cdot|y)$.

Lemma 5 and (5) imply the following corollary.

Corollary 6: Given a finite set $\mathcal{Z}$, there exists some mapping $f\colon\mathcal{X}\times\mathcal{Y}\to\mathcal{Z}$ such that

$$\min_{G(\cdot|Y,Z)}\mathbb{E}\big[G(X|Y,Z)^\rho\big] < 1 + 2^\rho|\mathcal{Z}|^{-\rho}\min_{G(\cdot|Y)}\mathbb{E}\big[G(X|Y)^\rho\big] \tag{28}$$

where Z denotes $f(X,Y)$. Conversely, for every chance variable Z that takes values in $\mathcal{Z}$

$$\min_{G(\cdot|Y,Z)}\mathbb{E}\big[G(X|Y,Z)^\rho\big] \geq |\mathcal{Z}|^{-\rho}\min_{G(\cdot|Y)}\mathbb{E}\big[G(X|Y)^\rho\big] \vee 1. \tag{29}$$

From Corollary 6 and Theorem 3, which characterizes the performance of optimal guessing functions $G(\cdot|Y)$, we obtain the following upper and lower bounds on the smallest ambiguity $\min_{G(\cdot|Y,Z)}\mathbb{E}\big[G(X|Y,Z)^\rho\big]$ that is achievable for a given $|\mathcal{Z}|$. The bounds are tight up to polylogarithmic factors of $|\mathcal{X}|$.

Corollary 7: Given a finite set $\mathcal{Z}$, there exists some mapping $f\colon\mathcal{X}\times\mathcal{Y}\to\mathcal{Z}$ for which

$$\min_{G(\cdot|Y,Z)}\mathbb{E}\big[G(X|Y,Z)^\rho\big] < 1 + 2^{\rho(H_{\tilde{\rho}}(X|Y)-\log|\mathcal{Z}|+1)} \tag{30}$$

where Z denotes $f(X,Y)$. Conversely, for every chance variable Z that takes values in $\mathcal{Z}$

$$\min_{G(\cdot|Y,Z)}\mathbb{E}\big[G(X|Y,Z)^\rho\big] \geq \big(1+\ln|\mathcal{X}|\big)^{-\rho}2^{\rho(H_{\tilde{\rho}}(X|Y)-\log|\mathcal{Z}|)} \vee 1. \tag{31}$$

Note that (31) also follows from (11) in Theorem 3 and the properties of conditional Rényi entropy in Lemmas 1 and 2.

The performance guarantees for optimal guessing functions (Theorem 3 and Corollary 7) and task-encoders (Theorem 4) are remarkably similar. Some intuition for this is provided in [7] where it is shown that a "good" guessing function "induces" a "good" task-encoder and vice versa.[3] This result is stated formally in the following theorem.

Theorem 8 [7]: Let $\mathcal{Z}$ be a finite set.

[3]We call a guessing function or task-encoder "good" if its performance is nearly optimal, and "induce" means here that—without knowing the PMF $P_{X,Y}$—we can construct from a guessing function a task-encoder and vice versa.

1) Given any stochastic task-encoder (14), the associated decoding lists $\{\mathcal{L}_z^y\}$ (15) induce a guessing function $G(\cdot|Y)$ that satisfies

$$\mathbb{E}\big[G(X|Y)^\rho\big] \le |\mathcal{Z}|^\rho \, \mathbb{E}\Big[\big|\mathcal{L}_Z^Y\big|^\rho\Big]. \tag{32}$$

2) Every guessing function $G(\cdot|Y)$ and every positive integer ω satisfying

$$\omega \le |\mathcal{X}| \quad \text{and} \quad |\mathcal{Z}| \ge \omega\left(1 + \left\lfloor \log\big\lceil |\mathcal{X}|/\omega \big\rceil \right\rfloor\right) \tag{33}$$

induce a deterministic task-encoder[4] whose associated decoding lists $\{\mathcal{L}_z^y\}$ (15) satisfy

$$\mathbb{E}\Big[\big|\mathcal{L}_Z^Y\big|^\rho\Big] \le \mathbb{E}\Big[\big\lceil G(X|Y)/\omega \big\rceil^\rho\Big]. \tag{34}$$

It is noted that the first part of Theorem 8 implies that if one is provided with an optimal task encoder (which is characterized by the decoding lists $\mathcal{L}_Z^Y$), then the proof in [7] derives a guessing function from the task encoder that is asymptotically optimal ("good"). Similarly, due to the second part, if one is provided with an optimal guessing function, one can construct a task-encoder that is asymptotically optimal. To better understand the second part of Theorem 8, we briefly discuss the construction of a deterministic task-encoder from an optimal guessing function $G^\star(\cdot|Y)$ (which minimizes $\mathbb{E}\big[G(X|Y)^\rho\big]$). If $G^\star(\cdot|Y)$ is an optimal guessing function, then the two-step construction in the proof of Theorem 8 can be alternatively described as follows: We construct a task-encoder that describes X by

$$Z = (O, S) \tag{35}$$

where O takes values in some set $\mathcal{O}$ of size ω, where

$$1 \le \omega \le |\mathcal{X}|, \tag{36}$$

and S takes values in some set $\mathcal{S}$ of size

$$1 + \left\lfloor \log\big\lceil |\mathcal{X}|/\omega \big\rceil \right\rfloor \le 1 + \log|\mathcal{X}|. \tag{37}$$

(Note that the description Z assumes at most $|\mathcal{O}|\,|\mathcal{S}|$ different values, and by (33) $|\mathcal{O}|\,|\mathcal{S}| \le |\mathcal{Z}|$.) In the first step of the construction, we choose the first part of the description, O. We choose O as one that—among all O's that are drawn from $\mathcal{O}$ according to some conditional PMF $P_{O|X,Y}$—minimizes $\min_{G(\cdot|Y,O)} \mathbb{E}\big[G(X|Y,O)^\rho\big]$. From Lemma 5 (and the subsequent paragraph) we already know how to construct O. Indeed, from Lemma 5 it follows that

$$\min_{G(\cdot|Y,O)} \mathbb{E}\big[G(X|Y,O)^\rho\big] \ge \mathbb{E}\Big[\big\lceil G^\star(X|Y)/\,|\mathcal{O}|\big\rceil^\rho\Big] \tag{38}$$

where equality is achieved by choosing $O = f_1(X,Y)$ for some mapping $f_1 : \mathcal{X}\times\mathcal{Y} \to \mathcal{O}$ for which $f_1(x,y) = f_1(\tilde{x},y)$ implies either $\big\lceil G^\star(x|y)/|\mathcal{O}|\big\rceil \ne \big\lceil G^\star(\tilde{x}|y)/|\mathcal{O}|\big\rceil$ or $x = \tilde{x}$. For example, in the case where $\mathcal{O} = \{0,\dots,\omega-1\}$ we can choose O as the remainder of the Euclidean division of $G(X|Y)-1$ by $|\mathcal{O}|$. Based on the optimal guessing function $G^\star(\cdot|Y)$ and the first part of the description, O, we can construct an optimal guessing function $G^\star(\cdot|Y,O)$ (which minimizes $\mathbb{E}\big[G(X|Y,O)^\rho\big]$) by choosing some $G^\star(\cdot|Y,O)$ for which

$$G^\star\big(x|y, f_1(x,y)\big) = \big\lceil G^\star(x|y)/|\mathcal{O}|\big\rceil, \quad \forall\,(x,y) \in \mathcal{X}\times\mathcal{Y}. \tag{39}$$

In the second step of the construction we choose the second part of the description, S. We choose $S = f_2(x,y)$, where

$$f_2(x,y) = \Big\lfloor \log G^\star\big(x|y, f_1(x,y)\big) \Big\rfloor, \quad \forall\,(x,y) \in \mathcal{X}\times\mathcal{Y}. \tag{40}$$

This will guarantee that the decoding lists satisfy

$$\mathbb{E}\Big[\big|\mathcal{L}_Z^Y\big|^\rho\Big] \le \mathbb{E}\big[G^\star(X|Y,O)^\rho\big] = \mathbb{E}\Big[\big\lceil G^\star(X|Y)/|\mathcal{O}|\big\rceil^\rho\Big] \tag{41}$$

where

$$Z = (O,S) = \big(f_1(X,Y), f_2(X,Y)\big). \tag{42}$$

Note that the size of the support $\mathcal{S}$ of S is only logarithmic in $|\mathcal{X}|$ and thus negligible in asymptotic settings, i.e., in asymptotic settings $|\mathcal{Z}| \approx |\mathcal{O}|$.

The following corollary results from Theorem 8 and (5) by setting

$$\omega = \left\lfloor \frac{|\mathcal{Z}|}{1 + \big\lfloor \log|\mathcal{X}| \big\rfloor} \right\rfloor \tag{43}$$

in Theorem 8.

Corollary 9: Given a set $\mathcal{Z}$ of cardinality $|\mathcal{Z}| \ge 1 + \big\lfloor \log|\mathcal{X}| \big\rfloor$, any guessing function $G(\cdot|Y)$ induces a deterministic task-encoder, whose associated decoding lists $\{\mathcal{L}_z^y\}$ (15) satisfy

$$\mathbb{E}\Big[\big|\mathcal{L}_Z^Y\big|^\rho\Big] \le 1 + 2^\rho \, \mathbb{E}\big[G(X|Y)^\rho\big]\left(\frac{|\mathcal{Z}|}{1+\log|\mathcal{X}|} - 1\right)^{-\rho}. \tag{44}$$

Combined with Theorem 3, which bounds the performance of an optimal guessing function, Equations (32) and (44) provide an upper and a lower bound on the smallest $\mathbb{E}\big[|\mathcal{L}_Z^Y|^\rho\big]$ that is achievable for a given $|\mathcal{Z}|$. These bounds are weaker than [6, Theorem I.1 and Theorem VI.1] (see Theorem 4) in the finite blocklength regime but tight enough to prove the asymptotic results [6, Theorem I.2 and Theorem VI.2].

Another interesting corollary to Theorem 8 results from the choice $\omega = 1$ in Theorem 8.

Corollary 10: Given a set $\mathcal{Z}$ of cardinality $|\mathcal{Z}| = 1 + \big\lfloor \log|\mathcal{X}| \big\rfloor$, any guessing function $G(\cdot|Y)$ induces a deterministic task-encoder, i.e., a stochastic task-encoder whose conditional PMF (14) is $\{0,1\}$-valued, whose associated decoding lists $\{\mathcal{L}_z^y\}$ (15) satisfy

$$\mathbb{E}\Big[\big|\mathcal{L}_Z^Y\big|^\rho\Big] \le \mathbb{E}\big[G(X|Y)^\rho\big]. \tag{45}$$

E.g., if

$$\mathcal{Z} = \big\{0,\dots,\big\lfloor \log|\mathcal{X}| \big\rfloor\big\} \tag{46}$$

then the task-encoder $f(\cdot|Y)$ defined by

$$f(\cdot|y) = \big\lfloor \log G(\cdot|y) \big\rfloor, \quad \forall\, y \in \mathcal{Y} \tag{47a}$$

satisfies (45) or, equivalently,

$$\mathbb{E}\Big[\big|f^{-1}\big(f(X|Y)\big|Y\big)\big|^\rho\Big] \le \mathbb{E}\big[G(X|Y)^\rho\big]. \tag{47b}$$

[4] A deterministic task-encoder can be viewed as a stochastic task-encoder whose conditional PMF (14) is $\{0,1\}$-valued.

An implication of Corollary 10 for the problems studied in this paper is discussed in Remark 17. Another example where Corollary 10 is useful is in determining the feedback listsize capacity of a DMC $W(y|x)$ with positive zero-error capacity. Corollary 10 can be used to give an elegant proof of the direct part of [10, Theorem I.1], which states that in the presence of perfect feedback the listsize capacity of $W(y|x)$ equals the cutoff rate $R_{\text{cutoff}}(\rho)$ with feedback (which is in fact equal to the cutoff rate without feedback [10, Corollary I.4]). To see this, suppose that we are given a sequence of (feedback) codes of rate R for which the ρ-th moment of the number of guesses $G^\star(M|Y^n)$ a decoder needs to guess the transmitted message M based on the channel-outputs Y^n approaches one as the blocklength n tends to infinity. (Recall that $R_{\text{cutoff}}(\rho)$ is the supremum of all rates for which such a sequence exists.) Suppose now that the transmission does not stop after n channel uses. Instead, the encoder computes

$$Z \triangleq \big\lfloor \log G^\star(M|Y^n) \big\rfloor \in \big\{0, \ldots, \lfloor nR \rfloor\big\} \tag{48}$$

from the feedback Y^n and uses another n' channel uses to transmit Z at a positive rate while guaranteeing that the receiver can decode it with probability one. Since a positive zero-error (feedback) capacity cannot be smaller than one [30], it is enough to take $n' \leq \lceil \log(nR) \rceil$. Hence, $(n+n')/n$ converges to one as n tends to infinity, and the rate of the code thus converges to R. At the same time, when we substitute (M, Y^n, Z) for (X, Y, Z) in Corollary 10, Corollary 10 implies that the size of the smallest decoding-list $\mathcal{L}^{Y^{n+n'}}$ that is guaranteed to contain M satisfies $\big|\mathcal{L}^{Y^{n+n'}}\big| = \big|\mathcal{L}_Z^{Y^n}\big| \leq G^\star(M|Y^n)$, and consequently that the ρ-th moment of $\big|\mathcal{L}^{Y^{n+n'}}\big|$ converges to one as n tends to infinity. This proves that in the presence of perfect feedback the listsize capacity of $W(y|x)$ is lower-bounded by $R_{\text{cutoff}}(\rho)$.

IV. Problem Statement and Main Results

We consider two problems: the "guessing version" and the "list version." The two differ in the definition of Bob's ambiguity. In both versions a pair (X, Y) is drawn from the finite set $\mathcal{X} \times \mathcal{Y}$ according to the PMF $P_{X,Y}$, and $\rho > 0$ is fixed. Upon observing $(X, Y) = (x, y)$, Alice draws the hints M_1 and M_2 from some finite set $\mathcal{M}_1 \times \mathcal{M}_2$ according to some conditional PMF

$$\mathbb{P}[M_1 = m_1, M_2 = m_2 | X = x, Y = y]. \tag{49}$$

Bob sees both hints and the side information Y. In the guessing version Bob's ambiguity about X is

$$\mathscr{A}_{\text{B}}^{(\text{g})}(P_{X,Y}) = \min_{G(\cdot|M_1,M_2)} \mathbb{E}\big[G(X|Y, M_1, M_2)^\rho\big]. \tag{50}$$

In the list version Bob's ambiguity about X is

$$\mathscr{A}_{\text{B}}^{(\text{l})}(P_{X,Y}) = \mathbb{E}\Big[\big|\mathcal{L}_{M_1,M_2}^{Y}\big|^\rho\Big] \tag{51}$$

where for all $y \in \mathcal{Y}$ and $(m_1, m_2) \in \mathcal{M}_1 \times \mathcal{M}_2$

$$\mathcal{L}_{m_1,m_2}^{y} = \big\{x \colon \mathbb{P}[X = x | Y = y, M_1 = m_1, M_2 = m_2] > 0\big\} \tag{52}$$

is the list of all the realizations of X of positive posterior probability

$$\mathbb{P}[X = x | Y = y, M_1 = m_1, M_2 = m_2] = \frac{P_{X,Y}(x, y)\, \mathbb{P}[M_1 = m_1, M_2 = m_2 | X = x, Y = y]}{\sum_{\tilde{x}} P_{X,Y}(\tilde{x}, y)\, \mathbb{P}[M_1 = m_1, M_2 = m_2 | X = \tilde{x}, Y = y]}. \tag{53}$$

Eve sees one of the hints and guesses X based on this hint and the side information Y. Which of the hints is revealed to her is determined by an accomplice of hers to minimize her guessing efforts. In both versions Eve's ambiguity about X is

$$\mathscr{A}_{\text{E}}(P_{X,Y}) = \min_{G_1(\cdot|Y,M_1),\, G_2(\cdot|Y,M_2)} \mathbb{E}\big[G_1(X|Y, M_1)^\rho \wedge G_2(X|Y, M_2)^\rho\big]. \tag{54}$$

Optimizing over Alice's mapping, i.e., the choice of the conditional PMF in (49), we wish to characterize the largest ambiguity that we can guarantee that Eve will have subject to a given upper bound on the ambiguity that Bob may have.

Note that by quantifying Eve's ambiguity using (54), we are implicitly assuming that Eve's accomplice observes X and Y before determining the hint that minimizes Eve's guessing efforts. Less conservative is the ambiguity

$$\tilde{\mathscr{A}}_{\text{E}}(P_{X,Y}) = \min_{k \in \{1,2\}} \min_{G_k(\cdot|Y,M_k)} \mathbb{E}\big[G_k(X|Y, M_k)^\rho\big] \tag{55}$$

which applies if the accomplice does not observe (X, Y) and reveals to Eve the hint that in expectation over (X, Y) minimizes her guessing efforts. Definition (55) is less conservative than (54) in the sense that

$$\mathscr{A}_{\text{E}}(P_{X,Y}) \leq \tilde{\mathscr{A}}_{\text{E}}(P_{X,Y}). \tag{56}$$

Why we prefer (54) over (55) is explained in Section V.

Of special interest to us is the asymptotic regime where (X, Y) is an n-tuple (not necessarily drawn IID), and where

$$\mathcal{M}_1 = \big\{1, \ldots, 2^{nR_1}\big\}, \quad \mathcal{M}_2 = \big\{1, \ldots, 2^{nR_2}\big\} \tag{57}$$

where (R_1, R_2) is a nonnegative pair corresponding to the rate.[5] For both versions of the problem, we shall characterize the largest exponential growth that we can guarantee for Eve's ambiguity subject to the constraint that Bob's ambiguity tend to one.[6] This asymptote turns out not to depend on the version of the problem, and in the asymptotic analysis $\mathscr{A}_{\text{B}}$ can stand for either $\mathscr{A}_{\text{B}}^{(\text{g})}$ or $\mathscr{A}_{\text{B}}^{(\text{l})}$.

The following definition phrases mathematically what we mean by the "largest exponential growth that we can guarantee for Eve's ambiguity."

Definition 11 (Privacy-Exponent): Let $\big\{(X_i, Y_i)\big\}_{i \in \mathbb{N}}$ be a stochastic process over the finite alphabet $\mathcal{X} \times \mathcal{Y}$, and denote by P_{X^n,Y^n} the PMF of (X^n, Y^n). Given a nonnegative rate-pair (R_1, R_2), we call E_{E} an *achievable ambiguity-exponent* if

[5] When we say that a positive integer $k \in \mathbb{N}$ assumes the value 2^{nR}, where $R > 0$ corresponds to a rate, we mean that $k = \lfloor 2^{nR} \rfloor$.

[6] Note that in the guessing version $G(X|Y, M_1, M_2)^\rho$ is one if, and only if, Bob's first guess is X^n, and in the list version $\big|\mathcal{L}_{M_1,M_2}^{Y}\big|^\rho$ is one if, and only if, Bob forms the "perfect" list comprising only X^n.

there exists a sequence of stochastic encoders such that Bob's ambiguity (which is always at least one) satisfies

$$\lim_{n\to\infty} \mathscr{A}_{\mathrm{B}}(P_{X^n,Y^n}) = 1, \tag{58}$$

and such that Eve's ambiguity satisfies

$$\liminf_{n\to\infty} \frac{\log\big(\mathscr{A}_{\mathrm{E}}(P_{X^n,Y^n})\big)}{n} \geq E_{\mathrm{E}}. \tag{59}$$

The *privacy-exponent* $\overline{E_{\mathrm{E}}}$ is the supremum of all achievable ambiguity-exponents. If (58) cannot be satisfied, then the set of achievable ambiguity-exponents is empty, and we define the privacy-exponent as negative infinity.

A modest requirement can be imposed on Bob's ambiguity in which it is allowed to grow exponentially with a given normalized (by n) exponent E_{B} as follows:

$$\limsup_{n\to\infty} \frac{\log\big(\mathscr{A}_{\mathrm{B}}(P_{X^n,Y^n})\big)}{n} \leq E_{\mathrm{B}}. \tag{60}$$

This case is thoroughly studied in [13].

We next present our results to the stated problems in the finite-blocklength regime (Section IV-A) and in the asymptotic regime (Section IV-B).

A. Finite-Blocklength Results

In the following theorem c_{s} is related to how much information can be gleaned about the secret X from the pair of hints (M_1, M_2) but not from one hint alone; c_1 is related to how much can be gleaned from M_1; and c_2 is related to how much can be gleaned from M_2.

Theorem 12 (Finite-Blocklength Guessing-Version): For every triple $(c_{\mathrm{s}}, c_1, c_2) \in \mathbb{N}^3$ satisfying

$$c_{\mathrm{s}} \leq |\mathcal{M}_1| \wedge |\mathcal{M}_2|, \quad c_1 \leq \big\lfloor |\mathcal{M}_1| / c_s \big\rfloor, \quad c_2 \leq \big\lfloor |\mathcal{M}_2| / c_s \big\rfloor \tag{61}$$

there is a choice of the conditional PMF in (49) for which Bob's ambiguity about X is upper-bounded by

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_{X,Y}) < 1 + 2^{\rho(H_{\tilde{\rho}}(X|Y) - \log(c_{\mathrm{s}} c_1\ c_2) + 1)} \tag{62}$$

and Eve's ambiguity about X is lower-bounded by

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \geq \big(1 + \ln|\mathcal{X}|\big)^{-\rho} 2^{\rho(H_{\tilde{\rho}}(X|Y) - \log(c_1 + c_2))}. \tag{63}$$

Conversely, for every conditional PMF, Bob's ambiguity is lower-bounded by

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_{X,Y}) \geq \big(1 + \ln|\mathcal{X}|\big)^{-\rho} 2^{\rho(H_{\tilde{\rho}}(X|Y) - \log(|\mathcal{M}_1|\,|\mathcal{M}_2|))} \vee 1 \tag{64}$$

and Eve's ambiguity is upper-bounded by

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \leq \big(|\mathcal{M}_1| \wedge |\mathcal{M}_2|\big)^{\rho} \mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_{X,Y}) \wedge 2^{\rho H_{\tilde{\rho}}(X|Y)} \tag{65}$$

where (65) holds even if we replace (54) by (55), i.e.,

$$\tilde{\mathscr{A}}_{\mathrm{E}}(P_{X,Y}) \leq \big(|\mathcal{M}_1| \wedge |\mathcal{M}_2|\big)^{\rho} \mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_{X,Y}) \wedge 2^{\rho H_{\tilde{\rho}}(X|Y)}. \tag{66}$$

Proof: See Section VI-A. ∎

Note that the choice of c_s as 1 in Theorem 12 results in the upper bound (62) being quite close to the lower bound (64). Other consequences of choosing c_s, c_1, and c_2 judiciously are presented in the corollary, where the finite-blocklength results in Theorem 12 are presented in a simplified and more accessible form. In particular, the corollary shows how much Bob's ambiguity can be decreased while assuring a guarantee on Eve's. The fact that the bounds are tight up to polylogarithmic factor of $|\mathcal{X}|$ provides the justification for the converse terminology in Theorems 12. In particular, the simplified achievability results (67)–(69) match the corresponding converse results (70)–(71) up to polylogarithmic factors of $|\mathcal{X}|$.

Corollary 13 (Simplified Finite-Blocklength Guessing-Version): For any constant $\mathscr{U}_{\mathrm{B}}$ satisfying

$$\mathscr{U}_{\mathrm{B}} \geq 1 + 2^{\rho}\big(|\mathcal{M}_1|\,|\mathcal{M}_2|\big)^{-\rho} 2^{\rho H_{\tilde{\rho}}(X|Y)} \tag{67}$$

there is a choice of the conditional PMF in (49) for which Bob's ambiguity about X is upper-bounded by

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_{X,Y}) < \mathscr{U}_{\mathrm{B}} \tag{68}$$

and Eve's ambiguity about X is lower-bounded by

$$\begin{aligned}\mathscr{A}_{\mathrm{E}}(P_{X,Y}) &\geq 2^{-\rho}\big(1 + \ln|\mathcal{X}|\big)^{-\rho}\Big[2^{-4\rho}\big(|\mathcal{M}_1| \wedge |\mathcal{M}_2|\big)^{\rho}(\mathscr{U}_{\mathrm{B}} - 1) \\ &\qquad \wedge 2^{\rho H_{\tilde{\rho}}(X|Y)}\Big].\end{aligned} \tag{69}$$

Conversely, (68) cannot hold for

$$\mathscr{U}_{\mathrm{B}} < \big(1 + \ln|\mathcal{X}|\big)^{-\rho}\big(|\mathcal{M}_1|\,|\mathcal{M}_2|\big)^{-\rho} 2^{\rho H_{\tilde{\rho}}(X|Y)} \vee 1 \tag{70}$$

and if Bob's ambiguity satisfies (68) for some $\mathscr{U}_{\mathrm{B}}$, then Eve's ambiguity about X is upper-bounded by

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \leq \big(|\mathcal{M}_1| \wedge |\mathcal{M}_2|\big)^{\rho} \mathscr{U}_{\mathrm{B}} \wedge 2^{\rho H_{\tilde{\rho}}(X|Y)}. \tag{71}$$

Proof: The result is a corollary to Theorem 12 (see Appendix A for a proof). ∎

The following theorem and corollary are the list version of the results in Theorem 12 and Corollary 13. As in the case of the guessing version in Theorem 12 and Corollary 13, the simplified achievability results (78)–(80) match the corresponding converse results (81)–(82) up to polylogarithmic factors of $|\mathcal{X}|$.

Theorem 14 (Finite-Blocklength List-Version): If $|\mathcal{M}_1|\,|\mathcal{M}_2| > \log|\mathcal{X}| + 2$, then for every triple $(c_{\mathrm{s}}, c_1, c_2) \in \mathbb{N}^3$ satisfying

$$c_{\mathrm{s}} \leq |\mathcal{M}_1| \wedge |\mathcal{M}_2|, \quad c_1 \leq \big\lfloor |\mathcal{M}_1| / c_{\mathrm{s}} \big\rfloor, \quad c_2 \leq \big\lfloor |\mathcal{M}_2| / c_{\mathrm{s}} \big\rfloor \tag{72a}$$

$$c_{\mathrm{s}} c_1\ c_2 > \log|\mathcal{X}| + 2 \tag{72b}$$

there is a choice of the conditional PMF in (49) for which Bob's ambiguity about X is upper-bounded by

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_{X,Y}) < 1 + 2^{\rho(H_{\tilde{\rho}}(X|Y) - \log(c_{\mathrm{s}} c_1\ c_2 - \log|\mathcal{X}| - 2) + 2)} \tag{73}$$

and Eve's ambiguity about X is lower-bounded by

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \geq \big(1 + \ln|\mathcal{X}|\big)^{-\rho} 2^{\rho(H_{\tilde{\rho}}(X|Y) - \log(c_1 + c_2))}. \tag{74}$$

Conversely, for every conditional PMF, Bob's ambiguity is lower-bounded by

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_{X,Y}) \geq 2^{\rho(H_{\tilde{\rho}}(X|Y) - \log(|\mathcal{M}_1|\,|\mathcal{M}_2|))} \vee 1 \tag{75}$$

and Eve's ambiguity is upper-bounded by

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \leq \big(|\mathcal{M}_1| \wedge |\mathcal{M}_2|\big)^{\rho} \mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_{X,Y}) \wedge 2^{\rho H_{\tilde{\rho}}(X|Y)} \tag{76}$$

where (76) holds even if we replace (54) by (55), i.e.,

$$\tilde{\mathscr{A}}_{\mathrm{E}}(P_{X,Y}) \le \big(|\mathcal{M}_1| \wedge |\mathcal{M}_2|\big)^{\rho} \mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_{X,Y}) \wedge 2^{\rho H_{\tilde{\rho}}(X|Y)}. \quad (77)$$

Proof: See Section VI-A. ∎

Corollary 15 (Simplified Finite-Blocklength List-Version): For $|\mathcal{M}_1|\,|\mathcal{M}_2| > \log|\mathcal{X}| + 2$ and any constant $\mathscr{U}_{\mathrm{B}}$ satisfying

$$\mathscr{U}_{\mathrm{B}} \ge 1 + 2^{\rho(H_{\tilde{\rho}}(X|Y) - \log(|\mathcal{M}_1|\,|\mathcal{M}_2| - \log|\mathcal{X}| - 2) + 2)} \quad (78)$$

there is a choice of the conditional PMF in (49) for which Bob's ambiguity about X is upper-bounded by

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_{X,Y}) < \mathscr{U}_{\mathrm{B}} \quad (79)$$

and Eve's ambiguity about X is lower-bounded by

$$\begin{aligned}\mathscr{A}_{\mathrm{E}}(P_{X,Y}) &\ge 2^{-\rho}\big(1 + \ln|\mathcal{X}|\big)^{-\rho}\Big[2^{-6\rho}\big(|\mathcal{M}_1| \wedge |\mathcal{M}_2|\big)^{\rho}(\mathscr{U}_{\mathrm{B}} - 1) \\ &\quad \wedge 2^{-4\rho}\big(2 + \log|\mathcal{X}|\big)^{-\rho}\big(|\mathcal{M}_1| \wedge |\mathcal{M}_2|\big)^{\rho} 2^{\rho H_{\tilde{\rho}}(X|Y)} \\ &\quad \wedge 2^{\rho H_{\tilde{\rho}}(X|Y)}\Big]. \end{aligned} \quad (80)$$

Conversely, (79) cannot hold for

$$\mathscr{U}_{\mathrm{B}} < \big(|\mathcal{M}_1|\;|\mathcal{M}_2|\big)^{-\rho} 2^{\rho H_{\tilde{\rho}}(X|Y)} \vee 1 \quad (81)$$

and if Bob's ambiguity satisfies (79) for some $\mathscr{U}_{\mathrm{B}}$, then Eve's ambiguity about X is upper-bounded by

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \le \big(|\mathcal{M}_1| \wedge |\mathcal{M}_2|\big)^{\rho} \mathscr{U}_{\mathrm{B}} \wedge 2^{\rho H_{\tilde{\rho}}(X|Y)}. \quad (82)$$

Proof: The result is a corollary to Theorem 14 (see Appendix B for a proof). ∎

B. Asymptotic Results

Suppose now that (X, Y) is an n-tuple. We study the asymptotic regime in which n tends to infinity. Recall that in this regime we refer to both $\mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}$ and $\mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}$ by $\mathscr{A}_{\mathrm{B}}$, because the results are the same for both versions of the problem. Theorems 12 and 14 imply the following asymptotic result.

Theorem 16 (Privacy-Exponent): Let $\big\{(X_i, Y_i)\big\}_{i\in\mathbb{N}}$ be a discrete-time stochastic process with finite alphabet $\mathcal{X}\times\mathcal{Y}$, and suppose its conditional Rényi entropy-rate $H_{\tilde{\rho}}(\boldsymbol{X}|\boldsymbol{Y})$ is well-defined. Given any positive rate-pair (R_1, R_2), the privacy-exponent is

$$\overline{E_{\mathrm{E}}} = \begin{cases} \rho\big(R_1 \wedge R_2 \wedge H_{\tilde{\rho}}(\boldsymbol{X}|\boldsymbol{Y})\big) & R_1 + R_2 > H_{\tilde{\rho}}(\boldsymbol{X}|\boldsymbol{Y}), \\ -\infty & R_1 + R_2 < H_{\tilde{\rho}}(\boldsymbol{X}|\boldsymbol{Y}). \end{cases} \quad (83)$$

Proof: See Section VI-B. ∎

V. Discussion

The following remark explains why the results for the guessing and the list version differ only by polylogarithmic factors of $|\mathcal{X}|$ (and are consequently the same in the asymptotic regime).

Remark 17 (Why Do the Two Criteria for Bob Lead to Similar Results?): Consider any choice of the conditional PMF in (49). In the guessing version Bob uses an optimal guessing function $G^{\star}(\cdot|Y, M_1, M_2)$ (which minimizes $\mathbb{E}\big[G(X|Y, M_1, M_2)^{\rho}\big]$) to guess X based on the side information Y and the hints M_1 and M_2, and his ambiguity is $\mathbb{E}\big[G^{\star}(X|Y, M_1, M_2)^{\rho}\big]$. By Corollary 10 we can construct from $G^{\star}(\cdot|Y, M_1, M_2)$ an additional hint M that takes values in a set of size at most $1 + \big\lfloor \log|\mathcal{X}| \big\rfloor$ such that

$$\mathbb{E}\Big[\big|\mathcal{L}^{Y}_{M_1,M_2,M}\big|^{\rho}\Big] \le \mathbb{E}\big[G^{\star}(X|Y, M_1, M_2)^{\rho}\big] \quad (84)$$

where $\mathcal{L}^{Y}_{M_1,M_2,M}$ is the smallest list that is guaranteed to contain X given (Y, M_1, M_2, M). Suppose now that Alice maps X to the hints $M_1' \triangleq (M_1, M)$ and $M_2' \triangleq M_2$. This implies that Bob's ambiguity in the list version is

$$\mathbb{E}\Big[\big|\mathcal{L}^{Y}_{M_1',M_2'}\big|^{\rho}\Big] = \mathbb{E}\Big[\big|\mathcal{L}^{Y}_{M_1,M_2,M}\big|^{\rho}\Big] \quad (85)$$

and consequently no larger than $\mathbb{E}\big[G^{\star}(X|Y, M_1, M_2)^{\rho}\big]$. Moreover, because M takes values in a set of size at most $1 + \big\lfloor \log|\mathcal{X}| \big\rfloor$, we can use Lemma 5 to show that—compared to the case where the hints are M_1 and M_2—Eve's ambiguity decreases by at most a polylogarithmic factor of $|\mathcal{X}|$.

We next explain why we choose to quantify Eve's ambiguity by (54) and not by (55). As we have seen, (54) is more conservative than (55) in the sense that (56) holds. Consequently, it follows from (66) and (77) that the results of Theorems 12 and 14 hold irrespective of whether we quantify Eve's ambiguity by (54) or by (55). We prefer to quantify Eve's ambiguity by (54), because—as the following example shows—(55) leads to a weaker notion of secrecy than (54).

Example 18: Suppose that Y is null, X is uniform over $\mathcal{X}$, and Alice produces the hints at random: They are equally likely to be $(M_1 = X, M_2 = *)$ or $(M_1 = *, M_2 = X)$, where the symbol $*$ is not in $\mathcal{X}$. Since Bob can recover X from (M_1, M_2) (by producing the hint that is not $*$),

$$\min_{G(\cdot|M_1,M_2)} \mathbb{E}\big[G(X|M_1, M_2)^{\rho}\big] = \mathbb{E}\Big[\big|\mathcal{L}_{M_1,M_2}\big|^{\rho}\Big] = 1. \quad (86)$$

The system is insecure, because one of the hints always reveals X, and $\mathscr{A}_{\mathrm{E}}(P_{X,Y}) = 1$. However, as we next argue, this weakness is not captured by $\tilde{\mathscr{A}}_{\mathrm{E}}(P_{X,Y})$. The probability of M_1 being $*$ is $1/2$, so the ρ-th moment of $G_1(X|M_1)$ is at least $\min_{G(\cdot)} \mathbb{E}\big[G(X)^{\rho}\big]/2$. Likewise, by symmetry, for $G_2(X|M_2)$. Thus $\tilde{\mathscr{A}}_{\mathrm{E}}(P_{X,Y})$ differs from $\min_{G(\cdot)} \mathbb{E}\big[G(X)^{\rho}\big]$ by a factor of at most $1/2$. ♢

So far, we have explained why we prefer (54) over (55). But why do we allow Eve to guess even in the list version of our problem? That is, why do we prefer (54) over

$$\mathscr{A}_{\mathrm{E}}^{(\mathrm{l})} = \mathbb{E}\Big[\big|\mathcal{L}^{Y}_{M_1}\big|^{\rho} \wedge \big|\mathcal{L}^{Y}_{M_2}\big|^{\rho}\Big] \quad (87)$$

even when Bob must form a list?

We prefer (54) over (87) because, as Theorem 19 ahead will show, forcing Eve to produce a short list—i.e., insisting that the set of realizations of X that she cannot rule out be small—would severely handicap her and make it trivial to defeat her: When Eve must form a list, perfect secrecy is almost free.

Theorem 19 (Eve Must Form a List): If

$$|\mathcal{M}_1| \wedge |\mathcal{M}_2| \ge 1 + \big\lfloor \log|\mathcal{X}| \big\rfloor \quad (88)$$

then there exists a conditional PMF as in (49) for which Bob's ambiguity about X is upper-bounded by

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_{X,Y}) \leq 1 + 2^{\rho(H_{\tilde{\rho}}(X|Y)-\log(|\mathcal{M}_1|\,|\mathcal{M}_2|)+2\log(1+\lfloor\log|\mathcal{X}\rfloor)+3)} \tag{89}$$

and Eve's ambiguity about X is

$$\mathscr{A}_{\mathrm{E}}^{(\mathrm{l})}(P_{X,Y}) = \mathbb{E}\big[|\mathcal{L}_Y|^{\rho}\big] \tag{90}$$

where

$$\mathbb{E}\big[|\mathcal{L}_Y|^{\rho}\big] = \sum_y P_Y(y)\,\big|\{x \in \mathcal{X}\colon P_{X|Y}(x|y) > 0\}\big|^{\rho}. \tag{91}$$

Conversely, for every conditional PMF, Bob's ambiguity is lower-bounded by

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_{X,Y}) \geq 2^{\rho(H_{\tilde{\rho}}(X|Y)-\log(|\mathcal{M}_1|\,|\mathcal{M}_2|))} \vee 1 \tag{92}$$

and Eve's ambiguity is upper-bounded by

$$\mathscr{A}_{\mathrm{E}}^{(\mathrm{l})}(P_{X,Y}) \leq \mathbb{E}\big[|\mathcal{L}_Y|^{\rho}\big]. \tag{93}$$

Proof: See Appendix C. ∎

To see why perfect secrecy is almost free when Eve is required to form a list, note that the RHS of (90) would also be Eve's list size if she only saw Y and did not get to see *any* hint, so in this sense achieving (90) is tantamount to achieving perfect secrecy. And the cost is very small: Condition (88) is satisfied in the large-blocklength regime whenever the rates of the two hints are positive; and the RHS of (89) will tend to one in this regime whenever the sum of the rates exceeds the conditional Rényi entropy rate—a condition that is necessary even in the absence of an adversary (Theorem 4).

That perfect secrecy is (almost) free when we quantify Eve's ambiguity by (87) is highly intuitive: By forcing Eve to form a list that is guaranteed to contain X, we force her to include in her list all the realizations of X that have a positive posterior probability, no matter how small. This implies that, if Eve were to form a list, then perfect secrecy could be attained by hiding very little information from Eve. The situation is different in case Eve guesses X, because allowing Eve to guess X, i.e., quantifying Eve's ambiguity by (54), is tantamount to first indexing the elements of the list in (87)—which she would otherwise have to form—in decreasing order of their posterior probability, and to then downweigh the large indices of the realizations at the bottom of the list by their small posterior probabilities.

To conclude the discussion of how to quantify Eve's ambiguity, we relate Eve's ambiguity (54) to the concept of *equivocation*. In the classical Shannon cipher system [31], a popular way to measure imperfect secrecy is in terms of equivocation, i.e., in terms of the conditional entropy $H(X|Z)$, where X denotes some sensitive information and Z Eve's observation. In the settings where Bob is a list-decoder or a guessing decoder, Rényi entropy plays the role of Shannon entropy in the sense that the minimum required rate to encode an n-tuple $X = X^n$ is the Rényi entropy rate $H_{\tilde{\rho}}(\boldsymbol{X})$ rather than the Shannon entropy rate $H(\boldsymbol{X}) = H_1(\boldsymbol{X})$ (this follows from Theorems 4 and Corollary 7). Consequently, in these settings the conditional Rényi entropy $H_{\tilde{\rho}}(X|Z)$ qualifies as a "natural" equivalent for equivocation. But $H_{\tilde{\rho}}(X|Z)$ has a nice operational characterization: $2^{\rho H_{\tilde{\rho}}(X|Z)}$ is (up to polylogarithmic factors of $|X|$) the ρ-th moment of the number of guesses that Eve needs to guess X from her observation Z (see Theorem 3). This is another reason why it makes sense to quantify Eve's ambiguity in terms of the ρ-th moment of the number of guesses that she needs to guess X.

In the remainder of this section we briefly discuss how the results of Theorems 12 and 14 change in the following two scenarios: 1) Alice knows which hint Eve observes; or 2) Alice describes X using only one hint, but Alice and Bob share a secret key, which is unknown to Eve. We begin with Scenario 1. In this scenario Alice draws the public hint M_{p} and the secret hint M_{s} from some finite set $\mathcal{M}_{\mathrm{p}} \times \mathcal{M}_{\mathrm{s}}$ according to some conditional PMF

$$\mathbb{P}[M_{\mathrm{p}} = m_{\mathrm{p}}, M_{\mathrm{s}} = m_{\mathrm{s}}|X = x, Y = y]. \tag{94}$$

Bob sees both hints. In the guessing version his ambiguity about X is

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_{X,Y}) = \min_{G(\cdot|Y,M_{\mathrm{p}},M_{\mathrm{s}})} \mathbb{E}\big[G(X|Y, M_{\mathrm{p}}, M_{\mathrm{s}})^{\rho}\big] \tag{95}$$

and in the list version

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_{X,Y}) = \mathbb{E}\Big[\big|\mathcal{L}^{Y}_{M_{\mathrm{p}},M_{\mathrm{s}}}\big|^{\rho}\Big]. \tag{96}$$

Eve sees only the public hint. In both versions her ambiguity about X is

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) = \min_{G(\cdot|Y,M_{\mathrm{p}})} \mathbb{E}\big[G(X|Y, M_{\mathrm{p}})^{\rho}\big]. \tag{97}$$

The next two theorems characterize the largest ambiguity that we can guarantee that Eve will have subject to a given upper bound on the ambiguity that Bob may have (see Appendix D for a proof). As in the case where the hints are not secret and public, the guessing and the list version lead to similar results (cf. Remark 17). In the next two theorems c is related to how much can be gleaned about X from M_{p}.

Theorem 20 (Secret Hint Guessing-Version): For every $c \in \mathbb{N}$ satisfying

$$c \leq |\mathcal{M}_{\mathrm{p}}| \tag{98}$$

there is a $\{0, 1\}$-valued choice of the conditional PMF in (94) for which Bob's ambiguity about X is upper-bounded by

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_{X,Y}) < 1 + 2^{\rho(H_{\tilde{\rho}}(X|Y)-\log(c\,|\mathcal{M}_{\mathrm{s}}|)+1)} \tag{99}$$

and Eve's ambiguity about X is lower-bounded by

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \geq \big(1 + \ln|\mathcal{X}|\big)^{-\rho} 2^{\rho(H_{\tilde{\rho}}(X|Y)-\log c)}. \tag{100}$$

Conversely, for every conditional PMF, Bob's ambiguity is lower-bounded by

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_{X,Y}) \geq \big(1 + \ln|\mathcal{X}|\big)^{-\rho} 2^{\rho(H_{\tilde{\rho}}(X|Y)-\log(|\mathcal{M}_{\mathrm{p}}|\,|\mathcal{M}_{\mathrm{s}}|))} \vee 1 \tag{101}$$

and Eve's ambiguity is upper-bounded by

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \leq |\mathcal{M}_{\mathrm{s}}|^{\rho}\,\mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_{X,Y}) \wedge 2^{\rho H_{\tilde{\rho}}(X|Y)}. \tag{102}$$

Theorem 21 (Secret Hint List-Version): If $|\mathcal{M}_\mathrm{p}|\,|\mathcal{M}_\mathrm{s}| > \log|\mathcal{X}|+2$, then for every $c\in\mathbb{N}$ satisfying

$$c\le|\mathcal{M}_\mathrm{p}|,\quad c\,|\mathcal{M}_\mathrm{s}|>\log|\mathcal{X}|+2 \tag{103}$$

there is a $\{0,1\}$-valued choice of the conditional PMF in (94) for which Bob's ambiguity about X is upper-bounded by

$$\mathscr{A}_\mathrm{B}^{(\mathrm{l})}(P_{X,Y})<1+2^{\rho(H_{\tilde\rho}(X|Y)-\log(c\,|\mathcal{M}_\mathrm{s}|-\log|\mathcal{X}|-2)+2)} \tag{104}$$

and Eve's ambiguity about X is lower-bounded by

$$\mathscr{A}_\mathrm{E}(P_{X,Y})\ge\big(1+\ln|\mathcal{X}|\big)^{-\rho}2^{\rho(H_{\tilde\rho}(X|Y)-\log c)}. \tag{105}$$

Conversely, for every conditional PMF, Bob's ambiguity is lower-bounded by

$$\mathscr{A}_\mathrm{B}^{(\mathrm{l})}(P_{X,Y})\ge 2^{\rho(H_{\tilde\rho}(X|Y)-\log(|\mathcal{M}_\mathrm{p}|\,|\mathcal{M}_\mathrm{s}|)}\vee 1 \tag{106}$$

and Eve's ambiguity is upper-bounded by

$$\mathscr{A}_\mathrm{E}(P_{X,Y})\le|\mathcal{M}_\mathrm{s}|^\rho\mathscr{A}_\mathrm{B}^{(\mathrm{l})}(P_{X,Y})\wedge 2^{\rho H_{\tilde\rho}(X|Y)}. \tag{107}$$

We next contrast Theorems 20 and 21 to their counterparts in the previous scenario, i.e., to Theorems 12 and 14. By comparing the respective upper and lower bounds on Eve's ambiguity, we see that c and $|\mathcal{M}_\mathrm{s}|$ in the current scenario, which relate to how much information can be gleaned about X from M_p and M_s, play the roles of $c_1+c_2\approx c_1\vee c_2$ and $|\mathcal{M}_1|\wedge|\mathcal{M}_2|$ in the previous scenario, which relate to how much information can be gleaned about X from the hint that—among M_1 and M_2—reveals more information about X and the one that—among M_1 and M_2—reveals less information about X. This reflects the fact that in the current scenario Eve always sees M_p, whereas in the previous scenario she sees the hint that reveals more information about X and hence minimizes her ambiguity.

Unlike Theorem 12, Theorem 20 implies that in the current scenario Alice can describe X deterministically. To see why, recall that in the current scenario Eve sees only the public hint M_p, and hence there is no need to encrypt information that can be gleaned from the secret hint M_s. Consequently, as is further explained in the proof of Theorem 20, Alice need not draw a one-time-pad-like random variable to ensure that some information can be gleaned about X from $(M_\mathrm{p},M_\mathrm{s})$ but not from one hint alone. Instead, she can store that information on M_s without prior encryption. It is noted that the same observation carries over to Theorems 14 and 21.

We now proceed to Scenario 2, where Alice describes X using only one hint, but Alice and Bob share a secret key, which is unknown to Eve. The secret key K is drawn independently of the pair (X,Y) and uniformly over some finite set $\mathcal{K}$. Upon observing $(X,Y)=(x,y)$ and $K=k$, Alice draws the hint M from some finite set $\mathcal{M}$ according to some conditional PMF

$$\mathbb{P}[M=m|X=x,Y=y,K=k]. \tag{108}$$

Throughout, we assume that $|\mathcal{K}|\le|\mathcal{M}|$. Bob sees the secret key and the hint. In the guessing version his ambiguity about X is

$$\mathscr{A}_\mathrm{B}^{(\mathrm{g})}(P_{X,Y})=\min_{G(\cdot|Y,K,M)}\mathbb{E}\big[G(X|Y,K,M)^\rho\big] \tag{109}$$

and in the list version

$$\mathscr{A}_\mathrm{B}^{(\mathrm{l})}(P_{X,Y})=\mathbb{E}\Big[\big|\mathcal{L}_M^{Y,K}\big|^\rho\Big]. \tag{110}$$

Eve sees sees only the hint. In both versions her ambiguity about X is

$$\mathscr{A}_\mathrm{E}(P_{X,Y})=\min_{G(\cdot|Y,M)}\mathbb{E}\big[G(X|Y,M)^\rho\big]. \tag{111}$$

The next two theorems characterize the largest ambiguity that we can guarantee that Eve will have subject to a given upper bound on the ambiguity that Bob may have (see Appendix E for a proof). Again, the guessing and the list version lead to similar results. Here $|\mathcal{K}|$ is related to how much information can be gleaned about X from (K,M) but not from M alone, i.e., to the "encrypted" information stored on M, and c is related to how much information can be gleaned about X from M, i.e., to the "unencrypted" information stored on M.

Theorem 22 (Secret Key Guessing-Version): For every $c\in\mathbb{N}$ satisfying

$$c\,|\mathcal{K}|\le|\mathcal{M}| \tag{112}$$

there is a $\{0,1\}$-valued choice of the conditional PMF in (108) for which Bob's ambiguity about X is upper-bounded by

$$\mathscr{A}_\mathrm{B}^{(\mathrm{g})}(P_{X,Y})<1+2^{\rho(H_{\tilde\rho}(X|Y)-\log(c\,|\mathcal{K}|)+1)} \tag{113}$$

and Eve's ambiguity about X is lower-bounded by

$$\mathscr{A}_\mathrm{E}(P_{X,Y})\ge\big(1+\ln|\mathcal{X}|\big)^{-\rho}2^{\rho(H_{\tilde\rho}(X|Y)-\log c)}. \tag{114}$$

Conversely, for every conditional PMF, Bob's ambiguity is lower-bounded by

$$\mathscr{A}_\mathrm{B}^{(\mathrm{g})}(P_{X,Y})\ge\big(1+\ln|\mathcal{X}|\big)^{-\rho}2^{\rho(H_{\tilde\rho}(X|Y)-\log|\mathcal{M}|)}\vee 1 \tag{115}$$

and Eve's ambiguity is upper-bounded by

$$\mathscr{A}_\mathrm{E}(P_{X,Y})\le|\mathcal{K}|^\rho\mathscr{A}_\mathrm{B}^{(\mathrm{g})}(P_{X,Y})\wedge 2^{\rho H_{\tilde\rho}(X|Y)}. \tag{116}$$

Theorem 23 (Secret Key List-Version): If $\big\lfloor|\mathcal{M}|/|\mathcal{K}|\big\rfloor|\mathcal{K}|>\log|\mathcal{X}|+2$, then for every $c\in\mathbb{N}$ satisfying

$$c\,|\mathcal{K}|\le|\mathcal{M}|,\quad c\,|\mathcal{K}|>\log|\mathcal{X}|+2 \tag{117}$$

there is a $\{0,1\}$-valued choice of the conditional PMF in (108) for which Bob's ambiguity about X is upper-bounded by

$$\mathscr{A}_\mathrm{B}^{(\mathrm{l})}(P_{X,Y})<1+2^{\rho(H_{\tilde\rho}(X|Y)-\log(c\,|\mathcal{K}|-\log|\mathcal{X}|-2)+2)} \tag{118}$$

and Eve's ambiguity about X is lower-bounded by

$$\mathscr{A}_\mathrm{E}(P_{X,Y})\ge\big(1+\ln|\mathcal{X}|\big)^{-\rho}2^{\rho(H_{\tilde\rho}(X|Y)-\log c)}. \tag{119}$$

Conversely, for every conditional PMF, Bob's ambiguity is lower-bounded by

$$\mathscr{A}_\mathrm{B}^{(\mathrm{l})}(P_{X,Y})\ge 2^{\rho(H_{\tilde\rho}(X|Y)-\log|\mathcal{M}|)}\vee 1 \tag{120}$$

and Eve's ambiguity is upper-bounded by

$$\mathscr{A}_\mathrm{E}(P_{X,Y})\le|\mathcal{K}|^\rho\mathscr{A}_\mathrm{B}^{(\mathrm{l})}(P_{X,Y})\wedge 2^{\rho H_{\tilde\rho}(X|Y)}. \tag{121}$$

Theorems 22 and 23 are reminiscent of their counterparts for the scenario with a public and a secret hint, i.e., of Theorems 20 and 21. The main difference is that in the current scenario c and $|\mathcal{K}|$, which relate to the "unencrypted" and the

"encrypted" information stored on M, respectively, play the roles of c and $|\mathcal{M}_{\mathrm{s}}|$, which in the previous scenario relate to the information stored on the public and the secret hint, respectively. Like Theorems 20 and 21, Theorems 22 and 23 imply that in the current scenario Alice can describe X deterministically; there is no need for Alice to draw a one-time-pad like random variable, because she can use the secret key K as a one-time-pad.

VI. Proofs of Main Results

A. Proof of Theorems 12 and 14

We first establish the achievability results, i.e., (62)–(63) in the guessing version and (73)–(74) in the list version. To this end, fix $(c_{\mathrm{s}}, c_1, c_2) \in \mathbb{N}^3$ satisfying (61) in the guessing version and (72) in the list version.

Both (61) and (72) imply that

$$|\mathcal{M}_1| \geq c_{\mathrm{s}} c_1 \quad \text{and} \quad |\mathcal{M}_2| \geq c_{\mathrm{s}} c_2 \tag{122}$$

i.e., that the number of different hints from which M_1 can be chosen is at least $c_{\mathrm{s}} c_1$, and similarly for M_2. Our achievability scheme will, in fact, assign M_1 at most $c_{\mathrm{s}} c_1$ different values, so—of the $|\mathcal{M}_1|$ possible hints that M_1 can take on—only $c_{\mathrm{s}} c_1$ will be used. Similarly for M_2. Since the labels we assign the different hints do not matter, there is no loss of generality in assuming, as we shall, that the hint alphabets are

$$\mathcal{M}_1 = \mathcal{V}_{\mathrm{s}} \times \mathcal{V}_1 \quad \text{and} \quad \mathcal{M}_2 = \mathcal{V}_{\mathrm{s}} \times \mathcal{V}_2 \tag{123}$$

where

$$\mathcal{V}_\nu = \{0, \ldots, c_\nu - 1\}, \quad \nu \in \{\mathrm{s}, 1, 2\}. \tag{124}$$

For every $\nu \in \{\mathrm{s}, 1, 2\}$ let V_ν be a chance variable taking values in $\mathcal{V}_\nu$. For the proof of the guessing version, we note that Corollary 7 implies that there exists some $\{0, 1\}$-valued conditional PMF $\mathbb{P}\big[(V_{\mathrm{s}}, V_1, V_2) = (v_{\mathrm{s}}, v_1, v_2) \big| X = x, Y = y\big]$ for which

$$\min_{G(\cdot|Y, V_{\mathrm{s}}, V_1, V_2)} \mathbb{E}\big[G(X|Y, V_{\mathrm{s}}, V_1, V_2)^\rho\big] < 1 + 2^{\rho(H_{\tilde{\rho}}(X|Y) - \log(c_{\mathrm{s}} c_1 \ c_2) + 1)}. \tag{125}$$

For the proof of the list version, we note that Theorem 4 implies that there exists some deterministic task-encoder $f(\cdot|Y)\colon \ \mathcal{X} \to \mathcal{V}_{\mathrm{s}} \times \mathcal{V}_1 \times \mathcal{V}_2$ for which

$$\mathbb{E}\Big[\big|\mathcal{L}^Y_{V_s, V_1, V_2}\big|^\rho\Big] < 1 + 2^{\rho(H_{\tilde{\rho}}(X|Y) - \log(c_s c_1 \ c_2 - \log|\mathcal{X}| - 2) + 2)} \tag{126}$$

where $(V_{\mathrm{s}}, V_1, V_2) = f(X|Y)$. For both versions we choose $M_1 = (V_{\mathrm{s}} \oplus_{c_{\mathrm{s}}} U, V_1)$ and $M_2 = (U, V_2)$, where $(V_{\mathrm{s}}, V_1, V_2)$ is drawn according to one of the above conditional PMFs depending on the version, and where U is independent of $(X, Y, V_{\mathrm{s}}, V_1, V_2)$ and uniform over $\mathcal{V}_{\mathrm{s}}$. Bob observes both hints and can thus recover $(V_{\mathrm{s}}, V_1, V_2)$. Hence, in the guessing version (62) follows from (125) and in the list version (73) follows from (126).

The proof of (63) and (74) is more involved. It builds on the following two intermediate claims, which we prove next:

1) We can assume w.l.g. that Eve must guess not only X but the pair (X, U).
2) Given any pair of guessing functions $G_1(\cdot, \cdot|Y, M_1)$ and $G_2(\cdot, \cdot|Y, M_2)$ for (X, U), there exist a chance variable Z that takes values in a set of size at most $c_{\mathrm{s}}(c_1 + c_2)$ and a guessing function $G(\cdot, \cdot|Y, Z)$ for (X, U) for which

$$G(X, U|Y, Z) = G_1(X, U|Y, M_1) \wedge G_2(X, U|Y, M_2). \tag{127}$$

We first prove the first intermediate claim. In both versions (guessing and list), once X has been guessed one can compute U, so there exist mappings $g_1\colon \mathcal{X} \times \mathcal{Y} \times \mathcal{M}_1 \to \mathcal{V}_s$ and $g_2\colon \mathcal{X} \times \mathcal{Y} \times \mathcal{M}_2 \to \mathcal{V}_s$ for which

$$U = g_1(X, Y, M_1) = g_2(X, Y, M_2). \tag{128}$$

Given any guessing functions $G_1(\cdot|Y, M_1)$ and $G_2(\cdot|Y, M_2)$ for X, introduce some guessing functions $G_1(\cdot, \cdot|Y, M_1)$ and $G_2(\cdot, \cdot|Y, M_2)$ for (X, U) satisfying, for every $(x, y) \in \mathcal{X} \times \mathcal{Y}$, $m_1 \in \mathcal{M}_1$, and $m_2 \in \mathcal{M}_2$, that

$$G_k\big(x, g_k(x, y, m_k)\big|y, m_k\big) = G_k(x|y, m_k), \quad \forall\, k \in \{1, 2\}. \tag{129}$$

From (128) it follows that

$$G_k(X, U|Y, M_k) = G_k(X|Y, M_k), \quad \forall\, k \in \{1, 2\}. \tag{130}$$

Consequently, Eve can guess X and the pair (X, U) with the same number of guesses. This proves the first intermediate claim.

We next prove the second intermediate claim. Given any pair of guessing functions $G_1(\cdot, \cdot|Y, M_1)$ and $G_2(\cdot, \cdot|Y, M_2)$ for (X, U), define the triple of chance variables

$$(I, \hat{U}, \hat{V}) \triangleq \begin{cases} (1, V_{\mathrm{s}} \oplus_{c_{\mathrm{s}}} U, V_1) & \text{if } G_1(X, U|Y, M_1) \\ & \quad \leq G_2(X, U|Y, M_2), \\ (2, U, V_2) & \text{otherwise} \end{cases} \tag{131}$$

over the alphabet $\mathcal{I} \times \mathcal{V}_{\mathrm{s}} \times \hat{\mathcal{V}}$, where $\mathcal{I} = \{1, 2\}$ and $\hat{\mathcal{V}} = \{0, 1, \ldots, c_1 \vee c_2 - 1\}$. Observing $(Y, I, \hat{U}, \hat{V})$, Eve can guess (X, U) using either G_1 or G_2 depending on the value of I. That is, Eve can guess (X, U) using some guessing function $G(\cdot, \cdot|Y, I, \hat{U}, \hat{V})$ satisfying, for every $y \in \mathcal{Y}$, $i \in \mathcal{I}$, $\hat{u} \in \mathcal{V}_s$, and $\hat{v} \in \{0, 1, \ldots, c_i - 1\}$, that

$$G(\cdot, \cdot|y, i, \hat{u}, \hat{v}) = G_i\big(\cdot, \cdot|y, (\hat{u}, \hat{v})\big). \tag{132}$$

By (131) the number of guesses that she needs to do so is given by

$$\begin{aligned} &G(X, U|Y, I, \hat{U}, \hat{V}) \\ &\quad = G_I\big(X, U|Y, (\hat{U}, \hat{V})\big) && (133)\\ &\quad = G_I(X, U|Y, M_I) && (134)\\ &\quad = G_1(X, U|Y, M_1) \wedge G_2(X, U|Y, M_2). && (135) \end{aligned}$$

Consequently, (127) holds when we set $Z = (I, \hat{U}, \hat{V})$. To conclude the proof of the second intermediate claim, note that the triple $(I, \hat{U}, \hat{V})$ takes values in the set

$$\begin{aligned} &\big\{(1, \hat{u}, \hat{v})\colon (\hat{u}, \hat{v}) \in \mathcal{V}_{\mathrm{s}} \times \mathcal{V}_1\big\} \\ &\quad \cup \big\{(2, \hat{u}, \hat{v})\colon (\hat{u}, \hat{v}) \in \mathcal{V}_{\mathrm{s}} \times \mathcal{V}_2\big\} \end{aligned} \tag{136}$$

whose cardinality is given by

$$|\mathcal{V}_{\mathrm{s}} \times \mathcal{V}_1| + |\mathcal{V}_{\mathrm{s}} \times \mathcal{V}_2| = c_{\mathrm{s}}(c_1 + c_2). \tag{137}$$

We are now ready to prove (63) and (74):

$$\begin{aligned}
&\mathbb{E}\big[G_1(X|Y, M_1)^\rho \wedge G_2(X|Y, M_2)^\rho\big] \\
&\quad \overset{(a)}{=} \mathbb{E}\big[G_1(X, U|Y, M_1)^\rho \wedge G_2(X, U|Y, M_2)^\rho\big] && (138)\\
&\quad \overset{(b)}{=} \mathbb{E}\big[G(X, U|Y, I, \hat{U}, \hat{V})^\rho\big] && (139)\\
&\quad \overset{(c)}{\geq} \big(1 + \ln|\mathcal{X}|\big)^{-\rho} 2^{\rho(H_{\tilde{\rho}}(X,U|Y) - \log(c_{\mathrm{s}}(c_1+c_2)))} && (140)\\
&\quad \overset{(d)}{=} \big(1 + \ln|\mathcal{X}|\big)^{-\rho} 2^{\rho(H_{\tilde{\rho}}(X|Y) - \log(c_1+c_2))} && (141)
\end{aligned}$$

where (a) holds by (130); (b) holds by (135); (c) follows from Corollary 7 and the fact that $(I, \hat{U}, \hat{V})$ takes values in a set of size $c_{\mathrm{s}}(c_1 + c_2)$; and (d) holds because

$$\begin{aligned}
&H_{\tilde{\rho}}(X, U|Y) \\
&\quad = \frac{1}{\rho} \log \sum_{y\in\mathcal{Y}} \Bigg(\sum_{x\in\mathcal{X}} \sum_{u\in\mathcal{V}_{\mathrm{s}}} \big(P_{X,Y}(x, y)/|\mathcal{V}_{\mathrm{s}}|\big)^{\tilde{\rho}} \Bigg)^{1+\rho} && (142)\\
&\quad = \frac{1}{\rho} \log \Bigg(\sum_{y\in\mathcal{Y}} \Bigg(\sum_{x\in\mathcal{X}} P_{X,Y}(x, y)^{\tilde{\rho}} \Bigg)^{1+\rho} |\mathcal{V}_{\mathrm{s}}|^\rho \Bigg) && (143)\\
&\quad = H_{\tilde{\rho}}(X|Y) + \log c_{\mathrm{s}}. && (144)
\end{aligned}$$

The equality in (142) holds because U is independent of (X, Y) and uniform over the set $\mathcal{V}_{\mathrm{s}}$ of size $|\mathcal{V}_{\mathrm{s}}| = c_{\mathrm{s}}$. This concludes the proof of the achievability results.

It remains to establish the converse results, i.e., (64)–(66) in the guessing version and (75)–(77) in the list version. In the guessing version (64) follows from Corollary 7, and in the list version (75) follows from Theorem 4. From (56) we see that (65) and (76) follow from (66) and (77), respectively, and hence it only remains to establish (66) and (77). By Corollary 6, it holds for every $k \in \{1, 2\}$ and $l \in \{1, 2\}\backslash\{k\}$ that

$$\begin{aligned}
&\min_{G(\cdot|Y,M_1,M_2)} \mathbb{E}\big[G(X|Y, M_1, M_2)^\rho\big] \\
&\qquad \geq |\mathcal{M}_l|^{-\rho} \min_{G_k(\cdot|Y,M_k)} \mathbb{E}\big[G_k(X|Y, M_k)^\rho\big]. && (145)
\end{aligned}$$

Since

$$\min_{G(\cdot|Y,M_1,M_2)} \mathbb{E}\big[G(X|Y, M_1, M_2)^\rho\big] \leq \mathbb{E}\Big[\big|\mathcal{L}^Y_{M_1,M_2}\big|^\rho\Big] \tag{146}$$

(145) implies that in both versions the ambiguity $\tilde{\mathscr{A}}_{\mathrm{E}}(P_{X,Y})$ exceeds Bob's ambiguity by at most a factor of $\big(|\mathcal{M}_1| \wedge |\mathcal{M}_2|\big)^\rho$. That is, $\tilde{\mathscr{A}}_{\mathrm{E}}(P_{X,Y}) \leq \big(|\mathcal{M}_1| \wedge |\mathcal{M}_2|\big)^\rho \mathscr{A}^{(\mathrm{g})}_{\mathrm{B}}(P_{X,Y})$ and $\tilde{\mathscr{A}}_{\mathrm{E}}(P_{X,Y}) \leq \big(|\mathcal{M}_1| \wedge |\mathcal{M}_2|\big)^\rho \mathscr{A}^{(\mathrm{l})}_{\mathrm{B}}(P_{X,Y})$. Another upper bound on $\tilde{\mathscr{A}}_{\mathrm{E}}(P_{X,Y})$ is obtained by considering the case where Eve ignores the hint that she observes and guesses X based on Y alone. In this case it follows from Theorem 3 that

$$\min_{G_k(\cdot|Y,M_k)} \mathbb{E}\big[G_k(X|Y, M_k)^\rho\big] \leq 2^{\rho H_{\tilde{\rho}}(X|Y)}, \quad \forall\, k \in \{1, 2\}. \tag{147}$$

B. Proof of Theorem 16

If $R_1 + R_2 < H_{\tilde{\rho}}(\boldsymbol{X}|\boldsymbol{Y})$, then (64) in the guessing version and (75) in the list version imply that the privacy-exponent is negative infinity. We hence assume that $R_1 + R_2 > H_{\tilde{\rho}}(\boldsymbol{X}|\boldsymbol{Y})$.

We first show that the privacy-exponent cannot exceed the RHS of (83). To this end suppose that (58) holds and consequently

$$\limsup_{n\to\infty} \frac{\log\big(\mathscr{A}_{\mathrm{B}}(P_{X^n,Y^n})\big)}{n} = 0. \tag{148}$$

This, combined with (65) in the guessing version and (76) in the list version, implies that

$$\limsup_{n\to\infty} \frac{\log\big(\mathscr{A}_{\mathrm{E}}(P_{X^n,Y^n})\big)}{n} \leq \rho\big(R_1 \wedge R_2 \wedge H_{\tilde{\rho}}(\boldsymbol{X}|\boldsymbol{Y})\big). \tag{149}$$

Hence, the privacy-exponent cannot exceed the RHS of (83).

We next show that the privacy-exponent cannot be smaller than the RHS of (83). By possibly relabeling the hints, we can assume w.l.g. that $R_2 = R_1 \wedge R_2$. Fix some $\epsilon > 0$ satisfying

$$\epsilon \leq R_1 + R_2 - H_{\tilde{\rho}}(\boldsymbol{X}|\boldsymbol{Y}). \tag{150}$$

Choose a nonnegative rate-triple $(R_{\mathrm{s}}, \tilde{R}_1, \tilde{R}_2) \in (\mathbb{R}^+_0)^3$ as follows:

1) If $R_2 \leq H_{\tilde{\rho}}(\boldsymbol{X}|\boldsymbol{Y})/2$, then choose
$$R_{\mathrm{s}} = 0, \quad \tilde{R}_1 = H_{\tilde{\rho}}(\boldsymbol{X}|\boldsymbol{Y}) - R_2 + \epsilon, \quad \tilde{R}_2 = R_2. \tag{151}$$
2) Else if $H_{\tilde{\rho}}(\boldsymbol{X}|\boldsymbol{Y})/2 < R_2 \leq H_{\tilde{\rho}}(\boldsymbol{X}|\boldsymbol{Y})$, then choose
$$R_{\mathrm{s}} = 2R_2 - H_{\tilde{\rho}}(\boldsymbol{X}|\boldsymbol{Y}) - \epsilon, \tag{152a}$$
$$\tilde{R}_1 = \tilde{R}_2 = H_{\tilde{\rho}}(\boldsymbol{X}|\boldsymbol{Y}) - R_2 + \epsilon. \tag{152b}$$
(To guarantee that $R_{\mathrm{s}} \geq 0$, we assume in this case that $\epsilon > 0$ is sufficiently small so that, in addition to (150), also
$$\epsilon < 2R_2 - H_{\tilde{\rho}}(\boldsymbol{X}|\boldsymbol{Y}) \tag{153}$$
holds.)
3) Else if $H_{\tilde{\rho}}(\boldsymbol{X}|\boldsymbol{Y}) < R_2$, then choose
$$R_{\mathrm{s}} = R_2, \quad \tilde{R}_1 = \tilde{R}_2 = 0. \tag{154}$$

We note that in all cases,

$$R_{\mathrm{s}} + \tilde{R}_1 + \tilde{R}_2 > H_{\tilde{\rho}}(\boldsymbol{X}|\boldsymbol{Y}). \tag{155}$$

Having chosen $(R_{\mathrm{s}}, \tilde{R}_1, \tilde{R}_2)$, choose the triple $(c_{\mathrm{s}}, c_1, c_2) \in \mathbb{N}^3$ as

$$\big(c_{\mathrm{s}}, c_1, c_2\big) = \big(2^{nR_{\mathrm{s}}}, 2^{n\tilde{R}_1}, 2^{n\tilde{R}_2}\big). \tag{156}$$

For every sufficiently-large n, this choice implies (61) and (72), and by Theorems 12 and Theorem 14 we can thus guarantee (62)–(63) in the guessing version and (73)–(74) in the list version.

Combining (155) and (156) with (62) in the guessing version and with (73) in the list version yields that Bob's ambiguity tends to 1, i.e., (58). As to Eve's, combining (156)

with (63) in the guessing version and with (74) in the list version implies that

$$\liminf_{n\to\infty} \frac{\log\big(\mathscr{A}_{\mathrm{E}}(P_{X^n,Y^n})\big)}{n} \geq \rho\big(H_{\tilde{\rho}}(\boldsymbol{X}|\boldsymbol{Y}) - (\tilde{R}_1 \vee \tilde{R}_2)\big) \quad (157)$$

$$\geq \rho\big((R_1 \wedge R_2 - \epsilon) \wedge H_{\tilde{\rho}}(\boldsymbol{X}|\boldsymbol{Y})\big) \quad (158)$$

where (158) follows from (157) by plugging-in the settings for $\tilde{R}_1$ and $\tilde{R}_2$ for each of the 3 cases as detailed in (151)–(154). Letting ϵ tend to zero proves that the privacy-exponent cannot be smaller than the RHS of (83).

VII. Resilience against Disk Failures

In this section we generalize the model of Section IV to allow for Alice to produce δ hints (not necessarily two) and store them on different disks, for Bob to see $\nu \leq \delta$ (not necessarily 2) of those hints, and for Eve to see $\eta < \nu$ (not necessarily one) of the hints. We assume that, after observing X and Y, an adversarial "genie" reveals to Bob the ν hints that maximize his ambiguity and to Eve the η hints that minimize her ambiguity. The former guarantees that the system be robust against $\delta - \nu$ disk failures, no matter which disks fail; and the latter guarantees that Eve's ambiguity be "large" no matter which η hints she sees. We allow the genie to observe (X, Y), because, as we have seen, not allowing the genie to observe (X, Y) would lead to a weaker form of secrecy (see Example 18).

The current network can be described as follows. As in Section IV, we consider two problems, the "guessing version" and the "list version," which differ in the definition of Bob's ambiguity. Upon observing $(X, Y) = (x, y)$, Alice draws the δ-tuple $\boldsymbol{M} = (M_1, \ldots, M_\delta)$ from the finite set $\mathbb{F}_{2^s}^{\delta}$ according to some conditional PMF

$$\mathbb{P}[\boldsymbol{M} = \mathbf{m}|X = x, Y = y], \quad \mathbf{m} \in \mathbb{F}_{2^s}^{\delta}. \quad (159)$$

We assume here that each hint comprises s bits (i.e., that $\boldsymbol{M}$ takes values in $\mathbb{F}_{2^s}^{\delta}$); why this assumption is reasonable will be explained shortly (see Theorem 27 and Remark 28 ahead). Bob gets to see a size-ν set $\mathcal{B} \subseteq \{1, \ldots, \delta\}$, the components $\boldsymbol{M}_{\mathcal{B}}$ of $\boldsymbol{M}$ indexed by $\mathcal{B}$, and the side information Y. As already mentioned, the index set $\mathcal{B}$ is chosen by an adversary of his. In the guessing version Bob guesses X using an optimal guessing function $G_{\mathcal{B}}(\cdot|Y, \boldsymbol{M}_{\mathcal{B}})$, which minimizes the ρ-th moment of the number of guesses that he needs. (As indicated by the subscript, the guessing function $G_{\mathcal{B}}(\cdot|Y, \boldsymbol{M}_{\mathcal{B}})$ can depend on $\mathcal{B}$.) His min-max ambiguity about X is thus given by

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_{X,Y}) = \min_{G_{\mathcal{B}^*}(\cdot|Y,\boldsymbol{M}_{\mathcal{B}^*})} \mathbb{E}\Big[\max_{\mathcal{B}} G_{\mathcal{B}}(X|Y, \boldsymbol{M}_{\mathcal{B}})^{\rho}\Big] \quad (160)$$

where $\mathcal{B}^*$ is the maximization-achieving set. In the list version Bob's ambiguity about X is

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_{X,Y}) = \mathbb{E}\Big[\max_{\mathcal{B}} \big|\mathcal{L}^{Y}_{\boldsymbol{M}_{\mathcal{B}}}\big|^{\rho}\Big] \quad (161)$$

where for all $y \in \mathcal{Y}$ and $\mathbf{m}_{\mathcal{B}} \in \mathbb{F}_{2^s}^{\delta}$

$$\mathcal{L}^{y}_{\mathbf{m}_{\mathcal{B}}} = \big\{x \colon \mathbb{P}[X = x|Y = y, \boldsymbol{M}_{\mathcal{B}} = \mathbf{m}_{\mathcal{B}}] > 0\big\} \quad (162)$$

is the list of all the realizations of X of positive posterior probability

$$\mathbb{P}[X = x|Y = y, \boldsymbol{M}_{\mathcal{B}} = \mathbf{m}_{\mathcal{B}}] = \frac{P_{X,Y}(x, y)\,\mathbb{P}[\boldsymbol{M}_{\mathcal{B}} = \mathbf{m}_{\mathcal{B}}|X = x, Y = y]}{\sum_{\tilde{x}} P_{X,Y}(\tilde{x}, y)\,\mathbb{P}[\boldsymbol{M}_{\mathcal{B}} = \mathbf{m}_{\mathcal{B}}|X = \tilde{x}, Y = y]}. \quad (163)$$

Note that for $\mathcal{B}^c \triangleq \{1, \ldots, \delta\} \setminus \mathcal{B}$ we have

$$\mathbb{P}[\boldsymbol{M}_{\mathcal{B}} = \mathbf{m}_{\mathcal{B}}|X = x, Y = y] = \sum_{\mathbf{m}_{\mathcal{B}^c}} \mathbb{P}[\boldsymbol{M} = \mathbf{m}|X = x, Y = y]. \quad (164)$$

Eve observes a size-η set $\mathcal{E} \subseteq \{1, \ldots, \delta\}$, the components $\boldsymbol{M}_{\mathcal{E}}$ of $\boldsymbol{M}$ indexed by $\mathcal{E}$, and the side information Y. The index set $\mathcal{E}$ is chosen by an accomplice of hers. Eve guesses X using an optimal guessing function $G_{\mathcal{E}}(\cdot|X, \boldsymbol{M}_{\mathcal{E}})$, which minimizes the ρ-th moment of the number of guesses that she needs. (The guessing function $G_{\mathcal{E}}(\cdot|X, \boldsymbol{M}_{\mathcal{E}})$ can depend on $\mathcal{E}$.) In both versions her ambiguity about X is thus given by

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) = \min_{G_{\mathcal{E}^*}(\cdot|X,\boldsymbol{M}_{\mathcal{E}^*})} \mathbb{E}\Big[\min_{\mathcal{E}} G_{\mathcal{E}}(X|Y, \boldsymbol{M}_{\mathcal{E}})^{\rho}\Big] \quad (165)$$

where $\mathcal{E}^*$ is the maximization achieving set.

Optimizing over Alice's choice of the conditional PMF in (159), we wish to characterize the largest ambiguity that we can guarantee that Eve will have subject to a given upper bound on the ambiguity that Bob may have.

Of special interest to us is the asymptotic regime where (X, Y) is an n-tuple (not necessarily drawn IID), and where each hint stores

$$s = nR_s \quad (166)$$

bits, where R_s is nonnegative and corresponds to the per-hint storage-rate. (We assume that δ, ν, and η are fixed.) For both versions of the problem, we shall characterize the largest exponential growth that we can guarantee for Eve's ambiguity subject to the constraint that Bob's ambiguity tend to one, i.e., we shall characterize the privacy-exponent $\overline{E_{\mathrm{E}}}$ defined in Definition 11.

In the next two theorems $(\nu - \eta)r$ should be viewed as the number of information-bits that can be gleaned about X from ν but not from η hints. Moreover, for every $\gamma \in \{\eta, \nu\}$, γp should be viewed as the number of information-bits that any γ hints reveal about X. By adapting the proof of Theorems 24 and 25 to the case at hand (see Appendix F), we obtain the following results.

Theorem 24 (Finite-Blocklength Guessing-Version): For every pair $(p, r) \in \{0, \ldots, s\}^2$ satisfying

$$p + r = s \quad (167a)$$

$$p,\ r \in \{0\} \cup \big\{\lceil \log \delta \rceil,\ \lceil \log \delta \rceil + 1, \ldots\big\} \quad (167b)$$

there is a choice of the conditional PMF in (159) for which Bob's ambiguity about X is upper-bounded by

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_{X,Y}) < 1 + 2^{\rho(H_{\tilde{\rho}}(X|Y) - \nu s + \eta r + 1)} \quad (168)$$

and Eve's ambiguity about X is lower-bounded by

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \geq 2^{\rho(H_{\tilde{\rho}}(X|Y) - \eta(s-r) - \eta \log \delta - \log(1 + \ln|\mathcal{X}|))}. \quad (169)$$

Conversely, for every conditional PMF, Bob's ambiguity is lower-bounded by

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_{X,Y}) \geq 2^{\rho(H_{\tilde{p}}(X|Y)-\nu s-\log(1+\ln|\mathcal{X}|))} \vee 1 \quad (170)$$

and Eve's ambiguity is upper-bounded by

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \leq 2^{\rho(\nu-\eta)s}\mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_{X,Y}) \wedge 2^{\rho H_{\tilde{p}}(X|Y)}. \quad (171)$$

Proof: See Appendix F. ∎

Theorem 25 (Finite-Blocklength List-Version): If $2^{\nu s} > \log|\mathcal{X}|+2$, then for every pair $(p,r) \in \{0,\ldots,s\}$ satisfying

$$p+r=s \quad (172a)$$
$$p,\ r \in \{0\} \cup \left\{\lceil \log\delta \rceil, \lceil \log\delta \rceil + 1, \ldots\right\} \quad (172b)$$
$$2^{\nu s-\eta r} > \log|\mathcal{X}|+2 \quad (172c)$$

there is a choice of the conditional PMF in (159) for which Bob's ambiguity about X is upper-bounded by

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_{X,Y}) < 1 + 2^{\rho(H_{\tilde{p}}(X|Y)-\log(2^{\nu s-\eta r}-\log|\mathcal{X}|-2)+2)} \quad (173)$$

and Eve's ambiguity about X is lower-bounded by

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \geq 2^{\rho(H_{\tilde{p}}(X|Y)-\eta(s-r)-\eta\log\delta-\log(1+\ln|\mathcal{X}|))}. \quad (174)$$

Conversely, for every conditional PMF, Bob's ambiguity is lower-bounded by

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_{X,Y}) \geq 2^{\rho(H_{\tilde{p}}(X|Y)-\nu s)} \vee 1 \quad (175)$$

and Eve's ambiguity is upper-bounded by

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \leq 2^{\rho(\nu-\eta)s}\mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_{X,Y}) \wedge 2^{\rho H_{\tilde{p}}(X|Y)}. \quad (176)$$

Proof: See Appendix F. ∎

The bounds in Theorems 24 and 25 are tight in the sense that, with a judicious choice of p and r, the achievability results (namely (168)–(169) in the guessing version and (173)–(174) in the list version) match the corresponding converse results (namely (170)–(171) in the guessing version and (175)–(176) in the list version) up to polynomial factors of δ^{η} and of $\ln|\mathcal{X}|$. This can be seen from the following corollary to Theorems 24 and 25, which states the achievability results in a simplified and more accessible form.

Corollary 26 (Simplified Finite-Blocklength Achievability-Results): In the guessing version, for any constant $\mathscr{U}_{\mathrm{B}}$ satisfying

$$\mathscr{U}_{\mathrm{B}} \geq 1 + 2^{\rho(H_{\tilde{p}}(X|Y)-\nu s+1)} \quad (177)$$

there is a choice of the conditional PMF in (159) for which Bob's ambiguity about X is upper-bounded by

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_{X,Y}) < \mathscr{U}_{\mathrm{B}} \quad (178)$$

and Eve's ambiguity about X is lower-bounded by

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \geq \left(\delta^{\eta}(1+\ln|\mathcal{X}|)\right)^{-\rho}\Big(\left((2\delta)^{-\rho\eta}2^{\rho(\nu-\eta)s}(\mathscr{U}_{\mathrm{B}}-1)\right) \wedge 2^{\rho H_{\tilde{p}}(X|Y)}\Big). \quad (179)$$

In the list version, for any constant $\mathscr{U}_{\mathrm{B}}$ satisfying

$$\mathscr{U}_{\mathrm{B}} \geq 1 + 2^{\rho(H_{\tilde{p}}(X|Y)-\log(2^{\nu s}-\log|\mathcal{X}|-2)+2)} \quad (180)$$

there is a choice of the conditional PMF in (159) for which Bob's ambiguity about X is upper-bounded by

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_{X,Y}) < \mathscr{U}_{\mathrm{B}} \quad (181)$$

and Eve's ambiguity about X is lower-bounded by

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \geq \left(\delta^{\eta}(1+\ln|\mathcal{X}|)\right)^{-\rho}\Big(\left(2^{-3\rho}(2\delta)^{-\rho\eta}2^{\rho(\nu-\eta)s}(\mathscr{U}_{\mathrm{B}}-1)\right) \wedge 2^{\rho H_{\tilde{p}}(X|Y)} \wedge \Big(\left(2(2\delta)^{\eta}\left(2+\log|\mathcal{X}|\right)\right)^{-\rho}2^{\rho((\nu-\eta)s+H_{\tilde{p}}(X|Y))}\Big)\Big). \quad (182)$$

Proof: The result is a corollary to Theorems 24 and 25. See Appendix G for a detailed proof. ∎

We conclude this section by explaining why it is a good idea to store an equal number of bits on each disk. This can be seen from the next theorem.

Theorem 27 (Converse Results: Disk ℓ stores s_ℓ Bits): Suppose that for every $\ell \in \{1,\ldots,\delta\}$ Disk ℓ stores s_ℓ bits, where $s_1 \leq \ldots \leq s_\delta$. For every conditional PMF in (159), Bob's ambiguity about X is—depending on the version of the problem—lower-bounded by

$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_{X,Y}) \geq 2^{\rho(H_{\tilde{p}}(X|Y)-\sum_{\ell=1}^{\nu}s_\ell-\log(1+\ln|\mathcal{X}|))} \vee 1 \quad (183a)$$
$$\mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_{X,Y}) \geq 2^{\rho(H_{\tilde{p}}(X|Y)-\sum_{\ell=1}^{\nu}s_\ell)} \vee 1 \quad (183b)$$

and Eve's ambiguity about X is upper-bounded by

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \leq 2^{\rho\sum_{\ell=1}^{\nu-\eta}s_\ell}\mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_{X,Y}) \wedge 2^{\rho H_{\tilde{p}}(X|Y)} \quad (184a)$$
$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \leq 2^{\rho\sum_{\ell=1}^{\nu-\eta}s_\ell}\mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_{X,Y}) \wedge 2^{\rho H_{\tilde{p}}(X|Y)}. \quad (184b)$$

Proof: See Appendix H. ∎

Remark 28 (Why Store s Bits on Each Disk?): Compare a scenario where for every $\ell \in \{1,\ldots,\delta\}$ Disk ℓ stores s_ℓ bits, where $s_1 \leq \ldots \leq s_\delta$, with a scenario where each disk stores $\lfloor (s_1+\ldots+s_\delta)/\delta \rfloor$ bits. Based on Theorem 27 and Corollary 26, neglecting polynomial factors of δ^{η} and of $\ln|\mathcal{X}|$, every pair of ambiguities for Bob and Eve that is achievable in the former scenario is also achievable in the latter scenario.

VIII. Summary

This paper studies a distributed-storage system whose encoder, Alice, observes some sensitive information X (e.g., a password) that takes values in a finite set $\mathcal{X}$ and describes it using two hints, which she stores in different locations. The legitimate receiver, Bob, sees both hints, and—depending on the version of the problem—must either guess X (the guessing version) or must form a list that is guaranteed to contain X (the list version). The eavesdropper, Alice, sees only one of the hints; an accomplice of hers controls which. Based on her observation, Eve wishes to guess X. For an arbitrary $\rho > 0$, Bob's and Eve's ambiguity about X are quantified as follows: In the guessing version we quantify Bob's ambiguity by the ρ-th moment of the number of guesses that he needs to guess X, and in the list version we quantify Bob's ambiguity by the ρ-th moment of the size of the list that he must

form. In both versions we quantify Eve's ambiguity by the ρ-th moment of the number of guesses that she needs to guess X. For each version this paper characterizes—up to polylogarithmic factors of $|\mathcal{X}|$—the largest ambiguity that we can guarantee that Eve will have subject to a given upper bound on the ambiguity that Bob may have. Our results imply that, if the hint that is available to Bob but not to Eve can assume σ realizations, then—up to polylogarithmic factors of $|\mathcal{X}|$—the ambiguity that we can guarantee that Eve will have either exceeds the ambiguity that Bob may have by a factor of σ^ρ or—in case the hint that Eve observes reveals no information about X—is as large as it can be. This holds even if we require that—up to polylogarithmic factors of $|\mathcal{X}|$—Bob's ambiguity be as small as it can be. The paper also discusses an extension to a distributed-storage system that is robust against disk failures and—in the supplementary material—a rate-distortion version of the problem.

The results for the guessing and the list version are remarkably similar: Every pair of ambiguities for Bob and Eve that is achievable in the guessing version is—up to polylogarithmic factors of $|\mathcal{X}|$—also achievable in the list version and vice versa. This can be explained by the close relation between Arikan's guessing problem [5] and Bunte and Lapidoth's task-encoding problem [6] that this paper reveals. The relation can be used to give alternative proofs of [6, Theorems I.2 and VI.2] as well as the direct part of [10, Theorem I.1]. As we show in the supplementary material, the relation holds also for the rate-distortion versions of the guessing and task-encoding problems, which were introduced in [6], [12]; and in this case it can be used to give an alternative proof of [6, Theorem VII.1].

Appendix A
Proof of Corollary 13

The converse results readily follow from the converse results of Theorem 12: (64) implies (70) and (65) implies (71). The proof of the achievability results (68)–(69) is more involved. Suppose that (67) holds. To show that there is a choice of the conditional PMF in (49) for which (68)–(69) hold, we will exhibit a judicious choice of the triple $(c_\mathrm{s}, c_1, c_2) \in \mathbb{N}^3$ for which (68) follows from (62) and (69) from (63). By possibly relabeling the hints, we can assume w.l.g. that $|\mathcal{M}_2| = |\mathcal{M}_1| \wedge |\mathcal{M}_2|$. Our choice of (c_s, c_1, c_2) depends on the constant $\mathscr{U}_\mathrm{B}$ and the cardinalities $|\mathcal{M}_1|$ and $|\mathcal{M}_2|$. Specifically, we distinguish between three different cases.

The first case is the case where

$$\mathscr{U}_\mathrm{B} \geq 1 + 2^{\rho(H_{\tilde{\rho}}(X|Y) - \log|\mathcal{M}_2| + 1)}. \tag{185}$$

In this case we choose

$$c_\mathrm{s} = |\mathcal{M}_2| \text{ and } c_1 = c_2 = 1. \tag{186}$$

Note that this choice satisfies (61). Consequently, (62) implies that Bob's ambiguity satisfies (68):

$$\mathscr{A}_\mathrm{B}^{(\mathrm{g})}(P_{X,Y}) < 1 + 2^{\rho(H_{\tilde{\rho}}(X|Y) - \log|\mathcal{M}_2| + 1)} \tag{187}$$

$$\leq \mathscr{U}_\mathrm{B} \tag{188}$$

where the second inequality holds by (185). Moreover, it follows from (63) that Eve's ambiguity satisfies (69):

$$\mathscr{A}_\mathrm{E}(P_{X,Y}) \geq (1 + \ln|\mathcal{X}|)^{-\rho} 2^{\rho(H_{\tilde{\rho}}(X|Y) - \log 2)} \tag{189}$$

$$= 2^{-\rho}(1 + \ln|\mathcal{X}|)^{-\rho} 2^{\rho H_{\tilde{\rho}}(X|Y)}. \tag{190}$$

The second case is the case where

$$\mathscr{U}_\mathrm{B} \geq 1 + \big\lfloor |\mathcal{M}_1|/|\mathcal{M}_2| \big\rfloor^{-\rho} 2^{\rho(H_{\tilde{\rho}}(X|Y) - \log|\mathcal{M}_2| + 1)} \tag{191a}$$

and

$$\mathscr{U}_\mathrm{B} < 1 + 2^{\rho(H_{\tilde{\rho}}(X|Y) - \log|\mathcal{M}_2| + 1)}. \tag{191b}$$

In this case we choose

$$c_\mathrm{s} = |\mathcal{M}_2| \tag{192a}$$

$$c_1 = \left\lceil 2^{H_{\tilde{\rho}}(X|Y) - \log|\mathcal{M}_2| + 1 - \rho^{-1}\log(\mathscr{U}_\mathrm{B} - 1)} \right\rceil \tag{192b}$$

$$c_2 = 1. \tag{192c}$$

By (191a), this choice satisfies (61). Moreover, note that

$$c_\mathrm{s} c_1 \; c_2 \geq |\mathcal{M}_2| \, 2^{H_{\tilde{\rho}}(X|Y) - \log|\mathcal{M}_2| + 1 - \rho^{-1}\log(\mathscr{U}_\mathrm{B} - 1)} \tag{193}$$

$$= 2^{H_{\tilde{\rho}}(X|Y) + 1 - \rho^{-1}\log(\mathscr{U}_\mathrm{B} - 1)}. \tag{194}$$

Consequently, it follows from (62) that Bob's ambiguity satisfies (68):

$$\mathscr{A}_\mathrm{B}^{(\mathrm{g})}(P_{X,Y}) < 1 + 2^{\rho(H_{\tilde{\rho}}(X|Y) - (H_{\tilde{\rho}}(X|Y) + 1 - \rho^{-1}\log(\mathscr{U}_\mathrm{B} - 1)) + 1)} \tag{195}$$

$$= \mathscr{U}_\mathrm{B}. \tag{196}$$

From (191b) it follows that

$$1 < 2^{H_{\tilde{\rho}}(X|Y) - \log|\mathcal{M}_2| + 1 - \rho^{-1}\log(\mathscr{U}_\mathrm{B} - 1)}. \tag{197}$$

Note that, for every $\xi > 1$, it holds that $\lceil \xi \rceil < 2\xi$. Consequently, (192) and (197) imply that

$$\lceil \xi \rceil < 2\xi, \quad \xi > 1 \tag{198}$$

imply that

$$c_1 + c_2 = c_1 + 1 \tag{199}$$

$$< 2 \; c_1 \tag{200}$$

$$< 2^{H_{\tilde{\rho}}(X|Y) - \log|\mathcal{M}_2| + 3 - \rho^{-1}\log(\mathscr{U}_\mathrm{B} - 1)}. \tag{201}$$

Eve's ambiguity satisfies (69), because from (63) and (201) it follows that:

$$\mathscr{A}_\mathrm{E}(P_{X,Y}) > \big(1 + \ln|\mathcal{X}|\big)^{-\rho} \cdot 2^{\rho(H_{\tilde{\rho}}(X|Y) - (H_{\tilde{\rho}}(X|Y) - \log|\mathcal{M}_2| + 3 - \rho^{-1}\log(\mathscr{U}_\mathrm{B} - 1)))} \tag{202}$$

$$= 2^{-3\rho}\big(1 + \ln|\mathcal{X}|\big)^{-\rho} |\mathcal{M}_2|^\rho (\mathscr{U}_\mathrm{B} - 1) \tag{203}$$

$$= 2^{-3\rho}\big(1 + \ln|\mathcal{X}|\big)^{-\rho} \big(|\mathcal{M}_1| \wedge |\mathcal{M}_2|\big)^\rho (\mathscr{U}_\mathrm{B} - 1) \tag{204}$$

where the last equality holds by the assumption that $|\mathcal{M}_2| = |\mathcal{M}_1| \wedge |\mathcal{M}_2|$.

The third and last case is the case where

$$\mathscr{U}_\mathrm{B} < 1 + \big\lfloor |\mathcal{M}_1|/|\mathcal{M}_2| \big\rfloor^{-\rho} 2^{\rho(H_{\tilde{\rho}}(X|Y) - \log|\mathcal{M}_2| + 1)}. \tag{205}$$

In this case we let $k^\star \in \mathbb{N}$ be the largest positive integer k for which

$$1 + 2^{\rho} k^{-\rho} \left\lfloor |\mathcal{M}_1|/k \right\rfloor^{-\rho} \left\lfloor |\mathcal{M}_2|/k \right\rfloor^{-\rho} 2^{\rho H_{\tilde{p}}(X|Y)} \le \mathscr{U}_{\mathrm{B}} \quad (206)$$

and we choose

$$c_{\mathrm{s}} = k^\star, \quad c_1 = \left\lfloor |\mathcal{M}_1|/k^\star \right\rfloor, \quad c_2 = \left\lfloor |\mathcal{M}_2|/k^\star \right\rfloor. \quad (207)$$

The existence of such a $k^\star$ follows from (67), which implies that (206) holds when we substitute 1 for k. The choice in (207) satisfies (61). Consequently, (62) implies that Bob's ambiguity satisfies (68):

$$\begin{aligned} \mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_{X,Y}) &< 1 + 2^{\rho(H_{\tilde{p}}(X|Y) - \log(c_{\mathrm{s}} \lfloor |\mathcal{M}_1|/c_{\mathrm{s}} \rfloor \lfloor |\mathcal{M}_2|/c_{\mathrm{s}} \rfloor) + 1)} && (208) \\ &\le \mathscr{U}_{\mathrm{B}} && (209) \end{aligned}$$

where in the second inequality we used that (206) holds when we substitute c_{s} for k. By the choice of c_{s} in (207) we also have

$$\begin{aligned} 2^{-\rho H_{\tilde{p}}(X|Y)} (\mathscr{U}_{\mathrm{B}} - 1) &< 2^{\rho} (c_{\mathrm{s}} + 1)^{-\rho} \left\lfloor \frac{|\mathcal{M}_1|}{c_{\mathrm{s}} + 1} \right\rfloor^{-\rho} \left\lfloor \frac{|\mathcal{M}_2|}{c_{\mathrm{s}} + 1} \right\rfloor^{-\rho} && (210) \\ &< 2^{3\rho} \left(\frac{c_{\mathrm{s}} + 1}{|\mathcal{M}_1|\,|\mathcal{M}_2|} \right)^{\rho} && (211) \\ &\le 2^{4\rho} \left(\frac{c_{\mathrm{s}}}{|\mathcal{M}_1|\,|\mathcal{M}_2|} \right)^{\rho} && (212) \end{aligned}$$

where (210) holds because c_{s} is the largest positive integer k for which (206) holds and consequently

$$\mathscr{U}_{\mathrm{B}} < 1 + 2^{\rho} (c_{\mathrm{s}} + 1)^{-\rho} \left\lfloor \frac{|\mathcal{M}_1|}{c_{\mathrm{s}} + 1} \right\rfloor^{-\rho} \left\lfloor \frac{|\mathcal{M}_2|}{c_{\mathrm{s}} + 1} \right\rfloor^{-\rho} 2^{\rho H_{\tilde{p}}(X|Y)}; \quad (213)$$

(211) holds because (205) and the fact that (206) holds for every positive integer $k < c_{\mathrm{s}} + 1$ imply that $|\mathcal{M}_2| \ge c_{\mathrm{s}} + 1$ and consequently that $|\mathcal{M}_1| \wedge |\mathcal{M}_2| \ge c_{\mathrm{s}} + 1$, and because

$$\xi/2 < \lfloor \xi \rfloor, \quad \xi \ge 1; \quad (214)$$

and (212) holds because $c_{\mathrm{s}} \ge 1$ and consequently $c_{\mathrm{s}} + 1 \le 2\, c_{\mathrm{s}}$. From (212) we obtain that

$$\begin{aligned} (c_1 + c_2)^{-\rho} &= \left(\left\lfloor |\mathcal{M}_1|/c_{\mathrm{s}} \right\rfloor + \left\lfloor |\mathcal{M}_2|/c_{\mathrm{s}} \right\rfloor \right)^{-\rho} && (215) \\ &\ge 2^{-\rho} \left(\frac{c_{\mathrm{s}}}{|\mathcal{M}_1|} \right)^{\rho} && (216) \\ &> 2^{-5\rho} |\mathcal{M}_2|^{\rho}\, 2^{-\rho H_{\tilde{p}}(X|Y)} (\mathscr{U}_{\mathrm{B}} - 1) && (217) \end{aligned}$$

where (215) holds by (207); (216) holds by the assumption that $|\mathcal{M}_2| \le |\mathcal{M}_1|$; and (217) holds by (212). From (217) and (63) we obtain that Eve's ambiguity satisfies (69):

$$\begin{aligned} \mathscr{A}_{\mathrm{E}}(P_{X,Y}) &> 2^{-5\rho} \left(1 + \ln |\mathcal{X}|\right)^{-\rho} |\mathcal{M}_2|^{\rho} (\mathscr{U}_{\mathrm{B}} - 1) && (218) \\ &= 2^{-5\rho} \left(1 + \ln |\mathcal{X}|\right)^{-\rho} \left(|\mathcal{M}_1| \wedge |\mathcal{M}_2|\right)^{\rho} (\mathscr{U}_{\mathrm{B}} - 1) && (219) \end{aligned}$$

where the last equality holds by the assumption that $|\mathcal{M}_2| = |\mathcal{M}_1| \wedge |\mathcal{M}_2|$.

APPENDIX B
PROOF OF COROLLARY 15

The converse results readily follow from the converse results of Theorem 14: (75) implies (81), and (76) implies (82). The proof of the achievability results (79)–(80) is more involved. Suppose that $|\mathcal{M}_1|\,|\mathcal{M}_2| > \log|\mathcal{X}| + 2$ and that (78) holds. To show that there is a choice of the conditional PMF in (49) for which (79)–(80) hold, we will exhibit a judicious choice of the triple $(c_{\mathrm{s}}, c_1, c_2) \in \mathbb{N}^3$ for which (79) follows from (73) and (80) from (74). By possibly relabeling the hints, we can assume w.l.g. that $|\mathcal{M}_2| = |\mathcal{M}_1| \wedge |\mathcal{M}_2|$. Our choice of $(c_{\mathrm{s}}, c_1, c_2)$ depends on $\mathscr{U}_{\mathrm{B}}$, $|\mathcal{M}_1|$, and $|\mathcal{M}_2|$; specifically, we distinguish three different cases.

The first case is the case where

$$\mathscr{U}_{\mathrm{B}} \ge 1 + 2^{\rho(H_{\tilde{p}}(X|Y) - \log(|\mathcal{M}_2| - \log|\mathcal{X}| - 2) + 2)}. \quad (220)$$

In this case we choose

$$c_{\mathrm{s}} = |\mathcal{M}_2|, \quad c_1 = c_2 = 1. \quad (221)$$

Note that this choice satisfies (72). Consequently, (73) implies that Bob's ambiguity satisfies (79), because

$$\begin{aligned} \mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_{X,Y}) &< 1 + 2^{\rho(H_{\tilde{p}}(X|Y) - \log(|\mathcal{M}_2| - \log|\mathcal{X}| - 2) + 2)} && (222) \\ &\le \mathscr{U}_{\mathrm{B}} && (223) \end{aligned}$$

where the second inequality holds by (220). Moreover, from (74) it follows that Eve's ambiguity satisfies (80):

$$\begin{aligned} \mathscr{A}_{\mathrm{E}}(P_{X,Y}) &\ge \left(1 + \ln |\mathcal{X}|\right)^{-\rho} 2^{\rho(H_{\tilde{p}}(X|Y) - \log 2)} && (224) \\ &= 2^{-\rho} \left(1 + \ln |\mathcal{X}|\right)^{-\rho} 2^{\rho H_{\tilde{p}}(X|Y)}. && (225) \end{aligned}$$

The second case is the case where

$$\mathscr{U}_{\mathrm{B}} \ge 1 + 2^{\rho(H_{\tilde{p}}(X|Y) - \log(|\mathcal{M}_2|\, \lfloor |\mathcal{M}_1|/|\mathcal{M}_2| \rfloor - \log|\mathcal{X}| - 2) + 2)} \quad (226a)$$

and

$$\mathscr{U}_{\mathrm{B}} < 1 + 2^{\rho(H_{\tilde{p}}(X|Y) - \log(|\mathcal{M}_2| - \log|\mathcal{X}| - 2) + 2)}. \quad (226b)$$

In this case we choose

$$\begin{aligned} c_{\mathrm{s}} &= |\mathcal{M}_2| && (227a) \\ c_1 &= \left\lceil \left(2^{H_{\tilde{p}}(X|Y) + 2 - \rho^{-1} \log(\mathscr{U}_{\mathrm{B}} - 1)} + \log|\mathcal{X}| + 2\right)/|\mathcal{M}_2| \right\rceil && (227b) \\ c_2 &= 1. && (227c) \end{aligned}$$

By (226a), this choice satisfies (72). Moreover, note that

$$c_{\mathrm{s}} c_1\ c_2 \ge 2^{H_{\tilde{p}}(X|Y) + 2 - \rho^{-1} \log(\mathscr{U}_{\mathrm{B}} - 1)} + \log|\mathcal{X}| + 2. \quad (228)$$

Consequently, (73) implies that Bob's ambiguity satisfies (79), because

$$\begin{aligned} \mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_{X,Y}) &< 1 + 2^{\rho\left(H_{\tilde{p}}(X|Y) - \log\left(2^{H_{\tilde{p}}(X|Y) + 2 - \rho^{-1} \log(\mathscr{U}_{\mathrm{B}} - 1)}\right) + 2\right)} && (229) \\ &= \mathscr{U}_{\mathrm{B}}. && (230) \end{aligned}$$

From (226b) it follows that

$$1 < \left(2^{H_{\tilde{p}}(X|Y) + 2 - \rho^{-1} \log(\mathscr{U}_{\mathrm{B}} - 1)} + \log|\mathcal{X}| + 2\right)/|\mathcal{M}_2|. \quad (231)$$

Note that, for every $\xi > 1$, it holds that $\lceil \xi \rceil < 2\xi$. Consequently, (227) and (231) imply that

$$\begin{aligned} &c_1 + c_2 \\ &= c_1 + 1 && (232)\\ &< 2c_1 && (233)\\ &< 4\Big(2^{H_{\tilde{p}}(X|Y)+2-\rho^{-1}\log(\mathscr{U}_{\mathrm{B}}-1)} + \log|\mathcal{X}| + 2\Big)/|\mathcal{M}_2|. && (234)\end{aligned}$$

From (74) and (234) it follows that Eve's ambiguity satisfies (80):

$$\begin{aligned} &\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \\ &> 2^{-2\rho}\big(1+\ln|\mathcal{X}|\big)^{-\rho}|\mathcal{M}_2|^{\rho} \\ &\quad \cdot 2^{\rho\left(H_{\tilde{p}}(X|Y)-\log\left(2^{H_{\tilde{p}}(X|Y)+2-\rho^{-1}\log(\mathscr{U}_{\mathrm{B}}-1)}+\log|\mathcal{X}|+2\right)\right)} && (235)\\ &= 2^{-2\rho}\big(1+\ln|\mathcal{X}|\big)^{-\rho}|\mathcal{M}_2|^{\rho}\, 2^{\rho H_{\tilde{p}}(X|Y)} \\ &\quad \cdot \big(2^{H_{\tilde{p}}(X|Y)+2-\rho^{-1}\log(\mathscr{U}_{\mathrm{B}}-1)} + \log|\mathcal{X}| + 2\big)^{-\rho} && (236)\\ &\geq 2^{-5\rho}\big(1+\ln|\mathcal{X}|\big)^{-\rho}|\mathcal{M}_2|^{\rho}(\mathscr{U}_{\mathrm{B}}-1) \\ &\quad \wedge 2^{-3\rho}\big(1+\ln|\mathcal{X}|\big)^{-\rho}(2+\log|\mathcal{X}|)^{-\rho}|\mathcal{M}_2|^{\rho}\, 2^{\rho H_{\tilde{p}}(X|Y)} && (237)\\ &= 2^{-5\rho}\big(1+\ln|\mathcal{X}|\big)^{-\rho}\big(|\mathcal{M}_1|\wedge|\mathcal{M}_2|\big)^{\rho}(\mathscr{U}_{\mathrm{B}}-1) \\ &\quad \wedge 2^{-3\rho}\big(1+\ln|\mathcal{X}|\big)^{-\rho}(2+\log|\mathcal{X}|)^{-\rho}\big(|\mathcal{M}_1|\wedge|\mathcal{M}_2|\big)^{\rho} \\ &\quad \cdot 2^{\rho H_{\tilde{p}}(X|Y)} && (238)\end{aligned}$$

where (237) holds because

$$\frac{1}{a+b} \geq \frac{1}{2a} \wedge \frac{1}{2b}, \quad a,\, b > 0; \tag{239}$$

and (238) holds by the assumption that $|\mathcal{M}_2| = |\mathcal{M}_1| \wedge |\mathcal{M}_2|$.

The third and last case is the case where

$$\mathscr{U}_{\mathrm{B}} < 1 + 2^{\rho(H_{\tilde{p}}(X|Y)-\log(|\mathcal{M}_2|\,\lfloor|\mathcal{M}_1|/|\mathcal{M}_2|\rfloor-\log|\mathcal{X}|-2)+2)}. \tag{240}$$

In this case we let $k^\star \in \mathbb{N}$ be the largest positive integer k for which

$$1 + 2^{\rho(H_{\tilde{p}}(X|Y)-\log(k\lfloor|\mathcal{M}_1|/k\rfloor\lfloor|\mathcal{M}_2|/k\rfloor-\log|\mathcal{X}|-2)+2)} \leq \mathscr{U}_{\mathrm{B}} \tag{241}$$

and we choose

$$c_{\mathrm{s}} = k^\star, \quad c_1 = \big\lfloor |\mathcal{M}_1|/k^\star \big\rfloor, \quad c_2 = \big\lfloor |\mathcal{M}_2|/k^\star \big\rfloor. \tag{242}$$

The existence of such a $k^\star$ follows from (78), which implies that (241) holds when we substitute 1 for k. Note that the choice in (242) satisfies (72). Consequently, (73) implies that Bob's ambiguity satisfies (79), because

$$\begin{aligned} &\mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_{X,Y}) \\ &< 1 + 2^{\rho(H_{\tilde{p}}(X|Y)-\log(c_{\mathrm{s}}\lfloor|\mathcal{M}_1|/c_{\mathrm{s}}\rfloor\lfloor|\mathcal{M}_2|/c_{\mathrm{s}}\rfloor-\log|\mathcal{X}|-2)+2)} && (243)\\ &\leq \mathscr{U}_{\mathrm{B}} && (244)\end{aligned}$$

where in the second inequality we used that (241) holds when we substitute c_{s} for k. By the choice of c_{s} in (242) we also have

$$\begin{aligned} &2^{-\rho(H_{\tilde{p}}(X|Y)+2)}(\mathscr{U}_{\mathrm{B}}-1) \\ &< \left((c_{\mathrm{s}}+1)\left\lfloor\frac{|\mathcal{M}_1|}{c_{\mathrm{s}}+1}\right\rfloor\left\lfloor\frac{|\mathcal{M}_2|}{c_{\mathrm{s}}+1}\right\rfloor - \log|\mathcal{X}| - 2\right)^{-\rho} && (245)\\ &< \left(\frac{|\mathcal{M}_1|\,|\mathcal{M}_2|}{4(c_{\mathrm{s}}+1)} - \log|\mathcal{X}| - 2\right)^{-\rho} && (246)\\ &\leq \left(\frac{|\mathcal{M}_1|\,|\mathcal{M}_2|}{8c_{\mathrm{s}}} - \log|\mathcal{X}| - 2\right)^{-\rho} && (247)\end{aligned}$$

where (245) holds because c_{s} is the largest positive integer k for which (241) holds and consequently

$$\mathscr{U}_{\mathrm{B}} < 1 + 2^{\rho\left(H_{\tilde{p}}(X|Y)-\log\left((c_{\mathrm{s}}+1)\left\lfloor\frac{|\mathcal{M}_1|}{c_{\mathrm{s}}+1}\right\rfloor\left\lfloor\frac{|\mathcal{M}_2|}{c_{\mathrm{s}}+1}\right\rfloor-\log|\mathcal{X}|-2\right)+2\right)}; \tag{248}$$

(246) holds because (240) and the fact that (241) holds for every positive integer $k < c_{\mathrm{s}} + 1$ imply that $|\mathcal{M}_2| \geq c_{\mathrm{s}} + 1$ and consequently that $|\mathcal{M}_1| \wedge |\mathcal{M}_2| \geq c_{\mathrm{s}} + 1$, and because

$$\xi/2 < \lfloor \xi \rfloor, \quad \xi \geq 1; \tag{249}$$

and (247) holds because $c_{\mathrm{s}} \geq 1$ and consequently $c_{\mathrm{s}}+1 \leq 2\, c_{\mathrm{s}}$. From (247) we obtain that

$$\left(\frac{c_{\mathrm{s}}}{|\mathcal{M}_1|}\right)^{\rho} > 2^{-3\rho}|\mathcal{M}_2|^{\rho}\Big((\mathscr{U}_{\mathrm{B}}-1)^{-1/\rho}2^{H_{\tilde{p}}(X|Y)+2} + \log|\mathcal{X}| + 2\Big)^{-\rho} \tag{250}$$

and consequently that

$$\begin{aligned} &(c_1+c_2)^{-\rho} \\ &= \Big(\big\lfloor|\mathcal{M}_1|/c_{\mathrm{s}}\big\rfloor + \big\lfloor|\mathcal{M}_2|/c_{\mathrm{s}}\big\rfloor\Big)^{-\rho} && (251)\\ &\geq 2^{-\rho}\left(\frac{c_{\mathrm{s}}}{|\mathcal{M}_1|}\right)^{\rho} && (252)\\ &> 2^{-4\rho}|\mathcal{M}_2|^{\rho}\Big((\mathscr{U}_{\mathrm{B}}-1)^{-1/\rho}2^{H_{\tilde{p}}(X|Y)+2} + \log|\mathcal{X}| + 2\Big)^{-\rho} && (253)\\ &\geq 2^{-7\rho}|\mathcal{M}_2|^{\rho}(\mathscr{U}_{\mathrm{B}}-1)2^{-\rho H_{\tilde{p}}(X|Y)} \\ &\quad \wedge 2^{-5\rho}(2+\log|\mathcal{X}|)^{-\rho}|\mathcal{M}_2|^{\rho} && (254)\end{aligned}$$

where (251) holds by (242); (252) holds by the assumption that $|\mathcal{M}_2| \leq |\mathcal{M}_1|$; (253) holds by (250); and (254) holds because

$$\frac{1}{a+b} \geq \frac{1}{2a} \wedge \frac{1}{2b}, \quad a,\, b > 0. \tag{255}$$

From (254) and (74) we obtain that Eve's ambiguity satisfies (80):

$$\begin{aligned} &\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \\ &> 2^{-5\rho}\big(1+\ln|\mathcal{X}|\big)^{-\rho}|\mathcal{M}_2|^{\rho} \\ &\quad \cdot \Big(2^{-2\rho}(\mathscr{U}_{\mathrm{B}}-1) \wedge \big(2+\log|\mathcal{X}|\big)^{-\rho}2^{\rho H_{\tilde{p}}(X|Y)}\Big) && (256)\\ &= 2^{-5\rho}\big(1+\ln|\mathcal{X}|\big)^{-\rho}\big(|\mathcal{M}_1|\wedge|\mathcal{M}_2|\big)^{\rho} \\ &\quad \cdot \Big(2^{-2\rho}(\mathscr{U}_{\mathrm{B}}-1) \wedge \big(2+\log|\mathcal{X}|\big)^{-\rho}2^{\rho H_{\tilde{p}}(X|Y)}\Big) && (257)\end{aligned}$$

where the last equality holds by the assumption that $|\mathcal{M}_2| = |\mathcal{M}_1| \wedge |\mathcal{M}_2|$.

APPENDIX C
PROOF OF THEOREM 19

We first establish the achievability results, i.e., (89)–(90). To this end suppose that $|\mathcal{M}_1| \wedge |\mathcal{M}_2| \geq 1 + \lfloor \log|\mathcal{X}| \rfloor$. Let

$$c_{\mathrm{s}} = 1 + \lfloor \log|\mathcal{X}| \rfloor, \quad c_1 = \left\lfloor \frac{|\mathcal{M}_1|}{c_{\mathrm{s}}} \right\rfloor, \quad c_2 = \left\lfloor \frac{|\mathcal{M}_2|}{c_{\mathrm{s}}} \right\rfloor \tag{258}$$

and for each $\nu \in \{c_{\mathrm{s}}, c_1, c_2\}$ let V_ν be a chance variable taking values in the set $\mathcal{V}_\nu = \{0, \ldots, c_\nu - 1\}$. Corollary 7 implies that there exists some $\{0, 1\}$-valued conditional PMF $\mathbb{P}\big[(V_1, V_2) = (v_1, v_2) \big| X = x, Y = y\big]$ for which

$$\min_{G(\cdot|Y,V_1,V_2)} \mathbb{E}\big[G(X|Y, V_1, V_2)^\rho\big] < 1 + 2^{\rho(H_{\tilde{p}}(X|Y) - \log(c_1\ c_2) + 1)}. \tag{259}$$

Draw (V_1, V_2) from $\mathcal{V}_1 \times \mathcal{V}_2$ according to the above conditional PMF. Fix $\epsilon > 0$ and draw (V_1', V_2') from $\mathcal{V}_1 \times \mathcal{V}_2$ according to the conditional PMF

$$\mathbb{P}\big[(V_1', V_2') = (v_1', v_2') \big| (V_1, V_2) = (v_1, v_2)\big] = \left(1 - 2^{-\epsilon} - \frac{2^{-\epsilon}}{|\mathcal{V}_1|\,|\mathcal{V}_2|}\right) \mathbb{1}_{\{(v_1', v_2') = (v_1, v_2)\}} + \frac{2^{-\epsilon}}{|\mathcal{V}_1|\,|\mathcal{V}_2|}. \tag{260}$$

Note that, irrespective of the realization (v_1, v_2) of (V_1', V_2'), the probability that (V_1', V_2') equals (v_1, v_2) is $1 - 2^{-\epsilon}$. Let $G_\star(\cdot|Y, V_1, V_2)$ be an optimal guessing function, which minimizes $\mathbb{E}\big[G(X|Y, V_1, V_2)^\rho\big]$. Define the guessing function $G(\cdot|Y, V_1', V_2')$ by

$$G(x|y, v_1', v_2') = G_\star(x|y, v_1', v_2'), \quad \forall\, (x, y, v_1', v_2') \in \mathcal{X} \times \mathcal{Y} \times \mathcal{V}_1 \times \mathcal{V}_2. \tag{261}$$

Using the trivial bound

$$G(x|y, v_1', v_2') \leq |\mathcal{X}|, \quad \forall\, (x, y, v_1', v_2') \in \mathcal{X} \times \mathcal{Y} \times \mathcal{V}_1 \times \mathcal{V}_2 \tag{262}$$

we obtain that

$$\mathbb{E}\big[G(X|Y, V_1', V_2')^\rho\big] \leq (1 - 2^{-\epsilon})\, \mathbb{E}\big[G_\star(X|Y, V_1, V_2)^\rho\big] + 2^{-\epsilon}|\mathcal{X}|^\rho. \tag{263}$$

Consequently,

$$\min_{G(\cdot|Y,V_1',V_2')} \mathbb{E}\big[G(X|Y, V_1', V_2')^\rho\big] \leq (1 - 2^{-\epsilon}) \min_{G(\cdot|Y,V_1,V_2)} \mathbb{E}\big[G(X|Y, V_1, V_2)^\rho\big] + 2^{-\epsilon}|\mathcal{X}|^\rho \tag{264}$$

$$< 1 + 2^{-(\epsilon - \rho\log|\mathcal{X}|)} + 2^{\rho(H_{\tilde{p}}(X|Y) - \log(c_1\ c_2) + 1)} \tag{265}$$

where (265) follows from (259). Corollary 10 and (258) imply that there exists some $\{0, 1\}$-valued conditional PMF

$$\mathbb{P}[V_{\mathrm{s}} = v_{\mathrm{s}} | X = x, Y = y, V_1' = v_1, V_2' = v_2]$$

for which

$$\mathbb{E}\Big[\big|\mathcal{L}^Y_{V_{\mathrm{s}}, V_1', V_2'}\big|^\rho\Big] \leq \min_{G(\cdot|Y,V_1',V_2')} \mathbb{E}\big[G(X|Y, V_1', V_2')^\rho\big] \tag{266}$$

$$< 1 + 2^{-(\epsilon - \rho\log|\mathcal{X}|)} + 2^{\rho(H_{\tilde{p}}(X|Y) - \log(c_1\ c_2) + 1)}. \tag{267}$$

Draw V_{s} from $\mathcal{V}_{\mathrm{s}}$ according to the above conditional PMF. Using the assumption that $|\mathcal{M}_1| \wedge |\mathcal{M}_2| \geq 1 + \lfloor \log|\mathcal{X}| \rfloor$ and (258), we obtain that

$$c_k > \frac{|\mathcal{M}_k|}{2\big(1 + \lfloor \log|\mathcal{X}| \rfloor\big)}, \quad k \in \{1, 2\}. \tag{268}$$

From (267) and (268) it follows that

$$\mathbb{E}\Big[\big|\mathcal{L}^Y_{V_{\mathrm{s}}, V_1', V_2'}\big|^\rho\Big] < 1 + 2^{-(\epsilon - \rho\log|\mathcal{X}|)} + 2^{\rho(H_{\tilde{p}}(X|Y) - \log(|\mathcal{M}_1|\,|\mathcal{M}_2|) + 2\log(1 + \lfloor \log|\mathcal{X}| \rfloor) + 3)}. \tag{269}$$

By (258) $|\mathcal{M}_1| \geq c_{\mathrm{s}} c_1$ and $|\mathcal{M}_2| \geq c_{\mathrm{s}} c_2$, and hence it suffices to prove (89)–(90) for a conditional PMF (49) that assigns positive probability only to $c_{\mathrm{s}} c_1$ elements of $\mathcal{M}_1$ and $c_{\mathrm{s}} c_2$ elements of $\mathcal{M}_2$, and we thus assume w.l.g. that $\mathcal{M}_1 = \mathcal{V}_{\mathrm{s}} \times \mathcal{V}_1$ and $\mathcal{M}_2 = \mathcal{V}_{\mathrm{s}} \times \mathcal{V}_2$. That is, we can choose $M_1 = (V_{\mathrm{s}} \oplus_{c_{\mathrm{s}}} U, V_1')$ and $M_2 = (U, V_2')$, where U is independent of $(X, Y, V_{\mathrm{s}}, V_1', V_2')$ and uniform over $\mathcal{V}_{\mathrm{s}}$. For this choice it follows from (269) that

$$\mathscr{A}^{(\mathrm{l})}_{\mathrm{B}}(P_{X,Y}) < 1 + 2^{-(\epsilon - \rho\log|\mathcal{X}|)} + 2^{\rho(H_{\tilde{p}}(X|Y) - \log(|\mathcal{M}_1|\,|\mathcal{M}_2|) + 2\log(1 + \lfloor \log|\mathcal{X}| \rfloor) + 3)}. \tag{270}$$

This proves that (89) holds for every sufficiently-large ϵ. As to (74), note that for every $\epsilon > 0$

$$\mathcal{L}^Y_{M_1} = \mathcal{L}^Y_{M_2} = \mathcal{L}^Y \tag{271}$$

because

$$\mathbb{P}[M_1 = m_1, M_2 = m_2 | X = x, Y = y] > 0, \quad \forall\, (x, y, m_1, m_2) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{M}_1 \times \mathcal{M}_2. \tag{272}$$

We next conclude by establishing the converse results (92)–(93). Theorem 4 implies (92); and (93) trivially holds, because the list that Eve forms based on Y and the hint that she observes cannot be larger than the list that she would have to form if she were to observe only Y.

APPENDIX D
PROOF OF THEOREMS 20 AND 21

We first establish the achievability results, i.e., (99)–(100) in the guessing version and (104)–(105) in the list version. To this end, fix $c \in \mathbb{N}$ satisfying (98) in the guessing version and (103) in the list version. Both (98) and (103) imply that $c \leq |\mathcal{M}_{\mathrm{p}}|$. Hence it suffices to prove (99)–(100) and (104)–(105) for a $\{0, 1\}$-valued conditional PMF as in (94) that assigns positive probability only to c elements of $\mathcal{M}_{\mathrm{p}}$. We can thus assume w.l.g. that $|\mathcal{M}_{\mathrm{p}}| = c$. Corollary 7 implies that there exists some $\{0, 1\}$-valued conditional PMF

$$\mathbb{P}[M_{\mathrm{p}} = m_{\mathrm{p}}, M_{\mathrm{s}} = m_{\mathrm{s}} | X = x, Y = y] \tag{273}$$

for which

$$\min_{G(\cdot|Y,M_{\mathrm{p}},M_{\mathrm{s}})} \mathbb{E}\big[G(X|Y, M_{\mathrm{p}}, M_s)^\rho\big] < 1 + 2^{\rho(H_{\tilde{p}}(X|Y) - \log(|\mathcal{M}_{\mathrm{p}}|\,|\mathcal{M}_{\mathrm{s}}|) + 1)} \tag{274}$$

$$= 1 + 2^{\rho(H_{\tilde{p}}(X|Y) - \log(c\,|\mathcal{M}_{\mathrm{s}}|) + 1)}. \tag{275}$$

In addition, Theorem 4 implies that there exists some deterministic task-encoder $f(\cdot|Y)\colon\ \mathcal{X} \to \mathcal{M}_{\mathrm{p}} \times \mathcal{M}_{\mathrm{s}}$ for which

$$\mathbb{E}\Big[\big|\mathcal{L}^{Y}_{M_{\mathrm{p}},M_{\mathrm{s}}}\big|^{\rho}\Big] < 1 + 2^{\rho(H_{\tilde{\rho}}(X|Y)-\log(|\mathcal{M}_{\mathrm{p}}\times\mathcal{M}_{\mathrm{s}}|-\log|\mathcal{X}|-2)+2)} \tag{276}$$

$$= 1 + 2^{\rho(H_{\tilde{\rho}}(X|Y)-\log(c\,|\mathcal{M}_{\mathrm{s}}|-\log|\mathcal{X}|-2)+2)} \tag{277}$$

where $(M_{\mathrm{p}}, M_{\mathrm{s}}) = f(X|Y)$. Accordingly, in the guessing version (99) follows from (275) and in the list version (104) follows from (277). Moreover, Corollary 7 implies (100) in the guessing version and (105) in the list version:

$$\min_{G(\cdot|Y,M_{\mathrm{p}})} \mathbb{E}\left[G(X|Y,M_{\mathrm{p}})^{\rho}\right] \geq \big(1+\ln|\mathcal{X}|\big)^{-\rho} 2^{\rho(H_{\tilde{\rho}}(X|Y)-\log|\mathcal{M}_{\mathrm{p}}|)} \tag{278}$$

$$= \big(1+\ln|\mathcal{X}|\big)^{-\rho} 2^{\rho(H_{\tilde{\rho}}(X|Y)-\log c)}. \tag{279}$$

It remains to establish the converse results, i.e., (101)–(102) in the guessing version and (106)–(107) in the list version. In the guessing version (101) follows from Corollary 7, and in the list version (106) follows from Theorem 4. To prove (102) and (107), we first note from Corollary 6 that

$$\min_{G(\cdot|Y,M_{\mathrm{p}},M_{\mathrm{s}})} \mathbb{E}\big[G(X|Y,M_{\mathrm{p}},M_{\mathrm{s}})^{\rho}\big] \geq |\mathcal{M}_{\mathrm{s}}|^{-\rho} \min_{G(\cdot|Y,M_{\mathrm{p}})} \mathbb{E}\big[G(X|Y,M_{\mathrm{p}})^{\rho}\big]. \tag{280}$$

Moreover, we also note that

$$\min_{G(\cdot|Y,M_{\mathrm{p}},M_{\mathrm{s}})} \mathbb{E}\big[G(X|Y,M_{\mathrm{p}},M_{\mathrm{s}})^{\rho}\big] \leq \mathbb{E}\Big[\big|\mathcal{L}^{Y}_{M_{\mathrm{p}},M_{\mathrm{s}}}\big|^{\rho}\Big]. \tag{281}$$

From (280) and (281) it follows that in both versions Eve's ambiguity exceeds Bob's by at most a factor of $|\mathcal{M}_{\mathrm{s}}|^{\rho}$, i.e., $\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \leq |\mathcal{M}_{\mathrm{s}}|^{\rho}\mathscr{A}^{(\mathrm{g})}_{\mathrm{B}}(P_{X,Y})$ and $\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \leq |\mathcal{M}_{\mathrm{s}}|^{\rho}\mathscr{A}^{(\mathrm{l})}_{\mathrm{B}}(P_{X,Y})$. Since Eve can ignore M_{p} and guess X based on Y alone, we obtain from Theorem 3 that in both versions Eve's ambiguity cannot exceed $2^{\rho H_{\tilde{\rho}}(X|Y)}$. That is,

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) = \min_{G(\cdot|Y,M_{\mathrm{p}})} \mathbb{E}\big[G(X|Y,M_{\mathrm{p}})^{\rho}\big] \leq 2^{\rho H_{\tilde{\rho}}(X|Y)}. \tag{282}$$

This concludes the proof of (102) and (107) and consequently that of the converse results.

Appendix E
Proof of Theorems 22 and 23

We first establish the achievability results, i.e., (113)–(114) in the guessing version and (118)–(119) in the list version. To this end fix $c \in \mathbb{N}$ satisfying (112) in the guessing version and (117) in the list version. Let M_{p} be a chance variable that takes values in the set $\mathcal{M}_{\mathrm{p}}$, and let M_{s} be a chance variable that takes values in the set $\mathcal{K}$. Corollary 7 implies that there exists some $\{0,1\}$-valued conditional PMF $\mathbb{P}[M_{\mathrm{p}} = m_{\mathrm{p}}, M_{\mathrm{s}} = m_{\mathrm{s}}|X = x, Y = y]$ for which

$$\min_{G(\cdot|Y,M_{\mathrm{p}},M_{\mathrm{s}})} \mathbb{E}\big[G(X|Y,M_{\mathrm{p}},M_{\mathrm{s}})^{\rho}\big] < 1 + 2^{\rho(H_{\tilde{\rho}}(X|Y)-\log(|\mathcal{M}_{\mathrm{p}}|\,|\mathcal{M}_{\mathrm{s}}|)-1)} \tag{283}$$

$$= 1 + 2^{\rho(H_{\tilde{\rho}}(X|Y)-\log(c\,|\mathcal{K}|)-1)}. \tag{284}$$

Theorem 4 implies that there exists some deterministic task-encoder $f(\cdot|Y)\colon \mathcal{X} \to \mathcal{M}_{\mathrm{p}} \times \mathcal{M}_{\mathrm{s}}$ for which

$$\mathbb{E}\Big[\big|\mathcal{L}^{Y}_{M_{\mathrm{p}},M_{\mathrm{s}}}\big|^{\rho}\Big] < 1 + 2^{\rho(H_{\tilde{\rho}}(X|Y)-\log(|\mathcal{M}_{\mathrm{p}}|\,|\mathcal{M}_{\mathrm{s}}|-\log|\mathcal{X}|-2)+2)} \tag{285}$$

$$= 1 + 2^{\rho(H_{\tilde{\rho}}(X|Y)-\log(c\,|\mathcal{K}|-\log|\mathcal{X}|-2)+2)} \tag{286}$$

where $(M_{\mathrm{p}}, M_{\mathrm{s}}) = f(X|Y)$. Both (112) and (117) imply that $c\,|\mathcal{K}| \leq |\mathcal{M}|$. Hence it suffices to prove (113)–(114) and (118)–(119) for a $\{0,1\}$-valued conditional PMF as in (108) that assigns positive probability only to $c\,|\mathcal{K}|$ elements of $\mathcal{M}$. We can thus assume w.l.g. that $\mathcal{M} = \mathcal{K} \times \mathcal{M}_{\mathrm{p}}$, where $\mathcal{M}_{\mathrm{p}}$ is a set of cardinality c, and $\mathcal{K} = \{0,\ldots,|\mathcal{K}|-1\}$. That is, we can choose $M = (M_{\mathrm{s}} \oplus_{|\mathcal{K}|} K, M_{\mathrm{p}})$, where $(M_{\mathrm{s}}, M_{\mathrm{p}})$ is drawn according to one of the above conditional PMFs depending on the version. Bob observes the hint M and the secret key K and can thus recover the pair $(M_{\mathrm{s}}, M_{\mathrm{p}})$. Hence, in the guessing version (113) follows from (284), and in the list version (118) follows from (286).

The proof of (114) and (119) is more involved. Note that in both versions (guessing and list) there exists some mapping $g\colon \mathcal{X}\times\mathcal{Y}\times\mathcal{M} \to \mathcal{K}$ for which

$$K = g(X,Y,M). \tag{287}$$

Given any guessing function $G(\cdot|Y,M)$ for X, introduce some guessing function $G(\cdot,\cdot|Y,M)$ for (X,K) satisfying that

$$G\big(x, g(x,y,m)\big|y,m\big) = G(x|y,m), \quad \forall\,(x,y,m) \in \mathcal{X}\times\mathcal{Y}\times\mathcal{M}. \tag{288}$$

From (287) it then follows that

$$G(X,K|Y,M) = G(X|Y,M), \tag{289}$$

and consequently that Eve can guess X and the pair (X,K) with the same number of guesses. In particular,

$$\mathbb{E}\big[G(X|Y,M)^{\rho}\big] = \mathbb{E}\big[G(X,K|Y,M)^{\rho}\big]. \tag{290}$$

Corollary 7 implies that

$$\min_{G(\cdot,\cdot|Y,M)} \mathbb{E}\big[G(X,K|Y,M)^{\rho}\big] \geq \big(1+\ln|\mathcal{X}|\big)^{-\rho} 2^{\rho(H_{\tilde{\rho}}(X,K|Y)-\log|\mathcal{M}|)} \tag{291}$$

$$= \big(1+\ln|\mathcal{X}|\big)^{-\rho} 2^{\rho(H_{\tilde{\rho}}(X,K|Y)-\log(c\,|\mathcal{K}|))}. \tag{292}$$

Note, that

$$H_{\tilde{\rho}}(X,K|Y) = \frac{1}{\rho}\log\sum_{y\in\mathcal{Y}}\left(\sum_{x\in\mathcal{X}}\sum_{k\in\mathcal{K}}\left(\frac{P_{X,Y}(x,y)}{|\mathcal{K}|}\right)^{\tilde{\rho}}\right)^{1+\rho} \tag{293}$$

$$= \frac{1}{\rho}\log\left(\sum_{y\in\mathcal{Y}}\left(\sum_{x\in\mathcal{X}}P_{X,Y}(x,y)^{\tilde{\rho}}\right)^{1+\rho}|\mathcal{K}|^{\rho}\right) \tag{294}$$

$$= H_{\tilde{\rho}}(X|Y) + \log|\mathcal{K}| \tag{295}$$

where the first equality holds because K is independent of (X,Y) and uniform over the set $\mathcal{K}$. Consequently, (290) and (292) imply (114) in the guessing version and (119) in the list version.

It remains to establish the converse results, i.e., (115)–(116) in the guessing version and (120)–(121) in the list version. To this end we first note that

$$\begin{aligned} &H_{\tilde{\rho}}(X|Y,K) \\ &\quad= \frac{\alpha}{1-\alpha}\log\sum_{y\in\mathcal{Y}}\sum_{k\in\mathcal{K}}\left(\sum_{x\in\mathcal{X}}\left(\frac{P_{X,Y}(x,y)}{|\mathcal{K}|}\right)^{\alpha}\right)^{\frac{1}{\alpha}} && (296)\\ &\quad= \frac{\alpha}{1-\alpha}\log\sum_{y\in\mathcal{Y}}\left(\sum_{x\in\mathcal{X}}P_{X,Y}(x,y)^{\alpha}\right)^{\frac{1}{\alpha}} && (297)\\ &\quad= H_{\tilde{\rho}}(X|Y) && (298)\end{aligned}$$

where the first equality holds because K is independent of (X,Y) and uniform over the set $\mathcal{K}$. In the guessing version (115) follows from Corollary 7 and (298), and in the list version (120) follows from Theorem 4 and (298). To prove (116) and (121), we first note that by Corollary 6

$$\begin{aligned}&\min_{G(\cdot|Y,K,M)}\mathbb{E}\big[G(X|Y,K,M)^{\rho}\big]\\ &\quad\geq|\mathcal{K}|^{-\rho}\min_{G(\cdot|Y,M)}\mathbb{E}\big[G(X|Y,M)^{\rho}\big].\end{aligned}\tag{299}$$

Because

$$\min_{G(\cdot|Y,K,M)}\mathbb{E}\big[G(X|Y,K,M)^{\rho}\big]\leq\mathbb{E}\Big[\big|\mathcal{L}_M^{Y,K}\big|^{\rho}\Big]\tag{300}$$

(299) implies that in both versions Eve's ambiguity exceeds Bob's by at most a factor of $|\mathcal{K}|^{\rho}$, i.e., $\mathscr{A}_{\mathrm{E}}(P_{X,Y})\leq|\mathcal{K}|^{\rho}\mathscr{A}_{\mathrm{B}}^{(\mathrm{g})}(P_{X,Y})$ and $\mathscr{A}_{\mathrm{E}}(P_{X,Y})\leq|\mathcal{K}|^{\rho}\mathscr{A}_{\mathrm{B}}^{(\mathrm{l})}(P_{X,Y})$. Since Eve can ignore M and guess X based on Y alone, we obtain from Theorem 3 that in both versions Eve's ambiguity cannot exceed $2^{\rho H_{\tilde{\rho}}(X|Y)}$:

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y})=\min_{G(\cdot|Y,M)}\mathbb{E}\big[G(X|Y,M)^{\rho}\big]\leq 2^{\rho H_{\tilde{\rho}}(X|Y)}.\tag{301}$$

This concludes the proof of (116) and (121) and consequently that of the converse results.

Appendix F
Proof of Theorems 24 and 25

Fix $p,r\in\{1,\dots,s\}$ satisfying (167) in the guessing version and (172) in the list version, and let V and W be chance variables taking values in $\mathcal{V}=\mathbb{F}_{2^p}^{\upsilon}$ and $\mathcal{W}=\mathbb{F}_{2^r}^{\upsilon-\eta}$, respectively. Corollary 7 implies that there exists some $\{0,1\}$-valued conditional PMF $\mathbb{P}\big[(V,W)=(v,w)\big|X=x,Y=y\big]$ for which

$$\min_{G(\cdot|Y,V,W)}\mathbb{E}\big[G(X|Y,V,W)^{\rho}\big]<1+2^{\rho(H_{\tilde{\rho}}(X|Y)-\upsilon s+\eta r+1)}.\tag{302}$$

Theorem 4 implies that there exists some deterministic task-encoder $f(\cdot|Y)\colon\mathcal{X}\to\mathcal{V}\times\mathcal{W}$ for which

$$\mathbb{E}\Big[\big|\mathcal{L}_{V,W}^{Y}\big|^{\rho}\Big]<1+2^{\rho(H_{\tilde{\rho}}(X|Y)-\log(2^{\upsilon s-\eta r}-\log|\mathcal{X}|-2)+2)}\tag{303}$$

where $(V,W)=f(X|Y)$. Draw U independently of (X,Y) and uniformly over $\mathbb{F}_{2^r}^{\eta}$. Choose $G_{\mathcal{V}}\in\mathbb{F}_{2^p}^{\upsilon\times\delta}$, $G_{\mathcal{W}}\in\mathbb{F}_{2^r}^{(\upsilon-\eta)\times\delta}$, and $G_{\mathcal{U}}\in\mathbb{F}_{2^r}^{\eta\times\delta}$ so that

$$G_{\mathcal{V}},\quad\begin{pmatrix}G_{\mathcal{U}}\\G_{\mathcal{W}}\end{pmatrix},\quad G_{\mathcal{U}}\tag{304}$$

are generator matrices of MDS codes. (This is possible, because both (167) and (172) imply that

$$p>0\implies 2^p\geq\delta\tag{305a}$$

$$r>0\implies 2^r\geq\delta;\tag{305b}$$

if $p=0$, then V can assume but one value, and hence we do not need $G_{\mathcal{V}}$; and if $r=0$, then (W,U) can assume but one value, and hence we do not need $G_{\mathcal{W}}$ and $G_{\mathcal{U}}$.) Define the chance variables

$$M_p=V\,G_{\mathcal{V}}\tag{306a}$$

$$M_r=U\,G_{\mathcal{U}}\oplus W\,G_{\mathcal{W}}=\begin{pmatrix}U & W\end{pmatrix}\begin{pmatrix}G_{\mathcal{U}}\\G_{\mathcal{W}}\end{pmatrix}\tag{306b}$$

where M_p is computed in the field $\mathbb{F}_{2^p}$ and M_r in $\mathbb{F}_{2^r}$. Note that $M_p\in\mathbb{F}_{2^p}^{\delta}$ and $M_r\in\mathbb{F}_{2^r}^{\delta}$. Since both (167) in the guessing version and (172) in the list version imply that $s=p+r$, Alice can choose the ℓ-th hint to comprise the ℓ-th components of M_p and M_r, so

$$M_\ell=\big([M_p]_\ell,[M_r]_\ell\big),\quad\ell\in\{1,\dots,\delta\}.\tag{307}$$

For this choice of the hints Bob can recover (V,W,U) no matter which υ hints he observes, because

$$G_{\mathcal{V}},\quad\begin{pmatrix}G_{\mathcal{U}}\\G_{\mathcal{W}}\end{pmatrix}\tag{308}$$

are generator matrices of MDS codes. Hence, in the guessing version (168) follows from (302), and in the list version (173) follows from (303).

The proof of (169) and (174) is more involved. Recall that Eve observes a size-η set $\mathcal{E}\subset\{1,\dots,\delta\}$ and the components $\boldsymbol{M}_{\mathcal{E}}$ of $\boldsymbol{M}$ indexed by $\mathcal{E}$. Index the possible sets that $\mathcal{E}$ could denote by the elements of some size-$\binom{\delta}{\eta}$ set $\mathcal{K}$, and denote by $\mathcal{E}(k)$ the set that is indexed by k. The proof of (169) and (174) builds on the following two intermediate claims, which we prove next:

1) Eve's ambiguity can be alternatively expressed as

$$\begin{aligned}&\mathscr{A}_{\mathrm{E}}(P_{X,Y})\\ &\quad=\min_{K,\,G(\cdot|Y,\boldsymbol{M}_{\mathcal{E}(K)},K)}\mathbb{E}\big[G(X|Y,\boldsymbol{M}_{\mathcal{E}(K)},K)^{\rho}\big]\end{aligned}\tag{309}$$

   where K is a chance variable of support $\mathcal{K}$, and where the minimization is over all conditional PMFs of K given $(X,Y,\boldsymbol{M})$ and all guessing functions $G(\cdot|Y,\boldsymbol{M}_{\mathcal{E}(K)},K)$.
2) We can assume w.l.g. that Eve must guess not only X but the pair (X,U).

We first prove Claim 1, i.e., that

$$\begin{aligned}&\min_{G_{\mathcal{E}}(\cdot|Y,\boldsymbol{M}_{\mathcal{E}})}\mathbb{E}\Big[\min_{\mathcal{E}}G_{\mathcal{E}}(X|Y,\boldsymbol{M}_{\mathcal{E}})^{\rho}\Big]\\ &\quad=\min_{K,\,G(\cdot|Y,\boldsymbol{M}_{\mathcal{E}(K)},K)}\mathbb{E}\big[G(X|Y,\boldsymbol{M}_{\mathcal{E}(K)},K)^{\rho}\big].\end{aligned}\tag{310}$$

Note that

$$\min_{\mathcal{E}}G_{\mathcal{E}}(X|Y,\boldsymbol{M}_{\mathcal{E}})=\min_{k}G_{\mathcal{E}(k)}(X|Y,\boldsymbol{M}_{\mathcal{E}(k)});\tag{311}$$

and for any given $G_{\mathcal{E}(k)}(\cdot|Y,\boldsymbol{M}_{\mathcal{E}(k)})$, $k\in\mathcal{K}$, define

$$K=\operatorname*{argmin}_{k}G_{\mathcal{E}(k)}(X|Y,\boldsymbol{M}_{\mathcal{E}(k)})\tag{312}$$

and introduce the guessing function $G(\cdot|Y, \boldsymbol{M}_{\mathcal{E}(K)}, K)$ satisfying that, for every $(x, y) \in \mathcal{X} \times \mathcal{Y}$, $\mathbf{m}_{\mathcal{E}(k)} \in \mathbb{F}_{2^s}^{\eta}$, and $k \in \mathcal{K}$,

$$G(x|y, \mathbf{m}_{\mathcal{E}(k)}, k) = G_{\mathcal{E}(k)}(x|y, \mathbf{m}_{\mathcal{E}(k)}). \tag{313}$$

We then obtain that

$$\mathbb{E}\big[G(X|Y, \boldsymbol{M}_{\mathcal{E}(K)}, K)^{\rho}\big] = \mathbb{E}\Big[\min_{\mathcal{E}} G_{\mathcal{E}}(X|Y, \boldsymbol{M}_{\mathcal{E}})^{\rho}\Big] \tag{314}$$

and consequently that

$$\begin{aligned}\min_{G_{\mathcal{E}}(\cdot|Y,\boldsymbol{M}_{\mathcal{E}})} &\mathbb{E}\Big[\min_{\mathcal{E}} G_{\mathcal{E}}(X|Y, \boldsymbol{M}_{\mathcal{E}})^{\rho}\Big] \\ &\geq \min_{K,\, G(\cdot|Y,\boldsymbol{M}_{\mathcal{E}},K)} \mathbb{E}\big[G(X|Y, \boldsymbol{M}_{\mathcal{E}(K)}, K)^{\rho}\big].\end{aligned} \tag{315}$$

To see that equality holds, note that, irrespective of K and $G(\cdot|Y, \boldsymbol{M}_{\mathcal{E}(K)}, K)$,

$$\mathbb{E}\big[G(X|Y, \boldsymbol{M}_{\mathcal{E}(K)}, K)^{\rho}\big] \geq \mathbb{E}\Big[\min_{k} G(X|Y, \boldsymbol{M}_{\mathcal{E}(k)}, k)^{\rho}\Big]. \tag{316}$$

For any given $G(\cdot|Y, \boldsymbol{M}_{\mathcal{E}(K)}, K)$ introduce the collection of guessing functions $G_{\mathcal{E}(k)}(\cdot|Y, \boldsymbol{M}_{\mathcal{E}(K)})$, $k \in \mathcal{K}$ that, for every $(x, y) \in \mathcal{X} \times \mathcal{Y}$ and $\mathbf{m}_{\mathcal{E}(k)} \in \mathbb{F}_{2^s}^{\eta}$, satisfy

$$G_{\mathcal{E}(k)}(x|y, \mathbf{m}_{\mathcal{E}(k)}) = G(x|y, \mathbf{m}_{\mathcal{E}(k)}, k). \tag{317}$$

We then obtain from (316) that

$$\mathbb{E}\big[G(X|Y, \boldsymbol{M}_{\mathcal{E}(K)}, K)^{\rho}\big] \geq \mathbb{E}\Big[\min_{k} G_{\mathcal{E}(k)}(X|Y, \boldsymbol{M}_{\mathcal{E}(k)})^{\rho}\Big] \tag{318}$$

and consequently that

$$\begin{aligned}\min_{G_{\mathcal{E}}(\cdot|Y,\boldsymbol{M}_{\mathcal{E}})} &\mathbb{E}\Big[\min_{\mathcal{E}} G_{\mathcal{E}}(X|Y, \boldsymbol{M}_{\mathcal{E}})^{\rho}\Big] \\ &\leq \min_{K,\, G(\cdot|Y,\boldsymbol{M}_{\mathcal{E}},K)} \mathbb{E}\big[G(X|Y, \boldsymbol{M}_{\mathcal{E}(K)}, K)^{\rho}\big].\end{aligned} \tag{319}$$

From (315) and (319) we conclude that (310) holds.

We next prove Claim 2. To this end we shall use Claim 1. Let K be any chance variable of finite support $\mathcal{K}$, and note that W is deterministic given (X, Y). By (306b)

$$[U\ G_{\mathcal{U}}]_{\mathcal{E}(K)} = [M_r]_{\mathcal{E}(K)} \ominus [W\ G_{\mathcal{V}}]_{\mathcal{E}(K)} \tag{320}$$

where $\ominus$ denotes subtraction in the field $\mathbb{F}_{2^r}$. Consequently, $[U\ G_{\mathcal{U}}]_{\mathcal{E}(K)}$ is deterministic given $(X, Y, \boldsymbol{M}_{\mathcal{E}(K)}, K)$. Because $G_{\mathcal{U}}$ is a generator matrix of an MDS code, and because $|\mathcal{E}(K)| = \eta$, it follows that U is deterministic given $(X, Y, \boldsymbol{M}_{\mathcal{E}(K)}, K)$, i.e., that there exists some mapping

$$g\colon \mathcal{X} \times \mathcal{Y} \times \mathbb{F}_{2^r}^{\eta} \times \mathcal{K} \to \mathcal{U} \tag{321}$$

for which

$$U = g(X, Y, \boldsymbol{M}_{\mathcal{E}(K)}, K). \tag{322}$$

Given any guessing function $G(\cdot|Y, \boldsymbol{M}_{\mathcal{E}(K)}, K)$ for X, introduce some guessing function $G(\cdot, \cdot|Y, \boldsymbol{M}_{\mathcal{E}(K)}, K)$ for (X, U) satisfying that

$$\begin{aligned}&G\big(X, g(X, Y, \boldsymbol{M}_{\mathcal{E}(K)}, K)\big|Y, \boldsymbol{M}_{\mathcal{E}(K)}, K\big) \\ &\quad = G(X|Y, \boldsymbol{M}_{\mathcal{E}(K)}, K)\end{aligned} \tag{323}$$

and note that

$$G(X, U|Y, \boldsymbol{M}_{\mathcal{E}(K)}, K) = G(X|Y, \boldsymbol{M}_{\mathcal{E}(K)}, K). \tag{324}$$

This proves Claim 2.

Having established Claims 1 and 2, we are now ready to prove (169) and (174):

$$\begin{aligned}&\min_{G_{\mathcal{E}}(\cdot|Y,\boldsymbol{M}_{\mathcal{E}})} \mathbb{E}\Big[\min_{\mathcal{E}} G_{\mathcal{E}}(X|Y, \boldsymbol{M}_{\mathcal{E}})^{\rho}\Big] \\ &\quad = \min_{K,\, G(\cdot|Y,\boldsymbol{M}_{\mathcal{E}},K)} \mathbb{E}\big[G(X|Y, \boldsymbol{M}_{\mathcal{E}(K)}, K)^{\rho}\big] && (325)\\ &\quad = \min_{K,\, G_{\mathcal{E}}(\cdot|Y,\boldsymbol{M}_{\mathcal{E}},K)} \mathbb{E}\big[G(X, U|Y, \boldsymbol{M}_{\mathcal{E}(K)}, K)^{\rho}\big] && (326)\\ &\quad \geq 2^{\rho(H_{\tilde{\rho}}(X,U|Y) - \eta s - \log\binom{\delta}{\eta} - \log(1+\ln|\mathcal{X}|))} && (327)\\ &\quad \geq 2^{\rho(H_{\tilde{\rho}}(X|Y) - \eta(s-r) - \eta\log\delta - \log(1+\ln|\mathcal{X}|))} && (328)\end{aligned}$$

where (325) holds by (310); (326) holds by (324); (327) follows from Corollary 7 and the fact that $(\boldsymbol{M}_{\mathcal{E}(K)}, K)$ takes values in a set of size $2^{\eta s}\binom{\delta}{\eta}$; and (328) holds because $\binom{\delta}{\eta} \leq \delta^{\eta}$ and

$$\begin{aligned}&H_{\tilde{\rho}}(X, U|Y) \\ &\quad = \frac{1}{\rho}\log\sum_{y\in\mathcal{Y}}\Bigg(\sum_{x\in\mathcal{X}}\sum_{u\in\mathbb{F}_{2^r}^{\eta}} \big(P_{X,Y}(x, y)/2^{\eta r}\big)^{\tilde{\rho}}\Bigg)^{1+\rho} && (329)\\ &\quad = \frac{1}{\rho}\log\Bigg(\sum_{y\in\mathcal{Y}}\Bigg(\sum_{x\in\mathcal{X}} P_{X,Y}(x, y)^{\tilde{\rho}}\Bigg)^{1+\rho} 2^{\rho\eta r}\Bigg) && (330)\\ &\quad = H_{\tilde{\rho}}(X|Y) + \eta r && (331)\end{aligned}$$

where (329) holds because U is independent of (X, Y) and uniform over the set $\mathbb{F}_{2^r}^{\eta}$ of size $2^{\eta r}$. This concludes the proof of the achievability results.

It remains to establish the converse results, i.e., (170)–(171) in the guessing version and (175)–(176) in the list version. To this end we first note that

$$\begin{aligned}\mathscr{A}_{\mathrm{B}}^{(g)}(P_{X,Y}) &= \min_{G_{\mathcal{B}}(\cdot|Y,\boldsymbol{M}_{\mathcal{B}})} \mathbb{E}\Big[\max_{\mathcal{B}} G_{\mathcal{B}}(X|Y, \boldsymbol{M}_{\mathcal{B}})^{\rho}\Big] \\ &\geq \min_{G_{\mathcal{B}}(\cdot|Y,\boldsymbol{M}_{\mathcal{B}})} \max_{\mathcal{B}} \mathbb{E}\big[G_{\mathcal{B}}(X|Y, \boldsymbol{M}_{\mathcal{B}})^{\rho}\big] && (332a)\\ \mathscr{A}_{\mathrm{B}}^{(l)}(P_{X,Y}) &= \mathbb{E}\Big[\max_{\mathcal{B}} \big|\mathcal{L}^{Y}_{\boldsymbol{M}_{\mathcal{B}}}\big|^{\rho}\Big] \\ &\geq \max_{\mathcal{B}} \mathbb{E}\Big[\big|\mathcal{L}^{Y}_{\boldsymbol{M}_{\mathcal{B}}}\big|^{\rho}\Big]. && (332b)\end{aligned}$$

Because $\mathcal{B} \subseteq \{1, \ldots, \delta\}$ is a size-ν set, in the guessing version (170) follows from (332a) and Corollary 7, and in the list version (175) follows from (332b) and Theorem 4. To prove (171) and (176), we first note that

$$\begin{aligned}\mathscr{A}_{\mathrm{E}}(P_{X,Y}) &= \min_{G_{\mathcal{E}}(\cdot|Y,\boldsymbol{M}_{\mathcal{E}})} \mathbb{E}\Big[\min_{\mathcal{E}} G_{\mathcal{E}}(X|Y, \boldsymbol{M}_{\mathcal{E}})^{\rho}\Big] && (333)\\ &\leq \min_{\mathcal{E},\, G_{\mathcal{E}}(\cdot|Y,\boldsymbol{M}_{\mathcal{E}})} \mathbb{E}\big[G_{\mathcal{E}}(X|Y, \boldsymbol{M}_{\mathcal{E}})^{\rho}\big]. && (334)\end{aligned}$$

Corollary 6 implies that, for every size-ν set $\mathcal{B} \subseteq \{1, \ldots, \delta\}$ and every size-η set $\mathcal{E} \subset \mathcal{B}$,

$$\begin{aligned}&\min_{G_{\mathcal{B}}(\cdot|Y,\boldsymbol{M}_{\mathcal{B}})} \mathbb{E}\big[G_{\mathcal{B}}(X|Y, \boldsymbol{M}_{\mathcal{B}})^{\rho}\big] \\ &\quad \geq 2^{-\rho(\nu-\eta)s} \min_{G_{\mathcal{E}}(\cdot|Y,\boldsymbol{M}_{\mathcal{E}})} \mathbb{E}\big[G_{\mathcal{E}}(X|Y, \boldsymbol{M}_{\mathcal{E}})^{\rho}\big];\end{aligned} \tag{335}$$

and, because

$$\min_{G_{\mathcal{B}}(\cdot|Y,\boldsymbol{M}_{\mathcal{B}})} \mathbb{E}\big[G_{\mathcal{B}}(X|Y,\boldsymbol{M}_{\mathcal{B}})^{\rho}\big] \le \mathbb{E}\Big[\big|\mathcal{L}^{Y}_{\boldsymbol{M}_{\mathcal{B}}}\big|\Big] \tag{336}$$

(334) and (335) imply that in both versions Eve's ambiguity exceeds Bob's by at most a factor of $2^{\rho(\nu-\eta)s}$, i.e., $\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \le 2^{\rho(\nu-\eta)s}\mathscr{A}^{(g)}_{\mathrm{B}}(P_{X,Y})$ and $\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \le 2^{\rho(\nu-\eta)s}\mathscr{A}^{(l)}_{\mathrm{B}}(P_{X,Y})$. Since Eve can ignore the hints that she observes and guess X based on Y alone, we obtain from Theorem 3 that, for every size-η set $\mathcal{E} \subset \{1,\dots,\delta\}$,

$$\min_{G_{\mathcal{E}}(\cdot|Y,\boldsymbol{M}_{\mathcal{E}})} \mathbb{E}\big[G_{\mathcal{E}}(X|Y,\boldsymbol{M}_{\mathcal{E}})^{\rho}\big] \le 2^{\rho H_{\tilde{\rho}}(X|Y)}; \tag{337}$$

and (334) and (337) imply that in both versions Eve's ambiguity cannot exceed $2^{\rho H_{\tilde{\rho}}(X|Y)}$, i.e., $\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \le 2^{\rho H_{\tilde{\rho}}(X|Y)}$. This concludes the proof of (171) and (176) and consequently that of the converse results.

Appendix G
Proof of Corollary 26

For the guessing version, the results in (178)–(179) follow from Theorem 24 if we let

$$\tilde{r} = \frac{\nu s + \rho^{-1}\log(\mathscr{U}_{\mathrm{B}}-1) - H_{\tilde{\rho}}(X|Y) - 1}{\eta} \tag{338}$$

$$r = \begin{cases} 0 & \lfloor\tilde{r}\rfloor \in (-\infty, \log\delta), \\ \lfloor\tilde{r}\rfloor & \lfloor\tilde{r}\rfloor \in [\log\delta, s-\log\delta), \\ s - \lceil\log\delta\rceil & \lfloor\tilde{r}\rfloor \in [s-\log\delta, s), \\ s & \lfloor\tilde{r}\rfloor \in [s,\infty) \end{cases} \tag{339}$$

$$p = s - r \tag{340}$$

and note that

$$r \ne s \implies \tilde{r} - r < \log\delta + 1. \tag{341}$$

To obtain the results in (181)–(182) for the list version, let

$$\tilde{r} = \frac{\nu s - \log\Big(2^{H_{\tilde{\rho}}(X|Y) - \frac{1}{\rho}\log(\mathscr{U}_{\mathrm{B}}-1)+2} + \log|\mathcal{X}| + 2\Big)}{\eta} \tag{342}$$

and choose r as in (339). Then, (173) implies that Bob's ambiguity satisfies (181). Since

$$r \ne s \implies \tilde{r} - r < \log\delta + 1 \tag{343}$$

we obtain from (174) that, if $r \ne s$, then

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) > 2^{\rho(H_{\tilde{\rho}}(X|Y)+(\nu-\eta)s - 2\eta\log\delta - \eta - \log(1+\ln|\mathcal{X}|))} \cdot \Big(2^{H_{\tilde{\rho}}(X|Y)-\frac{1}{\rho}\log(\mathscr{U}_{\mathrm{B}}-1)+2} + \log|\mathcal{X}| + 2\Big)^{-\rho}. \tag{344}$$

Because

$$\frac{1}{a+b} \ge \frac{1}{2}\,\frac{1}{a} \wedge \frac{1}{2}\,\frac{1}{b}, \quad a, b > 0 \tag{345}$$

the second factor satisfies the lower bound

$$\Big(2^{H_{\tilde{\rho}}(X|Y)-\frac{1}{\rho}\log(\mathscr{U}_{\mathrm{B}}-1)+2} + \log|\mathcal{X}| + 2\Big)^{-\rho} \ge 2^{-\rho(H_{\tilde{\rho}}(X|Y)-\frac{1}{\rho}\log(\mathscr{U}_{\mathrm{B}}-1)+3)} \wedge \big(2(\log|\mathcal{X}|+2)\big)^{-\rho}. \tag{346}$$

We are now ready to conclude the proof of (182): if $r \ne s$, then (182) follows from (344) and (346); and if $r = s$, then (174) implies that

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \ge 2^{\rho(H_{\tilde{\rho}}(X|Y) - \eta\log\delta - \log(1+\ln|\mathcal{X}|))} \tag{347}$$

and consequently that (182) holds.

Appendix H
Proof of Theorem 27

If we choose $\mathcal{B} = \{1,\dots,\nu\}$, then in the guessing version (183a) follows from (332a) and Corollary 7, and in the list version (183b) follows from (332b) and Theorem 4. For $\mathcal{B} = \{1,\dots,\nu\}$ and $\mathcal{E} = \{\nu-\eta+1,\dots,\nu\}$, Corollary 6 implies that

$$\min_{G_{\mathcal{B}}(\cdot|Y,\boldsymbol{M}_{\mathcal{B}})} \mathbb{E}\big[G_{\mathcal{B}}(X|Y,\boldsymbol{M}_{\mathcal{B}})^{\rho}\big] \ge 2^{-\rho\sum_{\ell=1}^{\eta-\nu} s_\ell} \min_{G_{\mathcal{E}}(\cdot|Y,\boldsymbol{M}_{\mathcal{E}})} \mathbb{E}\big[G_{\mathcal{E}}(X|Y,\boldsymbol{M}_{\mathcal{E}})^{\rho}\big]. \tag{348}$$

Since

$$\min_{G_{\mathcal{B}}(\cdot|Y,\boldsymbol{M}_{\mathcal{B}})} \mathbb{E}\big[G_{\mathcal{B}}(X|Y,\boldsymbol{M}_{\mathcal{B}})^{\rho}\big] \le \mathbb{E}\Big[\big|\mathcal{L}^{Y}_{\boldsymbol{M}_{\mathcal{B}}}\big|\Big] \tag{349}$$

(334) and (348) imply that in both versions Eve's ambiguity exceeds Bob's by at most a factor of $2^{\rho\sum_{\ell=1}^{\eta-\nu} s_\ell}$. That is,

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \le 2^{\rho\sum_{\ell=1}^{\eta-\nu} s_\ell}\mathscr{A}^{(g)}_{\mathrm{B}}(P_{X,Y}) \tag{350}$$

and

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \le 2^{\rho\sum_{\ell=1}^{\eta-\nu} s_\ell}\mathscr{A}^{(l)}_{\mathrm{B}}(P_{X,Y}). \tag{351}$$

Moreover, (334) and (337) imply that in both versions Eve's ambiguity cannot exceed $2^{\rho H_{\tilde{\rho}}(X|Y)}$. That is,

$$\mathscr{A}_{\mathrm{E}}(P_{X,Y}) \le 2^{\rho H_{\tilde{\rho}}(X|Y)} \tag{352}$$

which concludes the proof of (184).

Acknowledgment

The authors thank the Associate Editor and the anonymous referees for their helpful comments.

References

[1] P. Gasti and K. B. Rasmussen, "On the security of password manager database formats," in *Proc. Eur. Symp. Res. Comput. Secur.*, Pisa, Italy, Springer, Sep. 2012, pp. 770–787.
[2] D. Silver, S. Jana, D. Boneh, E. Chen, and C. Jackson, "Password managers: Attacks and defenses," in *Proc. USENIX Secur. Symp.*, San Diego, CA, USA, Aug. 2014, pp. 449–464.
[3] N. Merhav and E. Arikan, "The Shannon cipher system with a guessing wiretapper," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1860–1866, Sep. 1999.
[4] J. L. Massey, "Guessing and entropy," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun./Jul. 1994, p. 204.
[5] E. Arikan, "An inequality on guessing and its application to sequential decoding," *IEEE Trans. Inf. Theory*, vol. 42, no. 1, pp. 99–105, Jan. 1996.
[6] C. Bunte and A. Lapidoth, "Encoding tasks and Rényi entropy," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5065–5076, Sep. 2014.
[7] A. Bracher, E. Hof, and A. Lapidoth, "Distributed storage for data security," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Hobart, TAS, Australia, Nov. 2014, pp. 506–510.
[8] A. Bracher, A. Lapidoth, and C. Pfister, "Distributed task encoding," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Aachen, Germany, Jun. 2017, pp. 1993–1997.

[9] A. Bracher, A. Lapidoth, and C. Pfister, "Guessing with distributed encoders," *Entropy*, vol. 21, no. 3, p. 298, 2019. [Online]. Available: http://www.mdpi.com/1099-4300/21/3/298
[10] C. Bunte and A. Lapidoth, "On the listsize capacity with feedback," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6733–6748, Nov. 2014.
[11] A. Lapidoth and C. Pfister, "A method for the construction of optimal task encoders," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Hong Kong, Jun. 2015, pp. 2540–2544.
[12] E. Arikan and N. Merhav, "Guessing subject to distortion," *IEEE Trans. Inf. Theory*, vol. 44, no. 3, pp. 1041–1056, May 1998.
[13] A. Bracher, E. Hof, and A. Lapidoth, "Guessing attacks on distributed-storage systems," 2017, *arXiv:1701.01981*. [Online]. Available: https://arxiv.org/abs/1701.01981
[14] A. Subramanian and S. W. McLaughlin, "MDS codes on the erasure-erasure wiretap channel," 2009, *arXiv:0902.3286*. [Online]. Available: https://arxiv.org/abs/0902.3286
[15] N. Cai and R. W. Yeung, "Secure network coding on a wiretap network," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 424–435, Jan. 2011.
[16] S. El Rouayheb, E. Soljanin, and A. Sprintson, "Secure network coding for wiretap networks of type II," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1361–1371, Mar. 2012.
[17] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. AFIPS 79th Nat. Comput. Conf.*, Jun. 1979, pp. 313–317.
[18] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.
[19] G. R. Blakley and C. Meadows, "Security of ramp schemes," in *Advances in Cryptology—CRYPTO*, vol. 196. Berlin, Germany: Springer, 1985, pp. 242–268.
[20] C. E. Pfister and W. G. Sullivan, "Renyi entropy, guesswork moments, and large deviations," *IEEE Trans. Inf. Theory*, vol. 50, no. 11, pp. 2794–2800, Nov. 2004.
[21] R. Sundaresan, "Guessing under source uncertainty," *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 269–287, Jan. 2007.
[22] M. K. Hanawal and R. Sundaresan, "Guessing revisited: A large deviations approach," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 70–78, Jan. 2011.
[23] M. M. Christiansen and K. R. Duffy, "Guesswork, large deviations, and Shannon entropy," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 796–802, Feb. 2013.
[24] A. Beirami, R. Calderbank, K. Duffy, and M. Médard, "Quantifying computational security subject to source constraints, guesswork and inscrutability," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Hong Kong, Jun. 2015, pp. 2757–2761.
[25] R. Graczyk and A. Lapidoth, "Variations on the guessing problem," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Vail, CO, USA, Jun. 2018, pp. 231–235.
[26] Y. Hayashi and H. Yamamoto, "Coding theorems for the Shannon cipher system with a guessing wiretapper and correlated source outputs," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2808–2817, Jun. 2008.
[27] M. K. Hanawal and R. Sundaresan, "The Shannon cipher system with a guessing wiretapper: General sources," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2503–2516, Apr. 2011.
[28] S. Arimoto, "Information measures and capacity of order α for discrete memoryless channels," *Topics Inf. Theory*, vol. 17, no. 6, pp. 41–52, 1977.
[29] S. Fehr and S. Berens, "On the conditional Rényi entropy," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6801–6810, Nov. 2014.
[30] C. E. Shannon, "The zero error capacity of a noisy channel," *IRE Trans. Inf. Theory*, vol. 2, no. 3, pp. 8–19, Sep. 1956.
[31] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

Annina Bracher received the B.Sc. and M.Sc. degrees in electrical engineering (both with distinction) from ETH Zurich in 2010 and 2012 and an additional M.Sc. degree in engineering from Princeton University in 2014. She received the Ph.D. degree in electrical engineering from ETH Zurich in 2016. Dr. Bracher is now an Automotive Solutions and Risk Analytics Manager at Swiss Re.

Eran Hof received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from the Technion–Israel Institute of Technology, Haifa, Israel, in 2001, 2005, and 2010, respectively. During 2000–2001, he was with RAFAEL (Haifa, Israel). During 2001–2007, he was with the IDF communication R&D. During 2011–2017 he was with the Samsung semiconductor Israel R&D Center (Ramat-Gan, Israel). Since 2017 he is with Qualcomm Israel (Haifa, Israel).

Amos Lapidoth (S'89–M'95–SM'00–F'04) received the B.A. degree in Mathematics (*summa cum laude*, 1986), the B.Sc. degree in Electrical Engineering (*summa cum laude*, 1986), and the M.Sc. degree in Electrical Engineering (1990) all from the Technion—Israel Institute of Technology. His Ph.D. degree in Electrical Engineering is from Stanford University (1995).

In the years 1995–1999 he was an Assistant and Associate Professor at the department of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology (MIT), and was the KDD Career Development Associate Professor in Communications and Technology. He is now Professor of Information Theory at the Swiss Federal Institute of Technology (ETH) in Zurich, Switzerland

His research interests are in Digital Communications and Information Theory. He is the author of the textbook *A Foundation in Digital Communication*, second edition, Cambridge University Press, 2017.