Information Leakage in Zero-Error Source Coding: A Graph-Theoretic Perspective

Yucheng Liu†, Lawrence Ong†, Sarah Johnson†, Joerg Kliewer*, Parastoo Sadeghi‡, and Phee Lep Yeoh§
†The University of Newcastle, Australia (emails: {yucheng.liu, lawrence.ong, sarah.johnson}@newcastle.edu.au)
*New Jersey Institute of Technology, USA (email: jkliewer@njit.edu)
‡University of New South Wales, Canberra, Australia (email: p.sadeghi@unsw.edu.au)
§University of Sydney, Australia (email: phee.yeoh@sydney.edu.au)

2021 IEEE International Symposium on Information Theory (ISIT) | 978-1-5386-8209-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/ISIT45174.2021.9517778

***Abstract*—We study the information leakage to a guessing adversary in zero-error source coding. The source coding problem is defined by a confusion graph capturing the distinguishability between source symbols. The information leakage is measured by the ratio of the adversary's successful guessing probability after and before eavesdropping the codeword, maximized over all possible source distributions. Such measurement under the basic adversarial model where the adversary makes a single guess and the guess is regarded successful if and only if the estimator sequence equals to the true source sequence is known as the maximum min-entropy leakage or the maximal leakage in the literature. We develop a single-letter characterization of the optimal normalized leakage under the basic adversarial model, together with an optimum-achieving memoryless stochastic mapping scheme. An interesting observation is that the optimal normalized leakage is equal to the optimal compression rate with fixed-length source codes, both of which can be simultaneously achieved by some deterministic coding schemes. We then extend the leakage measurement to generalized adversarial models where the adversary makes multiple guesses and allows a certain level of distortion, for which we derive single-letter lower and upper bounds.**

I. Introduction

The classic problem of source coding introduced by Shannon [1] considers compression of an information source to represent data with fewer number of bits on average, allowing a vanishingly small average decoding error probability. In contrast, zero-error source coding is a different and related problem with its own significance in both a practical and theoretical sense. For an excellent survey, see [2]. In this work, we study the fundamental limits of information leakage in zero-error source coding from a graph-theoretic perspective.

Suppose we observe a source X and wish to transmit a compressed version of the source to a legitimate receiver. From the receiver's perspective, some source symbols are distinguishable (i.e., need to be distinguished) and some are not. The distinguishability relationship among source symbols is characterized by a *confusion graph* Γ for the source. For decoding to be considered successful, any distinguishable source sequences *must not* be mapped to the same codeword. This graph-theoretic model has various real-world applications. Consider the toy example in Fig. 1(a), where X denotes the water level of a reservoir, and a supervisor only needs to know whether the water level is relatively high or low to determine if refilling is needed.

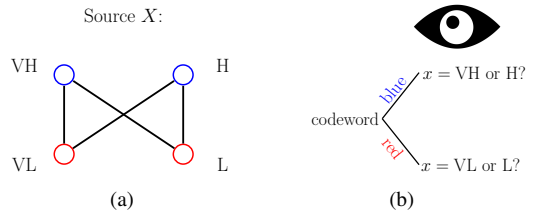

Figure 1. (a) From the perspective of the reservoir's supervisor, symbols VH (very high) and H (high) are indistinguishable (i.e., need not to be distinguished), and so are symbols VL (very low) and L (low). We draw an edge between any two distinguishable symbols, and then to satisfy the supervisor, we can only map non-adjacent symbols to the same codeword. (b) An adversary eavesdrops the codeword, based upon which it tries to guess the exact water level.

The source coding model we consider was originally introduced in a slightly different setup [3], where a vanishing error probability is allowed and the resulting optimal compression rate is defined as the *graph entropy* of the confusion graph. More recently, the joint source-channel coding problem has been analyzed [4] based on the same zero-error graph-theoretic setting as our model for the source coding.

Suppose that the transmitted codeword is eavesdropped by a guessing adversary, who knows the source distribution P_X and tries to guess the true source sequence via maximum likelihood estimation within a certain number of trials. See Fig. 1(b) for our toy example. Before observing the codeword, the adversary will guess the most likely water level among all four levels. After observing the codeword, say "blue", it will guess the more likely water level between VH and H.[1] In general, compared with guessing blindly (i.e., based only on P_X), the average successful guessing probability will increase as the adversary eavesdrops the codeword. We measure the information leakage from the codeword to the adversary by such a probability increase. More specifically, the leakage is quantified as the ratio be-

This work was supported by the ARC Discovery Scheme DP190100770; the US National Science Foundation Grant CNS-1815322; and the ARC Future Fellowship FT190100429.

[1]Like the receiver, in general the adversary may need not to distinguish all the source symbols, which can be characterized by an "adversary's confusion graph". Such case will be formally defined and studied in Section IV-B.

tween the adversary's probability of successful guessing *after and before* observing the codeword. This way of measuring information leakage was originally introduced in [5], leading to the leakage metric known as the *min-entropy leakage*.

Quite often in practice, the compression scheme is designed by the sender when the exact source distribution is unknown or subject to change. In such case, one can consider the *worst-case* leakage, which is the information leakage maximized over all possible source distributions P_X over a given source alphabet $\mathcal{X}$. The worst-case variant of the min-entropy leakage, namely the *maximum* min-entropy leakage, has been developed in [6].

A similar idea was independently explored in a different setup [7], [8] where the adversary is interested in guessing some randomized function U of X rather than X itself. The worst-case metric under such scenario is named as the *maximal leakage*. Interestingly, despite their different operational meanings, the maximal leakage and maximum min-entropy leakage turn out to be equal. For more works studying the maximal leakage or the maximum min-entropy leakage and their variants from both the information-theoretic and computer science perspectives, see [9]–[18]. In another related work [19], leakage in compression systems has been studied considering multiple leakage metrics, including the maximal leakage, under the assumption that the source code is deterministic and a random secret key is shared between the sender and the receiver. See [20]–[24] for more works on the general topic of information-theoretic secrecy and privacy.

Clearly we wish to keep the information leakage as small as possible by smartly designing a (possibly stochastic) source coding scheme. Therefore, our fundamental objective is to characterize the minimum leakage (normalized to the source sequence length) under the zero-error decoding requirement and also the optimum-achieving mapping scheme.

Contributions and organization: In Section II, we detail the problem of information leakage in source coding. In particular, we start with the basic adversarial model where the adversary makes a single guess and allows no distortion[2], and thus the resulting privacy metric is the normalized version of the maximal leakage [8] or the normalized maximum min-entropy leakage [6]. Our main contributions are as follows:

1) In Section III, we develop a single-letter characterization for the optimal normalized maximal leakage for the basic adversarial model. We also design a scalar stochastic mapping scheme that achieves this optimum. An interesting observation is that the optimal leakage can also be achieved using deterministic codes that simultaneously achieve the optimal fixed-length zero-error compression rate.

2) In Section IV, we extend our adversarial model to allow multiple guesses and distortion between an estimator (guess) and the true sequence, resulting in more generalized leakage metrics. Particularly, inspired by the notion of confusion graphs, we characterize the relationship between a sequence and its acceptable estimators for the adversary by another graph defined on the source alphabet.

[2]When no distortion is allowed, the adversary must guess the actual source sequence to be considered successful.

3) We then show that the optimal normalized leakage under the generalized models is always upper-bounded by the result in the original setup. Single-letter lower bounds (i.e., converse results) are also established.

Notation: For any discrete random variable Z with probability distribution P_Z, we denote its alphabet by $\mathcal{Z}$ with realizations $z \in \mathcal{Z}$. For any $K \subseteq \mathcal{Z}$, $P_Z(K) \doteq \sum_{z\in K} P_Z(z)$. For the definitions for basic graph-theoretic notions, see [25].

II. System Model and Problem Formulation

Source coding with confusion graph Γ: Consider a discrete memoryless stationary information source X that takes values in the alphabet $\mathcal{X}$ with full support. We wish to stochastically compress a source sequence $X^t \doteq (X_1, X_2, \ldots, X_t)$ to some codeword Y that takes values in the code alphabet $\mathcal{Y}$ and transmit it to a legitimate receiver via a noiseless channel. The randomized mapping scheme from $\mathcal{X}^t$ to $\mathcal{Y}$ is denoted by the conditional distribution $P_{Y|X^t}$.

To the receiver, the distinguishability relationship among source symbols is characterized by a confusion graph Γ, where the vertex set is the source alphabet, i.e., $V(\Gamma) = \mathcal{X}$, and any two symbols $x, x' \in \mathcal{X}$ are adjacent in Γ, i.e., $\{x, x'\} \in \mathcal{E}(\Gamma)$, if and only if (iff) they are distinguishable with each other. Any two source sequences, $x^t = (x_1, \ldots, x_t) \in \mathcal{X}^t$ and $v^t = (v_1, \ldots, v_t) \in \mathcal{X}^t$, are distinguishable iff at some $j \in [t]$, x_j and v_j are distinguishable. Therefore, the distinguishability among source sequences of length t is characterized by the confusion graph Γ_t, which is defined as the t-th power of Γ with respect to the *OR (disjunctive) graph product* [25, Section 3.4]: $\Gamma_t = \Gamma \vee \Gamma \vee \cdots \vee \Gamma = \Gamma^{\vee t}$.

To ensure zero-error decoding, any two source sequences that can be potentially mapped to the same codeword must not be distinguishable. More formally, given some $P_{Y|X^t}$, let

$$\mathcal{X}^t_{P_{Y|X^t}}(y) \doteq \{x^t \in \mathcal{X}^t : P_{Y|X^t}(y|x^t) > 0\} \tag{1}$$

denote the set of all x^t mapped to y with nonzero probability. When there is no ambiguity, we simply denote $\mathcal{X}^t_{P_{Y|X^t}}(y)$ by $\mathcal{X}^t(y)$. Therefore, a mapping scheme $P_{Y|X^t}$ is *valid* iff

$$\mathcal{X}^t(y) \in \mathcal{I}(\Gamma_t), \quad \forall y \in \mathcal{Y}, \tag{2}$$

where $\mathcal{I}(\cdot)$ denotes the set of independent sets of a graph.

Whenever we say a source coding problem Γ, we mean a zero-error source coding problem with confusion graph Γ.

Leakage to a guessing adversary: As a starting point, we assume that the adversary makes a single guess after observing each codeword and the guess is regarded successful iff the estimator sequence equals the true source sequence.

Consider any source coding problem Γ. The maximal leakage[3] for a given sequence length t and a given valid mapping $P_{Y|X^t}$ has been defined in [6] as:[4]

$$L^t(P_{Y|X^t}) \doteq \log \max_{P_X} \frac{\mathbb{E}_Y\left[\max\limits_{x^t\in\mathcal{X}^t} P_{X^t|Y}(x^t|Y)\right]}{\max\limits_{x^t\in\mathcal{X}^t} P_{X^t}(x^t)} \tag{3}$$

[3]For the rest of the paper, we adopt the name of maximal leakage [8].

[4]For notation brevity, we drop the reference to Γ noting that all leakage measures defined in this paper are dependent on Γ.

$$= \log \sum_{y \in \mathcal{Y}} \max_{x^t \in \mathcal{X}^t} P_{Y|X^t}(y|x^t), \tag{4}$$

where (4) is a re-statement of [6, Proposition 5.1]. The *optimal* maximal leakage for a given t is then defined as

$$\mathcal{L}^t \doteq \inf_{\substack{P_{Y|X^t}: \\ \mathcal{X}^t(y) \in \mathcal{I}(\Gamma_t), \forall y \in \mathcal{Y}}} L^t(P_{Y|X^t}). \tag{5}$$

Then we define the (optimal) maximal leakage rate as

$$\mathcal{L} \doteq \lim_{t \to \infty} t^{-1} \mathcal{L}^t. \tag{6}$$

III. Maximal Leakage Rate: Characterization

In the following we present a single-letter characterization of the maximal leakage rate $\mathcal{L}$.

Theorem 1: For any source coding problem Γ,

$$\mathcal{L} = \log \chi_f(\Gamma), \tag{7}$$

where $\chi_f(\Gamma)$ is the fractional chromatic number of Γ.

To prove Theorem 1, we introduce several useful lemmas.

We first prove that given any valid mapping, "merging" any two codewords does not increase the leakage (as long as the obtained mapping is still valid).

More precisely, consider any sequence length t and any valid mapping $P_{Y|X^t}$ such that there exists some *mergeable* codewords $y_1, y_2 \in \mathcal{Y}$, $y_1 \neq y_2$, satisfying $\mathcal{X}^t(y_1) \cup \mathcal{X}^t(y_2) \subseteq T$ for some $T \in \mathcal{I}_{\max}(\Gamma_t)$, where $\mathcal{I}_{\max}(\cdot)$ denotes the set of *maximal* independent sets of a graph. Construct $Y_{1,2}$ from Y by simply merging y_1 and y_2 to a new codeword $y_{1,2} \notin \mathcal{Y}$. Thus, $\mathcal{Y}_{1,2} = (\mathcal{Y} \setminus \{y_1, y_2\}) \cup \{y_{1,2}\}$, and for any $x^t \in \mathcal{X}^t$,

$$P_{Y_{1,2}|X^t}(y|x^t) = \begin{cases} P_{Y|X^t}(y_1|x^t) + P_{Y|X^t}(y_2|x^t), & \text{if } y = y_{1,2}, \\ P_{Y|X^t}(y|x^t), & \text{otherwise.} \end{cases} \tag{8}$$

As $Y_{1,2}$ is a deterministic function of Y, the Markov chain $X^t - Y - Y_{1,2}$ holds, and thus by [8, Lemma 1]], the result below holds.

Lemma 1: $L^t(P_{Y_{1,2}|X^t}) \leq L^t(P_{Y|X^t})$.

As specified in (2), for a valid mapping scheme, every codeword y should correspond to an independent set of the confusion graph Γ. As a consequence of Lemma 1, to characterize the optimal leakage, it suffices to consider only those mapping schemes for which all codewords y correspond to *distinct* maximal independent sets of Γ.

To formalize this observation, for any sequence length t, define the distortion function $d_t : \mathcal{X}^t \times \mathcal{I}_{\max}(\Gamma_t) \to \{0, 1\}$ such that for any $x^t \in \mathcal{X}^t$, $T \in \mathcal{I}_{\max}(\Gamma_t)$,

$$d(x^t, T) = \begin{cases} 0, & x^t \in T, \\ 1, & x^t \notin T. \end{cases} \tag{9}$$

Then the lemma below holds, where the proof can be found in the full version of this paper [26].

Lemma 2: To characterize $\mathcal{L}^t$ defined in (5), it suffices to assume the mapping $P_{Y|X^t}$ to satisfy that $\mathcal{Y} = \mathcal{I}_{\max}(\Gamma_t)$ and $d(X^t, Y) = 0$ almost surely. Thus by (4), we have

$$\mathcal{L}^t = \inf_{\substack{P_{Y|X^t}: \\ \mathcal{Y} = \mathcal{I}_{\max}(\Gamma_t), \\ d(X^t, Y) = 0}} \log \sum_{y \in \mathcal{Y}} \max_{x^t \in \mathcal{X}^t} P_{Y|X^t}(y|x^t). \tag{10}$$

The solution (i.e., the optimal objective value) to the optimization problem on the right hand side of (10) in Lemma 2 is characterized by [27, Corollary 1], based upon which we have the following result.

Lemma 3: $\mathcal{L}^t = -\log \eta_t$, where η_t is the solution to the following maxmin problem:

$$\text{maximize} \quad \min_{x^t \in \mathcal{X}^t} \sum_{T \in \mathcal{I}_{\max}(\Gamma_t): x^t \in T} \kappa_T, \tag{11a}$$

$$\text{subject to} \quad \sum_{T \in \mathcal{I}_{\max}(\Gamma_t)} \kappa_T = 1, \tag{11b}$$

$$\kappa_T \in [0, 1], \quad \forall T \in \mathcal{I}_{\max}(\Gamma_t). \tag{11c}$$

On the other hand, for any t, $\chi_f(\Gamma_t)$ is the solution to the following linear program [28, Section 2.2]:

$$\text{minimize} \quad \sum_{T \in \mathcal{I}_{\max}(\Gamma_t)} \lambda_T, \tag{12a}$$

$$\text{subject to} \quad \sum_{T \in \mathcal{I}_{\max}(\Gamma_t): x^t \in T} \lambda_T \geq 1, \quad \forall x^t \in \mathcal{X}^t, \tag{12b}$$

$$\lambda_T \in [0, 1], \quad \forall T \in \mathcal{I}_{\max}(\Gamma_t). \tag{12c}$$

We can show that the solutions to the optimization problems (11) and (12) are reciprocal to each other. That is,

$$\eta_t = 1/\chi_f(\Gamma_t), \tag{13}$$

where the proof is presented in Appendix A. The remaining proof of Theorem 1 follows easily from the above results.

Proof of Theorem 1: We have

$$\mathcal{L} \overset{(a)}{=} \lim_{t \to \infty} \frac{1}{t}(-\log \eta_t) \overset{(b)}{=} \lim_{t \to \infty} \frac{1}{t} \log \chi_f(\Gamma_t) \overset{(c)}{=} \log \chi_f(\Gamma).$$

where (a) follows from (6) and Lemma 3, (b) follows (13), and (c) follows from the fact that $\chi_f(\Gamma_t) = \chi_f(\Gamma^{\vee t}) = \chi_f(\Gamma)^t$ (cf. [25, Corollary 3.4.2]). ∎

Having characterized the optimal maximal leakage rate $\mathcal{L}$ in Theorem 1, in the following we design an optimal mapping scheme $P_{Y|X^t}$ for some t that achieves $\mathcal{L}$, which is based on the optimal fractional coloring of the confusion graph Γ.

Fix $t = 1$. For $\Gamma_1 = \Gamma$, there always exists some b-fold coloring $\mathcal{P} = \{T_1, T_2, \ldots, T_m\}$ for some finite positive integer b such that $\chi_f(\Gamma) = m/b$ (cf. [25, Section 3.1]).

Set $\mathcal{Y} = \mathcal{P}$ (and thus every codeword $y \in \mathcal{Y}$ is actually an independent set of Γ). Set

$$P_{Y|X}(y|x) = \begin{cases} 1/b, & \text{if } x \in y, \\ 0, & \text{otherwise.} \end{cases} \tag{14}$$

As every $x \in \mathcal{X}$ is in exactly b sets within $\mathcal{P}$, we have

$$\sum_{y \in \mathcal{Y}} P_{Y|X}(y|x) = \sum_{y \in \mathcal{Y}: x \in y} \frac{1}{b} + \sum_{y \in \mathcal{Y}: x \notin y} 0 = 1, \quad \forall x \in \mathcal{X},$$

and thus $P_{Y|X}$ is a valid mapping scheme. We have

$$L^1(P_{Y|X}) = \log \sum_{y \in \mathcal{Y}} \max_{x \in \mathcal{X}} P_{Y|X}(y|x) = \log \sum_{y \in \mathcal{P}} \frac{1}{b} = \log \frac{m}{b} = \log \chi_f(\Gamma), \tag{15}$$

and thus we know that the maximal leakage rate in Theorem 1 is indeed achievable by the mapping described in (14).

Remark 1: Consider any source coding problem Γ. We know that the optimal zero-error compression rate (with fixed-length deterministic source codes) is

$$\mathcal{R} = \lim_{t\to\infty} \frac{1}{t} \log \chi(\Gamma^{\vee t}) = \lim_{t\to\infty} \frac{1}{t} \log \chi_f(\Gamma^{\vee t}) = \log \chi_f(\Gamma),$$

where the second equality follows from [25, Corollary 3.4.3]. The above result holds even when we allow stochastic coding. Thus the maximal leakage rate $\mathcal{L}$ always equals to the optimal compression rate $\mathcal{R}$. Moreover, it can be verified that any $\mathcal{R}$-achieving deterministic code can simultaneously achieve $\mathcal{L}$. In other words, when considering fixed-length source coding, there is no trade-off between the compression rate and the leakage rate. Furthermore, we observe the following:

1) Our characterization of $\mathcal{L}$ holds generally and does not rely on the assumption of fixed-length coding;
2) While in general, the optimal zero-error compression rate $\mathcal{R}$ and the maximal leakage rate $\mathcal{L}$ can be simultaneously and asymptotically attained at the limit of increasing t, we showed in (15) that $\mathcal{L}$, on the other hand, can be achieved exactly even with $t = 1$ (using the symbol-by-symbol encoding scheme specified in (14) based on the factional coloring of Γ), but possibly at the expense of the compression rate.
3) For variable-length source coding, whether there is a compression-leakage trade-off remains unclear.

IV. Extensions on the Maximal Leakage Rate: Multiple and Approximate Guesses

In general, the adversary may be able to make multiple guesses. For example, the adversary may possess a testing mechanism to verify whether its guess is correct or not, and thus can perform a trial and error attack until it is stopped by the system. Also, for each true source sequence, there may be multiple estimators other than the true sequence itself that are "close enough" and thus can be regarded successful.

We generalize our definition of information leakage to cater to the above scenarios. Consider any source coding problem Γ, sequence length t, and valid mapping $P_{Y|X^t}$. Suppose the adversary generates a set of guesses $K \subseteq \mathcal{X}^t$. For each set K, define a "covering" set K^+, where $K \subseteq K^+ \subseteq \mathcal{X}^t$, such that if the true sequence is in K^+, then the adversary's guess list K is considered successful. Let

$$\mathcal{S} \doteq \{K^+ : K \text{ is a guess list the adversary can choose}\}$$

be the collection of all possible K^+. Then for the blind guessing, the successful probability is $\max_{S\in\mathcal{S}} \sum_{x^t\in S} P_{X^t}(x^t)$, and for guessing after observing Y, the average successful probability is $\mathbb{E}_Y\left[\max_{S\in\mathcal{S}} \sum_{x^t\in S} P_{X^t|Y}(x^t|Y)\right]$. In the same spirit of maximal leakage, we can define

$$\rho_t(P_{Y|X^t}, \mathcal{S}) \doteq \log \max_{P_X} \frac{\mathbb{E}_Y\left[\max_{S\in\mathcal{S}} \sum_{x^t\in S} P_{X^t|Y}(x^t|Y)\right]}{\max_{S\in\mathcal{S}} \sum_{x^t\in S} P_{X^t}(x^t)}$$

as the ratio between the a posteriori and a priori successful guessing probability. If we set $\mathcal{S}_{\text{singleton}} = \{\{x^t\} : x^t \in \mathcal{X}^t\}$, that is, the adversary is allowed one guess and it must guess the correct source sequence precisely, the maximal leakage defined in (3) can be equivalently written as

$$L^t(P_{Y|X^t}) = \rho_t(P_{Y|X^t}, \mathcal{S}_{\text{singleton}}).$$

In the next two subsections, we study different scenarios where the adversary makes multiple guesses allowing no distortion and one guess allowing certain distortion, respectively. For the investigation of the leakage under the generic adversarial model where the adversary makes multiple guesses allowing distortion, see the full version of this paper [26].

A. Leakage for the Case of Multiple Guesses

We first consider the case where the adversary makes multiple guesses, yet does not allow distortion.

We characterize the number of guesses the adversary can make by a *guessing capability* function $g(t)$, where $t \in \mathbb{Z}^+$ is the sequence length. We assume $g(t)$ to be positive, integer-valued, non-decreasing, and upper-bounded[5] by $\alpha(\Gamma_t) = \alpha(\Gamma^{\vee t}) = \alpha(\Gamma)^t$, where $\alpha(\cdot)$ denotes the independence number of a graph.

Consider any source coding problem Γ and any guessing-capability function g. For a given sequence length t and a given valid mapping $P_{Y|X^t}$, the maximal leakage naturally extends to the *multi-guess* maximal leakage, defined as

$$L_g^t(P_{Y|X^t}) \doteq \rho_t(P_{Y|X^t}, \mathcal{S}_g), \tag{16}$$

where $\mathcal{S}_g = \{K \subseteq \mathcal{X}^t : |K| = g(t)\}$. Then we can define the (optimal) multi-guess maximal leakage rate as

$$\mathcal{L}_g \doteq \lim_{t\to\infty} \frac{1}{t} \inf_{\substack{P_{Y|X^t}: \\ \mathcal{X}^t(y)\in\mathcal{I}(\Gamma_t),\forall y\in\mathcal{Y}}} L_g^t(P_{Y|X^t}). \tag{17}$$

We first show that the multi-guess maximal leakage rate is always not larger than the maximal leakage rate.

Lemma 4: We have $\mathcal{L}_g \le \mathcal{L}$.

Proof: It suffices to show $L_g^t(P_{Y|X^t}) \le L^t(P_{Y|X^t})$ for any t and $P_{Y|X^t}$. For any P_X, we have

$$\begin{aligned}
&\frac{\sum_{y\in\mathcal{Y}} \max_{K\subseteq\mathcal{X}^t:|K|=g(t)} \sum_{x^t\in K} P_{X^t,Y}(x^t, y)}{\max_{K\subseteq\mathcal{X}^t:|K|=g(t)} \sum_{x^t\in K} P_{X^t}(x^t)} \\
&\le \frac{\sum_{y\in\mathcal{Y}} \Big(\max_{K\subseteq\mathcal{X}^t:|K|=g(t)} \sum_{x^t\in K} P_{X^t}(x^t)\Big)\Big(\max_{\tilde{x}^t\in\mathcal{X}^t} P_{Y|X^t}(y|\tilde{x}^t)\Big)}{\max_{K\subseteq\mathcal{X}^t:|K|=g(t)} \sum_{x^t\in K} P_{X^t}(x^t)} \\
&= \sum_{y\in\mathcal{Y}} \max_{x^t\in\mathcal{X}^t} P_{Y|X^t}(y|x^t),
\end{aligned}$$

which implies that $L_g^t(P_{Y|X^t}) \le L^t(P_{Y|X^t})$. ∎

The following single-letter lower and upper bounds hold.

Theorem 2: We have

$$\log|V(\Gamma)| - \log\alpha(\Gamma) \le \mathcal{L}_g \le \log\chi_f(\Gamma). \tag{18}$$

[5]Suppose for some t we have $g(t) \ge \alpha(\Gamma_t)$. Then upon observing any codeword y, the adversary can always determine the true source value by exhaustively guessing all possible $x^t \in \mathcal{X}^t(y)$ as $|\mathcal{X}^t(y)| \le \alpha(\Gamma_t)$.

The proof of the above theorem can be found in the full version of this paper [26].

When the adversary guesses some randomized function U of X rather than X itself, the maximal leakage is equal to its multi-guess extension [8]. It remains to be investigated whether a similar equivalence holds generally in our setup. In the following, we confirm one special case where indeed $\mathcal{L}_g = \mathcal{L}$ and consequently, by Theorem 1, $\mathcal{L}_g = \log \chi_f(\Gamma)$.

Proposition 1: Consider any source coding problem Γ. If $\lim_{t\to\infty} \frac{1}{t} \log g(t) = 0$, then $\mathcal{L}_g = \mathcal{L} = \log \chi_f(\Gamma)$.

The proof of the above result is presented in [26]. Intuitively, Proposition 1 suggests that when the number of guesses the adversary can make does not grow "fast enough" with respect to t, it makes no difference whether the adversary is making one guess or multiple guesses (in terms of the leakage defined in (6) and (17)).

As a direct corollary of Theorem 2, the result below shows that $\mathcal{L}_g = \mathcal{L} = \log \chi_f(\Gamma)$ holds for another specific scenario.

Corollary 1: If Γ is vertex-transitive[6] [25, Section 1.3], then $\mathcal{L}_g = \mathcal{L} = \log \chi_f(\Gamma)$ for any function g.

Proof: Since Γ is vertex-transitive, by [25, Proposition 3.1.1], we have $\chi_f(\Gamma) = |V(\Gamma)|/\alpha(\Gamma)$, which indicates that lower and upper bounds in Theorem 2 match with each other, thus establishing $\mathcal{L}_g = \log \chi_f(\Gamma) = \mathcal{L}$. ∎

B. Leakage for the Case of One Approximate Guess

Suppose that the adversary makes only one guess, yet allows a certain level of distortion between its estimator and the true source value. That is, the guess is regarded successful as long as the estimator is an acceptable *approximation* to the true value. Inspired by the notion of confusion graph Γ that characterizes the distinguishability within the source symbols, we introduce another graph to characterize the approximation relationship among source symbols (from the adversary's perspective). We call this graph the adversary's approximation graph, or simply the approximation graph, denoted by Θ. The vertex set of Θ is just the source alphabet, i.e., $V(\Theta) = \mathcal{X}$, and any two source symbols $x \neq x' \in \mathcal{X}$ are acceptable approximations to each other iff they are adjacent in Θ, i.e., $\{x, x'\} \in \mathcal{E}(\Theta)$.

Given a sequence length t, any two sequences $x^t = (x_1, \ldots, x_t)$ and $v^t = (v_1, \ldots, v_t)$ are acceptable approximations to each other iff for every $j \in [t]$, $x_j = v_j$ or $\{x_j, v_j\} \in \mathcal{E}(\Theta)$. Hence the approximation graph Θ_t for sequence length t is the t-th power of Θ with respect to the *AND graph product* [29, Section 5.2]: $\Theta_t = \Theta \boxtimes \Theta \boxtimes \cdots \boxtimes \Theta = \Theta^{\boxtimes t}$.

For any vertex $x^t \in \mathcal{X}^t$, let $N(\Theta_t, x^t)$ denote the *neighborhood* of x^t within Θ_t, including the vertex x^t itself. That is, $N(\Theta_t, x^t) = \{v^t \in \mathcal{X}^t : v^t = x^t \text{ or } \{v^t, x^t\} \in \mathcal{E}(\Theta_t)\}$.

Consider any source coding problem Γ and any approximation graph Θ. For a given sequence length t and a given valid mapping $P_{Y|X^t}$, the maximal leakage naturally extends to the *approximate-guess* maximal leakage, defined as

$$L^t_\Theta(P_{Y|X^t}) \doteq \rho_t(P_{Y|X^t}, \mathcal{S}_\Theta), \tag{19}$$

where $\mathcal{S}_\Theta = \{N(\Theta_t, x^t) : x^t \in \mathcal{X}^t\}$. Then we can define the (optimal) approximate-guess maximal leakage rate as

$$\mathcal{L}_\Theta \doteq \lim_{t\to\infty} \frac{1}{t} \inf_{\substack{P_{Y|X^t}: \\ \mathcal{X}^t(y) \in \mathcal{I}(\Gamma_t), \forall y \in \mathcal{Y}}} L^t_\Theta(P_{Y|X^t}). \tag{20}$$

Similar to Lemma 4, we can show the following result.

Lemma 5: We have $\mathcal{L}_\Theta \leq \mathcal{L}$.

Before presenting single-letter bounds on $\mathcal{L}_\Theta$, we introduce the following graph-theoretic notion.

Consider any sequence length t. For any maximal independent set $T \in \mathcal{I}_{\max}(\Gamma_t)$, we define its *associated hypergraph* (see [25, Chapter 1] for basic definitions about hypergraphs).

Definition 1 (Associated Hypergraph): Consider any sequence length t. For any $T \in \mathcal{I}_{\max}(\Gamma_t)$, its associated hypergraph[7] $\mathcal{H}_t(T)$ is defined as $V(\mathcal{H}_t(T)) = T$ and $\mathcal{E}(\mathcal{H}_t(T)) = \{E \subseteq T : E \neq \emptyset, E = T \cap N(\Theta_t, x^t) \text{ for some } x^t \in \mathcal{X}^t\}$.

The following single-letter lower and upper bounds on $\mathcal{L}_\Theta$ hold, whose proof can be found in [26].

Theorem 3: We have

$$\log \frac{p_f(\Theta)}{\max\limits_{T \in \mathcal{I}_{\max}(\Gamma)} k_f(\mathcal{H}_1(T))} \leq \mathcal{L}_\Theta \leq \log \chi_f(\Gamma), \tag{21}$$

where $p_f(\cdot)$ denotes the fractional closed neighborhood packing number [25, Section 7.4] of a graph and $k_f(\cdot)$ denotes the fractional covering number [25, Section 1.2] of a hypergraph.

Appendix A
Proof of (13)

We first prove $\eta_t \leq 1/\chi_f(\Gamma_t)$. As η_t is the solution to (11), there exists some $0 \leq \kappa_T \leq 1, T \in \mathcal{I}_{\max}(\Gamma_t)$ so that

$$\min_{x^t \in \mathcal{X}^t} \sum_{T \in \mathcal{I}_{\max}(\Gamma_t): x^t \in T} \kappa_T = \eta_t, \tag{22}$$

$$\sum_{T \in \mathcal{I}_{\max}(\Gamma_t)} \kappa_T = 1. \tag{23}$$

Construct $\lambda_T = \kappa_T/\eta_t$ for every $T \in \mathcal{I}_{\max}(\Gamma_t)$. It can be verified by contradiction that $(\lambda_T : T \in \mathcal{I}_{\max}(\Gamma_t))$ satisfies the constraint in (12c). For more details, see the full version of this paper [26]. For any $x^t \in \mathcal{X}^t$, by (22), we have

$$\sum_{\substack{T \in \mathcal{I}_{\max}(\Gamma_t): \\ x^t \in T}} \lambda_T \geq \frac{1}{\eta_t} \min_{v^t \in \mathcal{X}^t} \sum_{\substack{T \in \mathcal{I}_{\max}(\Gamma_t): \\ v^t \in T}} \kappa_T = 1,$$

and thus we know that $(\lambda_T : T \in \mathcal{I}_{\max}(\Gamma_t))$ satisfies the constraints in (12b). Therefore, $(\lambda_T : T \in \mathcal{I}_{\max}(\Gamma_t))$ is a valid assignment satisfying the constraints in the optimization problem (12), with which the objective in (12a) becomes

$$\sum_{T \in \mathcal{I}_{\max}(\Gamma_t)} \lambda_T = \frac{1}{\eta_t} \sum_{T \in \mathcal{I}_{\max}(\Gamma_t)} \kappa_T = \frac{1}{\eta_t},$$

where the second equality follows from (23). Since $\chi_f(\Gamma_t)$ is the solution to the optimization problem (12), we conclude that $\chi_f(\Gamma_t) \leq 1/\eta_t$, which is equivalent to $\eta_t \leq 1/\chi_f(\Gamma_t)$.

The opposite direction $\eta_t \geq 1/\chi_f(\Gamma_t)$ can be proved similarly. Combining the two inequalities yields (13).

[6] While the definition in [25, Section 1.3] is for a *hypergraph*, it can be readily specialized to a graph since any graph is a special hypergraph, whose every hyperedge is a 2-element set.

[7] Note that, for brevity, the dependence of the associate hypergraph on the underlying approximation graph Θ is not shown in the notation $\mathcal{H}_t(T)$.

REFERENCES

[1] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, 1948.

[2] J. Korner and A. Orlitsky, "Zero-error information theory," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2207–2229, 1998.

[3] J. Körner, "Coding of an information source having ambiguous alphabet and the entropy of graphs," in *6th Prague conference on information theory*, 1973, pp. 411–425.

[4] L. Wang and O. Shayevitz, "Graph information ratio," *SIAM J. Discrete Math.*, vol. 31, no. 4, pp. 2703–2734, 2017.

[5] G. Smith, "On the foundations of quantitative information flow," in *International Conference on Foundations of Software Science and Computational Structures*. Springer, 2009, pp. 288–302.

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

[7] I. Issa, S. Kamath, and A. B. Wagner, "An operational measure of information leakage," in *Proc. Annu. Conf. Inf. Sci. Syst. (CISS)*, 2016, pp. 234–239.

[8] I. Issa, A. B. Wagner, and S. Kamath, "An operational approach to information leakage," *IEEE Trans. Inf. Theory*, 2019.

[9] J. Liao, L. Sankar, F. P. Calmon, and V. Y. Tan, "Hypothesis testing under maximal leakage privacy constraints," in *Proc. IEEE Int. Symp. on Information Theory (ISIT)*, 2017, pp. 779–783.

[10] M. Karmoose, L. Song, M. Cardone, and C. Fragouli, "Privacy in index coding: k-limited-access schemes," *IEEE Trans. Inf. Theory*, vol. 66, no. 5, pp. 2625–2641, 2019.

[11] A. R. Esposito, M. Gastpar, and I. Issa, "Learning and adaptive data analysis via maximal leakage," in *Proc. IEEE Information Theory Workshop (ITW)*, 2019, pp. 1–5.

[12] Y. Liu, N. Ding, P. Sadeghi, and T. Rakotoarivelo, "Privacy-utility tradeoff in a guessing framework inspired by index coding," in *Proc. IEEE Int. Symp. on Information Theory (ISIT)*, 2020, pp. 926–931.

[13] R. Zhou, T. Guo, and C. Tian, "Weakly private information retrieval under the maximal leakage metric," in *Proc. IEEE Int. Symp. on Information Theory (ISIT)*, 2020, pp. 1089–1094.

[14] B. Wu, A. B. Wagner, and G. E. Suh, "Optimal mechanisms under maximal leakage," in *Proc. IEEE Conf. on Comm. and Netw. Secur. (CNS)*, 2020, pp. 1–6.

[15] M. S. Alvim, K. Chatzikokolakis, C. Palamidessi, and G. Smith, "Measuring information leakage using generalized gain functions," in *2012 IEEE 25th Computer Security Foundations Symposium*, 2012, pp. 265–279.

[16] B. Espinoza and G. Smith, "Min-entropy as a resource," *Information and Computation*, vol. 226, pp. 57–75, 2013.

[17] M. S. Alvim, K. Chatzikokolakis, A. McIver, C. Morgan, C. Palamidessi, and G. Smith, "Additive and multiplicative notions of leakage, and their capacities," in *2014 IEEE 27th Computer Security Foundations Symposium*, 2014, pp. 308–322.

[18] G. Smith, "Recent developments in quantitative information flow (invited tutorial)," in *2015 30th Annual ACM/IEEE Symposium on Logic in Computer Science*, 2015, pp. 23–31.

[19] Y. Y. Shkel and H. V. Poor, "A compression perspective on secrecy measures," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 163–176, 2021.

[20] N. Merhav and E. Arikan, "The shannon cipher system with a guessing wiretapper," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1860–1866, 1999.

[21] C. Schieler and P. Cuff, "Rate-distortion theory for secrecy systems," *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7584–7605, 2014.

[22] N. Weinberger and N. Merhav, "A large deviations approach to secure lossy compression," *IEEE Trans. Inf. Theory*, vol. 63, no. 4, pp. 2533–2559, 2017.

[23] I. Issa and A. B. Wagner, "Measuring secrecy by the probability of a successful guess," *IEEE Trans. Inf. Theory*, vol. 63, no. 6, pp. 3783–3803, 2017.

[24] C. Schieler and P. Cuff, "The henchman problem: Measuring secrecy by the minimum distortion in a list," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3436–3450, 2016.

[25] E. R. Scheinerman and D. H. Ullman, *Fractional graph theory: a rational approach to the theory of graphs*. Courier Corporation, 2011.

[26] Y. Liu, L. Ong, S. Johnson, J. Kliewer, P. Sadeghi, and P. L. Yeoh, "Information leakage in zero-error source coding: a graph-theoretic perspective," *arXiv preprint arXiv:2102.01908*, 2021. [Online]. Available: http://arxiv.org/abs/2102.01908

[27] J. Liao, O. Kosut, L. Sankar, and F. du Pin Calmon, "Tunable measures for information leakage and applications to privacy-utility tradeoffs," *IEEE Trans. Inf. Theory*, vol. 65, no. 12, pp. 8043–8066, 2019.

[28] F. Arbabjolfaei and Y.-H. Kim, "Fundamentals of index coding," *Foundations and Trends® in Communications and Information Theory*, vol. 14, no. 3-4, pp. 163–346, 2018.

[29] R. Hammack, W. Imrich, and S. Klavžar, *Handbook of product graphs*. CRC press, 2011.