

# The Sender-Excited Secret Key Agreement Model: Capacity, Reliability and Secrecy Exponents

Tzu-Han Chou, Vincent Y. F. Tan, Stark C. Draper

**Abstract**—We consider the secret key generation problem when sources are randomly excited by the sender and there is a noiseless public discussion channel. Our setting is thus similar to recent works on channels with action-dependent states where the channel state may be influenced by some of the parties involved. We derive single-letter expressions for the secret key capacity through a type of source emulation analysis. We also derive lower bounds on the achievable reliability and secrecy exponents, i.e., the exponential rates of decay of the probability of decoding error and of the information leakage. These exponents allow us to determine a set of strongly-achievable secret key rates. For degraded eavesdroppers the maximum strongly-achievable rate equals the secret key capacity; our exponents can also be specialized to previously known results.

In deriving our strong achievability results we introduce a coding scheme that combines wiretap coding (to excite the channel) and key extraction (to distill keys from residual randomness). The secret key capacity is naturally seen to be a combination of both source- and channel-type randomness. Through examples we illustrate a fundamental interplay between the portion of the secret key rate due to each type of randomness. We also illustrate inherent tradeoffs between the achievable reliability and secrecy exponents. Our new scheme also naturally accommodates rate limits on the public discussion. We show that under rate constraints we are able to achieve larger rates than those that can be attained through a pure source emulation strategy.

**Index Terms**—Secret key capacity, Common randomness, Wiretap channel, Sender-excitation, Reliability exponent, Secrecy exponent, Degraded broadcast channel, Probing capacity

## I. INTRODUCTION

Within the realm of information-theoretic secrecy [2], the foundations of sharing a secret key between two parties in the presence of an eavesdropper were initiated in [3], [4]. Ahlswede and Csiszár [3] studied two models: the *source-type model with wiretapper* (Model SW) and the *channel-type model with wiretapper* (Model CW). In Model SW, users obtain their observations from a discrete memoryless multiple source (DMMS), and communicate to each other via a noiseless authenticated public channel, with the objective of generating jointly held secret keys. In Model CW, one

legitimate user (the sender) controls the input of a discrete memoryless broadcast channel (DMBC), sending information based upon which the legitimate receivers generate secret keys.

However, many applications cannot be exactly modeled as either a source- or a channel-type scenario. This work explores such a setting in which the sender has the ability to use a private source of randomness to excite (or influence) the “state” of the DMMS. This is similar in spirit to recent works on probing capacity and channels with action-dependent states [5]–[8]. We derive capacity, reliability exponent, and secrecy exponent results for this setting. At one extreme, when the sender has an unlimited ability to excite the channel, and the rate of public discussion is similarly unbounded, a particular type of source emulation strategy is capacity achieving. However, when constraints are placed on the rate of public discussion we demonstrate that source emulation becomes sub-optimal. We show this through the development of a more nuanced rate-limited excitation strategy that exceeds the capacity of the emulation-based approach when subject to rate constraints [9]. Our new strategy combines a wiretap-type probing mechanism (Model CW) with a key-distillation step (Model SW) that is applied to the residual randomness. In general, we find an interplay to exist between the secrecy rate derived from the wiretapping step and the secrecy rate derived via the key-distillation step. We illustrate the tradeoff via examples. In terms of our large deviation results we show that there is a natural tradeoff between the reliability and secrecy exponents. The former generalize Gallager’s classic results in [10, Sec. 5.6] and [11]; the latter may be specialized to Hayashi’s recent work that characterizes the rate of decay of information leakage [12] of the wiretap channels.

### A. Related Work

There are other investigations that consider non-source, non-channel models. For example, in [13], [14] users observe a DMMS and can also transmit information via a wiretap channel. However, no public discussion is allowed. The key generation scheme used is based on the observation that a public message can be transmitted via the DMBC confidentially, resulting in a higher secret key rate. In [9], [15], [16], public discussion is allowed and there may also be a helper. However, unlike our work, the sender does not also receive a sequence as part of the channel output. The sender’s ability to use both her channel output and her source of private randomness to generate the secret key is a crucial aspects of our model.

The authors in [17]–[21] considered the setting where a wiretap channel is influenced by a random state that is known

This work was supported in part by the Air Force Office of Scientific Research under grant FA9550-09-1-0140, by a grant from the Wisconsin Alumni Research Foundation, and by the National Science Foundation under CAREER grant CCF 0844539. The work of V. Y. F. Tan was also supported by A\*STAR, Singapore. This paper was presented in part at Allerton Conference on Communication, Control and Computing in Monticello, IL (September 2011) [1].

T.-H. Chou is with Qualcomm Inc, San Diego, CA. V. Y. F. Tan is with the Institute of Infocomm Research, Singapore and the Department of Electrical and Computer Engineering, National University of Singapore. S. C. Draper is with the Department of Electrical and Computer Engineering, University of Wisconsin, Madison, WI, 53706, USA (emails: tzuhanc@qti.qualcomm.com; vtan@nus.edu.sg; sdraper@ece.wisc.edu).

by the sender (and possibly by the receiver) and thus can be treated as a correlated source. In [17], [18], the sender transmits a confidential message and the random, noncausally known, state is exploited to confuse the eavesdropper. The lower bound is proved using a combination of Gel'fand-Pinsker coding and wiretap channel coding. A similar problem but with causal state information is studied in [19] and the coding scheme involves block Markov coding, Shannon strategies, and wiretap coding. In [20], [21], the goal is to generate a secret key when the encoder (and/or decoders) have noncausal state information. The authors present a single-letter expression for the secret key capacity. The key rate consists of two parts. The first can be attributed to the rate of the confidential message sent using wiretap channel coding where the state sequence is treated as a time-sharing sequence, while a second key, independent of the first, is produced by exploiting the common knowledge of the state at the sender and the legitimate receiver.

The model considered in this paper is a generalization of the “source excitation” model of [22]. That model is motivated by the large body of work on physical-layer security (see, e.g., [23], [24]) where the unpredictable variation in the wireless channel medium serves as the source of common randomness. One approach is to sound the wireless channel using a random signal and measure the observations generated (marginalizing over the sounding signal). This “source emulation” strategy is considered in [24]. Another approach studied in [22], [23] uses deterministic sounding (no marginalization is involved). Key extraction follows by denoising the observations using a public message. Deterministic sounding requires no source of private randomness (as does source emulation), all randomness is due to the channel. The current generalization is that we now explore the source excitation model when the exciter has a source of private randomness. This allows us to exploit both random sounding (using a wiretap code) and key generation (using conditional randomness). We regard the current model as stepping stone to understanding the fundamental limits of two-way randomized channel sounding in which secrecy rate is derived from the use of two wiretap codes and from the conditional randomness produced.

### B. Main Contributions: Capacity and Error Exponents

Figure 1 shows the system considered in this paper. We can think of the terminal labeled Alice as a base station on earth equipped with a sensor. This base station transmits a random message  $M$  (the selection of which is based on a private source of randomness) securely to a satellite encoder. The satellite produces sequence  $S^n$  according to some conditional probability law. This sequence is the input to a broadcast channel  $p(x, y, z|s)$  (the wireless medium). The channel produces observations  $X^n$ ,  $Y^n$  and  $Z^n$ , respectively received by Alice, the legitimate user Bob, and the malicious user Eve. The goal of the two legitimate users is to generate a shared secret key – Alice based on  $(M, X^n)$  and Bob based on  $(\Phi, Y^n)$ , where  $\Phi$  is a public message known to all parties.

We first consider the situation in which there are no rate limits on either the public discussion ( $\Phi$ ) or the excitation

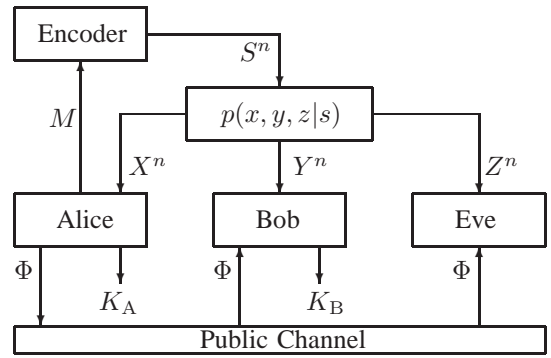


Fig. 1. Our problem setup: Based on her private source of randomness  $M$ , Alice excites the channel via the sounding signal  $S^n(M)$ . She generates a public message  $\Phi(M, X^n)$ , which is transmitted through the noiseless public channel and hence known to all parties. Alice and Bob generate keys  $K_A(M, X^n)$  and  $K_B(\Phi, Y^n)$  respectively. The keys should agree, while at the same time, they should be kept secret from Eve.

signal ( $M$ ). We derive a single-letter expression for the secret key capacity of this system. The result follows through a particular kind of source emulation where (i) Alice chooses the optimum source distribution to induce (potentially subject to cost constraints on  $S^n$ ), and (ii) Alice has the vector observation  $(S^n, X^n)$ .

We then turn to the rate-limited situation and study the effect of rate limits on (i) the achievable secrecy rate, (ii) the probability of erroneous decoding at the legitimate receiver, Bob, and (iii) the key leakage rate by the eavesdropper, Eve. We focus on degraded channels and characterize the error probability in terms of a *reliability exponent* and the key leakage rate in terms of a *secrecy exponent*. In contrast to [9] where the secret key capacity of one-way key generation subject to a rate constraint is characterized, we show that the flexibility Alice has in choosing the amount of private randomness she uses in the selection of  $M$  can allow a strictly higher achievable secret key rate than can be attained via pure source emulation.

We introduce a new type of decoder for the legitimate receiver, Bob, to use. This decoder is a combination of a maximum likelihood and a maximum *a-posteriori* (ML-MAP) decoder. Bob decodes jointly the sender's source  $X^n$  and the sender's private source of randomness (or message)  $M$ . The resulting reliability exponent expression can be specialized to Gallager's channel coding error exponent [10, Sec. 5.6] and Gallager's source coding error exponent [11]. On the other hand, in the key leakage analysis, the secrecy exponent we derive captures the leakage due to Eve's channel  $p(z|s)$  and the leakage due to the correlation between Alice's variable  $X$  and Eve's variable  $Z$  in a transparent manner. Our analysis builds on the work by Hayashi in [12], [25], where he links the leakage rate of a wiretap channel to channel resolvability and identification coding [26]. This connection is also examined Bloch and Laneman [27] where they derive the capacity of general wiretap channels from an information spectrum perspective [26]. Our secrecy exponent results, which are developed in Section IV, can be specialized to the wiretap channel [12], [25] and to the secret key generation from corre-

lated source setting [12], [22], [28], [29]. The difference vis-à-vis the motivating work [22] is that the methods used to bound the exponents for both reliability and secrecy involve both wiretap channel coding and source coding. This will become clear in Section IV where we specialize our results to various known problems. Note that the criterion for exponential decay of the key leakage rate is much stronger than the usual strong secrecy [4]. We focus on this exponential notion because it quantifies how fast the error probability and information rate decays to zero and because it reveals a natural tradeoff between the attainable reliability and secrecy exponents.

### C. Paper Organization

This paper is organized as follows: In Section II, we describe the system model. We also define the secret key capacity, the capacity-reliability-secrecy region and the notion of channel degradedness. Our main results pertaining to the secret key capacity are provided in Section III. We also prove a (sometimes loose) upper bound on the secret key capacity that does not contain any auxiliary random variables, and hence is amenable to evaluation. We show that this upper bound is tight for degraded channels. We present the reliability and secrecy exponents in Section IV and connect to previous work. In Section V, we present several examples to demonstrate how the main results can be applied to channels of interest. We show the inherent tradeoff between the portions of the secret key rate due to source- and to channel-type randomness. We also show the inherent tradeoff between the reliability exponent and the secrecy exponent. The proofs of the capacity theorems and the error exponent theorems are provided in Section VI and Section VII respectively.

### D. Notation

We generally adopt the notational conventions in the book by El Gamal and Kim [30], some of which we recap here. All logarithms are to base-2. Random variables are in upper case (e.g.,  $X$ ) and their realizations in lower case (e.g.,  $x$ ). The corresponding alphabets of random variables are in calligraphic font (e.g.,  $\mathcal{X}$ ) and so are all sets and events (e.g.,  $\mathcal{C}$ ). For vectors,  $X_j^i \triangleq (X_j, \dots, X_i)$  and if  $j = 1$ , the abbreviation  $X^i \triangleq X_1^i$  is used. In addition,  $X^{n \setminus i} \triangleq (X^{i-1}, X_{i+1}^n)$ . The probability mass function (pmf) of a discrete random variable  $X$  is denoted as  $p_X(x)$  or more simply as  $p(x)$ . Random codebooks are denoted by a special script font  $\mathcal{C}$  while a codebook realization is denoted as  $\mathcal{C}$ . For an  $a \geq 0$ , we also commonly use the notation  $[1 : 2^a] \triangleq \{1, \dots, 2^{\lceil a \rceil}\}$ .

## II. PROBLEM SETUP

### A. The Secret Key Generation Protocol

The setting is shown in Fig. 1. Consider a 3-receiver DMBC  $(\mathcal{S}, p(x, y, z|s), \mathcal{X} \times \mathcal{Y} \times \mathcal{Z})$  consisting of four finite sets  $\mathcal{S}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}$  and a collection of conditional pmfs  $p(x, y, z|s)$  on  $\mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ . Alice, at terminal  $\mathcal{X}$ , controls the channel input *sounding signal*  $s^n$  through the encoder via  $n$  uses of the channel. Alice has a private source of randomness used to select an index  $m$ , which influences  $s^n$ . The legitimate

receiver at terminal  $\mathcal{Y}$  is known as Bob and the eavesdropper at terminal  $\mathcal{Z}$  is known as Eve. There is also a noiseless public discussion channel which allows Alice to transmit a message  $\Phi$  to Bob and Eve. Let  $\Lambda : \mathcal{S} \rightarrow [0, \Lambda_{\max}]$  be a per-letter, bounded cost function and let  $\Gamma > 0$  be an admissible cost. A  $(2^{nR_M}, 2^{nR_\Phi}, n, \Gamma)$  code for the secret key generation protocol consists of a tuple of functions  $(f, \phi, k_A)$ . In particular,

- 1) *Channel Excitation*: Alice selects a message  $M \in [1 : 2^{nR_M}]$  uniformly at random. The (satellite) encoder sends a message-dependent input sequence  $S^n = f(M) \in \mathcal{S}^n$  ( $f$  possibly being random) satisfying

$$\mathbb{P} \left[ \frac{1}{n} \sum_{i=1}^n \Lambda(S_i) \leq \Gamma \right] = 1. \quad (1)$$

The input sequence  $S^n$  is transmitted over  $n$  uses of  $p(x, y, z|s)$ . The output sequences  $x^n$ ,  $y^n$  and  $z^n$  are observed by Alice, Bob (legitimate receiver) and Eve (eavesdropper) respectively.

- 2) *One-Way (Forward) Public Discussion*: After observing  $x^n$ , Alice generates a one-way public message<sup>1</sup>  $\phi = \phi(m, x^n) \in [1 : 2^{nR_\Phi}]$ , and transmits it over a noiseless public channel.
- 3) *Key Generation*: Alice generates a key  $k_A = k_A(m, x^n) \in \mathbb{N}$ . After receiving his channel output  $y^n$  and the public message  $\phi$ , Bob generates another key  $k_B = k_B(y^n, \phi) \in \mathbb{N}$ .

Note the conditional distribution of  $(X, Y, Z)$  given  $S$  can be factorized as  $p(x|s)p(y, z|x, s)$ . The first conditional distribution  $p(x|s)$  can be roughly thought of as Alice's influence on the channel state via the sounding signal  $s^n$ , while the second  $p(y, z|x, s)$  can be thought of as a state-dependent channel.

### B. Definitions

We now provide the definitions of achievable secret key rates, secret key capacity and error exponents. As a reminder, the random variables  $K_A$  and  $K_B$  respectively denote Alice's and Bob's key. The public message is denoted as  $\Phi$ .

**Definition 1** (Weak Achievability). *The secret key rate  $R_{SK} \in \mathbb{R}_+$  is  $\Gamma$ -weakly-achievable (or simply  $\Gamma$ -achievable) if there exists a sequence of  $(2^{nR_M}, 2^{nR_\Phi}, n, \Gamma)$  codes (for any  $(R_M, R_\Phi)$  pair) for the secret key generation protocol such that the following three conditions are satisfied:*

$$\lim_{n \rightarrow \infty} \mathbb{P}(K_A \neq K_B) = 0, \quad (2)$$

$$\lim_{n \rightarrow \infty} \frac{1}{n} I(K_A; Z^n, \Phi) = 0, \quad (3)$$

$$\liminf_{n \rightarrow \infty} \frac{1}{n} H(K_A) \geq R_{SK}, \quad (4)$$

**Definition 2** ((Forward) Secret Key Capacity). *The secret key capacity-cost function  $C_{SK}(\Gamma)$  is defined as follows:*

$$C_{SK}(\Gamma) := \sup \{ R_{SK} : R_{SK} \text{ is } \Gamma\text{-weakly-achievable} \}. \quad (5)$$

<sup>1</sup>As in [30], we use a common notation  $\phi$  to denote both the function  $\phi : [1 : 2^{nR_M}] \times \mathcal{X}^n \rightarrow [1 : 2^{nR_\Phi}]$  as well as the output of the function  $\phi \in [1 : 2^{nR_\Phi}]$ . This applies in the rest of the paper.



We will henceforth say that  $C_{\text{SK}}(\Gamma)$  is the (*forward*) *secret key capacity* (without reference to the cost  $\Gamma$ ). The *reliability condition* in (2) implies that we would like Alice's and Bob's keys to agree with high probability. The *secrecy condition* in (3) requires that the eavesdropper cannot estimate the key  $K_A \in [1 : 2^{nR_{\text{SK}}}]$  given her observation  $Z^n$  and the public message  $\Phi$ . This is manifested in that the *key leakage rate*  $\frac{1}{n}I(K_A; Z^n, \Phi)$  is arbitrarily small for sufficiently large blocklength  $n$ . The rate condition in (4) implies that the entropy of  $K_A$  should be close to  $R_{\text{SK}}$ . In other words the pmf of  $K_A$  should be close to that of a uniform pmf on  $[1 : 2^{nR_{\text{SK}}}]$ , so the eavesdropper can only glean a negligible amount of information.

In many practical settings, the fact that the error probability in (2) and the key leakage rate in (3) can be made arbitrarily small with increasing block length is insufficient. See Maurer's work in [31] and a more recent exposition in [27]. It would, in fact, be desirable to quantify their rates of decay and to devise coding schemes to ensure that these decay rates are as large as possible. We formalize this by defining the notion of an achievable secret key rate-exponent triple. To simplify the exposition, in our definitions (and corresponding results) of rates with exponents, we will assume that  $\Gamma = \infty$ . In other words, we do not impose a cost constraint on  $S^n$  as in (1).

**Definition 3** (Achievable Secret Key Rate-Exponent Triple). *The secret key rate-exponent triple  $(R_{\text{SK}}, E, F) \in \mathbb{R}_+^3$  is achievable if there exists a sequence of  $(2^{nR_M}, 2^{nR_\Phi}, n)$  codes for the secret key generation protocol such that in addition to (4), the following hold:*

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log P(K_A \neq K_B) \geq E, \quad (6)$$

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log I(K_A; Z^n, \Phi) \geq F. \quad (7)$$

In (6),  $E$  is known as the *reliability exponent* and in (7),  $F$  is known as the *secrecy exponent*. Collectively,  $E$  and  $F$  are known as *error exponents* (though  $I(K_A; Z^n, \Phi)$  is not, strictly speaking, an error probability but we abuse terminology to say that both are "errors"). Definition 3 can also be interpreted as follows: If a triple  $(R_{\text{SK}}, E, F)$  is achievable, then the error probability in (2) decays<sup>2</sup> as  $P(K_A \neq K_B) \leq 2^{-nE}$  and the key leakage decays as  $I(K_A; Z^n, \Phi) \leq 2^{-nF}$ . Naturally, the constraint on the entropy of the secret key in (4) is retained in the above definition.

**Definition 4** (Capacity-Reliability-Secrecy Region). *The (secret key) capacity-reliability-secrecy region  $\mathcal{R} \subset \mathbb{R}_+^3$  is the closure of the set of achievable secret key rate-exponent triples.*

In analogy to the notion of weak achievability, we can also define a more stringent notion known as strong achievability, also studied in [31], [32].

**Definition 5** (Strong Achievability). *The secret key rate  $R_{\text{SK}}$  is strongly-achievable if  $(R_{\text{SK}}, E, F)$  is achievable for some  $E > 0$  and  $F > 0$ .*

<sup>2</sup>Here and in the following, for a pair of positive sequences  $\{(a_n, b_n)\}_{n \in \mathbb{N}}$ , we say that  $a_n \leq b_n$  if  $\limsup_{n \rightarrow \infty} n^{-1} \log(a_n/b_n) \leq 0$ . The notation  $\geq$  is defined analogously. We say that  $a_n \doteq b_n$  if  $a_n \leq b_n$  and  $a_n \geq b_n$ .

We conclude our suite of definitions by formalizing the notion of degraded channels.

**Definition 6** (Degradedness). *We say that the DMBC  $p(x, y, z|s)$  is degraded if  $(X, S) - Y - Z$  form a Markov chain, i.e.,  $p(y, z|x, s) = p(y|x, s)p(z|y)$ .*

In this case, we also say that the DMBC  $p(x, y, z|s)$  is degraded in favor of Bob or equivalently that Eve's observation is a degraded version of Bob's. Note that we do not differentiate between physical and stochastic degradedness [30, Ch. 5]. The capacity results will turn out to be identical for both cases.

### III. BASIC CAPACITY RESULTS

We present our capacity results in this section. These correspond to Definitions 1 and 2 and we emphasize that  $R_M$  and  $R_\Phi$  are unconstrained here. We leverage on a source emulation result by Ahlswede-Csiszár [3] to give a single-letter expression for the secret key capacity containing two auxiliary random variables taking into account that  $S^n$  has to satisfy the cost constraint in (1). We also provide a looser upper bound that contains no auxiliary random variables. The upper bound is tight when the DMBC is degraded in favor of Bob. The capacity results in this section motivate the more refined error exponent analysis in the following section where  $R_\Phi$  can be constrained and we will see that a judicious choice of  $R_M$  does not reduce  $C_{\text{SK}}$  in the case of degraded DMBCs.

**Proposition 1** (Secret Key Capacity). *The secret key capacity of DMBC  $(\mathcal{S}, p(x, y, z|s), \mathcal{X} \times \mathcal{Y} \times \mathcal{Z})$  is*

$$C_{\text{SK}}(\Gamma) = \max [I(U; Y|W) - I(U; Z|W)], \quad (8)$$

where the maximization is over all joint distributions that factor in accordance to  $W - U - (X, S) - (Y, Z)$  or equivalently,

$$p(w, u, s, x, y, z) = p(w)p(u|w)p(x, s|u)p(y, z|x, s) \quad (9)$$

such that  $E[\Lambda(S)] \leq \Gamma$ .

By repeated applications of Bayes rule, the decomposition in (9) can be written as

$$p(w, u, s, x, y, z) = p(w|u)p(u|x, s)p(s)p(x, y, z|s). \quad (10)$$

Since the DMBC  $p(x, y, z|s)$  is given, the optimization in (8) is over the source distribution  $p(s)$  and the auxiliary conditional distributions  $p(w|u)$  and  $p(u|x, s)$ . Furthermore, by using the Fenchel-Eggleston-Carathéodory Theorem [30, App. C], it can be argued that the cardinalities of the auxiliary random variables  $W$  and  $U$  can be bounded as  $|W| \leq |\mathcal{X}||\mathcal{S}| + 3$  and  $|U| \leq (|\mathcal{X}||\mathcal{S}| + 3)(|\mathcal{X}||\mathcal{S}| + 1)$  respectively.

*Proof of Proposition 1:* Achievability follows from [3, Theorem 1] for Model SW with a slight modification to account for cost constraint on  $S^n$  in (1). Fix an  $\epsilon > 0$  and a joint distribution in (9) achieving  $E[\Lambda(S)] \leq \frac{\Gamma}{1+\epsilon}$ . Let  $S \sim p_S(s)$  be the  $\mathcal{S}$ -marginal of (9) and let its typical set<sup>3</sup> be  $\mathcal{T}_\epsilon^{(n)}(S)$ . Index all the elements in  $\mathcal{T}_\epsilon^{(n)}(S)$  as  $[1 : |\mathcal{T}_\epsilon^{(n)}(S)|]$ . We are

<sup>3</sup>The typical set defined in  $\mathcal{T}_\epsilon^{(n)}(S)$  [30, Sec. 2.4] consists of all sequences  $s^n$  whose type (empirical distribution)  $\pi(s; s^n)$  satisfies  $|\pi(s; s^n) - p_S(s)| \leq \epsilon p_S(s)$  for every  $s \in \mathcal{S}$ . The typical average lemma [30, Sec. 2.4] implies that  $n(1 - \epsilon)H(S) \leq \log |\mathcal{T}_\epsilon^{(n)}(S)| \leq n(1 + \epsilon)H(S)$ .

only going to excite the DMBC  $p(x, y, z|s)$  using sequences belonging to  $\mathcal{T}_\epsilon^{(n)}(S)$ . By the typical average lemma [30, Sec. 2.4], this ensures that for every  $n$ , the almost sure cost constraint in (1) is satisfied.

The encoder has the codebook  $\mathcal{T}_\epsilon^{(n)}(S)$ , which is known to all parties. Alice generates an index  $M \in [1 : |\mathcal{T}_\epsilon^{(n)}(S)|]$  uniformly at random so in this coding scheme,  $R_M = \frac{1}{n} \log |\mathcal{T}_\epsilon^{(n)}(S)| = H(S) + \delta(\epsilon)$  for some  $\delta(\epsilon) \downarrow 0$  as  $\epsilon \downarrow 0$ . Given  $M$ , the encoder transmits the sequence indexed by  $M$  in the codebook. Note that  $p_S^n(\mathcal{T}_\epsilon^{(n)}(S))$  is arbitrarily close to one for large enough  $n$ . Hence, just as in the proof of [3, Theorem 1], we can consecutively select mutually disjoint wiretap codes  $\{\mathcal{C}_i\}_{i=1}^N$  from  $\mathcal{T}_\epsilon^{(n)}(S) \times \mathcal{X}^n$  (with  $\eta$  in [3, Eq. (4.1)] replaced by  $2\eta$ , say) where each codebook  $\mathcal{C}_i$  contains codewords of the same type. The rest of the proof in [3, Theorem 1] follows verbatim with our  $(X, S)$  in the role of  $X$  there. This allows us to assert that  $I(U; Y|W) - I(U; Z|W)$  is a one-way (forward) achievable key rate. Note that in our setting, Alice receives  $X^n$  and also has  $S^n$  (a function of her privately generated index  $M$ ), Bob receives  $Y^n$  and Eve receives  $Z^n$ . The proof is completed by taking  $\epsilon \downarrow 0$  and using the continuity of  $\Gamma \mapsto C_{\text{SK}}(\Gamma)$ . That  $C_{\text{SK}}(\Gamma)$  is continuous follows from the continuity of  $I(U; Y|W)$ ,  $I(U; Z|W)$  and  $E[\Lambda(S)]$  in (9).

The converse proof of Theorem 1 is standard and we provide it in Section VI-A for completeness. It relies on a simple application of the Csiszár-sum-identity [30, Sec. 2.3] and an appropriate identification of the auxiliary random variables that satisfy the Markov conditions in (9). ■

To find the secret key capacity for specific channels, two auxiliary random variables  $W$  and  $U$  solving (8) have to be identified. This may be a difficult task. In the next proposition, we provide an (albeit looser) upper bound which does not involve any auxiliary random variables. This result will turn out to be important in Section V where we present several channels for which we can calculate the secret key capacity-cost function in closed-form.

**Proposition 2** (Upper Bound in Secret Key Capacity). *The secret key capacity is upper bounded as*

$$C_{\text{SK}}(\Gamma) \leq \max I(X, S; Y|Z), \quad (11)$$

where the maximization is over all input distributions  $p(s)$  such that  $E[\Lambda(S)] \leq \Gamma$ .

The proof of this proposition is given in Section VI-B. Roughly speaking, the expression in (11) can be interpreted as the secret key capacity when Alice and Bob have full knowledge (side information) of Eve's observation  $Z$ , hence the conditioning on  $Z$ . We note by using the techniques in Ahlswede-Csiszár [3] (and in particular Lemma 2.2 therein) that our upper bound also holds for the scenario where the parties Alice and Bob can exchange *multiple* messages—the multi-way discussion scenario.

In the case of degraded  $p(x, y, z|s)$ , the result in Proposition 2 is tight.

**Corollary 3** (Secret Key Capacity of Degraded DMBCs). *If the DMBC  $p(x, y, z|s)$  is degraded, the secret key capacity is*

$$C_{\text{SK}}(\Gamma) = \max [I(X, S; Y) - I(X, S; Z)], \quad (12)$$

where the maximization is over all input distributions  $p(s)$  such that  $E[\Lambda(S)] \leq \Gamma$ .

*Proof:* For achievability, we can choose  $W = \emptyset$  and  $U = (X, S)$  in (8). The Markov condition in (9) is satisfied.

For the converse, we observe from Proposition 2 that the secret key capacity of the degraded DMBC can be upper bounded as

$$C_{\text{SK}}(\Gamma) \leq I(X, S; Y|Z) \quad (13)$$

$$= I(X, S; Y) - I(X, S; Z). \quad (14)$$

The last equality is due to the fact that for degraded channels,  $(X, S) - Y - Z$  forms a Markov chain. ■

Notice that for a fixed  $p(s)$ , the difference of mutual informations in (12) can be decomposed into two parts:

$$I(X, S; Y) - I(X, S; Z) = R_{\text{ch}}[p(s)] + R_{\text{src}}[p(s)], \quad (15)$$

where the channel and source rates are respectively defined as

$$R_{\text{ch}}[p(s)] \triangleq I(S; Y) - I(S; Z), \quad \text{and} \quad (16)$$

$$R_{\text{src}}[p(s)] \triangleq I(X; Y|S) - I(X; Z|S). \quad (17)$$

The first rate  $R_{\text{ch}}[p(s)]$  can be interpreted as the confidential message rate of the wiretap channel  $p(y, z|s)$  [33]. The second rate  $R_{\text{src}}[p(s)]$  is the secret key rate from an excited correlated source  $(X, Y, Z)$  previously studied in [22] for a particular sounding signal  $s^n$  with type  $p(s)$ . In the present setup,  $s^n$  is randomly chosen by Alice. As such, we can optimize over its distribution  $p(s)$  to find the largest “sum rate”  $R_{\text{ch}}[p(s)] + R_{\text{src}}[p(s)]$ . It turns out that there is a natural interplay and tradeoff between  $R_{\text{ch}}[p(s)]$  and  $R_{\text{src}}[p(s)]$ . We illustrate this numerically using an example in Section V-A.

We provide an alternative proof of the capacity of degraded DMBCs via the error exponent route in the next section. We note that the flexibility of the amount of private randomness that Alice has in the form of the random message  $M$  (which we did not exploit in this section) allows us to operate at a lower  $R_\Phi$  and yet result in a positive capacity.

#### IV. ERROR EXPONENT THEOREM

In this section, we present an inner bound for the secret key capacity-reliability-secrecy region per Definition 4. Our general result is then specialized to other known results in the literature. Recall that for the error exponent results, we consider the case when there is no cost constraint on the codewords for simplicity (i.e.,  $\Gamma = \infty$ ).

We make the following two observations when we employ the achievability strategy proposed in this paper which is a random binning scheme. First, the decoding error probability  $P(K_A \neq K_B)$  is only a function of marginal distribution  $p(x, y, s) = p(s)p(x, y|s)$ . Second, the key leakage  $I(K_A; Z^n, \Phi)$  is only a function of marginal distribution  $p(x, z, s)$ . This means that we can characterize the achievable reliability and secrecy exponents separately as functions of each marginal distribution.

### A. Basic Definitions

Before we present our result, we begin with a few definitions. Let

$$\tilde{E}_o^{(1)}(p(s), \rho, R_\Phi) \triangleq \rho R_\Phi - \log \sum_{s,y} p(s)p(y|s) \left[ \sum_{s,x} p(x|y,s)^{\frac{1}{1+\rho}} \right]^{1+\rho}, \quad (18)$$

$$\tilde{E}_o^{(2)}(p(s), \rho, R_\Phi, R_M) \triangleq \rho(R_\Phi - R_M) - \log \sum_s \left[ \sum_{x,y} p(s)p(x,y|s)^{\frac{1}{1+\rho}} \right]^{1+\rho}, \quad (19)$$

$$\tilde{E}_o^{(3)}(p(s), \rho, R_\Phi, R_M) \triangleq \rho(R_\Phi - R_M) - \log \sum_y \left[ \sum_{s,x} p(s)p(x,y|s)^{\frac{1}{1+\rho}} \right]^{1+\rho}. \quad (20)$$

As well, define

$$E_o(p(s), R_\Phi, R_M) \triangleq \min \left\{ \max_{0 \leq \rho \leq 1} \tilde{E}_o^{(1)}(p(s), \rho, R_\Phi), \max_{0 \leq \rho \leq 1} \tilde{E}_o^{(2)}(p(s), \rho, R_\Phi, R_M), \max_{0 \leq \rho \leq 1} \tilde{E}_o^{(3)}(p(s), \rho, R_\Phi, R_M) \right\}. \quad (21)$$

Similarly, define

$$\begin{aligned} \tilde{F}_o(p(s), \alpha, R_{SK}, R_\Phi, R_M) &\triangleq \\ &-\alpha(R_{SK} + R_\Phi - R_M) - \log \sum_{x,z,s} p(x,z,s) \left[ \frac{p(x,z|s)}{p(z)} \right]^\alpha, \quad (22) \\ F_o(p(s), R_{SK}, R_\Phi, R_M) &\triangleq \sup_{0 < \alpha \leq 1} \tilde{F}_o(p(s), \alpha, R_{SK}, R_\Phi, R_M). \end{aligned} \quad (23)$$

We now define a rate-exponent region parameterized by the input distribution  $p(s)$  and the pair of auxiliary rates  $(R_\Phi, R_M)$ :

$$\begin{aligned} \tilde{\mathcal{R}}(p(s), R_\Phi, R_M) &= \left\{ (R_{SK}, \tilde{E}, \tilde{F}) \in \mathbb{R}_+^3 : \right. \\ &\quad \tilde{E} \leq E_o(p(s), R_\Phi, R_M) \\ &\quad \left. \tilde{F} \leq F_o(p(s), R_{SK}, R_\Phi, R_M) \right\}. \end{aligned} \quad (24)$$

### B. The Inner Bound

The following theorem provides an inner bound to the capacity-reliability-secrecy region  $\mathcal{R}$ .

**Theorem 4** (Inner Bound to the Capacity-Reliability-Secrecy Region). *The union of the regions in (24) is an inner bound to the secret key capacity-reliability-secrecy region, i.e.,*

$$\bigcup_{p(s), R_\Phi, R_M} \tilde{\mathcal{R}}(p(s), R_\Phi, R_M) \subseteq \mathcal{R}. \quad (25)$$

The proof of this theorem can be found in Section VII and hinges on an ML-MAP decoding strategy. More precisely, given  $(y^n, \phi)$ , Bob first uses the following rule to estimate Alice's source of private randomness  $\hat{m}$  and Alice's received sequence  $\hat{x}^n$ :

$$(\hat{m}, \hat{x}^n) \triangleq \arg \max_{(m, x^n): \phi(m, x^n) = \phi} p(y^n | s^n(m)) p(x^n | y^n, s^n(m)). \quad (26)$$

The function  $\phi(m, x^n)$  is a (random) binning function, which is defined and discussed in greater detail in Section VII-A. The exponents  $\tilde{E}_o^{(1)}$  and  $\tilde{E}_o^{(2)}$  represent the marginal events  $\{\hat{M} = M, \hat{X}^n \neq X^n\}$  and  $\{\hat{M} \neq M, \hat{X}^n = X^n\}$ , respectively. The former is a Slepian-Wolf-type exponent [11] ( $X$  to be reconstructed given vector side-information  $(Y, S)$ ) while the latter is a channel coding-type exponent [10, Sec. 5.6] (input  $S$  and vector output  $(X, Y)$ ). The exponent  $\tilde{E}_o^{(3)}$  represents the joint error event  $\hat{M} \neq M, \hat{X}^n \neq X^n$  and is a hybrid of Slepian-Wolf and channel coding. Upon the decoding of  $(\hat{m}, \hat{x}^n)$ , Bob declares his key to be  $k_B = k(\hat{m}, \hat{x}^n)$ , where  $k(\cdot, \cdot)$  is another (random) binning function. The proof for the secrecy exponent leverages on the properties of the Rényi entropy as in [12], [22].

The union of the regions in (25) is likely to be a strict inner bound since our coding scheme does not involve the use of any auxiliary random variables (unlike in Proposition 1). However, as we shall see in Section IV-D, our analysis of the ML-MAP strategy shows that all weakly-achievable rates  $R_{SK} < C_{SK}$  are strongly-achievable for degraded channels.

Another reason as to why the error exponent region is likely not tight may be distilled from works by Csiszár-Narayan [15], later extended by Gohari-Anantharam [34], [35]. Consider an external agent who can recover  $X^n$  perfectly after receiving Eve's information  $(Z^n, \Phi)$  and the shared secret key  $K_A$ . If the agent were not able to recover  $X^n$  there would be some piece of information about  $X^n$ , independent of  $(Z^n, \Phi, K_A)$ , that the external agent would require to know  $X^n$  perfectly. In such a setting, Alice could reveal the needed information on the public channel without lowering the secret key rate. This follows since what would be revealed is independent of  $K_A$ , and thus of no use to Eve. Thus, without loss of generality, we can assume the external agent knows  $X^n$  perfectly.

Now, say that  $Z$  is a degraded version of  $Y$ . In this setting Bob can simulate  $Z^n$ . Bob also has  $(\Phi, K_B)$  (note that  $K_B = K_A$  with high probability). So, Bob too can be assumed to recover  $X^n$  perfectly. In other words, in the degraded setting there is no loss in generality in requiring Bob to recover  $X^n$ . However, when there is a non-trivial joint distribution amongst  $X, Y$  and  $Z$  (i.e., the non-degraded case), it is not necessarily true that Bob can recover  $X^n$ . Hence the error-exponent strategy may be strictly suboptimal (at least in a capacity sense for non-degraded channels). This observation is consistent with the "separation" strategy elucidated in (16) and (17) as the separation strategy—which is optimal in the degraded case—in effect implies that Bob can decode  $X^n$  as discussed in the previous paragraph.

### C. Positivity of Error Exponents and Interpretations

For a particular choice of input distribution  $p(s)$ , the following proposition characterizes the boundary of the achievable rate-exponent region in (24).

**Proposition 5** (Positivity of Error Exponents). *For a fixed  $p(s)$ , the exponent  $E_o(p(s), R_\Phi, R_M)$  in (21) is positive if*

$$R_\Phi > H(X|Y, S) \quad \text{and} \quad (27)$$

$$R_\Phi - R_M > H(X|Y, S) - I(S; Y). \quad (28)$$



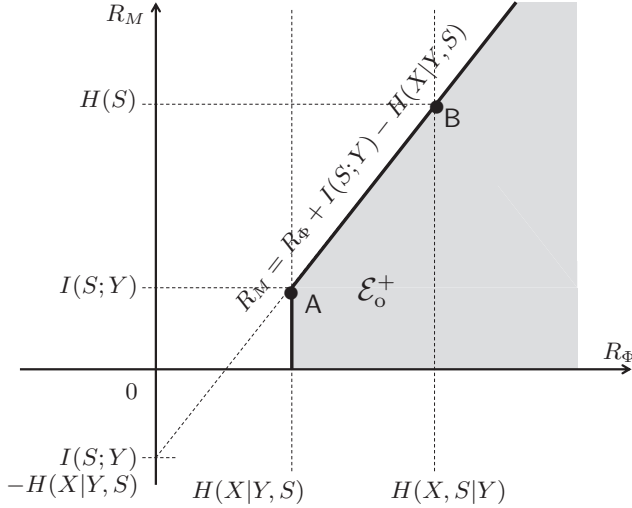


Fig. 2. The region where  $E_o(p(s), R_\Phi, R_M)$  is positive is denoted by the shaded set  $\mathcal{E}_o^+$ . See (27) and (28). Points A =  $(H(X|Y, S), I(S; Y))$  and B =  $(H(X, S|Y), H(S))$  respectively denote the two-step approach (of Bob first recovering  $M$  through channel decoding and then recovering  $X^n$  via Slepian-Wolf decoding) and the source emulation approach (with vector source  $(X, S)$  given  $Y$  just as in the achievability proof of Proposition 1) discussed in greater detail in Section IV-E-III. The semi-infinite ray emanating from A, passing through B, and extending northeast is the capacity-achieving set of  $(R_\Phi, R_M)$  for our error exponent scheme. For source emulation it only starts from B and extends northeast.

See Fig. 2. Similarly, the exponent  $F_o(p(s), R_{SK}, R_\Phi, R_M)$  in (23) is positive if

$$R_{SK} + R_\Phi - R_M < H(X|Z, S) - I(S; Z). \quad (29)$$

See Fig. 3.

The proposition can be proved by firstly verifying that  $\tilde{E}_o^{(j)}$ ,  $j = 1, 2, 3$  (resp.  $\tilde{F}_o$ ) are concave functions of  $\rho$  (resp.  $\alpha$ ); secondly by computing the partial derivative of  $\tilde{E}_o^{(j)}$  (resp.  $\tilde{F}_o$ ) with respect to  $\rho$  (resp.  $\alpha$ ); and finally by evaluating the slope at  $\rho = 0$  (resp.  $\alpha = 0$ ). This is a standard calculation and as such, we omit the details. See [22, Theorem 3] and the accompanying remarks for similar calculations. Note that there are only two rate constraints for reliability in (27) and (28). This is because the rate constraint required for  $\tilde{E}_o^{(2)} > 0$  is

$$R_M - R_\Phi < I(X, Y; S) \quad (30)$$

which is already implied by (28) since  $I(S; Y) - H(X|Y, S) = I(X, Y; S) - H(X|Y) \leq I(X, Y; S)$ . Note that in the derivation of  $\tilde{E}_o^{(2)}$  and (30), we treat  $(X, Y)$  as a vector output of a channel with input  $S$ . We had mentioned previously that  $R_\Phi$  can be reduced and yet the secret-key capacity would remain unchanged if we reduce  $R_M$  accordingly. However, we observe from (27) that there is nevertheless a lower bound on  $R_\Phi$  due to a marginal error event. Thus,  $R_\Phi$  cannot be reduced arbitrarily, and in particular not beyond the conditional entropy  $H(X|Y, S)$ . Intuitively, the corner point in Fig. 2 (point A) where  $R_\Phi = H(X|Y, S)$  and  $R_M = I(S; Y)$  may be achieved from a two-step decoding procedure where Bob first recovers  $M$  through channel decoding given  $Y^n$  and then recovers  $X^n$  via Slepian-Wolf decoding given the vector side-information

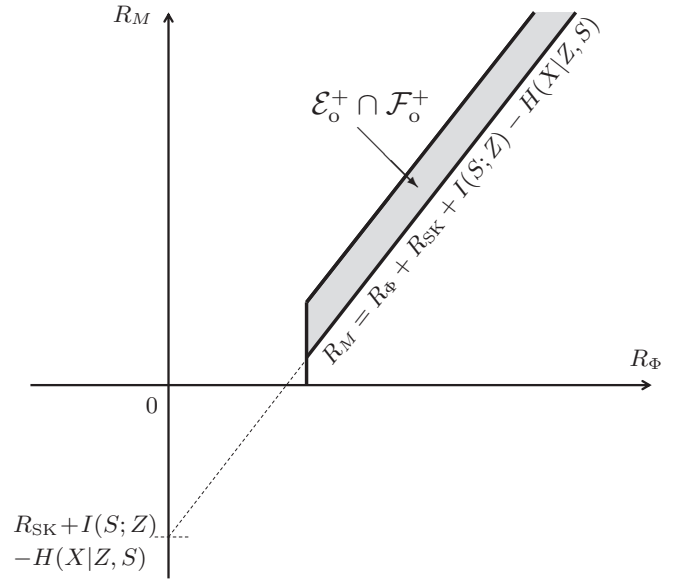


Fig. 3. This is the same as Fig. 2 with (29) also illustrated. The region where  $E_o(p(s), R_\Phi, R_M)$  and  $F_o(p(s), R_\Phi, R_M)$  are both positive is denoted by the shaded set  $\mathcal{E}_o^+ \cap \mathcal{F}_o^+$ . This combines the rate constraints in (27), (28) and (29). The intuition here is the following: To maximize  $R_{SK}$ , the line indicated by the equation  $R_M = R_\Phi + R_{SK} + I(S; Z) - H(X|Z, S)$  should be shifted upwards until the shaded region almost vanishes.

$(S^n(M), Y^n)$  ( $M$  assumed to be decoded correctly). This two-step decoding procedure is, however, not what we do in the ML-MAP decoding scheme in (26). The ML-MAP decoding scheme decodes  $M$  and  $X^n$  jointly so its exponent is likely to be higher than the two-step decoding scheme.

The first rate condition in (28) for the reliability exponent to be positive may be rewritten as follows:

$$R_M < I(S; Y) + [R_\Phi - H(X|Y, S)]. \quad (31)$$

Using (31), we see that if  $R_\Phi > H(X|Y, S)$  (i.e., the compression rate is strictly larger than the Slepian-Wolf limit  $H(X|Y, S)$  as allowed by (27)), we may transmit the message  $M$  reliably at rates higher than  $I(S; Y)$ , which is the maximum transmission rate when the input distribution  $p(s)$  is used for the channel  $p(y|s)$ .

The rate condition in (29) for the secrecy exponent to be positive may be written in the following equivalent forms:

$$R_{SK} + R_\Phi < H(X|Z, S) + [R_M - I(S; Z)], \quad (32a)$$

$$R_M > I(S; Z) - [H(X|Z, S) - (R_{SK} + R_\Phi)]. \quad (32b)$$

The authors in [22, Theorem 3] showed that the secrecy exponent is positive when  $R_{SK} + R_\Phi < H(X|Z, S)$ . However, we observe from (32a) that if  $R_M > I(S; Z)$  (i.e., the message rate is larger than what Eve can resolve with her channel  $p(z|s)$ ), the secrecy exponent is positive even though  $R_{SK} + R_\Phi$  may be larger than  $H(X|Z, S)$ . Similarly, observe from (32b) that if  $R_{SK} + R_\Phi < H(X|Z, S)$ , then  $R_M$  may be smaller than  $I(S; Z)$  for the secrecy exponent to be positive.

#### D. Strong Achievability and Connections to Degradedness

Assume that the DMBC  $p(x, y, z|s)$  is degraded. We then eliminate the rates  $R_\Phi$  and  $R_M$  in (28) and (29) and conclude

TABLE I  
SPECIALIZATION OF PROPOSITION 5 TO EXISTING RESULTS

	Specialization	Reliability $E_o$	Secrecy $F_o$
I	$X = \emptyset$ $R_\Phi = 0$	Channel coding [10, Theorem 5.6.2]	Wiretap channel coding [12, Theorem 3]
II	$S = \emptyset$ $R_M = 0$	Source coding with side information [11]	Secret key generation with public discussion [12]
III	$R_M = H(S)$	Source emulation ( $X, S$ ) applied to [11]	Source emulation ( $X, S$ ) applied to [12]

that  $R_{SK}$  is strongly-achievable if

$$\begin{aligned}
 R_{SK} &< H(X|Z, S) - I(S; Z) - (H(X|Y, S) - I(S; Y)) \\
 &= I(X; Y|S) - I(X; Z|S) - I(S; Z) + I(S; Y) \\
 &= I(X, S; Y) - I(X, S; Z) \\
 &= I(X, S; Y|Z); \tag{33}
 \end{aligned}$$

per (27) we also require that  $R_\Phi > H(X|Y, S)$ . The last equality holds due to the assumption of degradedness, cf. Defn. 6. See Fig. 3. This concurs with the result for the secret key capacity for degraded channels obtained using pure source emulation in Corollary 3. This alternative method of deriving the secret key capacity for the degraded case via the error exponent route demonstrates that for degraded channels, the weak and strong definitions for achievability (in Definitions 1 and 5 respectively) coincide.

#### E. Connections to Previous Results

The reliability exponent in (20) is akin to a combination of Gallager's exponents for channel coding [10, Sec. 5.6] and for source coding with side information [11]. The secrecy exponent has been studied for the secret key agreement source model [12], [28], the corresponding channel model [12], and the source model with external deterministic excitation [22]. Hayashi [12], [25] also analyzed the exponential decay of the information leakage rate for the wiretap channel. The expression in (22) is akin to a combination of the key leakage rate due to Eve's DMC  $p(z|s)$  [12] and the secrecy exponent of the excited DMMS  $p(x, z|s)$  [22].

In light of these observations, Proposition 5 may be specialized to derive conditions for the positivity of the exponents for the pure channel-type and the pure source-type models:

- I. *Alice has no access to the channel output ( $X \leftarrow \emptyset$ ) and no public discussion ( $R_\Phi = 0$ ):* This case specializes to the wiretap channel  $p(y, z|s)$ . In this case, the reliability exponent  $E_o(p(s), 0, R_M)$  reduces to that of channel coding over a discrete memoryless channel (DMC) [10, Theorem 5.6.2] and (28) reduces to the condition

$$R_M < I(S; Y), \tag{34}$$

which we recognize as the condition for reliable communication over the DMC  $p(y|s)$ .

In addition, our secrecy exponent  $F_o(p(s), R_{SK}, 0, R_M)$  reduces to Hayashi's wiretap secrecy exponent in [12, Eq. (14)] and (33) reduces to the confidential message rate constraint

$$R_{SK} < I(S; Y) - I(S; Z), \tag{35}$$

which we recognize as the condition for reliable communication and secrecy for the wiretap channel. Note that the usual auxiliary random variable " $U$ " [30, Theorem 22.1] has been taken to be equal to the source  $S$  in (35).

- II. *Alice has no control of the channel input:* This case specializes to the secret key generation model with public discussion characterized by the DMMS  $p(x, y, z) = \sum_s p(s)p(x, y, z|s)$  studied in [4], [15], [16], [34], [35]. The reliability exponent was characterized in [11] and was stated as a special case of the main result in [22]. By letting  $S \leftarrow \emptyset$  and  $R_M = 0$ , (28) simplifies to

$$R_\Phi > H(X|Y) \tag{36}$$

which we recognize as the condition for lossless source coding of  $X$  given side information  $Y$  [36]. This recovers an analogue of the result in [22, Theorem 3]. Inequality (36) also concurs with (27).

We remark that Watanabe et al. [29] showed that strongly secure privacy amplification is not achievable by Slepian-Wolf coding. But this does not contradict our error exponent result because the codes used in [29] have rates tending to the optimal compression rate  $H(X|Y)$  in (36) at a rate of  $b/\sqrt{n}$  for some  $b \in \mathbb{R}$  (cf. [37]). However, we operate at rates *strictly above*  $H(X|Y)$  in (36) so strong secrecy is indeed possible.

The secrecy exponent  $F_o(p(s), R_{SK}, R_\Phi, 0)$  was derived in [12], [22], [28]. Our secrecy exponent result in (29) specializes in this case to

$$R_{SK} + R_\Phi < H(X|Z) \tag{37}$$

which recovers an analogue of the main result in Chou et al. [22, Theorem 3].

- III. *Alice excites the channel with  $S^n$  generated in an i.i.d. manner according to  $p_S$  and considers the joint variable  $(X, S)$  as her source:* This is similar to the source emulation scheme adopted in the proof of Proposition 1 without cost constraint and ignoring the encoder but considering the three terminals: Alice with  $(X, S)$ , Bob with  $Y$ , and Eve with  $Z$ . This is point B in Fig. 2. The reliability and secrecy exponents will be of the form in [11] and [12], respectively, with i.i.d. source  $(X, S)$ . Thus substituting  $R_M = H(S)$  in (28) and (29) yields

$$\begin{aligned}
 R_\Phi &> H(X|Y, S) - I(S; Y) + H(S) \\
 &= H(X, S|Y) \tag{38}
 \end{aligned}$$

$$\begin{aligned}
 R_{SK} + R_\Phi &< H(X|Z, S) - I(S; Z) + H(S) \\
 &= H(X, S|Z). \tag{39}
 \end{aligned}$$

Upon the elimination of  $R_\Phi$  which, by (38), satisfies the required lower bound in (27), we have

$$\begin{aligned}
 R_{SK} &< H(X, S|Z) - H(X, S|Y) \\
 &= I(X, S; Y) - I(X, S; Z). \tag{40}
 \end{aligned}$$

Notice that the difference of mutual informations on the RHS of (40) is  $I(X, S; Y|Z)$  for degraded DMBCs. This concurs with the secret key capacity of degraded DMBCs in Corollary 3.



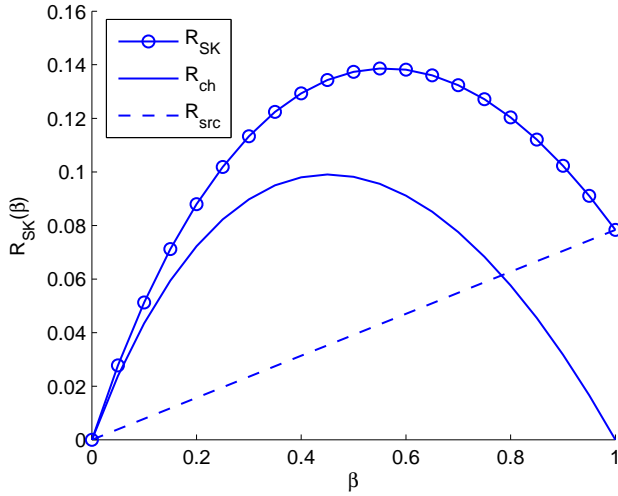


Fig. 4. Secret key rate of the binary on-off channel as a function of  $\beta$ . The input  $S \sim \text{Bern}(\beta)$ . The parameters are  $q = 0.5$ ,  $\tilde{q} = 0.8$ ,  $\delta = 0.1$ ,  $\delta_3 = 0.2$ . Note that  $C_{\text{SK}} = \max_{\beta \in [0,1]} R_{\text{SK}}(\beta)$  and the maximizing  $\beta^* \approx 0.59$ .

As is mentioned in the Introduction, while the source emulation scheme achieves the secret key capacity, this rate cannot be strongly achieved (per Definition 5) if  $R_\Phi$  is upper bounded by some quantity (but nonetheless still satisfies the lower bound in (27)) if we do not also have the flexibility to concurrently set the rate of the sounding signal  $R_M$ . Observe that the lower bound on  $R_\Phi$  in (38) resulting from the pure source emulation strategy (cf. the achievability proof of Proposition 1) is  $H(X, S|Y)$  which is at least as large as  $H(X|Y, S)$  in (27) in Proposition 5 and, in general, is strictly larger. Thus, our error exponent scheme which involves wiretap coding plus key distillation allows us to reduce  $R_\Phi$  from  $H(X, S|Y)$  to  $H(X|Y, S)$ —the difference being  $H(S|Y)$ .

The specializations are summarized in Table I.

## V. NUMERICAL EXAMPLES

We consider two examples in this section. The first example illustrates the tradeoffs involved in the capacity results in Section III. The second example illustrates the tradeoffs in the achievable error exponent results in Section IV.

### A. Capacity of the Binary On-off Channel

For our first example consider the binary on-off model

$$\begin{aligned} X &= H \cdot S \oplus N_1 \\ Y &= H \cdot S \oplus N_2 \\ Z &= (\tilde{H} \cdot H) \cdot S \oplus N_3, \end{aligned}$$

where all the variables are binary and where the operations are performed in the field of size 2. Hence, the addition above is binary modulo-2 addition. The “channel gain”  $H$  is  $\text{Bern}(q)$  and  $\tilde{H}$  is  $\text{Bern}(\tilde{q})$ .<sup>4</sup> Noise  $N_i$  is  $\text{Bern}(\delta_i)$  and the  $N_i$  are mutually independent. The channel describes a model

in which, in the absence of noise, Eve’s observation is strictly worse than that of Alice’s and Bob’s since  $\tilde{H}$  is present.

If  $\delta_1 = \delta_2 = \delta$  and  $\tilde{q}\delta < \delta_3$ , then Eve’s channel output is a degraded version of Bob’s. In this case, there exists a  $Z' \triangleq \tilde{H}' \cdot Y \oplus N'_3$  for some  $\tilde{H}'$ , with the same distribution as  $\tilde{H}$ , and independent  $N'_3 \sim \text{Bern}(\delta'_3)$  such that  $(X, S) - Y - Z'$ , where

$$\delta'_3 = \frac{\delta_3 - \tilde{q}\delta}{1 - 2\tilde{q}\delta}.$$

Let  $S \sim \text{Bern}(\beta)$ . The first term of  $R_{\text{ch}}$  is

$$\begin{aligned} I(S; Y) &= H(Y) - H(Y|S) \\ &= H_b(\beta q * \delta) - [\beta H(Y|S=1) + (1-\beta)H(Y|S=0)] \\ &= H_b(\beta q * \delta) - \beta H_b(q * \delta) - (1-\beta)H_b(\delta), \end{aligned}$$

where  $H_b(\cdot)$  is the binary entropy function and the operation  $a * b \triangleq a(1-b) + (1-a)b$ . Similarly, the second term of  $R_{\text{ch}}$  can be expressed as

$$I(S; Z) = H_b(\beta \tilde{q} q * \delta_3) - \beta H_b(\tilde{q} q * \delta_3) - (1-\beta)H_b(\delta_3).$$

The secret key rate due to source  $X$  can be calculated as

$$\begin{aligned} R_{\text{src}} &= I(X; Y|S) - I(X; Z|S) \\ &= \beta[I(X; Y|S=1) - I(X; Z|S=1)] \\ &= \beta[H_b(q * \delta) - H_b(\delta * \delta) - H_b(\tilde{q} q * \delta_3) \\ &\quad + (1 - q * \delta)H_b(\delta'_3) + (q * \delta)H_b(\tilde{q} * \delta'_3)]. \end{aligned}$$

The second equality follows because if  $S = 0$ , the source is not observed and so there is no mutual information between  $X$  and  $Y$  (nor between  $X$  and  $Z$ ).

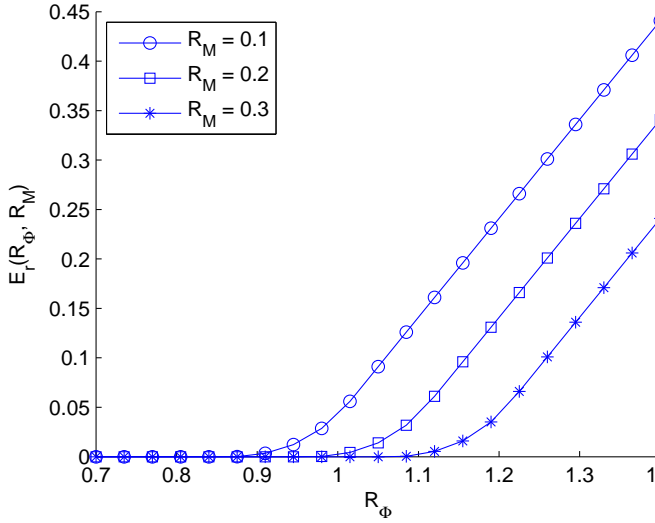
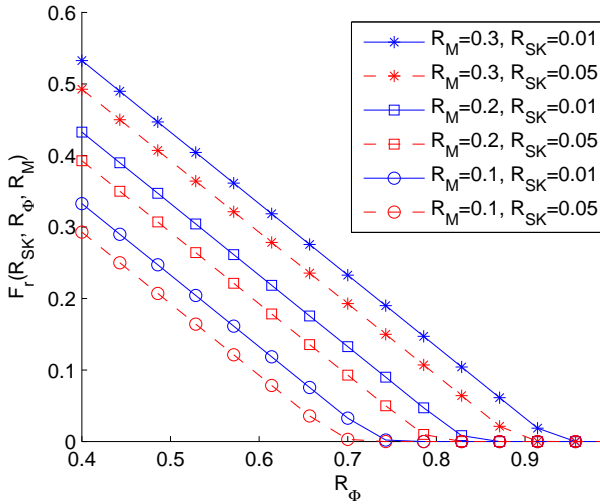
The secret key rate when the input is a  $\text{Bern}(\beta)$  source is  $R_{\text{SK}}(\beta) = R_{\text{ch}}(\beta) + R_{\text{src}}(\beta)$  which is plotted in Fig. 4 as a function of  $\beta$  for the following parameters:  $q = 0.5$ ,  $\tilde{q} = 0.8$ ,  $\delta = 0.1$ ,  $\delta_3 = 0.2$ . Note that  $R_{\text{ch}}$  is a concave function of  $\beta$  while  $R_{\text{src}}$  is a linear function of  $\beta$ . If  $\beta = 0$  then  $R_{\text{SK}} = 0$  since  $X, Y, Z$  are jointly statistically independent. On the other hand, if  $\beta = 1$  then  $S^n$  is the all ones sequence and the  $R_{\text{src}}$  is maximal since the input excites all common randomness due to the *common* on-off coefficient  $H$ . However, when  $\beta = 1$ , the secrecy rate of the wiretap channel  $R_{\text{ch}} = 0$ . As we decrease  $\beta$   $R_{\text{ch}}$  initially increases faster than  $R_{\text{src}}$  decreases, resulting in the maximum  $R_{\text{SK}}$  being achieved at an intermediate value of  $\beta$ . In this example we have observed an inherent tradeoff between the amount of the secret key rate due to common randomness and due to wiretap secrecy.

### B. Error Exponents

We now illustrate our error exponent results. We assume that all variables are binary valued, i.e.,  $\mathcal{X} = \mathcal{Y} = \mathcal{Z} = \mathcal{S} = \{0, 1\}$ . We selected the parameters of the DMBC  $p(x, y, z|s)$  to ensure that Eve’s observation  $Z$  is a degraded version of Bob’s  $Y$ . We do so by first selecting the parameters of the conditional distribution  $p(x, y|s)$ , then we proceeded to choose the parameters in the conditional distribution  $p(z|y)$ . We keep the channel  $p(x, y, z|s)$  fixed throughout this subsection. Define the *input distribution-optimized reliability exponent*

$$E_r(R_\Phi, R_M) \triangleq \max_{p(s)} E_o(p(s), R_\Phi, R_M), \quad (41)$$

<sup>4</sup>We say that a binary random variable  $X$  is  $\text{Bern}(\gamma)$  if  $\Pr[X = 1] = \gamma$ .

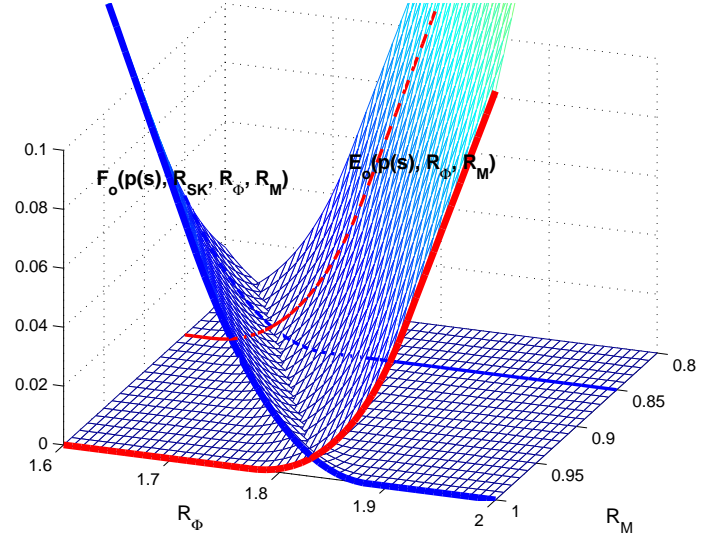
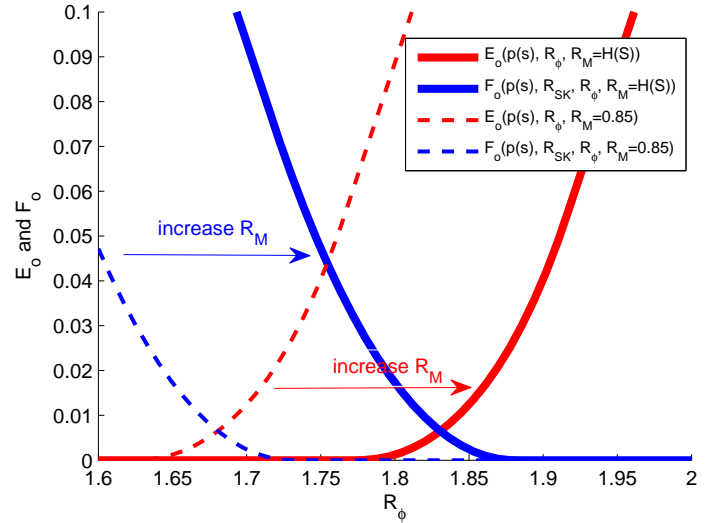

 Fig. 5. Plot of the random coding reliability exponent  $E_r$  in (41)

 Fig. 6. Plot of the random coding secrecy exponent  $F_r$  in (42)

where  $E_o$  was defined in (21). Also define the *input distribution-optimized secrecy exponent*:

$$F_r(R_{SK}, R_\Phi, R_M) \triangleq \max_{p(s)} F_o(p(s), R_{SK}, R_\Phi, R_M), \quad (42)$$

where  $F_o$  was defined in (23). Note that for a particular set of rates  $(R_{SK}, R_\Phi, R_M)$ , the optimal input distributions  $p^*(s)$  in (41) and (42) may be *different*. Hence, one has to use a *common*  $p(s)$  in (25). We append the subscript  $r$  to  $E_r(R_\Phi, R_M)$  and  $F_r(R_{SK}, R_\Phi, R_M)$  to allude to the fact that in the derivation of these exponents, we use both *random coding* [10] and *random binning* schemes [11].

The functions  $E_r(R_\Phi, R_M)$  and  $F_r(R_{SK}, R_\Phi, R_M)$  are plotted in Figs. 5 and 6 respectively. From Fig. 5, we observe that  $R_\Phi \mapsto E_r(R_\Phi, R_M)$  is a non-decreasing function. This is intuitive because given more information (i.e., when  $R_\Phi$  is large) and with  $R_M$  fixed, Bob can decode the key  $K_B$  with greater reliability. In contrast,  $R_M \mapsto E_r(R_\Phi, R_M)$  is a non-increasing function. This is also intuitive because Alice's


 Fig. 7. Plot of the reliability exponent  $E_o$  and secrecy exponent  $F_o$  for a fixed input distribution  $p(s) = \text{Bern}(0.5)$  with  $R_{SK} = 0.01$ . The exponents for two different values of  $R_M$  are shown.

 Fig. 8. Two-dimensional visualization of Fig. 7. The thick solid lines correspond to  $R_M = H(S) = 1$  and the thin dashed lines correspond to  $R_M = 0.85$ .

private source of randomness is increased if  $R_M$  is increased making it more challenging for Bob to decode the key.

From Fig. 6, we observe that  $R_\Phi \mapsto F_r(R_{SK}, R_\Phi, R_M)$  is a non-increasing function. This is because as more public information is made available to Bob, with all else fixed, the key leakage rate increases, resulting in a smaller secrecy exponent. The function  $R_M \mapsto F_r(R_{SK}, R_\Phi, R_M)$  is non-decreasing because as Alice increases the use of her private randomness through a larger  $R_M$ , she can conceal more of the key from Eve. Finally,  $R_{SK} \mapsto F_r(R_{SK}, R_\Phi, R_M)$  is non-increasing because  $R_{SK}$  can be interpreted as the residual source of secrecy that can be generated by Alice and Bob while keeping Eve ignorant of the key generated.

In Fig. 7, we plot the exponents as a function of  $R_\Phi$  and  $R_M$  for  $R_{SK} = 0.01$ . The input distribution  $p(s)$  is kept fixed. Note

that there is a non-empty region in the  $(R_\Phi, R_M)$  plane for which *both* exponents are positive, indicating that  $R_{SK} = 0.01$  is strongly achievable. For clarity, we also present a two-dimensional visualization in Fig. 8 which helps to show the utility of our sender-excited model. We observe the following: Suppose we want to have a secret key rate of  $R_{SK} = 0.01$  and that the public message rate must be limited to, say,  $R_\Phi \leq 1.68$  due to system constraints. Then by simply adopting a source emulation strategy,  $R_M = H(S) = 1$  (i.e., case (III) of Section IV-E), and the reliability exponent is zero even though the secrecy exponent is high. The reliability and secrecy exponents for this choice of parameters is plotted with the thick solid lines. Thus, we *cannot achieve* the key rate of  $R_{SK} = 0.01$  with the fixed input distribution  $p(s)$ . However, our model affords us the flexibility to tune  $R_M$ . If, for instance, we reduce it to  $R_M = 0.85$  while keeping  $R_\Phi = 1.68$  we tradeoff a reduction in the secrecy exponent for an increase in the reliability exponent. With this new choice of  $R_M$  *both* exponents will be positive and the key rate  $R_{SK} = 0.01$  is (strongly) achieved with the same fixed  $p(s)$ . The exponents for this choice of parameters are plotted by the thin dashed lines.

## VI. PROOFS OF RESULTS IN SECTION III

### A. Proof of Converse of Proposition 1

We start with a lemma [3, Lemma 4.1], which is a consequence of the Csiszár sum identity [30, Ch. 2].

**Lemma 6.** *The following equality holds for arbitrary random variables  $K, \Phi, Y^n, Z^n$ :*

$$\begin{aligned} I(K; Y^n | \Phi) - I(K; Z^n | \Phi) \\ = \sum_{i=1}^n I(K; Y_i | Y^{i-1}, Z_{i+1}^n, \Phi) - I(K; Z_i | Y^{i-1}, Z_{i+1}^n, \Phi). \end{aligned}$$

*Proof of Converse of Proposition 1:* Fix any sequence of  $(2^{nR_M}, 2^{nR_\Phi}, n, \Gamma)$  codes per Section II-A. Let  $R_{SK}$  be any  $\Gamma$ -weakly achievable rate per Definition 1. Consider,

$$nR_{SK} \leq I(K_A; Y^n, \Phi) + n\epsilon_n \quad (43)$$

$$\leq I(K_A; Y^n, \Phi) - I(K_A; Z^n, \Phi) + 2n\epsilon_n \quad (44)$$

$$= I(K_A; Y^n | \Phi) - I(K_A; Z^n | \Phi) + 2n\epsilon_n$$

$$\begin{aligned} &= \sum_{i=1}^n I(K_A; Y_i | Y^{i-1}, Z_{i+1}^n, \Phi) \\ &\quad - I(K_A; Z_i | Y^{i-1}, Z_{i+1}^n, \Phi) + 2n\epsilon_n \end{aligned} \quad (45)$$

where (43) is due to Fano's inequality ( $\epsilon_n \rightarrow 0$  as  $n \rightarrow \infty$ ), (44) is due to the secrecy condition in (3) and (45) by applying Lemma 6. Now we make the following identifications of the auxiliary random variables

$$W_i \triangleq (Y^{i-1}, Z_{i+1}^n, \Phi), \quad \text{and} \quad U_i \triangleq (K_A, W_i). \quad (46)$$

As can be readily verified, the chosen variables  $W_i$  and  $U_i$  satisfy the Markov condition

$$W_i - U_i - (S_i, X_i) - (Y_i, Z_i)$$

as required by (9). Note that since  $K_A$  and  $\Phi$  (random variables contained in our identifications in  $W_i$  and  $U_i$  in

(46)) are both functions of  $(M, X^n)$  (see Section II),  $S_i$  by itself does not separate  $(X_i, Y_i, Z_i)$  from  $W_i$  and  $U_i$ . However, the separation *does* hold when  $(S_i, X_i)$  are grouped together by the discrete memoryless nature of the channel  $p(x, y, z | s)$ . Substituting the choice of auxiliary random variables in (46) into (45) yields,

$$\begin{aligned} nR_{SK} &\leq \sum_{i=1}^n I(K_A; Y_i | W_i) - I(K_A; Z_i | W_i) + 2n\epsilon_n \\ &= \sum_{i=1}^n I(K_A, W_i; Y_i | W_i) - I(K_A, W_i; Z_i | W_i) + 2n\epsilon_n \\ &= \sum_{i=1}^n I(U_i; Y_i | W_i) - I(U_i; Z_i | W_i) + 2n\epsilon_n. \end{aligned}$$

Now, introduce the time-sharing random variable  $Q$  with uniform distribution  $P(Q = i) = 1/n$  for all  $i \in [1 : n]$  and independent of  $(W^n, U^n, S^n, X^n, Y^n, Z^n)$ . Define the random variables  $U \triangleq (U_Q, Q)$ ,  $W \triangleq (W_Q, Q)$ ,  $S \triangleq S_Q$ ,  $X \triangleq X_Q$ ,  $Y \triangleq Y_Q$  and  $Z \triangleq Z_Q$ . Then, we have

$$\begin{aligned} R_{SK} &\leq \sum_{q=1}^n P(Q = q) [I(U_q; Y_q | W_q) - I(U_q; Z_q | W_q)] + 2\epsilon_n \\ &= I(U_Q; Y_Q | W_Q, Q) - I(U_Q; Z_Q | W_Q, Q) + 2\epsilon_n \\ &= I(U_Q, Q; Y_Q | W_Q, Q) - I(U_Q, Q; Z_Q | W_Q, Q) + 2\epsilon_n \\ &= I(U; Y | W) - I(U; Z | W) + 2\epsilon_n. \end{aligned} \quad (47)$$

Note also that since  $S^n$  satisfies the almost sure cost constraint in (1),  $\frac{1}{n} \sum_{i=1}^n E[\Lambda(S_i)] \leq \Gamma$  holds. This implies from the definition of  $Q$  and  $S$  that  $E[\Lambda(S)] = E_Q\{E[\Lambda(S_Q) | Q]\} \leq \Gamma$ . Thus to remove the dependence on the code, we maximize (47) over all joint distributions that satisfy (9) and  $E[\Lambda(S)] \leq \Gamma$ , i.e.,

$$R_{SK} \leq \max_{\substack{W-U-(X,S)-(Y,Z) \\ E[\Lambda(S)] \leq \Gamma}} I(U; Y | W) - I(U; Z | W) + 2\epsilon_n.$$

Taking  $n \rightarrow \infty$  completes the proof of the converse. ■

### B. Proof of Proposition 2

*Proof:* We prove the upper bound in (11). Consider the inequalities:

$$nR_{SK} \leq I(K_A; Y^n, \Phi) + n\epsilon_n \quad (48)$$

$$\leq I(K_A; Y^n, \Phi, Z^n) + n\epsilon_n$$

$$= I(K_A; Y^n | \Phi, Z^n) + I(K_A; \Phi, Z^n) + n\epsilon_n$$

$$\leq I(K_A; Y^n | \Phi, Z^n) + 2n\epsilon_n \quad (49)$$

$$\leq I(K_A, \Phi; Y^n | Z^n) + 2n\epsilon_n, \quad (50)$$

where (48) follows Fano's inequality and (49) is due to the secrecy condition (3). Continuing from (50), we have

$$nR_{SK} \leq I(X^n, M; Y^n | Z^n) + 2n\epsilon_n \quad (51)$$

$$= I(X^n; Y^n | Z^n) + I(M; Y^n | X^n, Z^n) + 2n\epsilon_n$$

$$\leq I(X^n; Y^n | Z^n) + I(S^n; Y^n | X^n, Z^n) + 2n\epsilon_n \quad (52)$$

$$= I(S^n; Y^n | Z^n) + I(X^n; Y^n | S^n, Z^n) + 2n\epsilon_n, \quad (53)$$

where (51) follows because  $(K_A, \Phi)$  is a function of  $(X^n, M)$  and (52) follows because the channel only depends on  $S^n$  so



$M - S^n - (X^n, Y^n, Z^n)$ .<sup>5</sup> Now the first term (53) can be upper bounded as follows

$$\begin{aligned} I(S^n; Y^n | Z^n) &= H(Y^n | Z^n) - H(Y^n | S^n, Z^n) \\ &= \sum_{i=1}^n H(Y_i | Y^{i-1}, Z^n) - H(Y_i | Y^{i-1}, S^n, Z^n) \\ &\leq \sum_{i=1}^n H(Y_i | Z_i) - H(Y_i | S_i, Z_i) = \sum_{i=1}^n I(S_i; Y_i | Z_i), \end{aligned} \quad (54)$$

where the inequality follows by conditioning reduces entropy and the Markov chain  $(Y^{i-1}, Z^{n \setminus i}, S^{n \setminus i}) - (S_i, Z_i) - Y_i$ . The second term in (53) can be written as a sum:

$$I(X^n; Y^n | S^n, Z^n) = \sum_{i=1}^n I(X_i; Y_i | S_i, Z_i) \quad (55)$$

because the channel  $p(x, y, z | s)$  is memoryless. Substituting (54) and (55) into (53) yields

$$\begin{aligned} nR_{SK} &\leq \sum_{i=1}^n I(S_i; Y_i | Z_i) + I(X_i; Y_i | S_i, Z_i) + 2n\epsilon_n \\ &= \sum_{i=1}^n I(X_i, S_i; Y_i | Z_i) + 2n\epsilon_n. \end{aligned} \quad (56)$$

The proof can be completed using the time-sharing technique in the converse proof of Proposition 1. ■

## VII. PROOFS OF RESULTS IN SECTION IV

In this section, we provide the proof of Theorem 4 on the capacity-reliability-secrecy region. This section will be split into three subsections: In the first subsection, we collect some relevant definitions and describe the coding scheme. The second and third subsections contain the proofs of the achievability (lower bounds) of the reliability and secrecy exponents respectively. This proves the achievability of the region  $\tilde{\mathcal{R}}(p(s), R_\Phi, R_M)$  defined in (24).

### A. Definitions and Coding Scheme

We start with some definitions to describe the generation of the codewords  $s^n(m)$ , the key and the public message generation procedures.

**Definition 7** (Random code). A  $(2^{nR_M}, n)$  random code generated according to  $p(s)$  is a random subset of  $S^n$  which contains length- $n$  sequences  $s^n(m)$ ,  $m \in [1 : 2^{nR_M}]$  where each sequence  $s^n(m)$ , called a codeword, is drawn according to the pmf  $\prod_{i=1}^n p(s_i)$ .

Note that we do not place any cost constraints on  $p(s)$  because we assume that  $\Gamma = \infty$  in Section IV.

**Definition 8** (Random binning function [11]). A  $2^{nR}$  random binning function for an alphabet  $\mathcal{U}$  is a random map<sup>6</sup>  $\psi : u \in \mathcal{U} \rightarrow b \in [1 : 2^{nR}]$  that satisfies the following properties:

- **Uniformity:** Each element  $u \in \mathcal{U}$  is independently and uniformly assigned to an element of  $[1 : 2^{nR}]$ .

<sup>5</sup>In fact, (52) holds with equality because  $S^n = S^n(M)$  in addition to the stated Markov relationship.

<sup>6</sup>More precisely,  $\psi(b|u)$  is a matrix of conditional probabilities.

- **Pairwise Independence:** Each pair of different  $u, u' \in \mathcal{U}$  is mapped  $u \mapsto b$ ,  $u' \mapsto b'$  with probability  $2^{-2nR}$  for each pair of elements  $b, b' \in [1 : 2^{nR}]$  (not necessarily different).

- The random map  $\psi$  is independent of the random code generation process as per Definition 7. More precisely,

$$P(\{S^n = s^n\} \cap \{\psi(u) = b\}) = P(S^n = s^n)P(\psi(u) = b)$$

We now introduce the notion of a random binning code for the secret key generation protocol (See Section II-A).

**Definition 9** (Random binning secret key code). A  $(2^{nR_{SK}}, 2^{nR_M}, 2^{nR_\Phi}, n)$  random binning secret key code is a  $(2^{nR_M}, 2^{nR_\Phi}, n)$  code for the secret key generation protocol in which the public message and key are generated via two independent random binning functions:

$$\phi : \mathcal{M} \times \mathcal{X}^n \rightarrow \Phi = [1 : 2^{nR_\Phi}] \quad (57)$$

$$k_A : \mathcal{M} \times \mathcal{X}^n \rightarrow \mathcal{K} = [1 : 2^{nR_{SK}}]. \quad (58)$$

More precisely, note from (57) that  $\phi$  is a  $2^{nR_\Phi}$  random binning function for alphabet  $\mathcal{M} \times \mathcal{X}^n$  and from (58) that  $k_A$  is a  $2^{nR_{SK}}$  random binning function for alphabet  $\mathcal{M} \times \mathcal{X}^n$ .

**Codebook Generation and Encoding:** Fix  $p(s)$ . We use a  $(2^{nR_{SK}}, 2^{nR_M}, 2^{nR_\Phi}, n)$  random binning secret key code in which the codewords  $s^n(m)$ ,  $m \in \mathcal{M}$  belong to a  $(2^{nR_M}, n)$  random code generated according to  $p(s)$ . The codewords and bin assignments are revealed to all parties before communication starts. We emphasize that by construction, this  $(2^{nR_{SK}}, 2^{nR_M}, 2^{nR_\Phi}, n)$  code is a  $(2^{nR_M}, 2^{nR_\Phi}, n)$  code (in the sense of Section II-A with  $\Gamma = \infty$ ) such that secret key rate  $R_{SK}$  is achievable. This is because  $K_A$  is uniformly distributed on  $[1 : 2^{nR_{SK}}]$  so (4) is satisfied.

By the definition of  $\tilde{\mathcal{R}}(p(s), R_\Phi, R_M)$  in (24), it suffices to show the following two assertions hold true for any  $p(s)$ :

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log P(K_A \neq K_B) \geq E_o(p(s), R_\Phi, R_M),$$

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log I(K_A; Z^n, \Phi) \geq F_o(p(s), R_{SK}, R_\Phi, R_M).$$

This is what we prove in the next two subsections.

### B. Proof for the Reliability Exponent

In this section, we will prove that  $E_o$  is an achievable reliability exponent. Recall that Bob has access to his channel output  $y^n \in \mathcal{Y}^n$  and the public message  $\phi \in \Phi$ , which was generated by Alice in accordance to the random binning function in (58). In order to analyze the error event that Bob's key does not match Alice's

$$\mathcal{E}_{\text{key}} \triangleq \{K_A \neq K_B\}, \quad (59)$$

we stipulate that Bob decodes *both* Alice's received sequence  $x^n \in \mathcal{X}^n$  and Alice's source of randomness  $m \in \mathcal{M}$ .

We restate the ML-MAP decoding rule in (26): Given  $(y^n, \phi)$ , Bob declares that  $m$  is the message selected by Alice and  $x^n$  is the sequence sent to Alice if the public message bin index of  $(m, x^n)$  agrees with  $\phi$ , i.e.,

$$\phi(m, x^n) = \phi \quad (60)$$

and the probabilities satisfy

$$p(y^n|s^n(m))p(x^n|y^n, s^n(m)) \geq p(y^n|s^n(\tilde{m}))p(\tilde{x}^n|y^n, s^n(\tilde{m})) \quad (61)$$

for all other pairs  $(\tilde{m}, \tilde{x}^n)$  such that  $\phi(\tilde{m}, \tilde{x}^n) = \phi$ . As mentioned previously, this is a hybrid of an ML and an MAP rule. Observe that if we were just to maximize  $p(y^n|s^n(m))$  over  $m$ , this would correspond to a pure ML decoding rule for the channel  $p(y|s)$  as in [10, Sec. 5.6]. If instead we maximize  $p(x^n|y^n, s^n(m))$  over  $x^n$  given  $m$  is known, this would correspond to a pure MAP decoder for the source  $x^n$  given side information  $(m, y^n)$  as in [11].

By analyzing the ML-MAP decoder, we now upper bound the probability of event  $\mathcal{E}_{\text{key}}$  of the ensemble random binning secret key code  $\mathcal{C}$ , i.e.,  $P(\mathcal{E}_{\text{key}}) \triangleq E_{\mathcal{C}}[P(\mathcal{E}_{\text{key}}|\mathcal{C})] = \sum_{\mathcal{C}} p(\mathcal{C})P(\mathcal{E}_{\text{key}}|\mathcal{C})$ . Throughout, we use the notation  $\mathcal{C}$  to denote the random code (a random variable) and  $\mathcal{C}$  to denote a specific code. Define the error event that Bob decodes either  $M$  or  $X^n$  incorrectly

$$\mathcal{E} \triangleq \{(\hat{M}, \hat{X}^n) \neq (M, X^n)\}. \quad (62)$$

Clearly,  $\mathcal{E}_{\text{key}} \subset \mathcal{E}$ . Thus, an upper bound for  $P(\mathcal{E})$  also serves as an upper bound for  $P(\mathcal{E}_{\text{key}})$ . Similarly, a lower bound for the exponent of  $P(\mathcal{E})$  is also a lower bound for the exponent of  $P(\mathcal{E}_{\text{key}})$ . In the interest of tractability, we upper bound  $P(\mathcal{E})$  [instead of  $P(\mathcal{E}_{\text{key}})$ ] when the ML-MAP decoder described in (60) and (61) is used. In order to bound  $P(\mathcal{E})$ , we decompose  $\mathcal{E}$  into the following three disjoint error events:

$$\mathcal{E}_1 \triangleq \{\hat{M} = M, \hat{X}^n \neq X^n\} \quad (63)$$

$$\mathcal{E}_2 \triangleq \{\hat{M} \neq M, \hat{X}^n = X^n\} \quad (64)$$

$$\mathcal{E}_3 \triangleq \{\hat{M} \neq M, \hat{X}^n \neq X^n\} \quad (65)$$

Note that the error exponent is the minimum of the exponents for  $P(\mathcal{E}_1)$ ,  $P(\mathcal{E}_2)$  and  $P(\mathcal{E}_3)$ . In the following, we only provide a detailed derivation for  $P(\mathcal{E}_3)$  as it is the most interesting and unconventional. We note that for  $\mathcal{E}_1$ , if  $M = m$ ,  $p(\hat{x}^n|y^n, s^n(m)) \geq p(x^n|y^n, s^n(m))$  (the MAP decoding part) so this analysis parallels that by Gallager for Slepian-Wolf coding [11] (reconstructing  $X^n$  given side information  $(Y^n, S^n(M))$  and  $M$  is decoded correctly). Thus, we have

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log P(\mathcal{E}_1) \geq \rho R_{\Phi} - \log \sum_{s,y} p(s)p(y|s) \left( \sum_x p(x|y, s)^{1/(1+\rho)} \right)^{1+\rho}. \quad (66)$$

Similarly for  $\mathcal{E}_2$ , we have that  $p(x^n, y^n|s^n(\hat{m})) \geq p(x^n, y^n|s^n(m))$  (Bayes rule) so this is simply the error in ML decoding for channel coding with vector output  $(X, Y)$  and input  $S$ . Consequently, from Gallager's book [10, Sec. 5.6],

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log P(\mathcal{E}_2) \geq \rho(R_{\Phi} - R_M) - \log \sum_s \left( \sum_{x,y} p(s)p(x, y|s)^{1/(1+\rho)} \right)^{1+\rho}. \quad (67)$$

Here we note that there are  $\doteq 2^{nR_M}$  sounding sequences  $s^n(m)$  but by (60), we search within a particular bin indexed by  $\phi$  so effectively, there are only  $\doteq 2^{n(R_M - R_{\Phi})}$  sounding sequences explaining the leading term in (67).

Now, we analyze  $P(\mathcal{E}_3)$  in detail. Consider the probability of error given that  $m$  is the message sent,  $s^n(m)$  represents the ensemble of codewords associated to  $m$  (by the random codebook construction in Definition 7),  $x^n$  is Alice's received sequence and  $y^n$  is Bob's received sequence. That is, consider

$$P(\mathcal{E}_3|y^n, s^n(m), m, x^n) = P \left( \bigcup_{\hat{m} \neq m, s^n(\hat{m}), \hat{x}^n \neq x^n} \mathcal{A}(s^n(\hat{m}), \hat{m}, \hat{x}^n) \right). \quad (68)$$

In the above error probability,  $\mathcal{A}(s^n(\hat{m}), \hat{m}, \hat{x}^n)$  is defined as the error event that the message  $\hat{m} \neq m$ , codeword  $s^n(\hat{m})$  and Alice's sequence  $\hat{x}^n \neq x^n$  are selected in such a way that their ML-MAP objective value is higher than that of the true parameters  $(m, s^n(m), x^n)$ , i.e., that  $p(y^n|s^n(\hat{m}))p(\hat{x}^n|y^n, s^n(\hat{m})) \geq p(y^n|s^n(m))p(x^n|y^n, s^n(m))$  and also that  $\phi(\hat{m}, \hat{x}^n) = \phi(m, x^n)$ . Note in (68) that the error event is averaged over all incorrect codewords  $s^n(\hat{m})$  due to the random codebook construction (Definition 7). Now recall the assumption that the binning process is pairwise independent and also independent of the inputs (Definition 8). More precisely,

$$\begin{aligned} P(\{S^n = s^n(\hat{m})\} \cap \{\phi(m, x^n) = \phi(\hat{m}, \hat{x}^n)\}) \\ = P(S^n = s^n(\hat{m}))P(\phi(m, x^n) = \phi(\hat{m}, \hat{x}^n)) \\ = p(s^n(\hat{m})) \sum_{\phi \in \Phi} \frac{1}{|\Phi|^2} = \frac{p(s^n(\hat{m}))}{|\Phi|}. \end{aligned} \quad (69)$$

Let  $\mathbf{1}_{\mathcal{B}}$  be the indicator variable of the set  $\mathcal{B}$ . By using the definition of  $\mathcal{A}(s^n(\hat{m}), \hat{m}, \hat{x}^n)$  and (69), we can upper bound the probability of  $\mathcal{A}(s^n(\hat{m}), \hat{m}, \hat{x}^n)$  as follows:

$$\begin{aligned} P(\mathcal{A}(s^n(\hat{m}), \hat{m}, \hat{x}^n)) \\ = \frac{p(s^n(\hat{m}))}{|\Phi|} \mathbf{1}_{\{p(\hat{x}^n|y^n, s^n(\hat{m})) \geq p(x^n|y^n, s^n(m))\}} \\ \leq \frac{p(s^n(\hat{m}))}{|\Phi|} \left( \frac{p(y^n|s^n(\hat{m}))p(\hat{x}^n|y^n, s^n(\hat{m}))}{p(y^n|s^n(m))p(x^n|y^n, s^n(m))} \right)^t, \end{aligned}$$

for all  $t > 0$ , where the inequality follows because  $\mathbf{1}_{\{a \geq b\}} \leq (\frac{a}{b})^t$  for all  $t > 0$ . Let  $\rho \in [0, 1]$ . By applying the inequality  $P(\cup_{t=1}^T \mathcal{A}_t) \leq [\sum_{t=1}^T P(\mathcal{A}_t)]^{\rho}$  [10, pp. 136] to (68), we have

$$\begin{aligned} P(\mathcal{E}_3|y^n, s^n(m), m, x^n) \\ \leq \left[ \sum_{\hat{m} \neq m, s^n(\hat{m}), \hat{x}^n \neq x^n} \frac{p(s^n(\hat{m}))}{|\Phi|} \times \dots \right. \\ \left. \times \left( \frac{p(y^n|s^n(\hat{m}))p(\hat{x}^n|y^n, s^n(\hat{m}))}{p(y^n|s^n(m))p(x^n|y^n, s^n(m))} \right)^t \right]^{\rho} \end{aligned} \quad (70)$$

for any  $\rho \in [0, 1]$  and  $t > 0$ . Now consider the error probability  $P(\mathcal{E}_3|M = m)$  given message  $m$  is chosen by Alice, i.e.,  $\{M = m\}$  occurs. To bound this error probability, we average

over all codewords  $s^n(m)$ , all observed sequences  $y^n$  and all possible sequences received by Alice  $x^n$ , i.e.,

$$\begin{aligned} P(\mathcal{E}_3|m) &= \sum_{y^n} \sum_{s^n(m)} p(y^n|s^n(m))p(s^n(m)) \times \dots \\ &\times \sum_{x^n} p(x^n|y^n, s^n(m))P(\mathcal{E}_3|y^n, s^n(m), m, x^n). \end{aligned} \quad (71)$$

We now substitute the upper bound in (70) into (71). Pulling out  $p(x^n|y^n, s^n(m))$  from the innermost term in (70) (since it does not depend on  $\hat{m}$ ,  $s^n(\hat{m})$  and  $\hat{x}^n$ ), we see that  $P(\mathcal{E}_3|m)$  can be upper bounded as

$$\begin{aligned} P(\mathcal{E}_3|m) &\leq |\Phi|^{-\rho} \sum_{y^n} \sum_{s^n(m)} p(y^n|s^n(m))p(s^n(m)) \times \dots \\ &\times \sum_{x^n} p(x^n|y^n, s^n(m))^{1-\rho t} \left[ \sum_{\hat{m} \neq m} \sum_{s^n(\hat{m})} p(s^n(\hat{m})) \times \dots \right. \\ &\times \left. \left( \frac{p(y^n|s^n(\hat{m}))}{p(y^n|s^n(m))} \right)^t \sum_{\hat{x}^n \neq x^n} p(\hat{x}^n|y^n, s^n(\hat{m}))^t \right]^\rho \\ &= |\Phi|^{-\rho} (|\mathcal{M}| - 1)^\rho \sum_{y^n} \Psi_1(y^n, \rho, t) \Psi_2(y^n, \rho, t), \end{aligned} \quad (72)$$

where the functions  $\Psi_1(y^n, \rho, t)$  and  $\Psi_2(y^n, \rho, t)$  are defined as follows:

$$\begin{aligned} \Psi_1(y^n, \rho, t) &\triangleq \sum_{s^n(m)} p(s^n(m))p(y^n|s^n(m))^{1-\rho t} \times \dots \\ &\times \sum_{x^n} p(x^n|y^n, s^n(m))^{1-\rho t} \\ \Psi_2(y^n, \rho, t) &\triangleq \left[ \sum_{s^n(\hat{m})} p(s^n(\hat{m}))p(y^n|s^n(\hat{m}))^t \times \dots \right. \\ &\times \left. \sum_{\hat{x}^n} p(\hat{x}^n|y^n, s^n(\hat{m}))^t \right]^\rho. \end{aligned}$$

Equation (72) follows because  $\hat{m}$  in the line above is a dummy variable that can take on exactly  $|\mathcal{M}| - 1$  values and for each  $\hat{m}$ , we generate codewords  $s^n(\hat{m})$  in the *same* way in the random coding construction. Now notice that if we set  $t = 1/(1 + \rho)$ , then

$$\Psi_2(y^n, \rho, 1/(1 + \rho)) = \Psi_1(y^n, \rho, 1/(1 + \rho))^\rho$$

because  $\hat{x}^n$  and  $\hat{m}$  in the definition of  $\Psi_2$  are dummy variables. As such,  $P(\mathcal{E}_3|m)$  can be bounded as

$$P(\mathcal{E}_3|m) \leq |\Phi|^{-\rho} |\mathcal{M}|^\rho \sum_{y^n} \Psi_3(y^n, \rho), \quad (73)$$

where the function  $\Psi_3(y^n, \rho)$  is defined as

$$\begin{aligned} \Psi_3(y^n, \rho) &\triangleq \left[ \sum_{s^n(m)} p(s^n(m))p(y^n|s^n(m))^{1/(1+\rho)} \times \dots \right. \\ &\times \left. \sum_{x^n} p(x^n|y^n, s^n(m))^{1/(1+\rho)} \right]^{1+\rho}. \end{aligned}$$

Now, we recall the DMS and DMBC assumptions, i.e., that

$$\begin{aligned} p(s^n(m)) &= \prod_{i=1}^n p(s_i(m)), \\ p(x^n, y^n|s^n(m)) &= \prod_{i=1}^n p(x_i, y_i|s_i(m)). \end{aligned}$$

As a result,  $\Psi_3(y^n, \rho)$  simplifies to

$$\begin{aligned} \Psi_3(y^n, \rho) &= \left[ \prod_{i=1}^n \sum_{s_i(m)} p(s_i(m))p(y_i|s_i(m))^{1/(1+\rho)} \times \dots \right. \\ &\times \left. \sum_{x_i} p(x_i|y_i, s_i(m))^{1/(1+\rho)} \right]^{1+\rho}, \end{aligned}$$

and the sum in (73) can be written as a product of single-letterized terms:

$$\sum_{y^n} \Psi_3(y^n, \rho) = \prod_{i=1}^n \sum_{y_i} \Psi_4(y_i, \rho), \quad (74)$$

where the function  $\Psi_4(y, \rho)$  is defined as

$$\Psi_4(y, \rho) \triangleq \left[ \sum_s p(s)p(y|s)^{1/(1+\rho)} \sum_x p(x|y, s)^{1/(1+\rho)} \right]^{1+\rho}.$$

Because each of the codewords is generated identically, each of the terms in the product in (74) is also identical. Hence,

$$\sum_{y^n} \Psi_3(y^n, \rho) = \left[ \sum_y \Psi_4(y, \rho) \right]^n.$$

Recall that  $|\Phi| \triangleq 2^{nR_\Phi}$  and  $|\mathcal{M}| \triangleq 2^{nR_M}$ . In addition, note that  $P(\mathcal{E}_3) = \sum_{m'} p(m')P(\mathcal{E}_3|m') = P(\mathcal{E}_3|m)$  for every  $m \in \mathcal{M}$ . As such, taking the normalized logarithm and limit inferior of (73) yields

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log P(\mathcal{E}_3) \geq \rho(R_\Phi - R_M) - \log \sum_y \Psi_4(y, \rho). \quad (75)$$

Essentially, what we have done is to develop a “hybrid” of Gallager-style error exponents for channel and lossless source coding with side information. Thus, an achievable error exponent when input distribution  $p(s)$  is used is  $E_o^{(3)}(p(s), R_\Phi, R_M)$  defined in (21). The reliability exponent part of the theorem is proved for the random binning secret key code by combining the bounds for the exponents for  $P(\mathcal{E}_1)$ ,  $P(\mathcal{E}_2)$  and  $P(\mathcal{E}_3)$  in (66), (67) and (75) respectively.  $\square$

### C. Proof for the Secrecy Exponent

We now prove that the secrecy exponent is at least  $F_o$  using the same coding scheme. We can use steps analogous to the proof of the direct part of Theorem 2 in [22] to obtain the following bound on the key leakage  $I(K_A; Z^n, \Phi)$ .

**Lemma 7.** Define  $c(\alpha) \triangleq \alpha^{-1} \log e$  for  $0 < \alpha \leq 1$ . The key leakage can be bounded as follows:

$$\begin{aligned} I(K_A; Z^n, \Phi) &= E_{\mathcal{C}}[I(K_A; Z^n, \Phi|\mathcal{C})] \\ &\leq c(\alpha) |\mathcal{K}|^\alpha |\Phi|^\alpha \sum_{z^n} p(z^n) \sum_{m, x^n} p(m, x^n|z^n)^{1+\alpha}, \end{aligned} \quad (76)$$



for all  $0 < \alpha \leq 1$ .

The proof is provided at the end for completeness. Now we consider the inner sum in (76). By introducing the input  $s^n$  and by repeated applications of Bayes rule,

$$\begin{aligned} & \sum_{m, x^n} p(m, x^n | z^n)^{1+\alpha} \\ &= \sum_{x^n} \sum_m \left[ \sum_{s^n} p(m, x^n, s^n | z^n) \right]^{1+\alpha} \\ &= \sum_{x^n} \sum_m \left[ \sum_{s^n} \frac{p(m, x^n, s^n, z^n)}{p(z^n)} \right]^{1+\alpha} \\ &= \frac{1}{p(z^n)^{1+\alpha}} \sum_{x^n} \sum_m \Theta_1(m, x^n, z^n)^{1+\alpha} \end{aligned} \quad (77)$$

$$= \frac{1}{p(z^n)^{1+\alpha} |\mathcal{M}|^{1+\alpha}} \sum_{x^n} \sum_m \Theta_2(m, x^n, z^n)^{1+\alpha} \quad (78)$$

where the functions  $\Theta_1(m, x^n, z^n)$  and  $\Theta_2(m, x^n, z^n)$  are defined as

$$\begin{aligned} \Theta_1(m, x^n, z^n) &\triangleq \sum_{s^n} p(m) p(s^n | m) p(z^n | s^n) p(x^n | s^n, z^n) \\ \Theta_2(m, x^n, z^n) &\triangleq \sum_{s^n} p(s^n | m) p(z^n | s^n) p(x^n | s^n, z^n). \end{aligned}$$

Equation (77) follows because  $M - S^n - (X^n, Z^n)$  form a Markov chain so  $p(z^n | s^n, m) = p(z^n | s^n)$  and  $p(x^n | s^n, z^n, m) = p(x^n | s^n, z^n)$ . Equation (78) follows from the uniformity of the messages  $m$  in the message set  $\mathcal{M}$ , i.e., that  $p(m) = \frac{1}{|\mathcal{M}|}$  for all  $m \in \mathcal{M}$ . We now upper bound  $\Theta_2(m, x^n, z^n)^{1+\alpha}$ . This is done using the following lemma.

**Lemma 8.** *Let  $\{(\lambda_j, a_j)\}$  be a finite collection of non-negative numbers such that  $\sum_j \lambda_j = 1$ . Also, let  $r \geq 1$ . Then, the following inequality holds*

$$\left( \sum_j \lambda_j a_j \right)^r \leq \sum_j \lambda_j a_j^r.$$

This can be proven by noticing that  $t \mapsto t^r$  is convex. We omit the details. We now make the following identifications:  $a_{s^n} \equiv p(z^n | s^n) p(x^n | s^n, z^n)$ ,  $\lambda_{s^n} \equiv p(s^n | m)$  and  $r \equiv 1 + \alpha$  and apply Lemma 8 to  $\Theta_2(m, x^n, z^n)^{1+\alpha}$ . This yields the inequality

$$\Theta_2(m, x^n, z^n)^{1+\alpha} \leq \sum_{s^n} p(s^n | m) [p(z^n | s^n) p(x^n | s^n, z^n)]^{1+\alpha}. \quad (79)$$

On account of (76), (78) and (79), we have

$$\begin{aligned} \mathbb{E}_{\mathcal{C}}[I(K_A; Z^n, \Phi | \mathcal{C})] &\leq c(\alpha) |\mathcal{K}|^\alpha |\Phi|^\alpha |\mathcal{M}|^{-(1+\alpha)} \times \dots \\ &\sum_{z^n} p(z^n)^{-\alpha} \sum_{s^n, x^n, m} p(s^n | m) [p(z^n | s^n) p(x^n | s^n, z^n)]^{1+\alpha} \\ &= c(\alpha) |\mathcal{K}|^\alpha |\Phi|^\alpha |\mathcal{M}|^{-(1+\alpha)} \times \dots \\ &\sum_{s^n, x^n, z^n} \sum_m p(s^n, x^n, z^n | m) \left[ \frac{p(z^n | s^n)}{p(z^n)} p(x^n | s^n, z^n) \right]^\alpha, \end{aligned}$$

where the final equality follows because  $p(s^n, x^n, z^n | m) = p(s^n | m) p(z^n | s^n) p(x^n | s^n, z^n)$  by the Markov chain  $M - S^n -$

$(X^n, Z^n)$ . Now, pulling the  $p(m) = \frac{1}{|\mathcal{M}|}$  term into the sum, we get

$$\begin{aligned} \mathbb{E}_{\mathcal{C}}[I(K_A; Z^n, \Phi | \mathcal{C})] &\leq c(\alpha) |\mathcal{K}|^\alpha |\Phi|^\alpha |\mathcal{M}|^{-\alpha} \times \dots \\ &\sum_{s^n, x^n, z^n} \sum_m p(s^n, x^n, z^n | m) p(m) \left[ \frac{p(z^n | s^n)}{p(z^n)} p(x^n | s^n, z^n) \right]^\alpha \\ &= c(\alpha) |\mathcal{K}|^\alpha |\Phi|^\alpha |\mathcal{M}|^{-\alpha} \sum_{s^n, x^n, z^n} \Upsilon(s^n, x^n, z^n, \alpha), \end{aligned}$$

where the function  $\Upsilon(s^n, x^n, z^n, \alpha)$  is defined as

$$\Upsilon(s^n, x^n, z^n, \alpha) \triangleq p(s^n, x^n, z^n) \left[ \frac{p(z^n | s^n)}{p(z^n)} p(x^n | s^n, z^n) \right]^\alpha.$$

Now, recall that (i) the input  $S^n$  is a DMS when averaged over all codebooks and all messages  $m \in \mathcal{M}$  (because the generation of the codewords  $s^n(m), m \in \mathcal{M}$  is done identically) and (ii)  $p(x, y, z | s)$  is a DMBC. Then, we have the upper bound

$$\begin{aligned} \mathbb{E}_{\mathcal{C}}[I(K_A; Z^n, \Phi | \mathcal{C})] &\leq c(\alpha) |\mathcal{K}|^\alpha |\Phi|^\alpha |\mathcal{M}|^{-\alpha} \prod_{i=1}^n \sum_{s_i, x_i, z_i} \Upsilon(s_i, x_i, z_i, \alpha) \\ &= c(\alpha) |\mathcal{K}|^\alpha |\Phi|^\alpha |\mathcal{M}|^{-\alpha} \left[ \sum_{s, x, z} \Upsilon(s, x, z, \alpha) \right]^n. \end{aligned} \quad (80)$$

Note that the bound (80) holds for all  $0 < \alpha \leq 1$ . Recall also that  $\mathcal{K} = [1 : 2^{nR_{SK}}]$ ,  $\Phi = [1 : 2^{nR_\Phi}]$  and  $\mathcal{M} = [1 : 2^{nR_M}]$  so  $|\mathcal{K}|^\alpha |\Phi|^\alpha |\mathcal{M}|^{-\alpha} \doteq 2^{n\alpha(R_{SK} + R_\Phi - R_M)}$ . Now take the normalized logarithm and limit inferior of (80) to get

$$\begin{aligned} \liminf_{n \rightarrow \infty} -\frac{1}{n} \log \mathbb{E}_{\mathcal{C}}[I(K_A; Z^n, \Phi | \mathcal{C})] &\geq \\ &-\alpha(R_{SK} + R_\Phi - R_M) - \log \sum_{s, x, z} \Upsilon(s, x, z, \alpha). \end{aligned}$$

The joint distribution of  $(X, Z, S)$ , namely  $p(x, z, s) = p(x, z | s) p(s)$ , is induced by a particular input distribution  $p(s)$ . Essentially what we have done in this part of the proof is to develop a “hybrid” of the information leakage exponent for the wiretap channel model [12, Eq. (14)] and the excited source model [22, Theorem 3]. Hence, an achievable exponent for the key leakage given input distribution  $p(s)$  is  $F_o(p(s), R_{SK}, R_\Phi, R_M)$  defined in (23). The secrecy exponent part of the theorem is proved for the random binning secret key code.

*From Random Codes to a Deterministic Code:* Combining the proof in Section VII-B and proof in this section, we have shown that for the  $(2^{nR_{SK}}, 2^{nR_M}, 2^{nR_\Phi}, n)$  random binning secret key code, the expected probability of error decays with exponent (at least)  $E_o$  (expectation over codebooks and random binning functions) and the expected key leakage decays exponentially with exponent (at least)  $F_o$ . Since both are measured with respect the same (known) channel, there exists a binning secret key code that meets the ensemble behavior. More precisely, observe that  $P(\mathcal{E}) = \mathbb{E}_{\mathcal{C}}[P(\mathcal{E} | \mathcal{C})] = \sum_{\mathcal{C}} p(\mathcal{C}) P(\mathcal{E} | \mathcal{C})$ , where  $\mathcal{C}$  runs through all binning secret

key codes (a random code and two random binning functions) and the event  $\mathcal{E}$  is defined in (62). By Markov's inequality,

$$P_{\mathcal{C}}[P(\mathcal{E}|\mathcal{C}) \geq 3P(\mathcal{E})] \leq \frac{1}{3}. \quad (81)$$

Similarly, when averaged over all codes, the average key leakage is  $E_{\mathcal{C}}[I(K_A; Z^n, \Phi|\mathcal{C})] = \sum_{\mathcal{C}} p(\mathcal{C}) I(K_A; Z^n, \Phi|\mathcal{C} = \mathcal{C})$ , so by Markov's inequality,

$$P_{\mathcal{C}}[I(K_A; Z^n, \Phi|\mathcal{C}) \geq 3E_{\mathcal{C}}[I(K_A; Z^n, \Phi|\mathcal{C})]] \leq \frac{1}{3}. \quad (82)$$

From (81), by considering the complement of the event of interest, we can conclude that there exists a subset of binning secret key codes  $\mathcal{D}_1$  with total probability mass that exceeds  $2/3$  (i.e.,  $\sum_{\mathcal{C} \in \mathcal{D}_1} p(\mathcal{C}) \geq 2/3$ ) such that  $P(\mathcal{E}|\mathcal{C} = \mathcal{C}) < 3P(\mathcal{E})$  for every  $\mathcal{C} \in \mathcal{D}_1$ . Similarly, from (82) there exists a subset of binning secret key codes  $\mathcal{D}_2$  with total probability mass that exceeds  $2/3$  (i.e.,  $\sum_{\mathcal{C} \in \mathcal{D}_2} p(\mathcal{C}) \geq 2/3$ ) such that  $I(K_A; Z^n, \Phi|\mathcal{C} = \mathcal{C}) < 3E_{\mathcal{C}}[I(K_A; Z^n, \Phi|\mathcal{C})]$  for every  $\mathcal{C} \in \mathcal{D}_2$ . Note that  $P(\mathcal{D}_1 \cap \mathcal{D}_2) \geq 1/3$  so  $\mathcal{D}_1 \cap \mathcal{D}_2 \neq \emptyset$ . Thus, there exists at least one binning secret key code  $\mathcal{C}^*$  in the ensemble of (good) codes  $\mathcal{D}_1 \cap \mathcal{D}_2$  such that  $P(\mathcal{E}_{\text{key}}|\mathcal{C} = \mathcal{C}^*) \leq P(\mathcal{E}|\mathcal{C} = \mathcal{C}^*) \leq 2^{-nE_o}$  and  $I(K_A; Z^n, \Phi|\mathcal{C} = \mathcal{C}^*) \leq 2^{-nF_o}$ , where the event  $\mathcal{E}_{\text{key}}$  is defined in (59).  $\square$

*Proof of Lemma 7:* Recall the assumption that the key and public message binning processes are random, uniform and independent of the random codewords (See Section VII-A for definitions and the code construction). The key leakage can be expressed as follows:

$$\begin{aligned} E_{\mathcal{C}}[I(K_A; Z^n, \Phi|\mathcal{C})] &= E_{\mathcal{C}}[H(K_A|\mathcal{C}) - H(K_A|Z^n, \Phi|\mathcal{C})] \\ &= E_{\mathcal{C}}[H(K_A|\mathcal{C}) + H(\Phi|Z^n, \mathcal{C}) - H(K_A, \Phi|Z^n, \mathcal{C})] \\ &\leq \log |\mathcal{K}| + \log |\Phi| - E_{\mathcal{C}}[H(K_A, \Phi|Z^n, \mathcal{C})]. \end{aligned} \quad (83)$$

The conditioning is on the specific codebook used, i.e.,  $\mathcal{C} = \mathcal{C}$ . It remains to lower bound the conditional entropy in (83). For this purpose, let

$$H_{1+\alpha}(X) \triangleq -\frac{1}{\alpha} \log \sum_{x \in \mathcal{X}} p(x)^{1+\alpha} \quad (84)$$

be the Rényi entropy of order  $1 + \alpha$  for  $0 < \alpha \leq 1$ . Note that  $\lim_{\alpha \searrow 0} H_{1+\alpha}(X) = H(X)$ . Also, by the concavity of  $t \mapsto \log t$ , it can be verified that  $H(X) \geq H_{1+\alpha}(X)$  for all  $0 < \alpha \leq 1$ . Consider the conditional entropy in (83),

$$\begin{aligned} &E_{\mathcal{C}}[H(K_A, \Phi|Z^n, \mathcal{C})] \\ &= E_{\mathcal{C}} \left[ \sum_{z^n} p(z^n) H(K_A, \Phi|Z^n = z^n, \mathcal{C}) \right] \\ &\geq \sum_{z^n} p(z^n) E_{\mathcal{C}}[H_{1+\alpha}(K_A, \Phi|Z^n = z^n, \mathcal{C})] \\ &\geq \sum_{z^n} p(z^n) \left( -\frac{1}{\alpha} \log E_{\mathcal{C}} \left[ \sum_{(k_A, \phi) \in \mathcal{K} \times \Phi} p(k_A, \phi|z^n, \mathcal{C})^{1+\alpha} \right] \right). \end{aligned} \quad (85)$$

The last inequality is due to the definition of Rényi entropy in (84) and the application of Jensen's inequality noting that the function  $x \mapsto -\log x$  is convex.

Now let  $(\tilde{M}, \tilde{X}^n)$  be a pair of random variables identically distributed to, but conditionally independent of  $(M, X^n)$  given the events  $\{Z^n = z^n\}$  and  $\{\mathcal{C} = \mathcal{C}\}$ . Recall that  $k(\cdot, \cdot)$  and  $\phi(\cdot, \cdot)$  are the key and public message random binning functions respectively. See (57) and (58) for definitions. Define  $(\tilde{K}_A, \tilde{\Phi}) \triangleq (k(\tilde{M}, \tilde{X}^n), \phi(\tilde{M}, \tilde{X}^n))$ . Then,

$$\begin{aligned} &p(k_A, \phi|z^n, \mathcal{C})^{1+\alpha} \\ &= p(k_A, \phi|z^n, \mathcal{C}) P \left[ (\tilde{K}_A, \tilde{\Phi}) = (k_A, \phi) | Z^n = z^n, \mathcal{C} = \mathcal{C} \right]^{\alpha}, \end{aligned} \quad (87)$$

by interpreting the Rényi entropy in (84) in terms of an independent [from  $(K_A, \Phi)$ ] and identically distributed random variable  $(\tilde{K}_A, \tilde{\Phi})$ .

Define a shorthand notation for the indicator function as

$$1[k_A, \phi|m, x^n, \mathcal{C}] \triangleq 1[k_{\mathcal{C}}(m, x^n) = k_A, \phi_{\mathcal{C}}(m, x^n) = \phi]. \quad (88)$$

where  $k_{\mathcal{C}}(\cdot)$  and  $\phi_{\mathcal{C}}(\cdot)$  are the binning functions associated to a specific codebook  $\mathcal{C} = \mathcal{C}$ . We upper bound the expectation in the logarithm in (86) on the top of the next page.

The step (89) is a result of plugging (88) into the argument of the logarithm in (86). The step (90) follows by writing out the probability of a collision event in (87) explicitly as a sum. The step in (91) applies the law of total probability. We sum over all possible  $(m, x^n)$  that are assigned bin indices  $(k_A, \phi)$  for a given pair of binning function indexed by  $\mathcal{C}$ . Equation (92) follows by simple reordering of the sums.

The step (93) is an application of Jensen's Inequality to the term in brackets  $[\cdot]^{\alpha}$  since the sum over  $(k_A, \phi)$  is a sum over the probability mass function  $1[k_A, \phi|m, x^n, \mathcal{C}]$  (cf. (88) for the definition of this indicator function). Also, the function  $x \mapsto x^{\alpha}$  is concave for  $\alpha \in [0, 1]$ . We recall that  $m, x^n$ , and  $\mathcal{C}$  are all fixed for this inner sum, the last being fixed by the outer expectation over  $\mathcal{C}$ . Equation (94) follows from the same reasoning as (91), i.e., the law of total probability. Equation (95) follows by simple reordering of the sums.

In (96), we used the "sifting" property of the indicator function  $1[k_A = k'_A, \phi = \phi']$ . In (97) we split the sum over  $(m', x'^n)$  into two terms and distributed the sums over  $(k'_A, \phi')$ . Note that for the  $(m', x'^n) = (m, x^n)$  term,  $\sum_{k_A, \phi} 1[k_A, \phi|m, x^n, \mathcal{C}] = 1$ . We next applied the inequality  $(x + y)^{\alpha} \leq x^{\alpha} + y^{\alpha}$ , for  $0 \leq \alpha \leq 1$  to get (98).

In (99) we note that the first term is not a function of  $\mathcal{C}$ . Using the concavity of  $x \mapsto x^{\alpha}$  (for  $\alpha \in [0, 1]$ ), we move both the sum over  $(m, x^n)$  and the expectation over codebooks inside the function, a step justified by Jensen's Inequality.

In (100) we apply the uniformly random design of the binning functions. Since  $(m, x^n) \neq (m', x'^n)$  for every term in the sum, each of the indicator functions equals the (fixed) pair  $(k_A, \phi)$  with equal probability and independently. Thus, the probability that both equal  $(k_A, \phi)$  is the square (by the independence) of the reciprocal of the number of possibilities (by the uniformity), i.e.,  $E_{\mathcal{C}}[1[k_A, \phi|m, x^n, \mathcal{C}] 1[k_A, \phi|m', x'^n, \mathcal{C}]] = (|\mathcal{K}||\Phi|)^{-2}$ . In (101), we pulled out  $(|\mathcal{K}||\Phi|)^{-\alpha}$ . Finally, we note that  $p(m, x^n|z^n)p(m', x'^n|z^n)$  is a well defined (conditional) pmf

$$\mathbb{E}_{\mathcal{C}} \left\{ \sum_{k_A, \phi} p(k_A, \phi | z^n, \mathcal{C}) \mathbb{P} \left[ (\tilde{K}_A, \tilde{\Phi}) = (k_A, \phi) | Z^n = z^n, \mathcal{C} \right]^\alpha \right\} \quad (89)$$

$$= \mathbb{E}_{\mathcal{C}} \left\{ \sum_{k_A, \phi} \left[ p(k_A, \phi | z^n, \mathcal{C}) \left( \sum_{k'_A, \phi'} p(k'_A, \phi' | z^n, \mathcal{C}) \mathbf{1}[k_A = k'_A, \phi = \phi'] \right)^\alpha \right] \right\} \quad (90)$$

$$= \mathbb{E}_{\mathcal{C}} \left\{ \sum_{k_A, \phi} \left[ \left( \sum_{m, x^n} p(m, x^n | z^n) \mathbf{1}[k_A, \phi | m, x^n, \mathcal{C}] \right) \left( \sum_{k'_A, \phi'} p(k'_A, \phi' | z^n, \mathcal{C}) \mathbf{1}[k_A = k'_A, \phi = \phi'] \right)^\alpha \right] \right\} \quad (91)$$

$$= \mathbb{E}_{\mathcal{C}} \left\{ \sum_{m, x^n} p(m, x^n | z^n) \left[ \sum_{k_A, \phi} \mathbf{1}[k_A, \phi | m, x^n, \mathcal{C}] \left( \sum_{k'_A, \phi'} p(k'_A, \phi' | z^n, \mathcal{C}) \mathbf{1}[k_A = k'_A, \phi = \phi'] \right)^\alpha \right] \right\} \quad (92)$$

$$\leq \mathbb{E}_{\mathcal{C}} \left\{ \sum_{m, x^n} p(m, x^n | z^n) \left[ \sum_{k_A, \phi} \mathbf{1}[k_A, \phi | m, x^n, \mathcal{C}] \left( \sum_{k'_A, \phi'} p(k'_A, \phi' | z^n, \mathcal{C}) \mathbf{1}[k_A = k'_A, \phi = \phi'] \right)^\alpha \right] \right\} \quad (93)$$

$$= \mathbb{E}_{\mathcal{C}} \left\{ \sum_{m, x^n} p(m, x^n | z^n) \left[ \sum_{k_A, \phi} \mathbf{1}[k_A, \phi | m, x^n, \mathcal{C}] \times \left( \sum_{k'_A, \phi'} \left( \sum_{m', x'^n} p(m', x'^n | z^n) \mathbf{1}[k'_A, \phi' | m', x'^n, \mathcal{C}] \right) \mathbf{1}[k_A = k'_A, \phi = \phi'] \right)^\alpha \right] \right\} \quad (94)$$

$$= \mathbb{E}_{\mathcal{C}} \left\{ \sum_{m, x^n} p(m, x^n | z^n) \left[ \sum_{m', x'^n} p(m', x'^n | z^n) \times \left( \sum_{k_A, \phi} \sum_{k'_A, \phi'} \mathbf{1}[k_A, \phi | m, x^n, \mathcal{C}] \mathbf{1}[k'_A, \phi' | m', x'^n, \mathcal{C}] \mathbf{1}[k_A = k'_A, \phi = \phi'] \right)^\alpha \right] \right\} \quad (95)$$

$$= \mathbb{E}_{\mathcal{C}} \left\{ \sum_{m, x^n} p(m, x^n | z^n) \left[ \sum_{m', x'^n} p(m', x'^n | z^n) \left( \sum_{k_A, \phi} \mathbf{1}[k_A, \phi | m, x^n, \mathcal{C}] \mathbf{1}[k_A, \phi | m', x'^n, \mathcal{C}] \right)^\alpha \right] \right\} \quad (96)$$

$$= \mathbb{E}_{\mathcal{C}} \left\{ \sum_{m, x^n} p(m, x^n | z^n) \left[ p(m, x^n | z^n) + \sum_{(m', x'^n) \neq (m, x^n)} p(m', x'^n | z^n) \left( \sum_{k_A, \phi} \mathbf{1}[k_A, \phi | m, x^n, \mathcal{C}] \mathbf{1}[k_A, \phi | m', x'^n, \mathcal{C}] \right)^\alpha \right] \right\} \quad (97)$$

$$\leq \mathbb{E}_{\mathcal{C}} \left\{ \sum_{m, x^n} p(m, x^n | z^n) \left\{ p(m, x^n | z^n)^\alpha + \left[ \sum_{(m', x'^n) \neq (m, x^n)} p(m', x'^n | z^n) \left( \sum_{k_A, \phi} \mathbf{1}[k_A, \phi | m, x^n, \mathcal{C}] \mathbf{1}[k_A, \phi | m', x'^n, \mathcal{C}] \right)^\alpha \right] \right\} \right\} \quad (98)$$

$$\leq \sum_{m, x^n} p(m, x^n | z^n)^{1+\alpha} + \left[ \mathbb{E}_{\mathcal{C}} \left\{ \sum_{m, x^n} p(m, x^n | z^n) \sum_{(m', x'^n) \neq (m, x^n)} p(m', x'^n | z^n) \left( \sum_{k_A, \phi} \mathbf{1}[k_A, \phi | m, x^n, \mathcal{C}] \mathbf{1}[k_A, \phi | m', x'^n, \mathcal{C}] \right)^\alpha \right\} \right]^\alpha \quad (99)$$

$$= \sum_{m, x^n} p(m, x^n | z^n)^{1+\alpha} + \left[ \sum_{m, x^n} p(m, x^n | z^n) \sum_{(m', x'^n) \neq (m, x^n)} p(m, x^n | z^n) \left( \sum_{k_A, \phi} \frac{1}{(|\mathcal{K}| |\Phi|)^2} \right)^\alpha \right]^\alpha \quad (100)$$

$$= \sum_{m, x^n} p(m, x^n | z^n)^{1+\alpha} + \frac{1}{|\mathcal{K}|^\alpha |\Phi|^\alpha} \left[ \sum_{m, x^n} \sum_{(m', x'^n) \neq (m, x^n)} p(m, x^n | z^n) p(m', x'^n | z^n) \right]^\alpha \quad (101)$$

$$\leq \sum_{m, x^n} p(m, x^n | z^n)^{1+\alpha} + \frac{1}{|\mathcal{K}|^\alpha |\Phi|^\alpha}. \quad (102)$$



and that we are missing one term in the double sum. Hence, we get (102) by upper bounding the double sum by one.

Substituting (102) back into (86) gives

$$\begin{aligned} & \mathbb{E}_{\mathcal{C}}[H(K_A, \Phi | Z^n, \mathcal{C})] \\ & \geq \sum_{z^n} p(z^n) \left[ -\frac{1}{\alpha} \log \left( \frac{1}{|\mathcal{K}|^\alpha |\Phi|^\alpha} + \sum_{m, x^n} p(m, x^n | z^n)^{1+\alpha} \right) \right] \\ & = \log(|\mathcal{K}| |\Phi|) - \frac{1}{\alpha} \sum_{z^n} p(z^n) \times \dots \\ & \quad \times \log \left( 1 + |\mathcal{K}|^\alpha |\Phi|^\alpha \sum_{m, x^n} p(m, x^n | z^n)^{1+\alpha} \right) \quad (103) \end{aligned}$$

$$\begin{aligned} & \geq \log(|\mathcal{K}| |\Phi|) - \left( \frac{\log e}{\alpha} \right) |\mathcal{K}|^\alpha |\Phi|^\alpha \times \dots \\ & \quad \times \sum_{z^n} p(z^n) \sum_{m, x^n} p(m, x^n | z^n)^{1+\alpha}, \quad (104) \end{aligned}$$

where in (103) we pulled out the  $|\mathcal{K}|^{-\alpha} |\Phi|^{-\alpha}$  term from the logarithm above and in (104) we applied the relation  $\log(1+t) \leq t \log e$  (recall that  $\log = \log_2$ ). The proof of the lemma is completed by uniting (83) and (104).

#### Acknowledgments

The authors would like to acknowledge one of the reviewers whose insights led to the discussion on the connection of our work to that in Csiszár and Narayan [15] and Gohari and Anantharam [34] in Section IV-B.

#### REFERENCES

- [1] T.-H. Chou, V. Y. F. Tan, and S. C. Draper, "On the capacity of the sender-excited secret key agreement model," in *Proc. Allerton Conference on Communication, Control, and Computing*, 2011.
- [2] Y. Liang, H. V. Poor, and S. Shamai, *Information Theoretic Security*. Now Publishers Inc, 2009.
- [3] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography part I: Secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.
- [4] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 733–742, 1993.
- [5] T. Weissman, "Capacity of channels with action-dependent states," *IEEE Trans. Inform. Theory*, vol. 56, pp. 5396–5411, Nov 2010.
- [6] H. Asnani, H. Permuter, and T. Weissman, "Probing Capacity," *IEEE Trans. Inform. Theory*, vol. 57, pp. 7317–7332, Nov 2011.
- [7] K. Kittichokechai, T. J. Oechtering, M. Skoglund, and R. Thobaben, "Source and channel coding with action-dependent partially known two-sided state information," in *Proc. Int. Symp. Inform. Theory*, pp. 629–633, June 2010.
- [8] H. Permuter and T. Weissman, "Source coding with a side information 'vending machine'," *IEEE Trans. Inform. Theory*, vol. 57, pp. 4530–4544, Jul 2011.
- [9] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inform. Theory*, vol. 46, no. 2, pp. 344–366, 2000.
- [10] R. G. Gallager, *Information theory and reliable communication*. New York: Wiley, 1968.
- [11] R. G. Gallager, "Source coding with side information and universal coding," *M.I.T. LIDS-P-937*, 1976.
- [12] M. Hayashi, "Exponential decreasing rate of leaked information in universal random privacy amplification," *IEEE Trans. Inform. Theory*, vol. 57, pp. 3989–4001, June 2011.
- [13] A. Khisti, S. Diggavi, and G. Wornell, "Secret-key generation with correlated sources and noisy channels," in *Proc. Int. Symp. Inform. Theory*, pp. 1005–1009, July 2008.
- [14] V. Prabhakaran, K. Eswaran, and K. Ramchandran, "Secrecy via sources and channels – a secret key-secret message rate tradeoff region," in *Proc. Int. Symp. Inform. Theory*, pp. 1010–1014, July 2008.
- [15] I. Csiszár and P. Narayan, "The secret key capacity of multiple terminals," *IEEE Trans. Inform. Theory*, vol. 50, pp. 3047–3061, Dec 2004.
- [16] I. Csiszár and P. Narayan, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2437–2452, Jun 2008.
- [17] Y. Chen and A. J. Han Vinck, "Wiretap channel with side information," *IEEE Trans. Inform. Theory*, vol. 54, pp. 395–402, Jan. 2008.
- [18] W. Liu and B. Chen, "Wiretap channel with two-sided channel state information," in *Proc. Asilomar Conf. Signals, Systems and Computers*, 2007, pp. 893–897, Nov. 2007.
- [19] Y. K. Chia and A. El Gamal, "Wiretap channel with causal state information," *IEEE Trans. Inform. Theory*, vol. 58, pp. 2838–2849, May 2012.
- [20] A. Khisti, S. Diggavi, and G. Wornell, "Secret key agreement using asymmetry in channel state knowledge," in *Proc. Int. Symp. Inform. Theory*, pp. 2286–2290, 2009.
- [21] A. Khisti, S. Diggavi, and G. Wornell, "Secret-key agreement with channel state information at the transmitter," *IEEE Trans. on Foren. and Sec.*, vol. 6, pp. 672–681, Sep 2011.
- [22] T. Chou, S. C. Draper, and A. Sayeed, "Key generation using external source excitation: Capacity, reliability, and secrecy exponent," *IEEE Trans. Inform. Theory*, vol. 58, pp. 2455–2474, Apr. 2012.
- [23] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inform. Foren. and Sec.*, vol. 2, pp. 364–375, Sep. 2007.
- [24] A. Agrawal, Z. Rezk, A. Khisti, and M. Alouini, "Noncoherent capacity of secret-key agreement with public discussion," *IEEE Trans. Inform. Foren. and Sec.*, vol. 6, pp. 565–574, Sept. 2011.
- [25] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel," *IEEE Trans. Inform. Theory*, vol. 52, pp. 1562–1575, April 2006.
- [26] T. S. Han, *Information-Spectrum Methods in Information Theory*. Springer, 2002.
- [27] M. Bloch and J. N. Laneman, "Secrecy from Resolvability," *arXiv:1105.5419*, May 2011.
- [28] C. Bennett, G. Brassard, C. Crepeau, and U. Maurer, "Generalized privacy amplification," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1915–1923, Nov 1995.
- [29] S. Watanabe, R. Matsumoto, and T. Uyematsu, "Strongly Secure Privacy Amplification Cannot Be Obtained by Encoder of Slepian-Wolf Code," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E93.A, no. 9, pp. 1650–1659, 2010.
- [30] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2012.
- [31] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Lecture Notes in Computer Science*, pp. 351–368, Springer-Verlag, 2000.
- [32] U. M. Maurer, "The strong secret key rate of discrete random triples," *Communications and Cryptography: Two Sides of One Tapestry*, pp. 271–285, Nov 1994.
- [33] A. D. Wyner, "The wire-tap channel," *The Bell Systems Technical Journal*, vol. 54, pp. 1355–1387, 1975.
- [34] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals – I: Source model," *IEEE Trans. Inform. Theory*, vol. 56, pp. 3973–3996, Aug 2008.
- [35] A. A. Gohari and V. Anantharam, "Information-Theoretic Key Agreement of Multiple Terminals–Part II: Channel Model," *IEEE Trans. Inform. Theory*, vol. 56, pp. 3997–4010, Aug. 2010.
- [36] D. Slepian and J. Wolf, "Noiseless coding of correlated sources," *IEEE Trans. Inform. Theory*, vol. 19, pp. 471–480, Jul 1973.
- [37] V. Y. F. Tan and O. Kosut, "On the dispersions of three network information theory problems," *arXiv:1201.3901*, Feb 2012. [Online].