Key Generation Using an External Source of Excitation: Capacity, Reliability, and Secrecy Exponent

Tzu-Han Chou, Student Member, IEEE, Stark C. Draper, Member, IEEE, and Akbar M. Sayeed, Senior Member, IEEE.

Abstract—We study the fundamental limits to secret key generation from an excited distributed source (EDS). In an EDS a pair of terminals observe dependent sources of randomness excited by a pre-arranged signal. We first determine the secret key capacity for such systems with one-way public messaging. We then characterize a tradeoff between the secret key rate and exponential bounds on the probability of key agreement failure and on the secrecy of the key generated. We find that there is a fundamental tradeoff between reliability and secrecy.

We then explore this framework within the context of reciprocal wireless channels. In this setting, the users transmit pre-arranged sounding signals to each other. When the fading is Rayleigh, the observations of the users are jointly Gaussian sources. We show that an on-off sounding signal with an SNR-dependent duty cycle achieves the secret key capacity of this system. Furthermore, we characterize a fundamental metric – minimum energy per key bit for reliable key generation – and show that in contrast to conventional AWGN channels, there is a non-zero threshold SNR that achieves the minimum energy per key bit. The capacity achieving on-off sounding signal achieves the minimum energy per key bit at any SNR below the threshold. Finally, we build off our error exponent results to investigate the energy required to generate a key using a finite block length. Again we find that on-off sounding signals yield an improvement when compared to constant sounding signals. In addition to Rayleigh fading, we analyze the performance of a system based on binary channel phase quantization.

Index Terms—Secret key generation, public discussion, secret key capacity, error exponent, secrecy exponent, privacy amplification, reciprocal wireless channel, multipath randomness, channel sounding.

I. INTRODUCTION

In [3] Shannon laid the theoretical foundations of cryptography. He defined the notion of perfect secrecy achieved by a system wherein the posterior probability of the plain-text message conditioned on an eavesdropper’s knowledge is equal to the priori distribution. In other words, the eavesdropper can deduce no information about the plain-text based on his (or her) observations. Shannon also showed that, in order to achieve perfect secrecy, a secret key at least as large as the message must be shared by encrypter and decrypter. Due to the difficulty of distributing secret keys securely, much of cryptography has followed a distinct philosophy where the security is based on the computational hardness of certain mathematical problems. This is termed computational security.

Starting in the 1970s, information theorists followed up on Shannon’s work by exploring security systems that exploited auxiliary sources of randomness to facilitate key generation. Since our work is motivated by considering auxiliary sources based on channel randomness, we refer to this body of work as physical-layer secrecy. The earliest results along these lines came from Wyner who in [4] introduces the wire-tap channel. Wyner’s work is generalized by Csiszár and Körner in [5]. These results show that, given statistical knowledge of communication channels that link a transmitter to an intended receiver and to an eavesdropper, one may design a code such that messages can be successfully and confidentially sent without the transmitter and intended receiver having access to a shared key.

Later, first by Maurer in [6] and then by Ahlswede and Csiszár in [7], a different use of auxiliary randomness was posed. In these papers a secret key is generated from dependent auxiliary sources of randomness available to two users. The resulting key can then be used, as in Shannon’s original architecture, as a one-time pad. In this setting two legitimate users, Alice and Bob, observe dependent discrete memoryless sources (DMS) $X^n_a$ and $X^n_b$. An eavesdropper Eve observes a third statistically related source $X^n$. Based on $n$ observations of the sources and a public conversation between Alice and Bob, Alice and Bob want to generated a shared secret key. The public messages $\Phi$ that make up Alice and Bob’s conversation must not leak information of the resulting key to Eve. The largest achievable secret key rate (bits per source symbol) is termed the secret key capacity. One possible implementation is for Alice to send a single message to Bob (and to have Bob send no messages). The public message indexes a subset of all possible source sequences Alice might have observed, and in which her observed sequence lies. Using his observation and public message, Bob can determine with high probability which sequence Alice observed, while Eve is left with some ambiguity. The shared key can then be generated from the determined sequence. Cast in this setting, the key generation problem can be viewed as a variant of distributed source coding with side information [8]. Reliable recovery of $X^n_a$ by Bob requires the rate of the public message to be greater than $H(X_a|X_b)$.
In wireless communications, the channel itself can be used as the source of auxiliary randomness. In this case the randomness is due to multipath fading [9]. When transmissions are bi-directional and in the same frequency band (e.g., time-division duplexed systems), the reciprocity property [10] of electromagnetic wave propagation ensures that the channel in each direction is identical. If two channel soundings, one for each direction, are done within the coherence time, the two users’ observations are highly correlated. In this setting, $X_a, X_b, X_e$ can be generated by having each user transmit pre-arranged sounding signals. This motivates the general study of key generation from excited sources of randomness where the designer chooses the source of excitation. Returning to the wireless setting, the keys $K_a$ and $K_b$, are functions of the estimates of the common random channel observed by each user. For wideband and multi-antenna channels, the resulting keys can be quite large due to the large number of independent channel degrees of freedom. Secrecy from eavesdroppers is ensured by the physics of propagation. Consider, for instance, a rich multipath environment. If the eavesdropper is physically displaced from the legitimate users, by even a few wavelengths, its channel output $X_e$ will nearly be statistically independent of $X_a$ and $X_b$. For these reasons, reciprocal wireless channels provide an attractive source of randomness for key generation.

Motivated by the above discussion of wireless channels, in this paper we study secret key generation from excited distributed source (EDS) in which the shared randomness between two parties is excited by a design signal. We term such a source as an excited distributed memoryless source (EDMS) if the source is memoryless. We show that the secret key capacity of a general EDMS is an extension of secret key capacity of DMS in the following sense: for a fixed sounding sequence $s^n$ with type $P_{s^n}$, we achieve secret key rate $\sum_i P_{s^n}(s)C(s)$ by time sharing among the DMSs. Since $s^n$ is a design choice, and the set of types is dense in the set of all distributions, the secret key capacity of an EDMS is obtained by maximizing the secret key rate over all possible sounding distributions $p_S$, perhaps under some input cost constraint (such as power). This result is specialized to give the secret key capacity of an EDMS with a degraded eavesdropper. We also characterize a reliability-secrecy tradeoff by quantifying two exponents. The first exponent $E_R$ bounds the probability that two users cannot reconcile the same key, i.e., $E_R < -\frac{1}{n} \log \Pr[K_a \neq K_b]$. The second exponent $E_S$ bounds the information leakage to the eavesdropper, characterized by $E_S < -\frac{1}{n} \log I(K_a; X^n_e, S^n, \Phi)$. The overall result yields a strongly achievable secret key rate-exponent triplet $(R_{SK}, E_R, E_S)$. For a given $R_{SK}$ less than capacity, there is a tradeoff between achievable $E_R$ and $E_S$. An example of such a tradeoff is shown in Figure 1. For a set rate, the tradeoff between the two exponents is achieved by varying the rate of the public message.

We then apply our results on EDMSs to a reciprocal Rayleigh fading channel. We discuss the limiting cases of un-quantized Gaussian sources as well as binary sources that result from quantizing uniform channel phases. We show that the choice of sounding signal has a significant effect on the possible rates of key generation. In the case where the sounding signal is subject to a power constraint, a signal that uniformly distributes power across all channels degrees of freedom results in a secret key rate that is convex in low-SNR (signal-to-noise ratio) and concave in high-SNR. Due to the convexity in low-SNR, uniform sounding signals are not always optimal. We show that an on-off sounding signal which uses only a fraction of the available degrees of freedom (but at a higher SNR) is the optimal input distribution at low SNR and characterize the secret key capacity at all SNRs. Our analysis of Gaussian sources is based on an equivalent Gaussian noise model. This facilitates comparison with the conventional additive white Gaussian noise (AWGN) channel.

The behavior of the secret key capacity in the low-SNR regime also reveals a fundamental quantity, the minimum energy per key bit. This quantity is reciprocally related to the capacity per unit cost [11] of the system. We show that, unlike the minimum energy per bit for reliable communication in an AWGN channel, there is a non-zero threshold SNR at which the minimum energy per key bit for our system is achieved. At lower SNRs with the optimal on-off signaling, the key capacity-cost function has the same slope as at the threshold SNR. This means it yields the same minimum energy per key bit. Finally, we characterize the minimum energy required for reliable key generation with a finite block length. We give a lower bound on the energy required by building off our results on the reliability exponent.

A. Related work

As mentioned above, key generation from general correlated sources was originally studied in [6], [7]. Those papers introduce the basic model and characterize the secret key capacity. Regarding correlated Gaussian sources (which would be the
case if the wireless transmissions experience Rayleigh fading) [12] and [13] investigate key generation from jointly Gaussian variables where [12] uses LDPC coding and [13] uses nested lattice codes and vector quantization for reconciliation. Generation of secret keys based on the inherent randomness of wireless channel is studied in [14], [15], [16], [17], [18], [19], [20]. Early work regarding key extraction from reciprocal channel randomness did not consider the use of a public message. For example, in [14] the phase difference between two orthogonal sinusoids in a received signal is quantized and coding is applied to improve the probability of key acquisition. An uncoded protocol is considered in [15] which analyzes the energy resource required for key acquisition. Regarding the approaches that use public discussions and fall within the information-theoretic approaches, [16] and [17] exploit the random amplitude of time delay channels to generate a key where [16] studies the ultra-wideband (UWB) channel and [17] focuses on narrow band channels. In [18] the use of randomness from level crossing process is considered. Adaptive quantization of noisy channel outputs for key generation is investigated in [19] and [20]. There are also related works on secret key generation in which the key is not generated from channel randomness. In [21] a secret key agreement protocol is studied but the key itself is a pseudo-random sequence generated by the user and does not result from the inherent randomness of wireless channels. In [22] key generation is considered in a situation where in addition to the dependent randomness from which they want to distill a common key. We also define the class of key distillation systems with which we work. In Section II-B we give the performance measures we aim to optimize. In Section II-C we define a particular class of excited sources of common randomness based on reciprocal multipath fading channels. Based on these definitions, we state the main results in Section III.

B. Paper outline

This paper is organized as follows. In Section II, we define a general EDMS model and a Gaussian EDMS which results from exciting the randomness of Rayleigh fading channel. We introduce a one-way secret key generation system and state the performance measure considered in this paper. Our main results are summarized in Section III. In Section IV, we discuss the reliability-secrecy tradeoff of the system. For a Gaussian source, we show that an on-off sounding signal is a capacity achieving signal in low-SNR and discuss reliability exponent and the energy consumption of a key with a finite block length using an on-off signal. A simple key generation scheme using binary phase quantization is also presented in Section IV. The proofs of the main results are given in Section V. Section VI concludes the paper.

C. Notation

A random variable is represented by a capital letter such as $X$ and a fixed-value scalar is represented by a lower case letter such as $x$. A sequence $(X_i, X_{i+1}, \ldots, X_j)$ is denoted by $X^j_i$ and a similar notation $x^j_i$ for a fixed-value sequence. When a sequence starts from $i = 1$, we use $X^j$ (or $x^j$) as a shorthand. Sets are denoted by using a calligraphic font, e.g., $S$. The complement of a set $S$ is denoted by $S^c$. We will use the notation $p_X(x)$ for the probability distribution function of $X$ for both discrete and continuous cases. This will not cause any confusion: $p_X(x)$ represents a probability mass function when $X$ is a discrete random variable and it represents a probability density function when $X$ is a continuous random variable. We use capital $P_{x^n}(x)$ to denote the type (empirical distribution) of a sequence $x^n$. We also use a shorthand for state dependent distribution, e.g., $Q_s(x) = p_X|x(s | s)$ is the conditional distribution of $X$ when state $S = s$. Throughout the paper, $\log(\cdot)$ refers to the natural logarithm and $\log_2(\cdot)$ refers to the logarithm in base two.

II. SECRET KEY FROM EXCITED SOURCE: MODELS AND DEFINITIONS

In this section we provide basic definitions and introduce the models with which we work in this paper. We start in Section II-A by defining an excited source of common randomness where the users (Alice and Bob) can influence the source of randomness from which they want to distill a common key. We also define the class of key distillation systems with which we work. In Section II-B we give the performance measures we aim to optimize. In Section II-C we define a particular class of excited sources of common randomness based on reciprocal multipath fading channels. Based on these definitions, we state the main results in Section III.

A. Source and System Model

The study of secret key generation from common randomness was initiated in [7], [6] where the users have access to a source of randomness specified, in effect, by nature. However, there are many situations where the users themselves can excite some medium to generate the source of randomness. We formalize our model of such situations by defining an excited source of common randomness.

Definition 1: Let $X_a^n, X_b^n, X_c^n$ and $S$ are finite sets. A length-$n$ excited distributed source (EDS) of common randomness is specified by an arbitrary conditional distribution $p_{X_a^n, X_b^n, X_c^n|S^n}(x_a^n, x_b^n, x_c^n|s^n)$ on $X_a^n \times X_b^n \times X_c^n$ where the designer can choose $s^n \in S^n$. We further call this an excited distributed memoryless source (EDMS) if

$$p_{X_a^n, X_b^n, X_c^n|S^n}(x_a^n, x_b^n, x_c^n|s^n) = \prod_{i=1}^{n} p_{X_{a,i}, X_{b,i}, X_{c,i}|S(x_{a,i}, x_{b,i}, x_{c,i}|s_i)}.$$  \hspace{1cm} (1)

An EDMS is said to have input constraint $P_S$ (a set of probability mass distributions) if the type $P_{x^n}$ of $s^n$ is constrained to be in $P_S$ (for every $n$). We note that since $s^n$ is a system parameter (in effect the “excitation” or “sounding” signal) and is known by all parties – Alice, Bob, and Eve. It will be useful to consider each element of $S$ as a system state, known to all, upon which the source of randomness is conditioned. Hence we often refer to $s \in S$ as the system “state”.

We consider key generation systems in which Alice, Bob and Eve respectively observe $X_a^n, X_b^n$ and $X_c^n$. The sounding signal $S^n$ is known by all. Alice and Bob are allowed to communicate via an error-free public channel that is monitored, but not impeded, by Eve. We concentrate on secret key generation based on one-way (Alice to Bob) public discussions (cf., e.g. [7]) defined next.
Definition 2: A one-way secret key generation system with sounding signal $s^n$ (where $P_{s^n} \in \mathcal{P}_S$) is defined by a triplet of functions

$$f_a(\cdot; s^n) : \mathcal{X}_a^n \to \mathcal{K},$$
$$g(\cdot; s^n) : \mathcal{X}_a^n \to \mathcal{M},$$
$$f_b(\cdot; s^n) : \mathcal{X}_b^n \times \mathcal{M} \to \mathcal{K}. $$

Respectively, these three functions define Alice’s key, $K_a$, the public message sent by Alice to Bob, $\Phi$, and Bob’s key, $K_b$:

$$K_a = f_a(X_a^n; s^n),$$
$$\Phi = g(X_a^n; s^n),$$
$$K_b = f_b(X_b^n, \Phi; s^n).$$

A special case of source in which Eve (Bob) has degraded observation of Bob (Eve) is defined as follows.

Definition 3: Given an EDM we say that source $X_e$ is a degraded version of $X_b$ when $S = s$ if

$$p_{X_a, X_b, X_e|S}(x_a, x_b, x_e|s) = p_{X_a, X_e|S}(x_a, x_e|s)p_{X_b|X_a, s}(x_b|x_a, s).$$

In other words, if, conditioned on $S = s$, $X_a - X_b - X_e$ forms a Markov chain. An EDMS is termed an EDM with degraded states if for every $S = s$, either $X_a$ is a degraded version of $X_b$ or $X_b$ is a degraded version of $X_e$. Finally, an EDMS has a degraded eavesdropper if $X_e$ is a degraded version of $X_b$ for all states.

B. Performance Measures

We next consider the performance measures of interest. These include capacity-type measures on secret key generation, error-exponent measures on the reliability of key generation, and guarantees on the secrecy of the generated key.

Definition 4: A secret key rate $R_{SK}$ is (weakly) achievable if for any $\epsilon > 0$ there exists an $n_0$ such that for all $n > n_0$, there exists a one-way secret key generation system (for some sounding signal $s^n$, $P_{s^n} \in \mathcal{P}_S$) satisfying

$$\frac{1}{n} H(K_a|S^n = s^n) > \frac{1}{n} \log |\mathcal{K}| - \epsilon, \quad (2)$$
$$\frac{1}{n} H(K_b|S^n = s^n) > R_{SK} - \epsilon, \quad (3)$$
$$\frac{1}{n} I(K_a; X_e^n, \Phi|S^n = s^n) < \epsilon, \quad (4)$$
$$\Pr[K_a \neq K_b] < \epsilon. \quad (5)$$

A secret key rate-exponent triplet $(R_{SK}, E_R, E_S) \in \mathbb{R}_+^3$ is achievable if (4) and (5) are replaced by stronger conditions

$$I(K_a; X_e^n, \Phi|S^n = s^n) < e^{-nE_R}, \quad (6)$$
$$\Pr[K_a \neq K_b] < e^{-nE_S}. \quad (7)$$

The rate-exponent triplet is termed strongly achievable if the exponent $E_R, E_S$ are strictly positive.

We remark that in Definition 4 condition (2) means that the key is almost uniformly distributed across the set $\mathcal{K}$. Conditions (3) and (4) imply $\frac{1}{n} H(K_a|X_e^n, \Phi, S^n = s^n) \geq R_{SK} - 2\epsilon$, i.e., Eve’s observation reveals almost no information about the key. Finally, conditions (6) and (7) respectively specify the exponential preservation of secrecy and exponential reliability of key reconciliation. Generally there will be a tradeoff between the two.

Definition 5: The secret key capacity of a one-way secret key generation system is

$$C_K = \lim_{n \to \infty} \sup_{(R_{SK}, E_R, E_S) \in \mathcal{R}} \frac{R_{SK}}{n}, \quad (8)$$

where the supremum is over $\mathcal{R}$, the closure of all achievable triplets $(R_{SK}, E_R, E_S)$, and the choice of $s^n$ satisfying constraint $\mathcal{P}_S$.

C. Multipath Channel Models: A Gaussian EDMS

An example of EDMs that we study in depth is based on reciprocal wireless fading channels. Say that Alice and Bob are linked by such a channel. Then, to generate a secret key, Alice and Bob alternately use the channel $n$ times to transmit a known sounding sequence $s^n$ to each other. We assume that the channel coefficients remain static over the two successive soundings by Alice and Bob and are independent to each other times. Under these assumptions, the respective outputs observed by Alice and Bob are

$$X_{a,i} = H_i s_i + N_{a,i}, \quad (9a)$$
$$X_{b,i} = H_i s_i + N_{b,i}, \quad (9b)$$

for $1 \leq i \leq n$, where $\{H_i\}$ are the i.i.d. reciprocal channel coefficients. We study the case of rich multipath Rayleigh fading where $H_i$ is a zero-mean complex Gaussian random variable with variance one, i.e., $CN(0, 1)$. The noise at Alice (Bob) and Bob (Alice) are respectively independent $CN(0, \sigma_a^2)$ and $CN(0, \sigma_b^2)$ random variables. We will constrain the sounding sequence $s^n$ to satisfy an average power constraint $\frac{1}{n} \sum_{i=1}^{n} |s_i|^2 < \mathcal{E}$. The received signal-to-noise ratio (SNR) at Alice (resp. Bob) is defined as $\gamma_a = \mathcal{E}/\sigma_a^2$ (resp. $\gamma_b = \mathcal{E}/\sigma_b^2$).

Eve gets two looks at each channel coefficient, one induced by Alice’s sounding signal, the other by Bob’s. Respectively, these outputs are $X_{ea,i} = H_{ea,i}s_i + N_{ea,i}$ and $X_{eb,i} = H_{eb,i}s_i + N_{eb,i}$. In a rich multipath environment, $H_{ea,i}$ and $H_{eb,i}$ will be independent of the main channel coefficient $H_i$ due to strong spatial decorrelation between channel coefficients. Thus, Eve’s channel observation $X_e$ is not useful for estimating the secret key. Thus, she can only use her knowledge of the sounding signal and the public message to estimate the secret key. This is a special case of EDMs with a degraded eavesdropper. When $S^n = s^n$ with $s_i = s$ a constant for all $i$, this situation specializes to Model S in [7].

The correlation between the Gaussian sources $X_a$ and $X_b$ given in (9) depends on the transmission power of the sounding signal. We are interested in the most power efficient regime for key generation. In this case, in addition to secret key capacity, we also characterize another fundamental quantity: minimum energy per key bit. We note that in this paper we assume the public channel is error-free and restrict attention to the energy consumption in the sounding signal. The following definition is the reciprocal of the capacity per unit cost defined in [11].
Definition 6: The minimum energy per key bit is defined to be
\[
\left( \frac{\mathcal{E}}{\sigma^2} \right)_{\text{min}} = \inf_{\gamma > 0} \frac{\gamma}{C_K(\gamma)} \log 2, \tag{10}
\]
where, for simplicity, we assume \( \sigma^2 = \sigma_0^2 = \sigma^2 \), \( \gamma = \mathcal{E}/\sigma^2 \) is the system SNR, and \( C_K(\gamma) \) is the secret key capacity as a function of \( \gamma \).

III. MAIN RESULTS

Given the setup of Section II we are now prepared to state the main results of the paper. Theorem 1 gives the secret key capacity for a general EDMS. Strongly achievable \((R_{SK}, E_R, E_S)\) for a degraded eavesdropper is presented in Theorem 2 and Theorem 3. Theorem 4 and 5 present the results for Gaussian EDMS.

A. General EDMS

Our first result gives the secret key capacity of a general EDMS with input constraint \( P_S \).

**Theorem 1:** The secret key capacity of an EDMS \((X_a, X_b, X_e, S)\) is
\[
C_K = \max_{U,T} \left[ I(T; X_b|U, S) - I(T; X_e|U, S) \right]. \tag{11}
\]
The maximization is over distribution \( P_S \in P_S \) and auxiliary variables \( U,T \) with distribution
\[
p_{U,T|S}(u, t|s)p_{X_a|T}(s|a|u, t)p_{X_b|X_a,S}(b|x, x_a, s) \tag{12}
\]
Further, the secret key capacity is bounded from above as
\[
C_K \leq \max_{P_S} \max_{U,T} I(X_a; X_b|X_e, S) \tag{13}
\]
Theorem 1 can be understood by using the interpretation of the known \( s^n \) as a sequence of system states. The secret key capacity (11) is expanded as
\[
C_K = \max_{P_S} \sum_s p_S(s) \max_{U^*,T^*} \left[ I(T^*; X_b|U^*, S = s) - I(T^*; X_e|U^*, S = s) \right]. \tag{14}
\]
where \( U^*, T^* \) are state-dependent auxiliary random variables. For any particular value \( S = s \), the source \((X_a, X_b, X_e)\) is a discrete memoryless source (DMS) distributed according to \( p_{X_a, X_b, X_e|S}(x_a, x_b, x_e|x_a, x_b, x_e)\). The capacity-achieving scheme of [7, Theorem 1] for DMSs can be applied to this system point-wise for each state. The secret key capacity is the weighted sum of state-wise secret key capacity, weighted according to the maximizing \( P_S \in P_S \). Capacity is achieved by selecting a sequence of sounding signals \( s^n \) so that \( P_{s^n} \) approaches \( P_S \) as \( n \to \infty \).

Since the designer has control of the sounding signal, the best choice is to choose \( P_S(s) \in P_S \) to maximize the achievable rate. In the special case in which there is no constraint imposed on \( P_S \), we have
\[
C_K = \max_{s \in S} \max_{U,T} I(T; X_b|U, S = s) - I(T; X_e|U, S = s). \tag{15}
\]
Namely, we choose a state that has the largest achievable secret key rate.

B. EDMS with Degraded Eavesdropper

In the degraded setting, a stronger result follows from Theorem 1.

**Corollary 1:** For an EDMS with degraded states the secret key capacity is
\[
C_K = \max_{P_S} \sum_{s \in S} p_S(s)|I(X_a; X_b|S = s) - I(X_a; X_e|S = s)|^+, \tag{16}
\]
where \(|x|^+ = \max\{x, 0\}\). Further, if the EDMS has a degraded eavesdropper, the secret key capacity is
\[
C_K = \max_{P_S} I(X_a; X_b|S) - I(X_a; X_e|S). \tag{17}
\]

To emphasize the state dependence, in the following, we use notation \( Q_s(x) = p_{X_a|S}(s|x) \) and \( Q_a(x) = p_{X_a|S}(x|s) \) as the conditional distribution of \( X_a \) and \( X_e \) respectively when input \( S = s \) and denote the corresponding channel law as \( W_s(x_a|x_b) = p_{X_a|X_b,S}(x_a|x_b, s) \) and \( V_s(x_a|x_e) = p_{X_a|X_e,S}(x_a|x_e, s) \).

In order to get a small error probability Alice must transmit enough information so that Bob can recover Alice’s key. However, while a larger public message rate increases the reliability of key recovery it also reveals more about \( X^n_a \) to Eve. In Theorem 2 we study this tradeoff by bounding the reliability and secrecy exponents, \( E_R \) and \( E_S \) respectively, of the strongly achievable rate-exponent triple \((R_{SK}, E_R, E_S)\).

**Definition 7:** An \((n, R)\) random binning code for alphabet \( \mathcal{X} \) is a random map \( f: \mathcal{X}^n \to \mathcal{B} = \{1, 2, \ldots, \lfloor e^{nR} \rfloor\} \) in which each \( x^n \in \mathcal{X}^n \) is independently and uniformly assigned to an element of \( \mathcal{B} \).

Thus, we get the definition of a random binning secret key generation system.

**Definition 8:** An \((n, R_{SK}, R_M)\) random binning secret key code with sounding signal \( s^n \) consists of two independent random binning codes:
\[
f_a(\cdot; s^n): \mathcal{X}^n_a \to \mathcal{K} = \{1, 2, \ldots, \lfloor e^{nR_{SK}} \rfloor\}; \tag{18}
\]
\[
g(\cdot; s^n): \mathcal{X}^n_e \to \mathcal{M} = \{1, 2, \ldots, \lfloor e^{nR_M} \rfloor\} \tag{19}
\]
where \( f_a(\cdot; s^n) \) is an \((n, R_{SK})\) random-binning code and \( g(\cdot; s^n) \) is an \((n, R_M)\) random-binning code.

**Theorem 2:** A sequence of \((n, R_{SK}, R_M)\) random-binning secret-key codes with sounding signals \( s^n \) exists that satisfies
\[
\lim_{n \to \infty} P_{s^n}(s) = p_S(s) \text{ for all } s \in S
\]
\[
- \lim_{n \to \infty} \frac{1}{n} \log \Pr[K_a \neq K_b] \geq E_R(R_M) \tag{20}
\]
\[
- \lim_{n \to \infty} \frac{1}{n} \log I(K_a; X^n_e, \Phi|S^n = s^n) \geq E_S(R_M, R_{SK}) \tag{21}
\]
where
\[
E_R(R_M) = \max_{0 \leq \rho \leq 1} \rho R_M - E_0(\rho, p_S),
\]
\[
E_0(\rho, p_S) = \sum_{s \in S} p_S(s) \tilde{E}_0(\rho, s),
\]
\[
\tilde{E}_0(\rho, s) = \log \left( \sum_{x_b} Q_s(x_b) \left( \sum_{x_a} W(x_a | x_b) \right)^{1+\rho} \right).
\]

and
\[
E_S(R_M, R_{SK}) = \max_{0 \leq \alpha \leq 1} F_0(\alpha, p_S) - \alpha (R_M + R_{SK})
\]
\[
F_0(\alpha, p_S) = \sum_{s \in S} p_S(s) \tilde{F}_0(\alpha, s)
\]
\[
\tilde{F}_0(\alpha, s) = -\log \left( \sum_{x_e} \tilde{Q}_s(x_e) \sum_{x_a} V_s(x_a | x_e)^{1+\alpha} \right).
\]

When there is no secrecy constraint, the key distillation problem becomes a classic Slepian-Wolf problem [8] for which the reliability exponent \(E_R\) is due to Gallager [23]. A slight difference is that, due to the known sounding signal, in (24) the reliability exponent is expressed in terms of the state dependent channel law.

A secrecy condition akin to (6) has been studied in [24], [25] in the setting where Alice and Bob have the same observation, i.e., the special case of Theorem 2 when \(X_a = X_b\). In this setting a public discussion is not required. Since reconciliation of \(X_a\) and \(X_b\) is not required, a tradeoff between reliability and secrecy (e.g., illustrated in Fig. 1) cannot be observed. In this paper we build off that analysis (termed “privacy amplification”) to understand the effects of the public discussion and of the sounding signal.

The secrecy exponent of (25)-(27) has a form similar to that of a state-dependent Gallager’s exponent, expressed in terms of the sum rate \(R_M + R_{SK}\). The resulting \(\tilde{E}_0(\rho, s)\) and \(\tilde{F}_0(\alpha, s)\) have properties similar to Gallager’s exponent, as is summarized in the following theorem.

**Theorem 3:**

1) \(\tilde{E}_0(\rho, s)\) is a non-decreasing non-negative function of \(\rho\) for \(\rho \geq 0\) and \(\tilde{E}_0(0, s) = 0\). Furthermore, \(\tilde{E}_0(\rho, s)\) is a convex function of \(\rho\) and
\[
\frac{\partial \tilde{E}_0(\rho, s)}{\partial \rho} \bigg|_{\rho=0} = H(X_a | X_b, S = s)
\]

2) \(\tilde{F}_0(\alpha, s)\) is a non-decreasing non-negative function of \(\alpha\) for \(\alpha \geq 0\) and \(\tilde{F}_0(0, s) = 0\). Furthermore, \(\tilde{F}_0(\alpha, s)\) is a concave function of \(\alpha\) and
\[
\frac{\partial \tilde{F}_0(\alpha, s)}{\partial \alpha} \bigg|_{\alpha=0} = H(X_a | X_e, S = s)
\]

With these properties we can find the conditions on \(R_{SK}\) and \(R_M\) for which \((R_{SK}, E_R, E_S)\) is strongly achievable. Taking derivative of (22) with respect to \(\rho\), we can find that
\[
R_M = \frac{\partial E_0(\rho, p_S)}{\partial \rho}
\]
when the optimal \(\rho\) is in \((0, 1)\). For \(R_M \leq \frac{\partial E_0(\rho, p_S)}{\partial \rho} \bigg|_{\rho=0}\), \(E_R\) is maximized by \(\rho = 0\) which corresponds to \(E_R(R_M) = 0\). Thus \(E_R(R_M)\) is positive if
\[
R_M > \frac{\partial E_0(\rho, p_S)}{\partial \rho} \bigg|_{\rho=0} = H(X_a | X_b, S)
\]
by Theorem 3. Similarly, the secrecy exponent \(E_S(R_M, R_{SK})\) is positive if
\[
R_M + R_{SK} < \frac{\partial F_0(\alpha, p_S)}{\partial \alpha} \bigg|_{\alpha=0} = H(X_a | X_e, S).
\]

In order to achieve positive \(E_R\) and \(E_S\), the key rate \(R_{SK}\) has to satisfy both (28) and (29). Namely,
\[
R_{SK} < H(X_a | X_e, S) - H(X_a | X_b, S) = I(X_a; X_b | S) - I(X_a; X_e | S).
\]

The upper bound (30) is the secret key capacity with degraded eavesdropper (17) if \(p_S\) is the capacity achieving input distribution.

**Remark 1:** The results of Theorems 2 and 3, while derived for degraded channels, can also be applied to the non-degraded case. However, the binning achievability scheme used may not be capacity achieving in those settings. This applicability of these results follows from two observations. The first is that \(\Pr[K_a \neq K_b]\) and \(I(K_a; X^n_a, S^n, \Phi)\) respectively depends only on the marginal joint distributions \(p_{X_a, X_b | S}(x_a, x_b | s)\) and \(p_{X_a, X_e | S}(x_a, x_e | s)\). The second observation is that the reliability and secrecy exponents derived in the theorems are expressed in terms of \(p_{X_a, X_b | S}(x_a, x_b | s)\) and \(p_{X_a, X_e | S}(x_a, x_e | s)\) respectively.

Figure 1 depicts the achievable \((R_{SK}, E_R, E_S)\) for a fixed \(p_S\). We can see that when \(R_{SK}\) is fixed, there is a tradeoff between \(E_R\) and \(E_S\) (see Section IV-A). Note that although we have control on \(p_S \in P_S\), the optimal \(p_S\) that maximizes the reliability exponent and that maximizes secrecy exponent are in general different. To find the largest \(E_R\), we express reliability exponent in terms of secret key rate \(R_{SK}\) by substituting \(R_M = H(X_a | X_e, S) - R_{SK} - \varepsilon\) in (22). When \(\varepsilon \to 0\), it is equal to operating at one extreme case of the tradeoff, i.e., \(E_S \to 0\), and yields a curve on the \(R_{SK}-E_R\) plane in Figure 1. We optimize the reliability exponent over distribution \(p_S \in P_S\), namely,
\[
E_R(R_{SK}) = \max_{p_S \in P_S} \max_{0 \leq \rho \leq 1} \rho [H(X_a | X_e, S) - R_{SK}] - E_0(\rho, p_S).
\]

**C. Gaussian EDMS**

By Corollary 1 and for the Gaussian EDMS specified in Section II-C, the secret key capacity
\[
C_K = \max_{p_S \in P_S} I(X_a; X_b | S),
\]
since \(X_e\) is independent of \(X_a\). \(P_S = \{p_S : E[|S|^2] \leq E\}\) is a set of distribution satisfying the power constraint. If a (not
necessarily optimal) constant sounding signal \( S_i = s \) where \(|s|^2 = \mathcal{E}\) uniformly for all \( 1 \leq i \leq n \) is used, the resulting mutual information \( I(X_a; X_b|S = s) \) is easily calculated to be

\[
I_K(\gamma_a, \gamma_b) = \log(1 + \gamma_{eq}), \quad \text{where} \quad \gamma_{eq} = \left( \frac{1}{\gamma_a} + \frac{1}{\gamma_b} + \frac{1}{\gamma_a \cdot \gamma_b} \right)^{-1}. \tag{34}
\]

If, e.g., we fix \( \gamma_a \) and let \( \gamma_b \) grow without bound, the equivalent SNR \( \gamma_{eq} \) of the overall system is dominated by the worst SNR \( \gamma_{eq} \rightarrow \gamma_a \).

In the special case where Alice and Bob have the same SNR, i.e., \( \gamma_a = \gamma_b = \gamma \), we denote

\[
I_K(\gamma) = \log(1 + \gamma_{eq}), \quad \text{where} \quad \gamma_{eq} = \frac{\gamma^2}{1 + 2\gamma}. \tag{36}
\]

The following theorem specifies the secret key capacity of an equal-SNR Gaussian EDMS.

**Theorem 4:** The secret key capacity of Gaussian EDMS under power constraint \( E[|S|^2] \leq \gamma \sigma^2 \) is

\[
C_K(\gamma) = \max_{0 \leq \lambda \leq 1} \lambda I_K \left( \frac{\lambda}{\gamma} \right). \tag{37}
\]

As we will discuss in Section IV-C, the optimal \( \lambda \) is

\[
\lambda_c = \min \left\{ \frac{\gamma}{\gamma_c}, 1 \right\}, \tag{38}
\]

where \( \gamma_c \) is the positive root of the equation

\[
I_K(\gamma_c) = \gamma_c \cdot \frac{d}{d\gamma} I_K(\gamma) \bigg|_{\gamma = \gamma_c}. \tag{39}
\]

Furthermore, an on-off signal which uses fraction \( \lambda_c \) of the channel can achieve the capacity.

With the above results we can characterize the minimum energy per key bit.

**Theorem 5:** The minimum energy per key bit of Gaussian EDMS is

\[
\left( \frac{E_b}{\sigma^2} \right)_{\min} = \inf_{\gamma > 0} \frac{\gamma}{C_K(\gamma)} \log 2 = \frac{\gamma_c}{I_K(\gamma_c)} \log 2, \tag{40}
\]

Our final results bound the Gaussian reliability exponent in terms of \( R_{SK} \) and SNR (cf. (31)) when the input is a constant sounding signal.

**Theorem 6:** If we define \( I_c(\gamma) = \log \left( \frac{1+\gamma_{eq}}{2} \right) \) and \( \rho^* = \exp(I_K(\gamma) - R_{SK}) - 1 \), where \( I_K(\gamma) \) is defined in (35), then the reliability exponent given a uniform sounding signal, as a function of secret key rate and SNR breaks into three regions:

**Region 1** (high rate): If \( R_{SK} \geq I_K(\gamma) \) then

\[
E_R(R_{SK}, \gamma) = 0.
\]

**Region 2** (medium rate): If \( I_K(\gamma) > R_{SK} \geq I_c(\gamma) \) then

\[
E_R(R_{SK}, \gamma) = \rho^*[I_K(\gamma) - R_{SK} + 1] - (1 + \rho^*) \log(1 + \rho^*).
\]

**Region 3** (low rate): If \( I_c(\gamma) > I_K(\gamma) > R_{SK} \geq 0 \) then

\[
E_R(R_{SK}, \gamma) = \begin{cases} 
I_K(\gamma) - R_{SK} + 1 - 2 \log 2, & \text{if } \gamma_{eq} \geq 1, \\
\rho^*[I_K(\gamma) - R_{SK} + 1] - (1 + \rho^*) \log(1 + \rho^*), & \text{if } 1 > \gamma_{eq} \geq 0.
\end{cases}
\]

Although the optimal sounding signal to maximize Gaussian reliability exponent remains unknown, on-off signaling again improves the achieved exponent at low SNR. This improvement is discussed in Section IV.

**IV. DISCUSSIONS**

In this section we discuss various implications of the main results presented in Section III.

**A. Reliability-Secrecy Tradeoff**

The problem of secret key generation from a correlated source can be formulated as a distributed source coding problem with a secrecy constraint. On the one hand, we want to understand the system reliability, which corresponds to the error exponent of a Slepian-Wolf problem [23]. On the other hand, we want to develop an analogous measure of secrecy, which corresponds to the privacy amplification considered in [26], [24]. A main consequence of Theorem 2 is that reliability and the secrecy can both be quantified for system and we observe that there is a fundamental tradeoff between the two.

From (28) and (29), we know that \( E_R \) is positive if \( R_M > H(X_a|X_b, S) \) and \( E_S \) is positive if \( R_M + R_{SK} < H(X_a|X_b, S) \). More specifically, from (22) and (25), the public message rate \( R_M \) is a design parameter which allows us tradeoff \( E_R \) for \( E_S \). Figure 1 is a three dimensional plot of achievable \((R_{SK}, E_R, E_S)\) for a binary source from quantizing channel phase. Details are in Section IV-F. Figure 2(a) plots \( E_R \) vs \( E_S \) as a function of \( R_M \) for different values of \( R_{SK} \). By varying \( R_M \) for a fixed \( R_{SK} \), we get the \( E_R-E_S \) tradeoff curve shown in Figure 2(b). This curve corresponds to a slice of the surface in Figure 1 at a constant \( R_{SK} \).

**B. An Equivalent Noise Model of Gaussian EDMS**

The secret key rate function (35) can be observed to have the same form as the AWGN channel capacity if we replace SNR \( \gamma \) with \( \gamma_{eq} \). However, (35) is always less than AWGN channel capacity. To see this, note that from signal model (9), when \( S \) is a constant sounding signal \( s \) and \( |s|^2 = \mathcal{E} \), \( X_a, X_b \) and \( H \) form a Markov chain \( X_a \leftrightarrow sH \leftrightarrow X_b \). Thus,

\[
I(X_a; X_b) = I(sH; X_b) - I(sH; X_b|X_a). \tag{41}
\]

The first term has the same value as AWGN channel capacity while the second term is always non-negative. To obtain an insight of the secret key rate function \( I_K(\gamma) \), we present an equivalent Gaussian noise model in which the Bob’s channel output \( X_b \) is expressed as a combination of the component statistically aligned with \( X_a \) and the component orthogonal to \( X_a \), that is

\[
X_b = \beta X_a + Z \tag{42}
\]
known, the orthogonal error, mean-squared error (MMSE) estimate of $X$ is

$$
\beta X
$$

This can also be seen as follows:

$$
\text{Fig. 2. Binary source with}
$$

$$
\text{where}
$$

$$
\text{Fig. 3. (a) Original signal model (b) Equivalent Gaussian noise model}
$$

where

$$
\beta = \frac{E[X_b X_a^*]}{E[|X_a|^2]} = \frac{\mathcal{E}}{\mathcal{E} + \sigma_a^2} = \frac{\gamma_a}{\gamma_a + 1}
$$

This can also be seen as follows: $\beta X_a$ is the minimum mean-squared error (MMSE) estimate of $X_b$. Since $X_a$ and $X_b$ are jointly Gaussian with zero mean (recall that $S$ is known), the orthogonal error, $Z$, is also zero-mean Gaussian and independent of $X_a$ due to the orthogonality principle and Gaussianity. $X_a$ in (42) has the same distribution as in (9a) and $(X_a, X_b)$ has the same joint distribution as in (9). Figure 3 shows the relationship between $X_a$ and $X_b$ in the original and equivalent Gaussian model. The signal multiplication gain $\beta (\beta < 1)$ is a deterministic function of Alice’s SNR $\gamma_a$. The signal to noise ratio of the equivalent model (42) is

$$
\frac{E[|\beta X_a|^2]}{E[|Z|^2]} = \frac{\mathcal{E}^2}{\mathcal{E} + \sigma_a^2} = \frac{\mathcal{E}^2}{\mathcal{E} + \sigma_a^2} = \frac{\mathcal{E}^2}{\mathcal{E} + \sigma_a^2} = \gamma_{eq}.
$$

This is the same result we get from calculating the mutual information given in ((34). For the symmetric SNR case, it reduces to (36). In the high-SNR regime, $\gamma_{eq} \approx \gamma/2$ because $E[|X_a|^2] \approx \mathcal{E}$ and the end-to-end channel between $X_a$ and $X_b$ embeds two channel noises. The equivalent (compound) channel has multiplication gain $\beta \approx 1$ and the resulting secret key rate $I_K(\gamma) \approx \log(1 + \frac{\gamma}{2})$ is a concave function.

On the other hand, in the low-SNR regime $\gamma_{eq} \approx \gamma^2$ and $I_K(\gamma) \approx \log(1 + \gamma^2) \approx \gamma^2$ which is a convex function. Using the equivalent Gaussian noise model (42) when $\gamma \ll 1$, the signal multiplication gain $\beta \approx \gamma$ and

$$
X_b = \beta X_a + Z \approx \gamma X_a + Z.
$$

where $E[|X_a|^2] \approx \mathcal{E}$ and $\gamma_{eq} \approx 1$. This gain $\beta$ is linearly proportional to the operating SNR and the resulting secret key rate is $I_K(\gamma) \approx \log(1 + \gamma) \approx \gamma^2$, a convex function.

C. On-off Signaling Achieves Capacity

Due to the convexity of $I_K(\gamma)$ in low SNR, an on-off type sounding signal with distribution

$$
p_s(s) = (1 - \lambda)\delta(s) + \lambda\delta(s - s_1)
$$

with $s_1 = \sqrt{\gamma\sigma^2/\lambda}$ and $0 \leq \lambda \leq 1$, will achieve a higher secret key rate. The corresponding secret key rate is

$$
\lambda I_K \left( \frac{\gamma}{\lambda} \right).
$$

In the proof of Theorem 4 in Section V, we show that the secret key capacity is achieved by choosing $\lambda$ which maximizes (47). Taking the derivative of (47) with respect to $\lambda$, we can find the optimal parameter $\lambda$:

$$
\lambda_c \triangleq \arg \max_{0 \leq \lambda \leq 1} \lambda I_K \left( \frac{\gamma}{\lambda} \right) = \min \left\{ \frac{\gamma}{\gamma_c}, 1 \right\}
$$

where $\gamma_c$ is the positive root of the equation

$$
I_K(\gamma) = \gamma_c \frac{d}{d\gamma} I_K(\gamma) \bigg|_{\gamma=\gamma_c}.
$$
Solving $\gamma_c$ numerically we find $\gamma_c \approx 1.535$ (1.86 dB). Figure 4 shows the secret key rate for a uniform constant signal and an on-off signal. The operational interpretation of this result is as follows. When $\gamma$ is below $\gamma_c$, capacity is achieved by using the source $\lambda_e n$ times, each at SNR $\gamma_c$. The achievable key rate is equal to time-sharing between two SNRs (0 and $\gamma_c$). The sounding signal thus becomes sparse and peaky when $\gamma$ is low. We note that an analogous result from a non-coherent communication in which a sparse/peaky signal also achieves channel capacity in low SNR [27], [28].

We can also interpret the improvement of the optimal on-off signal using the equivalent noise model developed in Section IV-B. From (45), in the low-SNR regime (in particular $\gamma \leq \gamma_c$), the multiplication gain $\beta$ of the equivalent channel approximates the operating SNR. When we use the optimal on-off signal, it results in a higher SNR ($\gamma_c$). The resulting secret key rate is

$$\lambda_e I_K \left( \frac{\gamma}{\lambda_e} \right) = \lambda_e I_K (\gamma_c) \approx \lambda_e \gamma_c \gamma_c.$$  

The last approximation comes from $I_K (\gamma) \approx \gamma^2$. Thus, the secret key rate-cost function approximates a linear function of $\gamma$ instead of a quadratic function.

One of the most significant effects due to the linearity of $C_K(\gamma)$ in the low-SNR regime (because of the time-sharing effect) is the minimum energy per key bit $(\frac{E}{n})_{\min}$ given in Theorem 5. In particular, in contrast to the AWGN channel, $(\frac{E}{\sigma^2})_{\min}$ is achieved in all $\gamma < \gamma_c$. Figure 5(a) shows $\gamma / I_K (\gamma)$ and $\gamma / C_K(\gamma)$ as function of $\gamma$. Without using an on-off signaling, $(\frac{E}{\sigma^2})_{\min}$ is achieved only at $\gamma_c$.

**D. Gaussian Reliability Exponent Using An On-off Signal**

In Theorem 6 we give an expression of reliability exponent for the Gaussian EDMS when the input is a constant sounding signal. Furthermore, from the discussion in Section IV-C, we can expect that an on-off signal can achieve higher reliability exponent for a given average SNR $\gamma$. Consider a sounding scheme that uses fraction $\lambda$ of the available channel degrees of freedom. To achieve a target $R_{SK}$ with average SNR $\gamma$, the system operates at key rate $R_{SK}/\lambda$ and SNR $\gamma/\lambda$. The error probability is upper bounded by $e^{-\lambda n E_R (R_{SK}/\lambda, \gamma/\lambda)}$ which has effective exponent

$$\lambda E_R \left( \frac{R_{SK}}{\lambda}, \frac{\gamma}{\lambda} \right).$$

We maximize it over $0 \leq \lambda \leq 1$ to get the error exponent optimal on-off signal

$$\lambda_e \triangleq \arg \max_{0 \leq \lambda \leq 1} \lambda E_R \left( \frac{R_{SK}}{\lambda}, \frac{\gamma}{\lambda} \right) \tag{50}$$

and denote the error exponent achieved by the optimal on-off signal as

$$\bar{E}_R (R_{SK}, \gamma) = \lambda_e E_R \left( \frac{R_{SK}}{\lambda_e}, \frac{\gamma}{\lambda_e} \right). \tag{51}$$

Figure 6(a) and 6(b) show $E_R (R_{SK}, \gamma)$ and $\bar{E}_R (R_{SK}, \gamma)$ in low SNR as functions of $R_{SK}$ and $\gamma$, respectively. Although the optimal input distribution for the error exponent is still unknown, we can see the results in Figure 6 - the on-off signal has a large improvement at low rate and low SNR.

**E. Minimum Key Energy with A Finite Block Length**

We use the developed reliability exponent to characterize minimum key energy with a finite block length code $(\frac{E}{n})_{\min}$. In contrast to minimum energy per key bit, $(\frac{E}{\sigma^2})_{\min}$ is the minimum energy required to generate a $b_{key}$-bit key by using a finite block length such that the system meets the reliability requirement $\Pr[K_a \neq K_b] \leq \epsilon$. We provide an upper bound of such energy.

Consider using a source $n$ times and generate a $b_{key}$-bit key. The secret key rate is $R_{SK} = \log 2 b_{key}/n$ and the energy required to generate the key is $E_{key} = n E = n \gamma^2$. Since $E_{key}$ is linearly proportional to $n$, we apply exponential bound of error probability we have developed to find the minimum block length $n$ needed to satisfy reliability condition. Namely,

$$J(n, \gamma, b_{key}) \triangleq n E_R \left( \log 2 \frac{b_{key}}{n}, \gamma \right) \geq \log \frac{1}{\epsilon}. \tag{52}$$

Note that $J(n, \gamma, b_{key})$ is an increasing function of $n$ and $\gamma$ when $b_{key}$ is fixed. The normalized minimum energy of a $b_{key}$-bit key can be bounded above as

$$\left( \frac{E_{key}}{\sigma^2} \right)_{\min} \leq \min_{p_S \in P_S} \min_{\gamma \geq 0, n \in \mathbb{N}} \frac{\gamma n}{\epsilon} \tag{53}$$

subject to

$$J(n, \gamma, b_{key}) \geq \log \frac{1}{\epsilon},$$

where $P_S = \{p_S : E[|S|^2]/\sigma^2 \leq \gamma\}$. Given a $p_S \in P_S$, (53) is a nonlinear optimization problem with a nonlinear constraint. We examine the upper bound by using a uniform sounding input and an optimal on-off sounding input defined in (50), the latter is equivalent to replacing $E_R (\cdot, \cdot)$ with $\bar{E}_R (\cdot, \cdot)$ given in (51). Figure 5(b) shows the numerical result of this upper
bound for both $b_{\text{key}} = 64$ and 128 as a function of $\gamma$ wherein $n$ is chosen to be the minimum integer satisfying the reliability constraint (52). We see the similar behavior as in minimum energy per bit: an optimal on-off sounding signal achieves the minimum value for all SNRs below a threshold while a constant sounding achieves this value only at threshold SNR.

F: An Example: Binary Source from Quantized Channel Phases

In a practical implementation of a key generation from reciprocal multipath channel, each user has to quantize its observation. We consider a simple (symmetric) phase quantization scheme [15]. In this scheme, Alice and Bob perform the same phase quantization that maps the random phase to binary level \{0, 1\}, denoted by $Y_a$ and $Y_b$ respectively. The relation between $Y_a$ and $Y_b$ are characterized by a binary symmetric channel (BSC) with transition probability $\theta = Pr[Y_a \neq Y_b]$. In Appendix B, it is shown that with a constant sounding signal ($S = s$) input,

$$\theta = \frac{1}{2} - \frac{1}{\pi} \arctan(\sqrt{\gamma_{\text{eq}}}) , \quad (54)$$

where $\gamma_{\text{eq}}$ is defined in (36). Eve’s quantized output $Y_e$ is assumed to be independent of $Y_a$ and $Y_b$ in a rich multipath case.

1) Secret key capacity: The achievable secret key rate with a constant sounding signal is

$$I_K(\gamma) = I(Y_a; Y_b|S) = 1 - H_B(\theta) , \quad (55)$$

where $H_B(\theta) = -\theta \log \theta - (1 - \theta) \log(1 - \theta)$ is the binary entropy function. Similar to a Gaussian source, the $I_K(\gamma)$ again exhibits convexity in the low-SNR regime. The optimality of an on-off signal to achieve capacity follows via the same reason as Theorem 4 though the result $\gamma_c$ is naturally different from Gaussian case. The optimal operating SNR for the binary case is $\gamma_c \approx 1.28$ (1.07 dB).

2) Reliability exponent: In Appendix C, we derive the reliability exponent of the this binary source in terms of message rate $R_M$ and $\theta$ (54) when a constant sounding signal is applied. Since Eve has independent channel output, the conditional entropy of quantized binary variable $H(Y_a|Y_c, S) = 1$. From (29), the key rate $R_{SK}$ satisfying the secrecy condition is $R_M = H(Y_a|S = s) - R_{SK} = 1 - R_{SK}$. Thus, we get reliability exponent in terms of $R_{SK}$:

**Region 1** (high rate): If $R_{SK} \geq I_K(\gamma)$,

$$E_{R}(R_{SK}, \gamma) = 0.$$ 

where $I_K(\gamma)$ is defined in (55).

**Region 2** (medium rate): If $I_K(\gamma) > R_{SK} \geq I_c(\gamma)$ then

$$E_{R}(R_{SK}, \gamma) = T_\theta(\tau) - H_B(\tau) ,$$

where $\theta$ is defined in (54) and

$$I_c(\gamma) = 1 - H_B \left( \frac{\sqrt{\tau}}{\sqrt{\theta} + \sqrt{1 - \theta}} \right) \quad (56)$$

$$\tau = H_B^{-1}(1 - R_{SK}) \quad (57)$$

$$T_\theta(\tau) = -\tau \log(\theta) - (1 - \tau) \log(1 - \theta) \quad (58)$$

**Region 3** (low rate): If $I_c > R_{SK} \geq 0$ then

$$E_{R}(R_{SK}, \gamma) = 1 - 2 \log(\sqrt{\theta} + \sqrt{1 - \theta} - R_{SK}) - R_{SK}.$$ 

Figure 6(c) and 6(d) show the error exponent in the low SNR regime with constant and on-off input signals. Similar to the Gaussian case, the error exponent of an on-off signal improves for low SNR and for low rate.

3) Secrecy exponent: The result above consider a case that Eve’s $Y_e$ is independent of $Y_a$ and $Y_b$. Regarding the secrecy condition, it is insightful to consider the correlated eavesdropping. Let $Y_e$ is correlated with $Y_a$ by a BSC with transition probability $w = Pr[Y_a \neq Y_e] \leq 1/2$. From Theorem
2 and after some manipulation, we can find that

\[ F_0(\alpha, ps) = -\log(w^{1+\alpha} + (1-w)^{1+\alpha}) \]

and

\[ \frac{\partial F_0(\alpha, ps)}{\partial \alpha} = T_w(\delta), \]

where

\[ \delta = \frac{w^{1+\alpha}}{w^{1+\alpha} + (1-w)^{1+\alpha}} \]

and \( T_w(\delta) \) is defined the same as (58). The secrecy exponent is obtained by optimizing over \( 0 \leq \alpha \leq 1 \) and can be expressed as

\[
E_S(R_{SK}, R_M) = \begin{cases} 
0, & R_{SK} + R_M > H_B(w) \\
F_0(\alpha^*, ps) - \alpha^* (R_{SK} + R_M), & R_c < R_{SK} + R_M \leq H_B(w) \\
F_0(1, ps) - (R_{SK} + R_M), & R_{SK} + R_M \leq R_c
\end{cases}
\]

where \( \alpha^* \) is the solution of \( T_w(\delta) = R_{SK} + R_M \) and

\[ R_c = \frac{\partial F_0(\alpha, ps)}{\partial \alpha} \bigg|_{\alpha=1}. \]

Figure 2 shows the case where \( \theta = 0.01 \) and \( w = 0.3 \). This corresponds to \( H(X_a|X_b, S) = 0.08 \) and \( H(X_a|X_c, S) = 0.881 \).

V. PROOFS OF MAIN RESULTS

A. Proof of Theorem 1

To simplify notation let \( X^*_a, X^*_b, X^*_c \) denote a triplet of random variables with the same distribution as that introduced on \( X_a, X_b, X_c \) given \( S = s \). In other words, \( p_{X^*_a, X^*_b, X^*_c}(x_a, x_b, x_c) = p_{X_a, X_b, X_c|S}(x_a, x_b, x_c|s) \). The value of \( s \) is the state of the system. The state-dependent secret key capacity \( C_K(s) \) follows immediately from (7, Theorem 1):

\[ C_K(s) = \max_{U^*, T^*} I(T^*; X^*_b|U^*) - I(T^*; X^*_c|U^*). \]

The capacity is found by maximizing over a pair of state-dependent random variables \( U^* \) and \( T^* \) where the overall distribution is \( p_{U^*, T^*}(u, t)p_{X^*_a|T^*}(x_a|t)p_{X^*_b, X^*_c|X^*_a, x_a}(x_b, x_c|x_a) \). Since the sounding signal \( s^n \) is designer-chosen and need not be constant, i.e., we need not \( s_i = s \) for all \( i \) and some choice of \( s \). For any choice of \( s^n \) such that \( P_{s^n} \rightarrow P_{s} \in \mathcal{P}_s \) as \( n \rightarrow \infty \), we have an achievable secret key rate \( \sum_s p_S(s)C_K(s) \). Combine the state-dependent auxiliary random variables \( U^*, T^* \) and the state distribution \( p_S \), the auxiliary random variable \( U, T \) has joint distribution given in (12). We next upper bound the achievable rate to show that maximizing \( \sum_s p_S(s)C_K(s) \) yields the secret key capacity of an EDMS.

For the converse part of Theorem 1, we want to show that for any \( P_{s^n} \in \mathcal{P}_s \) and secret key rate \( R_{SK} \) satisfying (3)-(5), then there is some \( P_S \in \mathcal{P}_S \) and \( U, T \) such that

\[
R_{SK} \leq \sum_s p_{s}(I(T; X_b|U, S) - I(T; X_c|U, S))
\]

\[
= \sum_s p_{s}(I(T; X_b|U, S = s) - I(T; X_c|U, S = s)),
\]

Fig. 6. Error exponent of low-SNR for Gaussian and quantized channels.
For arbitrary random variables $U, V$ and sequences $X_b^n, X_e^n$, we have

$$I(U; X_b^n | V) - I(U; X_e^n | V) = \sum_{i=1}^{n} \left[ I(U; X_b,i | X_{b,i-1} X_{e,i+1} X_e^n) - I(U; X_e,i | X_{b,i-1} X_{e,i+1} X_e^n) \right]$$

Proceeding to the proof of the converse, we show the following set of inequalities for any sequence $s^n$:

$$n R_{SK} \leq H(K_a | S^n = s^n) + n \epsilon$$

$$= I(K_a; X_b^n, \Phi | S^n = s^n) + H(K_a | X_b^n, \Phi, S^n = s^n) + n \epsilon$$

$$\leq I(K_a; X_b^n, \Phi | S^n = s^n) + 2 n \epsilon$$

$$\leq I(K_a; X_b^n, \Phi | S^n = s^n) - I(K_a; X_b^n, \Phi | S^n = s^n) + 3 n \epsilon$$

$$= I(K_a; X_b^n, \Phi | S^n = s^n) - I(K_a; X_b^n, \Phi | S^n = s^n) + 3 n \epsilon$$

$$\leq \sum_{i=1}^{n} \left[ I(K_a; X_b,i | X_{b,i-1} X_{e,i+1} X_e^n) + 3 n \epsilon \right]$$

$$= \sum_{i=1}^{n} I(K_a; X_b,i | U, S_i = s_i) - I(K_a; X_e,i | U, S_i = s_i) + 3 n \epsilon$$

where (i) follows from (3), (ii) from Fano’s inequality and (iii) from the secrecy condition (4). The equality in (iv) follows from Lemma 1 where $S_{n|\lambda}$ denotes $S^{i-1} S_{n+1}$. Finally, (v) follows from letting $U_i = X_{b,i-1} X_{e,i+1} X_e^n$. Letting $J$ be a random variable independent of all others and uniformly distributed over $\{1, 2, \ldots, n\}$. The last sum can be written as

$$n \sum_{i=1}^{n} \Pr[J = i] \left[ I(K_a; X_b,i | U, S_i = s_i, J = i) - I(K_a; X_e,i | U, S_i = s_i, J = i) \right]$$

$$\leq \sum_{i=1}^{n} \left[ I(K_a; X_b,i | U, S_i = s_i) - I(K_a; X_e,i | U, S_i = s_i) \right]$$

for some $p_s \in P_S$. The final inequality is due to the fact that type $P_{s^n}$ is a subset of distributions in $P_S$ and $U = (U,j, J)$. Letting $T = (K_a, U)$, the construction of $T, X_a,j, X_b,j, X_e,j$ satisfies condition (12) for a given $S_j = s$ and $(X_a,j, X_b,j, X_e,j, S_j)$ have the same joint distribution as $(X_a, X_b, X_e, S)$. This demonstrates the tightness of (11).

We next develop the upper bound on the secret key rate specified in (13). The development of the bound agrees with the above development up to step (ii) in equation (61). From there we continue as below:

$$n R_{SK} \leq I(K_a; X_b^n, \Phi | S^n = s^n) + 2 n \epsilon$$

$$= I(K_a; X_b^n, \Phi, S^n = s^n) + 3 n \epsilon$$

$$= I(K_a; X_b^n, \Phi, S^n = s^n) - I(K_a, K_e, X^n | S = s^n) + 3 n \epsilon$$

$$= n \sum_{s \in S} p_s | I(X_a, X_b, X_e, S = s) + 3 n \epsilon$$

where $p_s \in P_S$. The inequality (vi) comes from the chain rule of mutual information and the secrecy condition (4). That in (vii) follows the fact that mutual information is non-negative and $K_a$ and $\Phi$ are function of $X_b^n$ and $S^n$, implying the Markov relation $\Phi, K_a \leftrightarrow S^n, X_b^n \leftrightarrow X_b^n, X_e^n$. Finally, (viii) uses the memoryless property of the source (cf. (1)) and is expressed in terms of the type $P_{s^n}$.

**B. Proof of Corollary 1**

Given any particular state $S = s$ an EDMS is a DMS. Recall that a DMS with degraded states is one in which for every $s \in S$ either $X_e$ is a degraded version of $X_b$ with respect to $X_a$ (i.e., $X_e^n \rightarrow X_b^n \rightarrow X_a^n$) or the reverse. Defining the set

$$D = \{ s \in S : X_e \text{ is a degraded version of } X_b \text{ in state } s \}$$

we immediately have from [7, Theorem 1] that

$$C_K(s) = I(X_a; X_b, X_e, S = s)$$

$$= \begin{cases} I(X_a; X_b, S = s) - I(X_a; X_e, S = s) & \text{if } s \in D \\ 0 & \text{else} \end{cases}$$

Average over all states and we arrive at

$$C_K = \max_{p_s \in P_S} \sum_{s \in S} p_s(s) C_K(s)$$

$$= \max_{p_s \in P_S} \sum_{s \in S} p_s(s) I(X_a, X_b | S = s) - I(X_a; X_e, S = s)$$

where the input constraint $p_s \in P_S$ may force the system to put non-zero probability mass on reversely degraded states $s \in D^c$. Finally, if the eavesdropper is degraded (in all states) we can drop the $| : \uparrow$ and average the mutual information expression with respect to $p_s$ giving (17).
C. Proof of Theorem 2

To prove our achievability result we use an \((n, R_{SK}, R_M)\) random binning secret key system according to Definition 8. We recall from that definition that the coding scheme involves two random binnings functions: the key binning \(f_a(\cdot; s^n)\), cf. (18), and the public message binning \(g(\cdot; s^n)\), cf. (19). All that remains to specify the system fully is to define Bob’s decoding function \(f_b(\cdot; s^n)\). Bob’s decoding function will be a concatenation of a maximum likelihood decoder with random key binning function.

For compactness of notation let \(W_{a^n}(x_{a^n}^n|x_b^n) = p_{X^n_a|X^n_b, S^n}(x_{a^n}^n|x_b^n, s^n)\). Bob’s ML estimate of \(X^n_a\) is

\[
\hat{X}^n_a = h(\phi, x_b^n, s^n) = \arg \max_{x_a^n \in \Omega_{a, s^n}} W_{a^n}(x_{a^n}^n|x_b^n) \tag{65}
\]

and generates his key as

\[
K_b = f_a(h(\Phi, \hat{X}^n_a, S^n); s^n). \tag{66}
\]

Define \(E_k\) to be the event that \(K_a \neq K_b\) and \(E_x\) to be the event that \(X^n_a \neq \hat{X}^n_a\). We bound the error probability by the probability of making an erroneous estimate of \(X^n_a\).

\[
\Pr[K_a \neq K_b] \leq \Pr[E_k \cap E_x] + \Pr[E_k \cap E_x^c] = \Pr[E_k \cap E_x] \leq \Pr[E_x]. \tag{67}
\]

In [23] Gallager analyzes the combination of random binning and ML decoding for Slepian-Wolf coding and bounds \(\Pr[E_x]\) as

\[
\Pr[E_x] \leq |M|^{-\rho} \sum_{x_b^n} Q_{a^n}(x_b^n) \left( \sum_{x_a^n} W_{a^n}(x_{a^n}^n|x_b^n) \right)^{1+\rho} \tag{68}
\]

for all \(0 \leq \rho \leq 1\). When the source and channel are memoryless, (67) simplifies further as,

\[
\Pr[K_a \neq K_b] \leq |M|^{-\rho} \prod_{i=1}^n Q_{a^n}(x_b^n) \left( \sum_{x_a^n} W_{a^n}(x_{a^n}^n|x_b^n) \right)^{1+\rho}
\]

\[
= \exp \left\{-n \left[ \rho R_M \ldots \right. \right. \right.
\]

\[
- \sum_{s \in S} P_S(s) \log \left( \sum_{x_b^n} Q_{a^n}(x_b^n) \left( \sum_{x_a^n} W_{a^n}(x_{a^n}^n|x_b^n) \right)^{1+\rho} \right) \right\}. \tag{69}
\]

where we choose the type \(P^*_s(\cdot)\) of the sounding signal \(s^n\) to converge to \(p_S(s)\) as \(n \to \infty\). Taking the logarithm on both sides and maximizing with respect to \(\rho, 0 \leq \rho \leq 1\), we get (22).

To develop the secrecy exponent, we build off the “privacy amplification” analysis technique used in [24] with \(\alpha = 1\) and in [25] for wire-tap channel problem. As discussed in Sec. III, in those papers \(X_a = X_b\), i.e., Alice and Bob’s observations are the same with probability one. Herein we incorporate the effect of the public message and of the sounding signal into the analysis technique.

The analysis uses the Renyi’s entropy of order \(1 + \alpha\) with \(0 \leq \alpha \leq 1\). The Renyi entropy of order \(1 + \alpha\) of a random variable \(X\) with distribution function \(p_X(\cdot)\) is

\[
H_{1+\alpha}(X) = \frac{1}{\alpha} \log \sum_x p_X(x)^{1+\alpha}. \tag{70}
\]

We can interpret Renyi entropy in terms of an independent but identically distributed random variable \(X'\), i.e., \(p_{X', X'}(a, b) = p_X(a)p_X(b)\), as follows

\[
H_{1+\alpha}(X) = -\frac{1}{\alpha} \log \left( \sum_x p_X(x) \left( \sum_a p_X(a) 1(x = a) \right)^\alpha \right)
\]

\[
= -\frac{1}{\alpha} \log \left( \sum_x p_X(x) \Pr[X' = x]^\alpha \right)
\]

where \(1(\cdot)\) is the indicator function.

One property of the Renyi entropy we find useful is that it is upper bounded by the Shannon entropy. It follows from Jensen’s inequality:

\[
H_{1+\alpha}(X) \leq -\frac{1}{\alpha} \sum_x p_X(x) \log p_X(x)^\alpha
\]

\[
\leq -\frac{1}{\alpha} \sum_x p_X(x) \log p_X(x) = H(X).
\]

We begin the exponential characterization of secrecy by first rewriting the mutual information \(I(K_a; X^n_a, \Phi, S^n = s^n)\) as

\[
I(K_a; X^n_a, \Phi|S^n = s^n) = H(K_a|S^n = s^n) - H(K_a|X^n_a, \Phi, S^n = s^n)
\]

\[
= H(K_a|S^n = s^n) - [H(K_a, \Phi|X^n_a, S^n = s^n) - H(K_a, \Phi|X^n_a, S^n = s^n)]
\]

\[
\leq nR_{SK} + nR_M - H(K_a, \Phi|X^n_a, S^n = s^n) \tag{71}
\]

For convenience, we use the notation

\[
\tilde{Q}_{a^n}(x_a^n) = p_{X_a^n|S^n}(x_a^n|s^n), \quad \tilde{V}_{a^n}(k, \phi|x_e^n) = p_{K_a^n, \Phi^n|X_e^n, S^n}(k, \phi|x_e^n) \tag{72}
\]

where \(\Omega_{k, \phi, s^n} = \{x_a^n : f_a(x_a^n; s^n) = k, g(s_a^n, s^n) = \phi\}\). We lower bound the conditional entropy

\[
H(K_a, \Phi|X_e^n, S^n = s^n) \tag{73}
\]

\[
\geq \sum_{x_a^n} \tilde{Q}_{a^n}(x_a^n) H_{1+\alpha}(K_a, \Phi|X_e^n = x_a^n, S^n = s^n)
\]

\[
= \sum_{x_a^n} \tilde{Q}_{a^n}(x_a^n) \frac{-1}{\alpha} \log \left( \sum_{k, \phi} \tilde{V}_{a^n}(k, \phi|x_e^n) \ldots \right)
\]

\[
\Pr[(K', \Phi') = (k, \phi)|x_e^n, s^n] \tag{74}
\]
where \( K'_a = f_a(X'_a^n; s^n) \) and \( \Phi' = g(X'_a^n; s^n) \). \( X'_a \) is a random variable conditionally independent of \( X_a \):

\[
p_{X'_a | X_a, S}(x'_a | x_a, s) = p_{X'_a | X_a, S}(x'_a | x_a, s)p_{X_a | X_a, S}(x_a | x_a, s).
\]

Let \( A(x''_a) \) be the event \( X''_a^n = x''_a^n \) and \( B \) be the event \( (K'_a, \Phi') = (k_a, \phi) \). We can bound the probability inside the logarithm as

\[
\sum_{k, \phi} \tilde{V}_S(k, \phi | x''_a^n) \Pr[(K', \Phi') = (k, \phi) | x''_a^n, s^n] = \sum_{k, \phi} \sum_{x''_a \in \Omega_{k, \phi, a, n}} V_S(x''_a | x'_a^n) \left( \Pr[B \cap A(x''_a^n) | x''_a^n, s^n] + \Pr[B \cap A(x''_a^n)^c | x''_a^n, s^n] \right)^\alpha
\]

\[
\leq \sum_{k, \phi} \sum_{x''_a \in \Omega_{k, \phi, a, n}} V_S(x''_a | x'_a^n) \left( V_S(x''_a | x'_a^n)^\alpha + \frac{1}{|K||M|} \right)
\]

\[
\leq \frac{1}{|K||M|} + \sum_{x''_a} V_S(x''_a | x'_a^n)^{1+\alpha}
\]

The first term in (a) follows because

\[
\Pr[B \cap A(x''_a^n) | x''_a^n, s^n] = \Pr[B \cap A(x''_a^n) | x''_a^n, s^n] \Pr[A(x''_a^n) | x''_a^n, s^n] = \Pr[A(x''_a^n) | x''_a^n, s^n] = V_S(x''_a | x'_a^n)
\]

due to \( \Pr[B \cap A(x''_a^n)] = 1 \) and the distribution of \( X''_a^n \).

The second term follows because the probability that a random binning code maps distinct sequences to the same key (resp. public message) is \( \frac{1}{|K||M|} \) (resp. \( \frac{1}{|M|} \)). Step (b) follows because

\[
(x + y)^\alpha \leq x^{\alpha} + y^{\alpha} \quad \text{for} \quad 0 \leq \alpha \leq 1.
\]

We continue (72) by pulling out a term that depends only on \( \log |K||M| = n(R_M + R_{SK}) \) and taking the sum over \( x''_a \) into the logarithm through an application of Jensen’s inequality.

\[
H(K'_a, \Phi | X'_a^n, S^n = s^n) \geq n(R_M + R_{SK}) \ldots
\]

\[
- \frac{1}{\alpha} \log \left( 1 + e^{\alpha(R_M + R_{SK})} \sum_{x''_a} \tilde{Q}_S(x''_a) \sum_{x''_a} V_S(x''_a | x'_a^n)^{1-\alpha} \right)
\]

\[
\geq n(R_M + R_{SK}) - \frac{1}{\alpha} \exp \left( -n \left[ F_0(\alpha, P_s^n) - \alpha(R_M + R_{SK}) \right] \right)
\]

(73)

where for the second inequality we apply the relation \( \log(1 + x) \leq x \) and let

\[
F_0(\alpha, P_s^n) = -\frac{1}{n} \log \left( \sum_{x''_a} \tilde{Q}_S(x''_a) \sum_{x''_a} V_S(x''_a | x'_a^n)^{1+\alpha} \right)
\]

Using the memoryless property of the source, we further simplify \( F_0(\alpha, P_s^n) \)

\[
F_0(\alpha, P_s^n) = -\frac{1}{n} \log \left( \prod_{i=1}^n \tilde{Q}_S(x_i) \sum_{x_i} V_{S_i}(x_i | x_i)^{1+\alpha} \right) = -\frac{1}{n} \log \left( \prod_{i \in S} \left[ \sum_{x_i} \tilde{Q}_S(x_i) \sum_{x_i} V_{S_i}(x_i | x_i)^{1+\alpha} \right]^{n_p}(s) \right) = \sum_{s \in S} P_s(s) \tilde{F}_0(\alpha, s)
\]

(75)

where

\[
\tilde{F}_0(\alpha, s) = -\log \left( \sum_{x_i} \tilde{Q}_S(x_i) \sum_{x_i} V_{S_i}(x_i | x_i)^{1+\alpha} \right)
\]

We complete the proof by combining (69), (73), (75) and letting \( P_s^n \to p_S \) as \( n \to \infty \).

D. Proof of Theorem 3

The properties of \( \tilde{E}_0(\rho, s) \) are developed in [23, Theorem 2]. Here we show the properties of \( \tilde{F}_0(\alpha, s) \).

It is easy to check \( \tilde{F}_0(0, s) = 0 \). Taking the derivative

\[
\frac{\partial \tilde{F}_0(\alpha, s)}{\partial \alpha} = -\sum_{x_i} \tilde{Q}_S(x_i) \sum_{x_i} V_{S_i}(x_i | x_i)^{1+\alpha} \log V_{S_i}(x_i | x_i)
\]

\[
\sum_{x_i} \tilde{Q}_S(x_i) \sum_{x_i} V_{S_i}(x_i | x_i)^{1+\alpha} \log V_{S_i}(x_i | x_i)
\]

we see \( \frac{\partial \tilde{F}_0(\alpha, s)}{\partial \alpha} \geq 0 \) for \( \alpha \geq 0 \). Thus, \( \tilde{F}_0(\alpha, s) \) is an increasing non-negative function for \( \alpha \geq 0 \). Also, \( \frac{\partial \tilde{F}_0(\alpha, s)}{\partial \alpha} \) equals \( H(X_a | X_e, S = s) \) when \( \alpha = 0 \). To see \( \tilde{F}_0(\alpha, s) \) is a concave function for \( \alpha \geq 0 \), let \( \alpha_3 = \lambda \alpha_1 + (1-\lambda)\alpha_2 \) where \( 0 < \lambda < 1 \).

\[
\sum_{x_i} \tilde{Q}_S(x_i) \sum_{x_i} V_{S_i}(x_i | x_i)^{1+\alpha_3}
\]

\[
= \sum_{x_i} \tilde{Q}_S(x_i) \left( \sum_{x_i} V_{S_i}(x_i | x_i)^{\lambda(1+\alpha_1)} V_{S_i}(x_i | x_i)^{(1-\lambda)(1+\alpha_2)} \right)
\]

\[
\leq \sum_{x_i} \tilde{Q}_S(x_i) \left( \sum_{x_i} V_{S_i}(x_i | x_i)^{1+\alpha_1} \right)^\lambda
\]

\[
\times \left( \sum_{x_i} V_{S_i}(x_i | x_i)^{1+\alpha_2} \right)^{1-\lambda}
\]

\[
\leq \left( \sum_{x_i} \tilde{Q}_S(x_i) \sum_{x_i} V_{S_i}(x_i | x_i)^{1+\alpha_2} \right)^{1-\lambda}
\]

(74)

where (i) follows by Hölder’s inequality:

\[
\sum_i a_i b_i \leq \left( \sum_i a_i^{1/\gamma} \right)^\gamma \left( \sum_i b_i^{1/(1-\gamma)} \right)^{1-\gamma},
\]

for \( 0 \leq \gamma \leq 1 \) where we use \( \gamma = \lambda \), and (ii) follows by a variant of Hölder’s inequality [29, Problem 4.15]:

\[
\sum_i p_i a_i b_i \leq \left( \sum_i p_i a_i^{1/\gamma} \right)^\gamma \left( \sum_i p_i b_i^{1/(1-\gamma)} \right)^{1-\gamma},
\]
where $0 \leq \gamma \leq 1$, $\sum p_i = 1$, and again we select $\gamma = \lambda$. Taking $-\log(\cdot)$ on both sides, we get

$$F_0(\alpha_3, s) \geq \lambda F_0(\alpha_1, s) + (1 - \lambda) F_0(\alpha_2, s).$$

\[E. \text{ Proof of Theorem 4}\]

In the equal-SNR case ($\gamma_a = \gamma_b = \gamma$), the secret key rate achieved using an on-off sounding with parameter $\lambda$ is $\lambda I_K(\gamma/\lambda)$ where $I_K(x) = \log(1 + x^2/(1 + 2x))$, cf. (33)–(34). In (48) we use $\lambda_c$ to denote the optimal on-off sounding parameter. Let $\tilde{I}_K(\gamma) = \lambda_c I_K(\gamma/\lambda_c)$. We note that $\tilde{I}_K(\gamma)$ is increasing and concave in $\gamma$. The latter follows from the observation made in Section IV-B that $I_K(\gamma)$ is concave at high-SNR and due to the time-sharing. We now show that $\tilde{I}_K(\gamma)$ is the secret key capacity of this system.

We start by bounding the secret key capacity from above by Theorem 1. In the following $\mathcal{P}_S = \{p_S: E[|S|^2] \leq \mathcal{E}\}$ is the allowable set of sounding signals and $\gamma = \mathcal{E}/\sigma^2$ is the maximum achievable system SNR.

$$C_K \leq \max_{p_S \in \mathcal{P}_S} I(X_a; X_b|S) = \max_{p_S \in \mathcal{P}_S} \sum_{s \in \mathcal{S}} I(X_a; X_b|S = s)p_S(s)$$

$$= \max_{p_S \in \mathcal{P}_S} \sum_{s \in \mathcal{S}} \left[ \tilde{I}_K \left( \frac{|s|^2}{\sigma^2} \right) \right] p_S(s)$$

$$\leq \max_{p_S \in \mathcal{P}_S} \sum_{s \in \mathcal{S}} \left[ \max_{\lambda \leq \mathcal{S} \leq 1} \lambda \tilde{I}_K \left( \frac{|s|^2}{\sigma^2 \lambda} \right) \right] p_S(s)$$

$$= \max_{p_S \in \mathcal{P}_S} \sum_{s \in \mathcal{S}} \tilde{I}_K \left( \frac{|s|^2}{\sigma^2} \right) p_S(s)$$

$$\leq \max_{p_S \in \mathcal{P}_S} \tilde{I}_K(\gamma_{p_S}) \leq \tilde{I}_K(\gamma),$$

where the last inequality follows from the concavity of $\tilde{I}_K(\cdot)$ and $\gamma_{p_S}$ is the SNR achieved by distribution $p_S$.

\[F. \text{ Proof of Theorem 6}\]

To characterize the achievable error exponents of EDMSSs with continuous random variables, in Appendix A we study the exponents achieved in a discretized (quantized) system and let the quantization get increasingly fine. In the limit the finite sum over the probability mass function (PMF) in (24) is replaced by an integral across a probability density function (PDF), and entropy in (31) is replaced by differential entropy. The resulting form of the exponent is

$$E_R(R_{SK}) = \max_{p_S \in \mathcal{P}_S} \max_{0 \leq \rho \leq 1} \rho [h(X_a|S) - R_{SK}] - E_0(\rho, p_S)$$

$$E_0(\rho, p_S) = \int s p_S(s) \left[ \log \int_{x_b} Q_s(x_b) \ldots \left( \int_{x_a} W_s(x_a|x_b) \frac{1}{1 + \rho} dx_a \right)^{1+\rho} dx_b \right] ds$$

(76)

For the rest of this section we consider the special case of Theorem 6, namely when the input sounding signal is a constant signal, i.e., $p_S(s) = \delta(s - s_0)$ with $\frac{|s_0|^2}{\sigma^2} = \gamma$. First note that since $s = s_0$ with probability one,

$$E_0(\rho, p_S) = \log \int_{x_b} Q_s(x_b) \left( \int_{x_a} W_s(x_a|x_b) \frac{1}{1 + \rho} dx_a \right)^{1+\rho} dx_b$$

(78)

Next, due to the use of a constant sounding signal, $X_a$ and $X_b$ are jointly Gaussian complex random variables. Their distribution is

$$\mathcal{CN} \left(0, \begin{bmatrix} \sigma^2 & \eta \sigma_a \sigma_b \\ \eta^2 \sigma_a \sigma_b & \sigma_b^2 \end{bmatrix} \right)$$

where $\eta$ is the correlation coefficient. In the case of the signal model considered in Section II-C, cf. (9a)-(9b), one can verify the relations

$$\sigma^2 = \sigma_b^2 = (1 + \gamma) \sigma^2,$$

$$\eta = \gamma + 1.$$

(79)

\[80\]

The conditional PDF $W_s(x_a|x_b)$ is also complex Gaussian with distribution $\mathcal{CN} \left(m_{a|b}, \sigma^2_{a|b} \right)$ where

$$m_{a|b} = \frac{\eta \sigma_a}{\sigma_b} y = \frac{\gamma}{1 + \gamma} y,$$

$$\sigma^2_{a|b} = (1 - \eta^2) \sigma_a^2 = \frac{\sigma^2_a}{1 + \gamma_{eq}},$$

and $\gamma_{eq} = \gamma^2/(1 + 2\gamma)$.

With these distributions, after some calculation it can show the inner integral of (78) is $(\pi \sigma^2_{a|b})^{-1} (1 + \rho)$ and (78) simplifies to

$$E_0(\rho, p_S) = \rho \log(\pi \sigma^2_{a|b}) + (1 + \rho) \log(1 + \rho).$$

To find $E_R(R_{SK}, \gamma)$, we take a partial derivative with respect to $\rho$ of $\rho [h(X_a|S) - R_{SK}] - E_0(\rho, p_S)$. Setting the result equal to zero yields

$$R_{SK} = h(X_a|S = s_0) - \frac{\partial E_0(\rho, p_S)}{\partial \rho}$$

$$= \log(\pi \sigma^2_a) - \log(\pi \sigma^2_{a|b}(1 + \rho))$$

$$= \log \left( \frac{1 + \gamma_{eq}}{1 + \rho} \right)$$

(80)

where $h(X_a|S = s_0) = \log(\pi \sigma^2_a)$ since the variables are jointly complex Gaussians. Using the relation $I_K(\gamma) = \log(1 + \gamma_{eq})$ we can solve for $\rho$ as

$$\rho = \exp[I_K(\gamma) - R_{SK}] - 1.$$  

(81)

Since $0 \leq \rho \leq 1$, the $\rho$ specified in (81) optimizes (78) only when $I_K(\gamma) - \log 2 \leq R_{SK} \leq I_K(\gamma)$. We conclude that, when $\gamma_{eq} \geq 1$, the error exponent expressed in terms of $\gamma$ falls into three regions. First, if $R_{SK} \geq I_K(\gamma)$ then

$$E_R(R_{SK}, \gamma) = 0.$$  

Next, if $I_\gamma(\gamma) \leq R_{SK} < I_K(\gamma)$, where $I_\gamma(\gamma) = \log \left( \frac{1 + \gamma_{eq}}{2} \right)$, then

$$E_R(R_{SK}, \gamma) = \rho[I_K(\gamma) - R_{SK} + 1] - (1 + \rho) \log(1 + \rho).$$
And, finally, if $0 \leq R_{SK} < I_c(\gamma)$

$$E_R(R_{SK}, \gamma) = I_K(\gamma) - R_{SK} + 1 - 2 \log 2.$$  

When $0 \leq \gamma_{eq} < 1$, only the first two regions exist since $I_c(\gamma) < 0$.

VI. CONCLUSIONS

We investigate secret key generation from EDMS in this paper. We characterize secret key capacity and show the strong achievability of secrecy and reliability. This achievable region shows the tradeoff between secrecy and reliability. The results are applied to a case in which the EDMS is the output of Rayleigh fading channels when the participants transmit sounding signals to excite the channel randomness. We show that an on-off signal can achieve secret key capacity for all SNRs. The capacity-achieving on-off signal has a vanishing duty cycle when SNR approaches zero. An on-off sounding signal also achieves a higher error exponent than a uniform sounding signal. All these improvements due to choosing an input sounding distribution have a great impact on energy consumption in the low-SNR regime.

APPENDIX A

RELIABILITY EXPONENT OF CONTINUOUS RANDOM VARIABLES

To deal with continuous random variables, such as jointly Gaussian variables, we quantize the variables, apply (31), (23) – (24), and characterize the limit of increasingly fine quantization. Let $X_a^b$, $X_b^c$ be the quantized versions of continuous random variables $X_a$ and $X_b$ with uniform step size $\Delta$. Let $Q_s(x_a, x_b)$ denote the joint PDF indexed by $S = s$, i.e., $Q_s(x_a, x_b) = p_{X_a, X_b}(x_a, x_b|S)$. Similarly, let $Q_s(x_b)$ and $W_s(x_a|x_b)$ denote its marginal and conditional distributions, respectively. Finally, let $Q_s^a(j, i)$, $Q_s^b(j, i)$ and $W_s^a(j, i)$ be the corresponding quantized PMFs. By the mean value theorem,

$$Q_s^a(j, i) W_s^a(j, i) = Q_s^a(j, i),$$

$$= \int_{x_a = j}^{(j+1)\Delta} \int_{x_a = i}^{(i+1)\Delta} Q_s(x_a, x_b) dx_a dx_b,$$

$$= Q_s(x_a, x_b) \Delta^2 = \sum_{s} W_s(x_a, x_b) \Delta^2,$$

for some $x_a, x_b \in (i\Delta, (i+1)\Delta)$ and $x_a, x_b \in (j\Delta, (j+1)\Delta)$. Applying (24) to the quantized variables gives

$$E_0^s (\rho, s) = \log \sum_j \left( \sum_i [Q_s(x_a, x_b) W_s(x_a, x_b) \rho^{a+b+\gamma} \Delta^{1+\rho} \Delta^{-\rho}] \right)^{1+\rho}.$$

Substituting this into (31) for a fixed $s$ gives

$$\max_{0 \leq \rho \leq 1} \rho \left( H(X_a^b | S = s) - R_{SK} - E_0^s (\rho, s) \right)$$

$$= \max_{0 \leq \rho \leq 1} \rho \left[ H(X_a^b | S = s) + \log \Delta - R_{SK} \right]$$

$$- \log \left( \sum_j \Delta Q_s(x_{b,j}) \left( \sum_i \Delta W_s(x_{a,i} | x_{b,j}) \right)^{1+\rho} \right).$$

In the limit of increasingly fine quantization, i.e., as $\Delta$ approaches 0, $H(X_a^b | S = s) + \log \Delta$ approaches $h(X_a | S = s)$, and the summation inside the logarithm approaches to an integral form. Thus, we can design a system whose reliability function can be made arbitrarily close to

$$E_R(R_{SK}) = \max_{0 \leq \rho \leq 1} \max_{p_0 \in P_0} \rho [h(X_a | S) - R_{SK}] - E_0(\rho, p_S),$$

where $E_0(\rho, p_S)$ is of the form (77).

APPENDIX B

TRANSITION PROBABILITY OF BINARY CHANNEL QUANTIZATION

Consider the equivalent Gaussian channel model presented in (42)–(44). We can write the equation for the real part as

$$Y = \beta X + W$$

(82)

where

$$\beta X \sim \mathcal{N}(0, \sigma_1^2), \quad \sigma_1^2 = \frac{\sigma_a^2}{\mathcal{E}^2 + \sigma_a^2}$$

(83)

$$W \sim \mathcal{N}(0, \sigma_0^2), \quad \sigma_0^2 = \frac{1}{2} \left( \mathcal{E} + \sigma_1^2 - \left( \frac{\mathcal{E}}{\mathcal{E} + \sigma_1^2} \right)^2 \right).$$

(84)

Let $\mathcal{H}_0 = \{x : x \geq 0\}$ and $\mathcal{H}_1 = \{x : x < 0\}$. Then, the transition probability can be calculated to be

$$\theta = \Pr[Y \in \mathcal{H}_1 | X \in \mathcal{H}_0] = \frac{\Pr[Y \in \mathcal{H}_1, X \in \mathcal{H}_0]}{\Pr[X \in \mathcal{H}_0]}$$

$$= 2 \int_{x \in \mathcal{H}_0} \Pr[Y \in \mathcal{H}_1 | X = x] p_X(x) dx$$

$$= 2 \int_{x > 0} \Pr[\beta X + W < 0 | X = x] p_X(x) dx$$

$$= 2 \int_{x > 0} \frac{1}{2} \left[ 1 - \text{erf} \left( \frac{x}{\sqrt{2\sigma_1^2}} \right) \right] \frac{1}{\sqrt{2\pi\sigma_0^2}} \exp \left( -\frac{x^2}{2\sigma_1^2} \right) dx$$

$$= 1 - \frac{1}{\sqrt{2\pi\sigma_1^2}} \int_{x > 0} \frac{1}{\sqrt{2\pi\sigma_0^2}} \exp \left( -\frac{x^2}{2\sigma_1^2} \right) dx$$

$$= 1 - \frac{1}{\sqrt{\sigma_0^2}} \arctan \left( \frac{\sigma_1}{\sigma_0} \right).$$

The last equality follows from the formula

$$\int_0^\infty e^{-b^2x^2} dx = \frac{1}{\sqrt{\pi b}} \arctan \left( \frac{\sigma_1}{\sigma_0} \right), \quad \text{for } b \neq 0.$$
APPENDIX C
ERROR EXPONENT OF BINARY SOURCES

For a discrete memoryless source \((X, Y)\) with distribution \(Q(y)W(x|y)\), in [23, Theorem 4] Gallager shows that the error exponent can be expressed as a generalized entropy function

\[
E_R = H(X, Y | R, Y) \triangleq \sum_{x, y} Q_{R}(y) W_{R}(x|y) \log \frac{Q_{R}(y) W_{R}(x|y)}{Q(y) W(x|y)} ,
\]

where \(0 \leq \rho \leq 1\) and \(Q_{R}(y)\) and \(W_{R}(x|y)\) are tilted distributions defined as

\[
Q_{R}(y) = \frac{Q(y) \left( \sum_{x} W(x|y)^{1/(1+\rho)} \right)^{(1+\rho)}}{\sum_{y} Q(y) \left( \sum_{x} W(x|y)^{1/(1+\rho)} \right)^{(1+\rho)}} ,
\]

\[
W_{R}(x|y) = \frac{W(x|y)^{1/(1+\rho)}}{\sum_{x} W(x|y)^{1/(1+\rho)}} .
\]

The message rate is parameterized by \(\rho\) and has the form

\[
R_M = H(X|Y_{\rho}) \triangleq \sum_{y} -Q_{R}(y) W_{R}(x|y) \log W_{R}(x|y) .
\]

For a binary source \((Q(y), W(x|y)) = (\frac{1}{2}, \frac{1}{2})\) and symmetric transition probability \(W(x|y) = \theta\) if \(x \neq y\) and \(W(x|y) = 1 - \theta\) if \(x = y\), \(Q_{R}(y)\) is uniformly \((\frac{1}{2}, \frac{1}{2})\) distributed and

\[
W_{R}(x|y) = \frac{\theta^{1/(1+\rho)}}{\theta^{1/(1+\rho)} + (1 - \theta)^{1/(1+\rho)}} \triangleq \tau\] if \(x \neq y\).

If \(0 \leq \rho \leq 1\) then \(0 \leq \tau \leq \frac{\sqrt{\theta}}{\sqrt{\theta} + \sqrt{1 - \theta}}\) and \(R_M\) is in the range

\[
H_B(\theta) \leq R_M \leq H_B \left( \frac{\sqrt{\theta}}{\sqrt{\theta} + \sqrt{1 - \theta}} \right) .
\]

The corresponding error exponent (85) can be simplified to

\[
E_R(R_M) = H(X|Y_{\rho}) \| XY' = \tau \log \frac{\tau}{\tau} + (1 - \tau) \log \frac{1 - \tau}{1 - \tau} = T_B(\tau) - H_B(\tau) ,
\]

where \(H_B(\cdot)\) is the binary entropy function and \(T_B(\tau) \triangleq -\tau \log(\tau) - (1 - \tau) \log(1 - \tau)\). When \(R_M < H_B(\theta)\) one finds that \(E_R(R_M) = 0\) (by choosing \(\rho = 0\)). When \(R_M > H_B \left( \frac{\sqrt{\theta}}{\sqrt{\theta} + \sqrt{1 - \theta}} \right)\), \(E_R(R_M)\) is maximized by \(\rho = 1\).

The resulting error exponent is

\[
E_R(R_M) = R_M - 2 \log(\sqrt{\theta} + \sqrt{1 - \theta}) .
\]

REFERENCES


