Minimum Energy Per Bit for Secret Key Acquisition Over Multipath Wireless Channels

Tzu-Han Chou
Electrical and Computer Engineering
University of Wisconsin
Madison, WI 53706, USA
Email: tchou2@wisc.edu

Akbar M. Sayeed
Electrical and Computer Engineering
University of Wisconsin
Madison, WI 53706, USA
Email: akbar@engr.wisc.edu

Stark C. Draper
Electrical and Computer Engineering
University of Wisconsin
Madison, WI 53706, USA
Email: sdraper@ece.wisc.edu

***Abstract*—We study fundamental limits on the generation of secret keys based on the randomness inherent to reciprocal wireless multipath channels. Estimates of the common channel at the two ends of a link are jointly Gaussian sources from which secret keys can be generated. The key generation problem is cast as an equivalent communication problem to characterize the secret key capacity. We analyze the low-SNR regime to quantify the minimum energy per secret key bit required for reliable key acquisition. Our results show that, in contrast to the low SNR behavior of conventional channel capacity, there is a non-zero SNR γ^* that achieves the minimum energy per key bit. A time-sharing scheme is proposed to achieve the minimum energy per key bit at any SNR below γ^*. We also investigate the reliability of secret key generation via error exponent analysis. In particular, our results yield a tight upper bound on the minimum energy required to generate a finite-length key with a specified probability of error in key acquisition.**

I. Introduction

Unconditional security, in contrast to computational security (of, e.g., public-key cryptography) is not based on hardness assumptions of certain mathematical problems. Shannon's one-time pad [1] was the first example of unconditional security. If a secret key that is at least as large as the unencrypted plaintext is shared by two users, then Shannon showed that the ciphertext can be made independent of the plaintext, revealing nothing about the original source. Unfortunately, this solution relies on the secure distribution of large secret keys, itself a difficult problem.

An alternate approach is to *generate* a secret key from sources of dependent randomness available to two users. A public discussion between the users is allowed to assist in the process. Here the technical hurdles are two-fold. First, how can the two sources of randomness be reconciled to produce a common source of identical randomness that can serve as a secret key? Second, how can the discussion be structured so as not to leak any information about the key to an eavesdropper? Maurer [2] and Ahlswede and Csiszár [3] show that this type of key-generation is possible. If the two legitimate users A and B observe dependent discrete memoryless random sources X and Y, and the eavesdropper E observes a third dependent random source Z, then the supremum of reliable secret key rate (Theorem 1 of [3]) is

$$C_{\mathrm{s}} = \max\left(I(T;Y|U) - I(T;Z|U)\right) \qquad (1)$$

which is called *secret key capacity*. The maximization in (1) is over all auxiliary variables U,T satisfying Markov condition $U{-}T{-}X{-}YZ$. Furthermore, the secret key capacity is upper bounded by

$$C_{\mathrm{s}} \leq I(X;Y|Z)\ . \qquad (2)$$

Based on N observations X^N and Y^N, the secret keys can be generated by one way discussion: user A generates the key $K_A = Q(X^N)$ and forwards message M to user B via public channel and user B generates the common key $\hat{K}_A$ based on Y^N and M (i.e., $\hat{K}_A = \hat{Q}(Y^N, M)$). The error probability $\Pr[K_A \neq \hat{K}_A]$ can be made arbitrarily small if N is sufficiently large. The public message M plays a crucial role. Without such a discussion the rate at which identical randomness can (with high probability) be extracted from two general sources of dependent randomness is zero [4].

Once cast into this setting, the generation of secret keys from dependent sources of randomness with a public discussion can be seen to be a type of distributed source coding problem. As such, it can be described in the Slepian-Wolf framework [5]. Reliable recovery of K_A requires the rate of the message M to be greater than $H(X|Y)$.

In wireless communications, the channel itself is a source of randomness resulting from multipath fading. In particular, when transmissions are bi-directional and in the same frequency (e.g., time-division duplexed systems), the reciprocity property [6] of electromagnetic wave propagation assures that both users observe the same channel. In this setting, K_A and $\hat{K}_A$ involve estimates of the common random channel at the respective users. For wideband and multi-antenna channels, the resulting keys can be quite large due to the large number of independent channel parameters. Secrecy from eavesdroppers is ensured by the physics of propagation: in a rich multipath environment, if the eavesdropper is physically separated (even by a few wavelengths) from the legitimate users, its channel output Z will be nearly statistically independent of X and Y. For these reasons, reciprocal wireless channels provide an attractive source of randomness for key generation. Previous related works include Hassan et al. [7] who use coding to improve the probability of key acquisition without the public message M, Wilson et al. [8] who study the ultrawideband channel and use a Slepian-Wolf scheme, and Sayeed et al. [9] who consider an uncoded communication protocol and analyze the minimum energy required for key acquisition.

In [10] Wyner provides the crucial insight that underlies all implementations of Slepian-Wolf coding: the distributed source coding problem, at its core, is a channel coding problem. In a similar vein, in this paper we cast the key acquisition problem into an equivalent communication problem.

Our main results involve quantifying two fundamental limits: the secret key capacity and the reliability (error exponents) of key generation in reciprocal wireless channels. We consider limits on key generation from the unquantized Gaussian sources that result from transmitting known training signals over reciprocal wireless channels and derive the secret key capacity by optimizing over the space of training signals with a given power constraint. We study the low-SNR regime to quantify the *minimum energy per key bit* required for reliable key generation. In contrast to the behavior of conventional channel capacity, the secret key capacity is not a concave function of SNR γ. As a result, the minimum energy per key bit is achieved at a non-zero SNR that we denote γ^*. We develop time-sharing strategies for achieving the minimum energy per key bit at any SNR below γ^*. Finally, we also study the reliability of our system via error exponent analysis. In particular, we bound the energy required to generate a key of a fixed finite length as a function of the probability of error in key acquisition.

II. System Model

Consider a wireless channel consisting of N parallel independently fading channels (e.g., OFDM sub-carriers). We assume that the parallel channel is static over at least two channel uses. Users A and B sequentially send a training signal, $\mathbf{d} = [d_1 \, d_2 \ldots d_N] \in \mathbb{C}^N$, over two uses of the parallel channel to estimate the channel. The received signals at A, B and E are

$$\begin{aligned} \mathbf{x}_A &= \mathbf{H}_{AB}\mathbf{d} + \mathbf{n}_A, & \mathbf{x}_B &= \mathbf{H}_{BA}\mathbf{d} + \mathbf{n}_B, \\ \mathbf{x}_{EA} &= \mathbf{H}_{EA}\mathbf{d} + \mathbf{n}_{EA}, & \mathbf{x}_{EB} &= \mathbf{H}_{EB}\mathbf{d} + \mathbf{n}_{EB}, \end{aligned} \tag{3}$$

where $\mathbf{n}_A \sim \mathcal{CN}\left(0, \sigma_A^2 \mathbf{I}_N\right)$ is the receiver noise at A, the $N \times N$ matrix $\mathbf{H}_{AB} = \operatorname{diag}(\mathbf{h}_{AB})$ where $\mathbf{h}_{AB} = \begin{bmatrix} H_{AB,1} & H_{AB,2} & \cdots & H_{AB,N} \end{bmatrix}^{\mathrm{T}}$ is the vector of channel gains. We consider Rayleigh fading channel $\mathbf{h}_{AB} \sim \mathcal{CN}\left(0, \mathbf{\Lambda}_{AB}\right)$. Other channel matrices and noise vectors are defined similarly. The noise vectors are independent of each other. We assume channel reciprocity whereby $\mathbf{h}_{AB} = \mathbf{h}_{BA} = \mathbf{h}$, and assume sufficiently rich scattering so that that this common channel $\mathbf{h}$ is independent of the eavesdropper channels $\mathbf{h}_{EA}$ and $\mathbf{h}_{EB}$. In this paper we focus on i.i.d. parallel fading channels and assume, without loss of generality, that the channel gains are of unit-variance, i.e., $\mathbf{\Lambda}_{AB} = \mathbf{I}_N$. In the case where $\frac{1}{N}\sum_{k=1}^{N}|d_k|^2 \leq \mathcal{E}_s$, (3) becomes N i.i.d. parallel channels in which the average signal-to-noise ratio (*per dimension* or *per sub-carrier*) at A is defined as $\gamma_A = \frac{\mathcal{E}_s}{\sigma_A^2}$. γ_B is defined similarly.

III. Main Results

In practice secret key generation involves estimation of $\mathbf{h}$ at both A and B (from $\mathbf{x}_A$ and $\mathbf{x}_B$), followed by quantization and reconciliation (i.e., the public discussion), resulting in the keys K_A and $\hat{K}_A$. Each pair of random variables at A and B associates with an equivalent channel, for example, $P_{\mathbf{x}_B|\mathbf{x}_A}$. Since the eavesdropper channels are independent of $\mathbf{h}$, for a given training signal $\mathbf{d}$, $\mathbf{x}_E = (\mathbf{x}_{EA}, \mathbf{x}_{EB})$ is conditionally independent of $\mathbf{x}_A$ and $\mathbf{x}_B$. By this independence, $\frac{1}{N}I(\mathbf{x}_A;\mathbf{x}_B|\mathbf{x}_E) = \frac{1}{N}I(\mathbf{x}_A;\mathbf{x}_B)$ bounds the achievable *secret key rate* R_{s}. In the i.i.d. parallel channel setting mentioned in previous section, the secret key capacity is found by optimizing over $\mathbf{d}$ satisfying $\frac{1}{N}\sum_{k=1}^{N}|d_k|^2 \leq \mathcal{E}_s$. This can be considered that the training symbol is i.i.d. random variable D with distribution in the set $\mathcal{D} = \{P_D : E[|D|^2] \leq \mathcal{E}_s\}$. (3) simplifies to

$$X_{A,k} = D_k H_k + N_{A,k}, \quad X_{B,k} = D_k H_k + N_{B,k} \ , \tag{4}$$

where the channels are i.i.d. for $1 \leq k \leq N$. $X_{E,k}$ is defined accordingly. The following Theorem 1 shows that the secret key capacity can be found by choosing the distribution of D in the set $\mathcal{D}$ that maximizes the conditional mutual information $I(X_A;X_B|D)$. As we will see, the optimal D is a deterministic at high SNR but corresponds to time-sharing at low SNR. This means the capacity-achieving training signal at low SNR is peaky. As noted in the Introduction, approaching these performance limits (e.g., via Slepian-Wolf coding) requires additional information M exchange between A and B. Thus, implicit in our analysis is an error-free public channel. For simplicity, in this paper we ignore the energy costs associated with transmission of M.

A. Secret Key Capacity

Theorem 1: Let D have distribution P_D where the realization of D is known by all users (including eavesdropper). When D satisfies average energy constraint, the secret key capacity of i.i.d. fading channel is

$$C_{\mathrm{s}} = \max_{P_D \in \mathcal{D}} I(X_A;X_B|D) \ . \tag{5}$$

Proof: From (2), the secret key capacity is upper bounded by $I(X_A, D; X_B, D|X_E, D) = I(X_A;X_B|D)$. From (1) and let $U = \text{const}$, $T = X = (X_A, D)$, $Y = (X_B, D)$ and $Z = (X_E, D)$, C_{s} is lower bounded by [1]

$$\begin{aligned} C_{\mathrm{s}} &\geq I(X_A, D; X_B, D) - I(X_A, D; X_E, D) \\ &= h(X_A, D|X_E, D) - h(X_A, D|X_B, D) \\ &= h(X_A|D) - h(X_A|X_B, D) = I(X_A;X_B|D) \ , \end{aligned}$$

which is equal to the upper bound. Here uses the fact that condition on D, X_E is independent of X_A and X_B. Optimizing over $P_D \in \mathcal{D}$ to get secret key capacity. ■

Corollary 1: (Deterministic training signal) In the case when $D = d$ (i.e., $D = d$ with probability one) and $|d|^2 = \mathcal{E}_s$, the achievable secret key rate as function of SNR is [2]

$$I_{\mathrm{s}}(\gamma) = \log(1 + \gamma_{\mathrm{eq}}) \ \text{nats/dimension} \tag{6}$$

$$\gamma_{\mathrm{eq}} = \left(\frac{1}{\gamma_A} + \frac{1}{\gamma_B} + \frac{1}{\gamma_A \cdot \gamma_B}\right)^{-1} \tag{7}$$

[1] $h(\cdot)$ is the differential entropy

[2] Thoroughout the paper, $\log(\cdot)$ and $\log_2(\cdot)$ refer to the logarithm in base e and 2, respectively.

Proof: From (4), $[X_A, X_B]^{\mathrm{T}} \sim \mathcal{CN}\left(0, \mathbf{K}_{AB}\right)$, where

$$\mathbf{K}_{AB} = \begin{bmatrix} \mathcal{E}_s + \sigma_A^2 & \mathcal{E}_s \\ \mathcal{E}_s & \mathcal{E}_s + \sigma_B^2 \end{bmatrix}$$

Since d is constant

$$\begin{aligned} I_{\mathrm{s}}(\gamma) &= I(X_A; X_B) = h(X_A) + h(X_B) - h(X_A, X_B) \\ &= \log\left(\frac{(\mathcal{E}_s + \sigma_A^2)(\mathcal{E}_s + \sigma_B^2)}{|\mathbf{K}_{AB}|}\right) = \log\left(1 + \gamma_{\mathrm{eq}}\right). \end{aligned}$$

■

Remark: The secret key rate function in (6) has the same form as conventional AWGN channel capacity by replacing SNR γ with γ_{eq}. This can be examined by noting the fact that the equivalent channel $P_{X_B|X_A}$ can be expressed in terms of an additive Gaussian noise model. Rewriting X_B in terms of its minimum mean-squared error estimate (MMSE) from X_A, we get

$$\begin{aligned} X_B &= \frac{E[X_B X_A^*]}{E[|X_A|^2]} X_A + W_B \\ &= \beta X_A + W_B \ , \end{aligned} \tag{8}$$

where $\beta = \frac{\mathcal{E}_s}{\mathcal{E}_s + \sigma_A^2}$. Since X_A and X_B are jointly Gaussian with zero mean (recall that d is known), the error in the estimate, W_B, is also zero-mean Gaussian and independent of X_A due to the orthogonality principle and Gaussianity. Using $E[|W_B|^2] = E[|X_B|^2] - E[|\beta X_A|^2]$, we get the overall signal to noise ratio $\frac{|\beta|^2 E[|X_A|^2]}{E[|W_B|^2]} = \gamma_{\mathrm{eq}}$.

From (7) we see that if we fix one user's SNR, say γ_B, and let $\gamma_A \to \infty$, then $\gamma_{\mathrm{eq}} \to \gamma_B$. The secret key capacity is thus dominated by the lower of the two SNRs. This is because the equivalent channel $P_{X_B|X_A}$ is induced by two underlying noisy channels and the compound channel is dominated by the worst noise in the extreme cases. It is often reasonable to assume that the two users operate at the same SNR or at nearly the same SNRs. In the rest of the paper we assume that $\gamma_A = \gamma_B = \gamma$, for which

$$\gamma_{\mathrm{eq}} = \frac{\gamma^2}{2\gamma + 1} \ . \tag{9}$$

In the high-SNR regime, $\gamma_{\mathrm{eq}} \approx \gamma/2$ because the equivalent (compound) channel embeds twice the noise and $I_{\mathrm{s}}(\gamma) \approx \log\left(1 + \frac{\gamma}{2}\right)$. In the low-SNR regime, $\gamma_{\mathrm{eq}} \approx \gamma^2$ and $I_{\mathrm{s}}(\gamma) \approx \log(1 + \gamma^2) \approx \gamma^2$.

B. Time-sharing Scheme and the Low-SNR Regime

At low SNRs, $I_{\mathrm{s}}(\gamma) \approx \gamma^2$ (i.e., convex) and so time sharing improves achievable rate. We now introduce a time-sharing scheme that operates between two SNRs (γ_0 and γ_1) with time-sharing factor $0 \leq \lambda \leq 1$. The average SNR and the achieved secret key rate are

$$\begin{aligned} \gamma &= (1-\lambda)\gamma_0 + \lambda\gamma_1 \\ I_{\mathrm{s}}^{TS}(\gamma, \lambda) &= (1-\lambda) I_{\mathrm{s}}(\gamma_0) + \lambda I_{\mathrm{s}}(\gamma_1) \end{aligned}$$

Since in the low-SNR regime $I_{\mathrm{s}} \approx \gamma^2$ is a convex function (see Fig. 1), $I_{\mathrm{s}}^{TS}(\gamma)$ yields a higher secret key capacity than $I_{\mathrm{s}}(\gamma)$. Thus, we choose $\gamma_0 = 0$ and define the optimal time-sharing scheme that maximizes the $I_{\mathrm{s}}^{TS}(\gamma, \lambda)$.

Definition 1: The optimal time-sharing secret key rate at the average $\gamma \geq 0$ is

$$I_{\mathrm{s}}^{TS}(\gamma) = \lambda^* I_{\mathrm{s}}(\gamma^*) = \lambda^* I_{\mathrm{s}}\left(\frac{\gamma}{\lambda^*}\right) \ , \tag{10}$$

where

$$\lambda^* = \arg\max_{0 \leq \lambda \leq 1} \lambda I_{\mathrm{s}}\left(\frac{\gamma}{\lambda}\right) \text{ and } \gamma^* = \frac{\gamma}{\lambda^*} \ . \tag{11}$$

No time-sharing corresponds to $\lambda = 1$. The optimal λ^* and $\gamma_1 = \gamma^*$ can be derived by taking the derivative of the argument of (11) with respect to λ and finding the stationary point. Using the relation $\gamma^* = \gamma/\lambda^*$, it can be shown that the optimal operating γ^* satisfies

$$I_{\mathrm{s}}(\gamma^*) = \gamma^* \cdot \frac{d}{d\gamma} I_{\mathrm{s}}(\gamma)\Big|_{\gamma = \gamma^*} \ . \tag{12}$$

Resulting $I_{\mathrm{s}}^{TS}(\gamma)$ is a concave envelope of $I_{\mathrm{s}}(\gamma)$ (see Fig. 1), thus, $I_{\mathrm{s}}^{TS}(\gamma) \geq I_{\mathrm{s}}(\gamma)$ for all $\gamma \geq 0$. Next theorem shows that the $I_{\mathrm{s}}^{TS}(\gamma)$ achieves secret key capacity in (5). Therefore, the optimal training signal is a peaky on-off signal switching between $\gamma = 0$ and γ^* with distribution

$$P_D = \begin{cases} \lambda^*, & \text{for } D = d, |d|^2 = \frac{\gamma\sigma^2}{\lambda^*} \\ 1 - \lambda^*, & \text{for } D = 0 \end{cases} \ . \tag{13}$$

Theorem 2: For the training signal satisfying average energy $\mathcal{E}_s \leq \gamma\sigma^2$, the secret key capacity is

$$C_{\mathrm{s}}(\gamma) = I_{\mathrm{s}}^{TS}(\gamma) \ . \tag{14}$$

Proof: From Corollary 1, for a given training signal $D = d$, $I_{\mathrm{s}}(\gamma)$ is an increasing function of SNR $|d|^2/\sigma^2$. Additionally, $I_{\mathrm{s}}^{TS}(\gamma) \geq I_{\mathrm{s}}(\gamma)$ is increasing and concave in γ. The secret key rate is upper bounded by

$$\begin{aligned} I(X_A; X_B|D) &= E[I(X_A; X_B|D = d)] = E\left[I_{\mathrm{s}}\left(|d|^2/\sigma^2\right)\right] \\ &\leq E\left[I_{\mathrm{s}}^{TS}\left(|d|^2/\sigma^2\right)\right] \overset{\text{(i)}}{\leq} I_{\mathrm{s}}^{TS}\left(E\left[|d|^2/\sigma^2\right]\right) \\ &\overset{\text{(ii)}}{\leq} I_{\mathrm{s}}^{TS}(\gamma) \ . \end{aligned}$$

where (i) follows Jensen's inequality and concavity of I_{s}^{TS}. (ii) is due to average energy constraint. ■

C. Minimum Energy Per Key Bit

In a conventional AWGN communication channel, it is well-known that the low-SNR regime ($\gamma \to 0$) is the most energy-efficient [11]. However, as just discussed, secret key capacity acts differently in the low-SNR regime. At a given average SNR γ, the reliable key rate (bits per dimension) is upper bounded by $I_{\mathrm{s}}(\gamma)\log_2 e$. The energy cost per dimension is $\mathcal{E}_s = \sigma^2\gamma$ so that the energy per bit normalized by the noise variance is lower bounded by

$$\frac{\mathcal{E}_b}{\sigma^2} \geq \frac{\gamma}{I_{\mathrm{s}}(\gamma)} \log 2 \tag{15}$$

The *minimum energy per key bit* for reliable key acquisition, $\left(\frac{\mathcal{E}_b}{\sigma^2}\right)_{\min}$, which is related to the reciprocal of capacity per unit cost [12], is obtained by minimizing the lower bound over all SNRs. Due to the convexity of $I_{\mathrm{s}}(\gamma)$ at low SNR, time-sharing is necessary to achieve $\left(\frac{\mathcal{E}_b}{\sigma^2}\right)_{\min}$. This is because $\frac{\gamma}{I_{\mathrm{s}}^{TS}(\gamma)} \leq \frac{\gamma}{I_{\mathrm{s}}(\gamma)}$ for all $\gamma \geq 0$ and the linearity of time-sharing $I_{\mathrm{s}}^{TS}(\gamma)$ for $\gamma \leq \gamma^*$ achieves the same $\left(\frac{\mathcal{E}_b}{\sigma^2}\right)_{\min}$ in this region (see Fig. 2). It can be further verified that $\left(\frac{\mathcal{E}_b}{\sigma^2}\right)_{\min} = \frac{\gamma^*}{I_{\mathrm{s}}(\gamma^*)} \log 2$ where γ^* is the solution of (12).

D. Random Coding Error Exponent

Thus far we have characterized the secret key capacity, $I_{\mathrm{s}}(\gamma)$, as a function of γ. This is an upper bound on the rate at which secret keys can reliably be shared between A and B. We now analyze the reliability of secret key acquisition through an error exponent analysis [13], [14]. This analysis also enables us to quantify the energy cost of reliably establishing a *finite length key* between A and B. Since we are interested in quantifying fundamental limits, we focus on error exponent analysis of key acquisition based on the raw measurements (X_A, X_B). For a given joint distribution $P_{X_A X_B}$, a given key rate $R_{\mathrm{s}} < I_{\mathrm{s}}(\gamma)$, and an implicit condition on public message M (e.g., via Slepian-Wolf coding), the random coding error exponent, $E_s(R_{\mathrm{s}})$, bounds the (exponential) rate at which the probability of error in key acquisition decays with the block length N

$$P_e \triangleq \Pr[K_A \neq \hat{K}_A | M] \leq e^{-N E_s(R_{\mathrm{s}})} \; . \tag{16}$$

As quantization becomes finer to its extreme, $E_s(R_{\mathrm{s}})$ approaches to Gaussian error exponent [15]. In our setting, the Gaussian joint distribution function $P_{X_A X_B}$ is a function of γ. Therefore, the error exponent is function of R_{s} and γ. The following theorem characterizes the random coding error exponent in this case, which we state without proof due to space limitations.

Theorem 3: For secret key generation from jointly Gaussian measurements (X_A, X_B) in (4) with deterministic training signal D, the error exponent is given by:

Case I: For $\gamma_{\mathrm{eq}} \geq 1$, $E_s(R_{\mathrm{s}}, \gamma) =$

$$\begin{cases} I_{\mathrm{s}}(\gamma) - R_{\mathrm{s}} + 1 - 2\log 2, & \text{if } 0 \leq R_{\mathrm{s}} < R_c \\ \rho[I_{\mathrm{s}}(\gamma) - R_{\mathrm{s}} + 1] - (1+\rho)\log(1+\rho), & \text{if } R_c \leq R_{\mathrm{s}} < I_{\mathrm{s}}(\gamma) \end{cases}$$

Case II: For $\gamma_{\mathrm{eq}} < 1$, $E_s(R_{\mathrm{s}}, \gamma) =$

$$\rho[I_{\mathrm{s}}(\gamma) - R_{\mathrm{s}} + 1] - (1+\rho)\log(1+\rho), \quad \text{if } 0 \leq R_{\mathrm{s}} < I_{\mathrm{s}}(\gamma)$$

and $E_s(R_{\mathrm{s}}, \gamma) = 0$ if $R_{\mathrm{s}} \geq I_{\mathrm{s}}$ where $R_c = \log(\frac{1+\gamma_{\mathrm{eq}}}{2})$, $\rho = (1+\gamma_{\mathrm{eq}})e^{-R_{\mathrm{s}}} - 1$, and $I_{\mathrm{s}}(\gamma)$ and γ_{eq} are defined in (6) and (9), respectively.

We also define a time-sharing error exponent similar to the time-sharing secret key capacity. Consider a time-sharing scheme with factor λ that uses a fraction λN of the block length N for key acquisition. To meet a desired key generation rate R_{s} at a desired average γ, the *operational* key rate and SNR are given by R_{s}/λ and γ/λ, respectively. The bound in (16) changes accordingly as

$$P_e \leq e^{-\lambda N E_s(\frac{R_{\mathrm{s}}}{\lambda}, \frac{\gamma}{\lambda})} \tag{17}$$

and the exponent is $\lambda E_s(\frac{R_{\mathrm{s}}}{\lambda}, \frac{\gamma}{\lambda})$. We maximize over $0 \leq \lambda \leq 1$ to attain the largest error exponent.

Definition 2: The optimal time-sharing random coding error exponent for a given average SNR is

$$E_s^{TS}(R_{\mathrm{s}}, \gamma) = \max_{0 \leq \lambda \leq 1} \lambda E_s\left(\frac{R_{\mathrm{s}}}{\lambda}, \frac{\gamma}{\lambda}\right) = \lambda^* E_s\left(\frac{R_{\mathrm{s}}}{\lambda^*}, \frac{\gamma}{\lambda^*}\right) \; . \tag{18}$$

We note that the optimal time-sharing factor λ^* (and the corresponding operating $\gamma^* = \gamma/\lambda^*$) in (18) is in general different from the optimal λ^* and γ^* in (11) that maximizes the time-sharing secret key capacity.

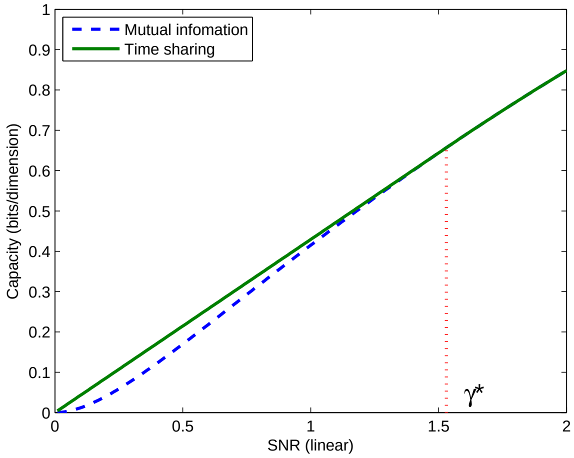

Fig. 1. Secret key capacity and time-sharing in the low-SNR regime.

IV. Discussion and Numerical Results

We have cast the problem of secret key generation from multipath randomness as a communication problem and our results characterize the fundamental limits to performance in reciprocal parallel wireless channels. Our analysis of secret key capacity reveals a new fundamental limit – minimum energy per bit for reliable key generation. The error exponent analysis quantifies the minimum energy required for reliable acquisition of a fixed-sized key. The resulting bounds on the probability of error also serve as a benchmark for the performance of any distributed source coding scheme, such as Slepian-Wolf coding, used in practice for secret key acquisition between an pair of users. We now elaborate on the main results and illustrate them with numerical examples.

Secret key capacity in the low-SNR regime. In a conventional AWGN channel, the channel capacity is $\log(1+\gamma) \approx \gamma$ as $\gamma \to 0$. In contrast, $I_{\mathrm{s}}(\gamma) \approx \gamma^2$ in the low-SNR regime. To see this behavior clearly, note from (8) that when SNR is low

$$X_B = \beta X_A + W_B = \left(\frac{\gamma}{\gamma+1}\right) X_A + W_B \approx \gamma X_A + W_B \tag{19}$$

and the ratio $\frac{E[\|X_A\|^2]}{E[\|W_B\|^2]} \approx 1$. Thus, the capacity of the equivalent channel in (19) is $I_{\mathrm{s}}(\gamma) \approx \log\left(1+\gamma^2\right)$. The quadratic decay of equivalent received SNR causes the first derivative of $I_{\mathrm{s}}(\gamma)$ to behave differently from that of conventional capacity $\log(1+\gamma)$. Figure 1 plots I_{s} in the low-SNR regime and we see that $I_{\mathrm{s}}(\gamma)$ is a convex function of γ ($\approx \gamma^2$).

On the other hand, the time-sharing scheme uses only $\lambda^* N$ channel dimensions (parallel channels) but operates at a higher γ^* while keeping the average SNR the same. Operationally, a time-sharing scheme uses a peaky signal resulting in a larger channel gain (in $\lambda^* N$ dimensions) in (19) and leading to a higher capacity:

$$\begin{aligned} C_{\mathrm{s}}(\gamma) &= \lambda^* I_{\mathrm{s}}(\gamma^*) \approx \lambda^*(\gamma^* \cdot \gamma^*) \\ &= \gamma^* \cdot \gamma \approx \beta^* \cdot \gamma \end{aligned}$$

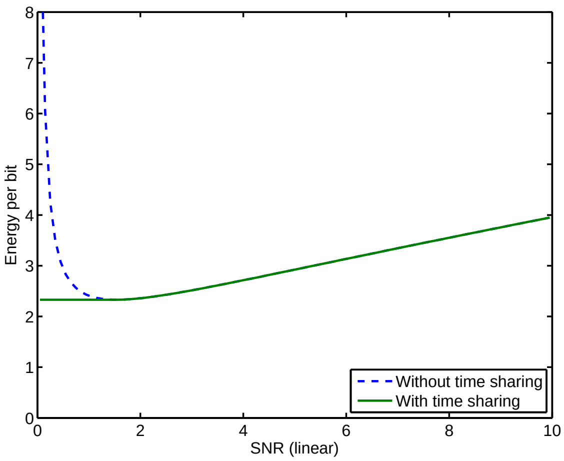

Fig. 2. Energy per key bit as a function of γ.

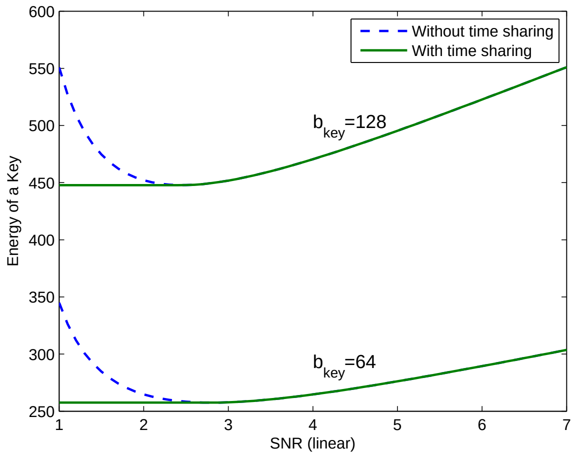

Fig. 3. Energy for a fixed-length key as a function of γ. $b_{\text{key}} = 64$ and 128, $\epsilon = 0.01$

Now $C_{\text{s}}(\gamma)$ approximates a linear (not quadratic) function of SNR with optimal gain β^* by choosing the operating γ^*. We note that peaky signals are also used for achieving capacity in non-coherent fading channels in the wideband/low-SNR regime [12]. Solving (12) numerically we get $\gamma^* \approx 1.535$ (1.861 dB). Figure 1 also shows $C_{\text{s}}(\gamma)$ $(= I_{\text{s}}^{TS}(\gamma))$.

Minimum energy per key bit. The first derivative of secret key capacity $C_{\text{s}}(\gamma)$ also affects the minimum energy per bit so $\left(\frac{\mathcal{E}_b}{\sigma^2}\right)_{\text{min}}$ depends on $\dot{C}_{\text{s}}(\gamma)^{-1}$ [12]. Since $I_{\text{s}}(\gamma) \approx \gamma^2$ at low SNR without time-sharing, it has zero slope when $\gamma \rightarrow 0$. To get $\left(\frac{\mathcal{E}_b}{\sigma^2}\right)_{\text{min}}$, we find the stationary point SNR of right hand side of (15). It can be shown that the resulting optimal operating SNR is same as what we get from (12) and $\left(\frac{\mathcal{E}_b}{\sigma^2}\right)_{\text{min}}$ evaluates to about 2.33 (3.67 dB) [15]. Time-sharing therefore gives a lower $\frac{\mathcal{E}_b}{\sigma^2}$ at low SNR. In particular, as stated in section III-C, a time-sharing scheme achieves $\left(\frac{\mathcal{E}_b}{\sigma^2}\right)_{\text{min}}$ for all $\gamma \leq \gamma^*$. Figure 2 plots energy per key bit as function of γ with and without time-sharing.

Minimum energy for a finite-length key. It is also useful to quantify the minimum energy needed to acquire a key of a fixed length (b_{key} bit) with a target key acquisition error probability ϵ. An upper bound on the minimum energy required to generate a finite-length key can be determined using an error exponent analysis. Given a key length b_{key} (bits), the key rate for a channel with N dimensions is $R_{\text{s}} = \frac{b_{\text{key}}}{N}\log 2$. A probability of error $P_e \leq \epsilon$ can be ensured if the random coding upper bound is less than ϵ,

$$e^{-NE_s \ \frac{b_{\text{key}}}{N}\log 2, \gamma} \leq \epsilon \tag{20}$$

which is equivalent to

$$NE_s\left(\frac{b_{\text{key}}}{N}\log 2, \gamma\right) \geq \log\frac{1}{\epsilon}. \tag{21}$$

For a given γ, the function on the left hand side increases in N. Thus, the minimum N satisfying (21), say N_{min}, is the root of (21) with equality. Since energy is a linear function of N (for a given γ), the minimum energy for acquiring the b_{key}-length key is

$$\mathcal{E}_{\text{key}} = N_{min} \cdot \gamma \cdot \sigma^2 \ . \tag{22}$$

Figure 3 plots $\mathcal{E}_{\text{key}}$ as function of γ with or without time-sharing for $b_{\text{key}} = 64$ and 128, $\epsilon = 0.01$. We can see a similar trend as in minimum energy per key bit. Without time sharing, $\mathcal{E}_{\text{key}}$ increases very fast as $\gamma \longrightarrow 0$. This is because in (21) as $\gamma \longrightarrow 0$, the error exponent decays faster than γ and, hence, the feasible solution N of (21) increases faster than $1/\gamma$. This causes $\mathcal{E}_{\text{key}}$ to go to infinity as $\gamma \longrightarrow 0$. On the other hand, with time-sharing, $\mathcal{E}_{\text{key}}$ at low SNR is as least as good as at the optimal higher SNR.

References

[1] C. E. Shannon. Communication theory of secrecy systems. *Bell Systems Tech. Journal*, 29:656–715, 1949.

[2] U. M. Maurer. Secret key agreement by public discussion from common information. *Information Theory, IEEE Transactions on*, 39(3):733–742, 1993.

[3] R. Ahlswede and I. Csiszár. Common randomness in information theory and cryptography part I: Secret sharing. *Information Theory, IEEE Transactions on*, 39(4):1121–1132, 1993.

[4] P. Gács and J. Körner. Common information is far less than mutual information. *Problems of Control and Information Theory*, 1973.

[5] D. Slepian and J. Wolf. Noiseless coding of correlated information sources. *Information Theory, IEEE Transactions on*, 19(4):471–480, Jul 1973.

[6] C. A. Balanis. *Antenna Theory: Analysis and Design*. New York: Wiley, 2nd edition, 1997.

[7] A. A. Hassan, W. E. Stark, J. E. Hersheyc, and Sandeep Chennakeshu. Cryptographic key agreement for mobile radio. *Digital Signal Processing*, 6(4):207–212, 1996.

[8] R. Wilson, D. Tse, and R. A. Scholtz. Channel identification: Secret sharing using reciprocity in ultrawideband channels. *Information Forensics and Security, IEEE Transactions on*, 2(3):364–375, 2007.

[9] A. Sayeed and A. Perrig. Secure wireless communications: Secret keys through multipath. In *ICASSP 2008. IEEE International Conference on*, pages 3013–3016, 2008.

[10] A. D. Wyner. Recent results in the Shannon theory. *IEEE Trans. Inform. Theory*, 20:2–10, January 1974.

[11] S. Verdu. On channel capacity per unit cost. *Information Theory, IEEE Transactions on*, 36(5):1019–1030, Sep 1990.

[12] S. Verdu. Spectral efficiency in the wideband regime. *Information Theory, IEEE Transactions on*, 48(6):1319–1343, Jun 2002.

[13] R. G. Gallager. *Information theory and reliable communication*. Wiley, New York, 1968.

[14] R. G. Gallager. Source coding with side information and universal coding. *M.I.T. LIDS-P-937*, 1976.

[15] T.-H. Chou, A. Sayeed, and S. Draper. Secret key generation from multipath randomness: Capacity and reliability. *in preparation*.