Secret-key generation with correlated sources and noisy channels

Ashish Khisti
EECS Dept.
MIT
Cambridge, MA, 02139
khisti@mit.edu

Suhas N. Diggavi
School of CCS
EPFL
1015, Lausanne, Switzerland
suhas.diggavi@epfl.ch

Gregory Wornell
EECS Dept.
MIT
Cambridge, MA, 02139
gww@mit.edu

Abstract— **A joint-source-channel setup for secret-key generation between remote terminals is considered. The sender communicates to the receiver over a discrete memoryless wiretap channel and the sender and receiver observe a pair of correlated discrete memoryless sources. Lower and upper bounds for the secret-key rate are presented and shown to coincide for the case when the underlying channel is a reversely degraded parallel channel. Our setup also provides an operational significance to the rate-equivocation tradeoff of the wiretap channel, and this is illustrated in detail for the Gaussian case.**

I. Introduction

There are two approaches for secret-key generation — the channel coding setup [1], [2] and the source coding setup [3], [4]. In the channel coding setup (also known as the wiretap channel), the source terminal is connected to the legitimate receiver and the eavesdropper over a discrete memoryless broadcast channel. The sender transmits a message to the legitimate receiver while guaranteeing a certain level of equivocation at the eavesdropper and the tradeoff between the information rate and equivocation is characterized. Which point to operate on this tradeoff depends on the application. For the secret-key-generation case, it is reasonable to require that the eavesdropper remain in (near) perfect equivocation. The maximum information rate in this case is known as the secrecy capacity of the wiretap channel. In the source coding setup, the sender and receiver observe correlated discrete memoryless sources and can communicate over a noiseless authenticated public channel. The requirement here is that the two terminals distil a secret-key, that is concealed from the eavesdropper who observes communication over the public channel. The maximum key rate in this setup is the secret-key-rate.

Given these two lines of work, it is of interest to consider a setup where the sender and legitimate receiver observe correlated sources and communicate over a noisy channel with a positive secrecy capacity. The requirement is that the sender and the legitimate receiver distil a common key that is concealed from the eavesdropper. Naturally, if the correlated sources are absent, this setup reduces to the standard wiretap channel, albeit for key generation. On the other hand, if the underlying channel is a noiseless channel, with a finite rate, the setup reduces to that in [5, Thm. 2.6]. How should one simultaneously take into account the equivocation due to the sources and the channel?

In this paper, we propose an approach that involves a separation between source and channel coding as well as a secret-key generation step that simultaneously takes into account both source and channel equivocations. We also provide an upper bound on the maximum secret-key-rate and establish the secret-key-capacity for reversely degraded parallel broadcast channels. For the case of Gaussian sources and Gaussian parallel channels, we establish the optimality of Gaussian codebooks.

Our source-channel setup also provides an operational significance for the rate-equivocation region of the wiretap channel. The rate-equivocation region captures the tradeoff between the information rate and the equivocation at the eavesdropper. In general these are conflicting requirements. In our setup, on one extreme, if we maximize the contribution of the correlated sources, we must operate at the Shannon capacity of the underlying channel. On the other extreme, if we maximize the contribution of the wiretap channel, we must operate at a point of maximum equivocation. In general, the optimal operating point is in between these two points and we illustrate this for the Gaussian example.

In a related problem, Merhav [6] studies a similar setup where the sender, receiver and eavesdropper observe correlated sources and communicate over a broadcast channel. The receiver wishes to reconstruct a lossy version of the source sequence with respect to a certain distortion metric. The complete tradeoff between the distortion and equivocation at the eavesdropper is characterized when both the sources and the channels are degraded. Note that, in contrast, our setup does not impose a distortion metric but requires that the sender and receiver distill a common secret-key. Also the motivations for the two problems are different. In [6] the setup has implications on systematic coding for the wiretap channel. In contrast, our setup is motivated for providing an operational significance to the rate-equivocation tradeoff of the wiretap channel. After the completion of our work, we were told of [7]

978-1-4244-2571-6/08/$25.00 ©2008 IEEE

where the authors consider transmitting a confidential message using correlated sources and noisy channels. This problem appears different ours, since we allow the key to be an arbitrary function of the source sequence.

II. Problem Statement

Our setup has three terminals: the sender, the (legitimate) receiver and the eavesdropper. They communicate over n uses of a discrete memoryless broadcast channel, whose transition probability is denoted by[1] $p_{\mathsf{y},\mathsf{z}|\mathsf{x}}(\cdot)$. In addition the sender and the legitimate receiver observe N independent copies of correlated random variables distributed according to the distribution $p_{\mathsf{u},\mathsf{v}}(\cdot)$. The setup is indicated in Fig. 1.

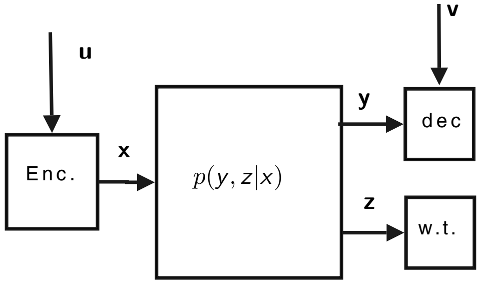

Fig. 1. Secret-key-generation setup using correlated sources and channels.

Definition 1: A (n, N) secret-key-code for this setup consists of two mappings at the encoder: $f_{n,N} : \mathcal{U}^N \to \mathcal{X}^n$, $\phi_{n,N} : \mathcal{U}^N \times \mathcal{X}^n \to \mathcal{K}$ and one mapping at the decoder $g_{n,N} : \mathcal{V}^N \times \mathcal{Y}^n \to \mathcal{K}$.

Definition 2: A secret-key-rate R is achievable with a bandwidth expansion factor β, if there exists a sequence of $(n, \beta n)$ secret-key-codes such that with $\mathsf{k} = \phi_{n,\beta n}(\mathbf{u}, \mathbf{x})$, (i) $\Pr(\mathsf{k} \neq g_{n,\beta n}(\mathbf{v}, \mathbf{y})) \leq \varepsilon_n$ and (ii) $\frac{1}{n}H(\mathsf{k}) \geq R - \varepsilon_n$ and (iii) $\frac{1}{n}I(\mathsf{k}; \mathbf{z}) \leq \varepsilon_n$, for some sequence ε_n that goes to zero as $n \to \infty$. The largest achievable rate in this setup is the secret-key-capacity.

We note in advance that a more general setup involves having another correlated source sequence at the eavesdropper. This more general setup is not treated in this paper although a rather straightforward extension of our result to the case of degraded sources and degraded channels [8]. For certain applications e.g., biometric measurements [9], it is natural to assume that the eavesdropper does not have access to a correlated source as we consider in this paper. Furthermore, a stronger notion of secrecy along the lines of [10] may be also considered in this setup.

III. Statement of main result

Our main result is the characterization of upper and lower bounds on the secret-key-rate for the setup in Fig. 1. We establish the secret-key-capacity for the case when the broadcast channel $p_{\mathsf{y},\mathsf{z}|\mathsf{x}}(\cdot)$ is reversely degraded and study the Gaussian case in detail.

Lemma 1: Let a and b be two random variables such that the distribution p_{abxyz} satisfies (i) the Markov condition, $\mathsf{b} \to \mathsf{a} \to \mathsf{x} \to (\mathsf{y}, \mathsf{z})$, (ii) $I(\mathsf{y}; \mathsf{b}) \leq I(\mathsf{z}; \mathsf{b})$ and (iii) $I(\mathsf{y}; \mathsf{a}|\mathsf{b}) \geq I(\mathsf{z}; \mathsf{a}|\mathsf{b})$. Define the quantities

$$R_{\mathrm{ch}} \triangleq I(\mathsf{y}; \mathsf{a}), \quad R_{\mathrm{eq}} \triangleq I(\mathsf{y}; \mathsf{a}|\mathsf{b}) - I(\mathsf{z}; \mathsf{a}|\mathsf{b}). \quad (1)$$

Let t be another random variable such that the distribution p_{tuv} satisfies $\mathsf{t} \to \mathsf{u} \to \mathsf{v}$ and define

$$R_{\mathrm{wz}} \triangleq I(\mathsf{t}; \mathsf{u}) - I(\mathsf{t}; \mathsf{v}), \quad R_{\mathrm{src}} \triangleq I(\mathsf{t}; \mathsf{v}). \quad (2)$$

Suppose, further that we have,

$$R_{\mathrm{ch}} \geq \beta R_{\mathrm{wz}}. \quad (3)$$

Then the rate

$$R_{\mathrm{key}} = \beta R_{\mathrm{src}} + R_{\mathrm{eq}} \quad (4)$$

is an achievable secret-key-rate.
Note that R_{eq} represents the level of equivocation at the eavesdropper due to the channel and R_{src} represents the level of equivocation due to sources. From (4), we have that the total secret-key-rate is the sum of these two terms.

Lemma 2: An upper bound on the secret-key-capacity is

$$C_{\mathrm{key}} \leq \max_{p_{\mathsf{x}} p_{\mathsf{t}|\mathsf{u}}} \{I(\mathsf{x}; \mathsf{y}|\mathsf{z}) + \beta I(\mathsf{v}; \mathsf{t})\}, \quad (5)$$

where the maximum is over all distributions p_{x} and $p_{\mathsf{t}|\mathsf{u}}$ such that $\mathsf{t} \to \mathsf{u} \to \mathsf{v}$ and

$$I(\mathsf{x}; \mathsf{y}) \geq \beta\{I(\mathsf{t}; \mathsf{u}) - I(\mathsf{t}; \mathsf{v})\}. \quad (6)$$

It suffices to restrict $|\mathcal{T}| \leq |\mathcal{U}| + 1$.

Our upper and lower bounds coincide for the case of reversely degraded channels.

Definition 3: A reversely degraded channel [11] with M independent sub channels, consists of an input alphabet $\mathcal{X} = \mathcal{X}_1 \times \ldots \times \mathcal{X}_M$ and output alphabets $\mathcal{Y} = \mathcal{Y}_1 \times \ldots \times \mathcal{Y}_M$, $\mathcal{Z} = \mathcal{Z}_1 \times \ldots \times \mathcal{Z}_M$, $p_{\mathsf{y}_1,\ldots,\mathsf{y}_M,\mathsf{z}_1,\ldots \mathsf{z}_M|\mathsf{x}_1,\ldots,\mathsf{x}_M}(\cdot) = \Pi_{i=1}^M p_{\mathsf{y}_i,\mathsf{z}_i|\mathsf{x}_i}(\cdot)$ and on channel i, $1 \leq i \leq M$, one of $\mathsf{x}_i \to \mathsf{y}_i \to \mathsf{z}_i$ or $\mathsf{x}_i \to \mathsf{z}_i \to \mathsf{y}_i$ holds.

The following result follows from Lemma 1 and 2 and will be established in [8].

Theorem 1: The secret-key-capacity for the reversely degraded channel is given by

$$C_{\mathrm{key}} = \max_{p_{\mathsf{x}_1},\ldots,p_{\mathsf{x}_M},p_{\mathsf{t}}} \left\{ \sum_{i=1}^M I(\mathsf{x}_i; \mathsf{y}_i|\mathsf{z}_i) + \beta I(\mathsf{v}; \mathsf{t}) \right\}, \quad (7)$$

where the maximum is over all (independent) distributions $p_{\mathsf{x}_1}, \ldots, p_{\mathsf{x}_M}$ and p_{t} such that t satisfies the same Markov conditions and cardinality bound in Lemma 2 and

$$\sum_{i=1}^M I(\mathsf{x}_i; \mathsf{y}_i) \geq \beta\{I(\mathsf{t}; \mathsf{u}) - I(\mathsf{t}; \mathsf{v})\}. \quad (8)$$

[1] Throughout we use the sans-serif font to denote the random variables, and regular (serif) font to denote the realization of random variables. Upper case, calligraphic fonts are used for the alphabet of random variables and sets. Bold case is used to denote vectors.

An important example of the reversely degraded channels is the Gaussian case.

Definition 4: A Gaussian source-channel setup consists of the following (i) A reversely degraded parallel channel, such that for each $1 \leq i \leq M$, we have $y_i = x_i + n_{r,i}$ and $z_i = x_i + n_{e,i}$ where $n_{r,i} \sim \mathcal{N}(0, \sigma^2_{r,i})$ and $n_{e,i} \sim \mathcal{N}(0, \sigma^2_{e,i})$. Furthermore the noise random variables are appropriately correlated such that $x_i \to y_i \to z_i$ if $\sigma_{r,i} \leq \sigma_{e,i}$ and $x_i \to z_i \to y_i$ holds otherwise and the noise random variables across the channels are independent. (ii) An average sum power constraint on the input $E[\sum_{i=1}^M x_i^2] \leq P$ (iii) Jointly Gaussian sources[2] i.e., $u \sim \mathcal{N}(0,1)$, $v = u + s$, where $s \sim \mathcal{N}(0, S)$ is independent of u.

We state the following capacity result for the Gaussian setup. The proof follows by combining Thm. 1 with the worst-case-additive-noise-Lemma in [12] to establish the optimality of Gaussian distribution [8].

Theorem 2: For the Gaussian source-channel setup in Def. 4, the secret-key-capacity is obtained by maximizing (7) over Gaussian distributions i.e., for some $P_1, \ldots, P_M$, $P_i \geq 0$, $\sum_{i=1}^M P_i \leq P$ and $D \in (0,1]$, we let $p_{x_i} = \mathcal{N}(0, P_i)$, $p_t = \mathcal{N}(0, 1-D)$ and $u = t + d$, where $d \sim \mathcal{N}(0, D)$ is independent of t and,

$$C^G_{\text{key}} = \max_{\{P_i\}_{i=1}^M, D} \frac{\beta}{2} \log\left(\frac{1+S}{D+S}\right) + \sum_{\substack{i:1\leq i\leq M\\ \sigma_{r,i}\leq\sigma_{e,i}}} \frac{1}{2}\log\left(\frac{1+P_i/\sigma^2_{r,i}}{1+P_i/\sigma^2_{e,i}}\right), \tag{9}$$

where $P_1, \ldots, P_M, D$ satisfy

$$\sum_{i=1}^M \log\left(1 + \frac{P_i}{\sigma^2_{r,i}}\right) \geq \beta\left\{\log\left(\frac{1}{D}\right) - \log\left(\frac{1+S}{D+S}\right)\right\}. \tag{10}$$

We now mention a few remarks. First, the condition in Def. 4 requires that the noise variables are physically degraded. As is well known [1], this condition can be relaxed to the case of stochastic degradation of noise random variables. Secondly, while we assumed scalar valued Gaussian sources in Def. 4, this assumption was only for simplicity. Our proof for optimality of Gaussian codebooks also holds when the sources (u, v) are multivariate jointly Gaussian, as it relies on the worst-case-additive-noise-Lemma in [12].

In general there is a tension between maximizing the two terms in (9). One one extreme, if we select $\{P_1, \ldots, P_M\}$ according to the water-filling solution we maximize the left hand side in (10) and this yields the smallest feasible value of D. On the other hand, to maximize the equivocation, i.e., the second term in (9), we must set $P_i = 0$ when $\sigma_{r,i} \geq \sigma_{e,i}$ and optimize over the remaining channels, but this choice in general yields a larger value of D. The optimal choice of $\{P_i\}$ that maximizes (9) balances this tension. We quantify this tradeoff via an example below.

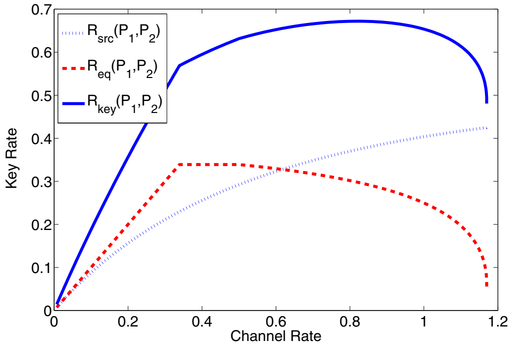

Fig. 2. Tradeoff inherent in the secret-key-capacity formulation. The solid curve is the secret-key-rate, which is the sum of the two other curves. The dotted curve represents the source equivocation, while the dashed curve represents the channel equivocation (see (2)). The secret-key-capacity is obtained at a point between the maximum equivocation and maximum rate.

Example: We illustrate the tradeoff with a numerical example. Consider two parallel channels,

$$\begin{aligned} y_1 &= a_1 x + n_{r,1}, \quad z_1 = b_1 x + n_{e,2} \\ y_2 &= a_2 x + n_{r,2}, \quad z_2 = y_2 \end{aligned} \tag{11}$$

where $a_1 = 1$, $a_2 = 2$, and $b_1 = 0.5$. Furthermore, $u \sim \mathcal{N}(0,1)$ and $v = u + s$, where $s \sim \mathcal{N}(0,1)$ is independent of u. The noise random variables are all $\mathcal{CN}(0,1)$. There is a power constraint $P = 1$ and the bandwidth expansion factor β equals unity.

In this example, the optimization in Corollary 2, takes the form:

$$C_{\text{key}} = \max_{P_1, P_2, D} R_{\text{eq}}(P_1, P_2) + \frac{1}{2}\log\frac{2}{1+D}, \tag{12}$$

such that,

$$R_{\text{wz}}(D) = \frac{1}{2}\log\frac{1}{D} - \frac{1}{2}\log\frac{2}{1+D} \tag{13}$$

$$\leq \frac{1}{2}\left(\log\left(1 + a_1^2 P_1\right) + \log(1 + a_2^2 P_2)\right), \tag{14}$$

$$R_{\text{eq}}(P_1, P_2) = \frac{1}{2}\left(\log(1 + a_1^2 P_1) - \log(1 + b_1^2 P_1)\right). \tag{15}$$

Fig. 2 illustrates the (fundamental) tradeoff between rate and equivocation for this channel, which is obtained as we vary power allocation between the two sub-channels. We also present the function $R_{\text{src}} = I(t; v)$ which monotonically increases with the rate, since larger the rate, smaller is the distortion in the source quantization, and the function R_{eq} which decreases as we increase the rate beyond $R_{\text{ch}} = 0.5$. The optimal point of operation is between these two extremes as indicated by the maximum of the solid line in Fig. 2. This corresponds to a power allocation $(P_1, P_2) \approx (0.29, 0.71)$ and the maximum value is $R_{\text{key}} \approx 0.6719$.

IV. Proof of Achievability

Due to space constraints we only sketch an outline of achievability.

[2] From Def. 2 note that one can separately scale both **u** and **v** without reducing the achievable rate. Thus this condition is satisfied without loss of generality for any jointly Gaussian scalar valued p_{uv}

Throughout we will consider strongly typical sequences and denote the set of length n, p_{v} $\eta-$typical sequences by $T^n_{v,\eta}$ and $p_{a|b}$ conditionally typical sequences by $T^n_{(a|b),\eta}(\mathbf{b})$. For a certain sufficiently small, $\delta > 0$, we suppose that

$$\beta R_{\rm wz} = R_{\rm ch} - \delta, \qquad (16)$$

and establish the achievability of (4) in Lemma 1 for (16) instead of (3).

If indeed $\beta R_{\rm wz} < R_{\rm ch} - \delta$, then we one can satisfy (16) for a modified β as follows. Note that for some $\alpha < 1$, we have that $\beta R_{\rm wz} = \alpha(R_{\rm ch} - \delta)$. In this case, for the first αn channel uses and use the code construction presented below. For the remaining $(1-\alpha)n$ channel uses, we transmit an independent message using another wiretap code at a secrecy rate of $R_{\rm eq}$. The resulting secret-key rate is given by

$$\alpha\left(\frac{\beta}{\alpha}R_{\rm src} + R_{\rm eq}\right) + (1-\alpha)R_{\rm eq} = R_{\rm key}, \qquad (17)$$

as required.

For some fixed $\varepsilon \in (0, R_{\rm ch} - R_{\rm eq} - 2\delta)$, let $F_{\rm WZ} = 2^{n(\beta R_{\rm wz} + 2\varepsilon)}$, $K_{\rm SK} = 2^{n(\beta R_{\rm src} + R_{\rm eq} + 2\varepsilon)}$ and $L_{\rm SK} = 2^{n(\beta R_{\rm wz} - R_{\rm eq} - \varepsilon)}$ and construct the following[3] codebooks.

1. **Secret-Key Codebook**: For each $1 \leq i \leq K_{\rm SK}$ and $1 \leq j \leq L_{\rm SK}$, select a codeword $\mathbf{t}_{i,j}$ uniformly and at random from $T^n_{t,\eta}$. Let $\mathcal{T}$ denote the set of all codewords, thus selected. We will refer to i as the bin-index of $\mathbf{t}_{i,j}$ in the secret-key codebook.
2. **Wyner-Ziv Codebook**: Assign each $\boldsymbol{t} \in \mathcal{T}$ to one of $F_{\rm WZ}$ bins uniformly and at random. Let $\mathcal{F}^i$ denote the set of codewords assigned to bin i, $1 \leq i \leq F_{\rm WZ}$.
3. **Wiretap Codebook** For a fixed $\delta_a > 0$ and $\delta_b > 0$, let $R_b = I(b; y)$ and $R_a = I(a; y|b)$. For each $1 \leq i \leq 2^{n(R_b - \delta_b)}$ select a codeword $\mathbf{b}_i$ uniformly from the set $T^n_{b,\eta}$ and denote the result set by $\mathcal{C}_b$. For each $\mathbf{b}_i \in \mathcal{C}_b$, and each $1 \leq j \leq 2^{n(R_a - \delta_a)}$, select a codeword $\mathbf{a}_j$ uniformly from the set $T^n_{(a|b),\eta}$ and denote the result set of codewords by $\mathcal{C}_a(\mathbf{b}_i)$.

The encoding and decoding functions are as follows. Given a $\mathbf{u}$, the encoder finds a jointly typical $\mathbf{t} \in \mathcal{T}$. It declares the bin index of $\mathbf{t}$ in the secret-key-codebook to be the secret-key $\Gamma_{\rm SK}$ and the bin index in the Wyner-Ziv codebook Φ_{WZ} constitutes the message for the secret-key codebook. This message is split into $[\Phi_b, \Phi_a]$, where since $H(\Phi_b) = I(b; y) - \delta_b$, Φ_b can be decoded by both the terminals, while since $H(\Phi_a) = I(a; y|b) - \delta_a$, Φ_a can be decoded by only the legitimate receiver. The decoder upon observing $\mathbf{y}$, decodes $\hat{\Phi}_{\rm WZ}$ and using $\mathbf{v}$ recovers $\mathbf{t}$ (whp). It declares the bin index of $\mathbf{t}$ in the secret-key-codebook as the key $\hat{\Gamma}_{\rm SK}$. Our codebook construction guarantees that $\frac{1}{n}H(\Gamma_{\rm SK}) \geq R_{\rm key} - o_\varepsilon(1)$ and $\Pr(\Gamma_{\rm SK} \neq \hat{\Gamma}_{\rm SK}) \leq o_\varepsilon(1)$, where $o_\varepsilon(1)$ goes to zero as $n \to \infty$ and $\varepsilon \to 0$.

It remains to show that for our code construction $\frac{1}{n}H(\Gamma_{\rm SK}|\mathbf{z}) \geq R_{\rm key} - o_\varepsilon(1)$. First, with some straightforward manipulation we can show that

$$H(\Gamma_{\rm SK}|\mathbf{z}) \geq H(\mathbf{t}|\Phi_{\rm WZ}) + H(\Phi_{\rm WZ}|\mathbf{z}) - H(\mathbf{t}|\mathbf{z}, \Gamma_{\rm SK}), \qquad (18)$$

and for our code construction we have that $\frac{1}{n}H(\mathbf{t}|\Phi_{\rm WZ}) \geq \beta I(t; v) - o_\varepsilon(1)$ and $\frac{1}{n}H(\Phi_{\rm WZ}|\mathbf{z}) \geq R_{\rm eq} - o_\varepsilon(1)$. From (4), we will complete the proof, if we show that $\frac{1}{n}H(\mathbf{t}|\mathbf{z}, \Gamma_{\rm SK}) = o_\varepsilon(1)$. Towards, this end, we show that the eavesdropper, when provided the knowledge of the secret-key $\Gamma_{\rm SK}$, is able to reproduce $\mathbf{t}$ with high probability. In particular the eavesdropper first decodes $\mathbf{b}$ from $\mathbf{z}$ (since $R_b \leq I(b; y) \leq I(b; z)$) and recovers Φ_b (whp). It searches for $1 \leq j \leq L_{\rm SK}$ such that $\hat{\Phi}_{\rm WZ}$ corresponding to $\mathbf{t}_{\Gamma_{\rm SK},j}$ is such that $\Phi_b = \hat{\Phi}_b$ and the codeword $\hat{\mathbf{a}}$ corresponding to $\hat{\Phi}_a$ in $\mathcal{C}_a(\mathbf{b})$ is jointly typical with $\mathbf{z}$. An error occurs if either $\hat{\mathbf{b}} \neq \mathbf{b}$ or there exists a $\hat{\mathbf{t}}$ such that $\hat{\Phi}_b = \Phi_b$ and the codeword $\hat{\mathbf{a}}$ is jointly typical with $\mathbf{z}$. It can be shown, via standard analysis, that these error events have vanishing probability and hence Fano's inequality yields that $\frac{1}{n}H(\mathbf{t}|\mathbf{z}, \Gamma_{\rm SK}) = o_\varepsilon(1)$, thus completing the proof.

V. Proof of the Upper Bound (Lemma 2)

Given a sequence of $(n, N = \beta n)$ codes that achieve a secret-key-rate $R_{\rm key}$, we have that for a sequence ε_n, such that $\varepsilon_n \to 0$ as $n \to \infty$

$$\frac{1}{n}H(k|\mathbf{y}, \mathbf{v}) \leq \varepsilon_n \qquad (19a)$$

$$\frac{1}{n}H(k|\mathbf{z}) \geq \frac{1}{n}H(k) - \varepsilon_n \qquad (19b)$$

We can now upper bound the rate $R_{\rm key}$ as follows.

$$\begin{aligned} nR_{\rm key} &= H(k) \\ &= H(k|\mathbf{y}, \mathbf{v}) + I(k; \mathbf{y}, \mathbf{v}) \\ &\leq n\varepsilon_n + I(k; \mathbf{y}, \mathbf{v}) - I(k; \mathbf{z}) + I(k; \mathbf{z}) && (20) \\ &\leq 2n\varepsilon_n + I(k; \mathbf{y}, \mathbf{v}) - I(k; \mathbf{z}) && (21) \\ &= 2n\varepsilon_n + I(k; \mathbf{y}) - I(k; \mathbf{z}) + I(k; \mathbf{v}|\mathbf{y}) \\ &\leq 2n\varepsilon_n + I(k; \mathbf{y}) - I(k; \mathbf{z}) + I(k, \mathbf{y}; \mathbf{v}) && (22) \end{aligned}$$

where (20) and (21) follow from (19a) and (19b) respectively.

Now, let J be a random variable uniformly distributed over the set $\{1, 2, \ldots, N\}$ and independent of everything else. Let $t_i = (k, \mathbf{y}, v_{i+1}^N, u_1^{i-1})$ and $t = (k, \mathbf{y}, v_{J+1}^N, u_1^{J-1}, J)$, and v_J be a random variable that conditioned on $J = i$ has the distribution of p_{v_i}. (Define u_J analogously.) Note that since $\mathbf{v}$ is memoryless, v_J is independent of J and has the same marginal distribution as v and also that $t \to u_J \to v_J$ holds.

[3] Notice that the exponent for $L_{\rm SK}$ is positive via (16).

$$
\begin{aligned}
I(k,\mathbf{y};\mathbf{v}) &= \sum_{i=1}^{N} I(k,\mathbf{y};v_i|v_{i+1}^{N}) \\
&\le \sum_{i=1}^{N} I(k,\mathbf{y},v_{i+1}^{n};v_i) \\
&\le \sum_{i=1}^{N} I(k,\mathbf{y},v_{i+1}^{n},u_1^{i-1};v_i) \\
&= NI(k,\mathbf{y},v_{J+1}^{n},u_1^{J-1};v_J|J) \\
&= NI(k,\mathbf{y},v_{J+1}^{n},u_1^{J-1},J;v_J) - I(J;v_J) \\
&= NI(t;v) \qquad (23)
\end{aligned}
$$

where (23) follows from the fact that v_J is independent of J and has the same marginal distribution as v.

Next, we upper bound $I(k;\mathbf{y})-I(k;\mathbf{z})$ as below. Let p_{x_i} denote the channel input distribution at time i and let p_{y_i,z_i} denote the corresponding output distribution. Let $p_x = \frac{1}{n}\sum_{i=1}^{n} p_{x_i}$ and let p_y and p_z be defined similarly.

$$
\begin{aligned}
I(k;\mathbf{y}) - I(k;\mathbf{z}) &\le I(k;\mathbf{y}|\mathbf{z}) \\
&\le I(\mathbf{x};\mathbf{y}|\mathbf{z}) \qquad (24) \\
&\le \sum_{i=1}^{n} I(x_i;y_i|z_i) \qquad (25) \\
&\le nI(x;y|z), \qquad (26)
\end{aligned}
$$

where (24) follows from the Markov condition $k \to \mathbf{x} \to (\mathbf{y},\mathbf{z})$ and (25) follows from the fact that the channel is memoryless and (26) from the fact that $I(x;y|z)$ is a concave function in $p_x(\cdot)$ (see e.g., [13, App. I])

Substituting (26) and (23) in (22) we have that

$$
R_{\text{key}} \le I(x;y|z) + \beta I(v;t) + 2n\varepsilon_n, \qquad (27)
$$

thus establishing the first half i.e., (5) in Lemma 2. It remains to establish (6). Since $\mathbf{u} \to \mathbf{x} \to \mathbf{y}$ holds, and the channel is memoryless, we have that

$$
\begin{aligned}
nI(x;y) \ge I(\mathbf{x};\mathbf{y}) &\ge I(\mathbf{u};\mathbf{y}) \qquad (28) \\
&\ge I(\mathbf{u};\mathbf{y},k) - I(\mathbf{v};\mathbf{y},k) - n\varepsilon_n, \qquad (29)
\end{aligned}
$$

where the last inequality holds, since

$$
\begin{aligned}
I(\mathbf{u};k|\mathbf{y}) - I(\mathbf{v};\mathbf{y},k) &= -I(\mathbf{v};\mathbf{y}) + I(\mathbf{u};k|\mathbf{y}) - I(\mathbf{v};k|\mathbf{y}) \\
&\le I(\mathbf{u};k|\mathbf{y}) - I(\mathbf{v};k|\mathbf{y}) \\
&= H(k|\mathbf{y},\mathbf{v}) - H(k|\mathbf{y},\mathbf{u}) \\
&\le n\varepsilon_n,
\end{aligned}
$$

where the last step holds via (19a) and the fact that $H(k|\mathbf{y},\mathbf{u}) > 0$.

Continuing (29), we have

$$
\begin{aligned}
&nI(x;y) \ge I(\mathbf{u};\mathbf{y},k) - I(\mathbf{v};\mathbf{y},k) - n\varepsilon_n \\
&= \\
&\sum_{i=1}^{N}\{I(u_i;\mathbf{y},k,u_1^{i-1}v_{i+1}^{n}) - I(v_i;\mathbf{y},k,u_1^{i-1}v_{i+1}^{n})\} - n\varepsilon_n
\end{aligned}
$$

$$
\begin{aligned}
&= \\
&N\{I(u_J;\mathbf{y},k,u_1^{J-1}v_{J+1}^{n}|J) - I(v_J;\mathbf{y},k,u_1^{J-1}v_{J+1}^{n}|J) - \varepsilon_n'\} \\
&= \\
&N\{I(u_J;t) - I(v_J;t) + I(v_J;J) - I(u_J;J) - \varepsilon_n'\} \\
&= N\{I(u;t) - I(v;t) - \varepsilon_n'\}.
\end{aligned}
$$

Where $\beta\varepsilon_n' = \varepsilon_n$ and the last step again follows from the fact that the random variables v_J and u_J are independent of J and have the same marginal distribution as v and u respectively. This establishes (6).

The cardinality bound on t is obtained via Caratheordory's theorem and will not be presented here.

Finally, since the upper bound expression does not depend on the joint distribution of (t,x), it suffices to optimize over those distributions where (t,x) are independent.

VI. Conclusion

The problem of secret-key-generation using correlated sources and channels is studied when the eavesdropper does not observe a side information source. Upper and lower bounds are derived and shown to match for the reversely degraded case. This broader view also provides an operational significance to the rate-equivocation tradeoff for the wiretap channel.

References

[1] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–87, 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, pp. 339–348, 1978.

[3] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, pp. 733–742, Mar. 1993.

[4] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography – Part I: Secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1121–1132, July 1993.

[5] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inform. Theory*, vol. 46, Mar. 2000.

[6] N. Merhav, "Shannon's secrecy system with informed receivers an its application to systematic coding for wiretapped channels," *IEEE Trans. Inform. Theory*, to appear, IEEE Trans. Inform. Theory, special issue on Information-Theoretic Security, June 2008.

[7] V. Prabhakaran and K. Ramachandran, "A separation result for secure communication," in *talk presented at the 45th Allerton Conf. Commun., Contr., Computing*, Oct. 2007.

[8] A. Khisti, S. N. Diggavi, and G. W. Wornell, "Secret-key generation with correlated sources and noisy channels," In Preparation, 2008.

[9] S. C. Draper, A. Khisti, E. Martinian, J. Yedidia, and A. Vetro, "Using distributed source coding to secure fingerprint biometrics," in *Proc. Int. Conf. Acoust. Speech, Signal Processing*, 2007.

[10] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *EUROCRYPT 2000, Lecture Notes in Computer Science, Springer-Verlag, vol. 1807*, 2000, pp. 351–368.

[11] A. A. El Gamal, "Capacity of the product and sum of two unmatched broadcast channels," *Probl. Information Transmission*, pp. 3–23, 1980.

[12] S. N. Diggavi and T. M. Cover, "The worst additive noise under a covariance constraint," *IEEE Trans. Inform. Theory*, vol. IT-47, no. 7, pp. 3072–3081, 2001.

[13] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure Broadcasting," *To Appear IEEE Trans. Inform. Theory, Special Issue on Information Theoretic Security*, 2008.