Secret-Key Generation using Correlated Sources and Channels

Ashish Khisti, *Student Member, IEEE*, and Suhas N. Diggavi, *Member, IEEE*, and Gregory W. Wornell, *Fellow, IEEE*

Abstract

We study the problem of generating a shared secret key between two terminals in a joint source-channel setup — the sender communicates to the receiver over a discrete memoryless wiretap channel and additionally the terminals have access to correlated discrete memoryless source sequences. We establish lower and upper bounds on the secret-key capacity. These bounds coincide, establishing the capacity, when the underlying channel consists of independent, parallel and reversely degraded wiretap channels. In the lower bound, the equivocation terms of the source and channel components are functionally additive. The secret-key rate is maximized by optimally balancing the the source and channel contributions. This tradeoff is illustrated in detail for the Gaussian case where it is also shown that Gaussian codebooks achieve the capacity. When the eavesdropper also observes a source sequence, the secret-key capacity is established when the sources and channels of the eavesdropper are a degraded version of the legitimate receiver. Finally the case when the terminals also have access to a public discussion channel is studied. We propose generating separate keys from the source and channel components and establish the optimality of this approach when the when the channel outputs of the receiver and the eavesdropper are conditionally independent given the input.

I. Introduction

Many applications in cryptography require that the legitimate terminals have shared secret-keys, not available to unauthorized parties. Information theoretic security encompasses the study of source and channel coding techniques to generate secret-keys between legitimate terminals. In the channel coding literature, an early work in this area is the wiretap channel model [19]. It consists of three terminals — one sender, one receiver and one eavesdropper. The sender communicates to the receiver and the eavesdropper over a discrete-memoryless broadcast channel. A notion of equivocation-rate — the normalized conditional entropy of the transmitted message given the observation at the eavesdropper, is introduced, and the tradeoff between information rate and equivocation rate is studied. Perfect secrecy capacity, defined as the maximum information rate under the constraint that the equivocation rate approaches the information rate asymptotically in the block length is of particular interest. Information transmitted at this rate can be naturally used as a shared secret-key between the sender and the receiver.

In the source coding setup [1], [15], the two terminals observe correlated source sequences and use a public discussion channel for communication. Any information sent over this channel is available to an eavesdropper. The terminals generate a common secret-key that is concealed from the eavesdropper in the same sense as the wiretap channel — the equivocation

Part of the material in this paper was presented at the 2008 Information Theory and its Application Workshop [11] and the 2008 International Symposium on Information Theory [12]. Ashish Khisti was with EECS Department, MIT (ashish.khisti@gmail.com). Suhas Diggavi is with the faculty of the School of Computer and Communication Sciences at EPFL (suhas.diggavi@epfl.ch). Gregory Wornell is with the faculty of EECS Dept., MIT (gww@mit.edu). The work of Ashish Khisti and Gregory Wornell was supported in part by NSF Grant No. CCF-0515109. The work of Suhas Diggavi was supported in part by the Swiss National Science Foundation through NCCR-MICS

rate asymptotically equals the secret-key rate. Several multiuser extensions of this problem have been subsequently studied. See e.g., [5], [6].

Motivated by the above works, we study a problem where the legitimate terminals observe correlated source sequences and communicate over a wiretap channel and are required to generate a common secret-key. One application of this setup is sensor networks, where terminals measure correlated physical processes. It is natural to investigate how these measurements can be used for secrecy. In addition, the sensor nodes communicate over a wireless channel where an eavesdropper could hear transmission albeit through a different channel. Another application is secret key generation using biometric measurements [7]. During the registration phase, an enrollment biometric is stored into a database. To generate a secret key subsequently, the user is required to provide another measurement of the same biometric. This new measurement differs from the enrollment biometric due to factors such as measurement noise and hence can be modeled as a correlated signal. Again when the database is remotely located, the communication happens over a channel which could be wiretapped.

The secret-key agreement scheme, [1], [15], generates a secret key only using the source sequences. On the other hand, the wiretap coding scheme [19] generates a secret-key by exploiting the structure of the underlying broadcast channel. Clearly in the present setup, we should consider schemes that take into account both the source and channel contributions. One simple approach is timesharing — for a certain fraction of time the wiretap channel is used as a (rate limited) transmission channel whereas for the remaining time, a wiretap code is used to transmit information at the secrecy capacity. However such an approach in general is sub-optimal. As we will see, a better approach involves simultaneously exploiting both the source and channel uncertainties at the eavesdropper. As our main result we present lower and upper bounds on the secret-key capacity. The lower bound is developed by providing a coding theorem that consists of a combination of a Wyner-Ziv codebook, a wiretap codebook and a secret-key generation codebook. Our upper and lower bounds coincide, establishing the secret-key-capacity, when the wiretap channel consists of parallel independent and degraded channels.

We also study the case when the eavesdropper observes a source sequence correlated with the legitimate terminals. The secret-key capacity is established when the sources sequence of the eavesdropper is a degraded version of the sequence of the legitimate receiver and the channel of the eavesdropper is a degraded version of the channel of the legitimate receiver. Another variation — when a public discussion channel is available for interactive communication, is also discussed and the secret-key capacity is established when the channel output symbols of the legitimate receiver and eavesdropper are conditionally independent given the input.

The problem studied in this paper also provides an operational significance for the rate-equivocation region of the wiretap channel. Recall that the rate-equivocation region captures the tradeoff between the conflicting requirements of maximizing the information rate to the legitimate receiver and the equivocation level at the eavesdropper [3]. To maximize the contribution of the correlated sources, we must operate at the Shannon capacity of the underlying channel. In contrast, to maximize the contribution of the wiretap channel, we operate at a point of maximum equivocation. In general, the optimal operating point lies in between these extremes. We illustrate this tradeoff in detail for the case of Gaussian sources and channels.

In related work [10], [16], [20] study a setup involving sources and channels, but require that a source sequence be reproduced at the destination subjected to an equivocation level at the eavesdropper. In contrast our paper does not impose any requirement on reproduction

of a source sequence, but instead requires that the terminals generate a common secret key. A recent work, [18], considers transmitting an independent confidential message using correlated sources and noisy channels. This problem is different from the secret-key generation problem, since the secret-key, by definition, is an arbitrary function of the source sequence, while the message is required to be independent of the source sequences. Independently and concurrently of our work the authors of [17] consider the scenario of joint secret-message-transmission and secret-key-generation, which when specialized to the case of no secret-message reduces to the scenario treated in this paper. While the expression for the achievable rate in [17] appears consistent with the expression in this paper, the optimality claims in [17] are limited to the case when either the sources or the channel do not provide any secrecy.

The rest of the paper is organized as follows. The problem of interest is formally introduced in section II and the main results of this work are summarized in section III. Proofs of the lower and upper bound appear in sections IV and V respectively. The secrecy capacity for the case of independent parallel reversely degraded channels is provided in section VI. The case when the wiretapper has access to a degraded source and observes transmission through a degraded channel is treated in section VII while section VIII considers the case when a public discussion channel allows interactive communication between the sender and the receiver. The conclusions appear in section IX.

II. Problem Statement

Fig. 1 shows the setup of interest. The sender and receiver communicate over a wiretap channel and have access to correlated sources. They can interact over a public-discussion channel. We consider two extreme scenarios: (a) the discussion channel does not exist (b) the discussion channel has unlimited capacity.

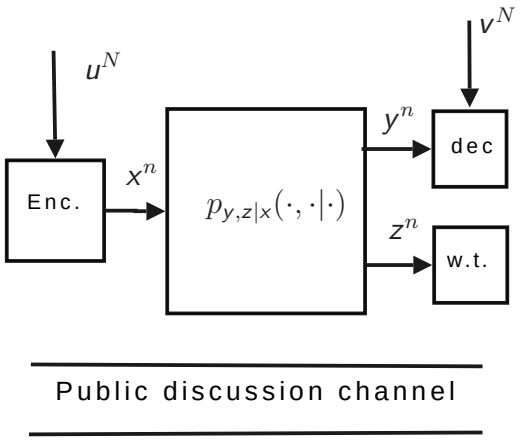

Fig. 1. Secret-key agreement over the wiretap channel with correlated sources. The sender and receiver communicate over a wiretap channel and have access to correlated sources. They communicate interactively over a public discussion channel of rate R, if it is available.

The channel from sender to receiver and wiretapper is a discrete-memoryless-channel (DMC), $p_{y,z|x}(\cdot,\cdot|\cdot)$. The sender and intended receiver observe discrete-memoryless-multiple-source (DMMS) $p_{u,v}(\cdot,\cdot)$ of length N and communicate over n uses of the DMC. We separately consider the cases when no public discussion is allowed and unlimited discussion is allowed.

A. No discussion channel is available

An (n, N) secrecy code is defined as follows. The sender samples a random variable m_{x} [1] from the conditional distribution $p_{\mathsf{m}_x|\mathsf{u}^N}(\cdot|u^n)$. The encoding function $f_n : \mathcal{M}_x \times \mathcal{U}^N \to \mathcal{X}^n$ maps the observed source sequence to the channel output. In addition, two key generation functions $\mathsf{k} = K_n(\mathcal{M}_x, \mathcal{U}^N)$ and $\mathsf{l} = L_n(\mathcal{V}^N, \mathcal{Y}^n)$ at the sender and the receiver are used for secret-key generation. A secret-key rate R is achievable with bandwidth expansion factor β if there exists a sequence of $(n, \beta n)$ codes, such that for a sequence ε_n that approaches zero as $n \to \infty$, we have (i) $\Pr(\mathsf{k} \neq \mathsf{l}) \leq \varepsilon_n$ (ii) $\frac{1}{n}H(\mathsf{k}) \geq R - \varepsilon_n$ (iii)$\frac{1}{n}I(\mathsf{k}; \mathsf{z}^n) \leq \varepsilon_n$. The secret-key-capacity is the supremum of all achievable rates.

For some of our results, we will also consider the case when the wiretapper observes a side information sequence w^N sampled i.i.d. $p_{\mathsf{w}}(\cdot)$. In this case, the secrecy condition in (iii) above is replaced with

$$\frac{1}{n}I(\mathsf{k}; \mathsf{z}^n, \mathsf{w}^N) \leq \varepsilon_n \tag{1}$$

In addition, for some of our results we will consider the special case when the wiretap channel consists of parallel and independent channels each of which is degraded.

1) Parallel Channels:

Definition 1: A *product* broadcast channel is one in which the M constituent subchannels have finite input and output alphabets, are memoryless and independent of each other, and are characterized by their transition probabilities

$$\Pr\left(\{y_m^n, z_m^n\}_{m=1,\ldots,M} \mid \{x_m^n\}_{m=1,\ldots,M}\right) = \prod_{m=1}^{M}\prod_{t=1}^{n}\Pr(y_m(t), z_m(t) \mid x_m(t)), \tag{2}$$

where $x_m^n = (x_m(1), x_m(2), \ldots, x_m(n))$ denotes the sequence of symbols transmitted on subchannel m, where $y_m^n = (y_m(1), y_m(2), \ldots, y_m(n))$ denotes the sequence of symbols obtained by the legitimate receiver on subchannel m, and where $z_m^n = (z_m(1), z_m(2), \ldots, z_m(n))$ denotes the sequence of symbols received by the eavesdropper on subchannel m.

■

A special class of product broadcast channels, known as the reversely degraded broadcast channel [8] are defined as follows.

Definition 2: A product broadcast channel is *reversely-degraded* when each of the M constituent subchannels is degraded in a prescribed order. In particular, for each subchannel m, one of $\mathsf{x}_m \to \mathsf{y}_m \to \mathsf{z}_m$ or $\mathsf{x}_m \to \mathsf{z}_m \to \mathsf{y}_m$ holds.

■

Note that in Def. 2 the order of degradation need not be the same for all subchannels, so the overall channel need not be degraded. We also emphasize that in any subchannel the receiver and eavesdropper are *physically* degraded. Our capacity results, however, only depend on the marginal distribution of receivers in each subchannel[2]. Accordingly, our results in fact hold for the larger class of channels in which there is only stochastic degradation in the subchannels.

We obtain further results when the channel is Gaussian.

[1]The alphabets associated with random variables will be denoted by calligraphy letters. Random variables are denoted by sans-serif font, while their realizations are denoted by standard font. A length n sequence is denoted by x^n.

[2]However, when we consider the presence of a public-discussion channel and interactive communication, the capacity does depend on joint distribution $p_{\mathsf{y},\mathsf{z}|\mathsf{x}}(\cdot)$

2) Parallel Gaussian Channels and Gaussian Sources:

Definition 3: A reversely-degraded product broadcast channel is *Gaussian* when it takes the form

$$\begin{aligned} y_m &= x_m + n_{\mathrm{r},m}, \\ z_m &= x_m + n_{\mathrm{e},m}, \end{aligned} \quad m = 1, \ldots, M \tag{3}$$

where the noise variables are all mutually independent, and $n_{\mathrm{r},m} \sim \mathcal{CN}(0, \sigma^2_{\mathrm{r},m})$ and $n_{\mathrm{e},m} \sim \mathcal{CN}(0, \sigma^2_{\mathrm{e},m})$. For this channel, there is also an average power constraint

$$E\left[\sum_{m=1}^{M} x_m^2\right] \leq P.$$

■

Furthermore we assume that u and v are jointly Gaussian (scalar valued) random variables, and without loss of generality we assume that $u \sim \mathcal{N}(0,1)$ and $v = u + s$, where $s \sim \mathcal{N}(0, S)$ is independent of u.

B. Presence of a public discussion channel

We will also consider a variation on the original setup when a public discussion channel is available for communication. This setup was first introduced in the pioneering works [1], [15] where the secret-key capacity was bounded for source and channel models. The sender and receiver can interactively exchange messages on the public discussion channel.

The sender transmits symbols $x_1, \ldots x_n$ at times $0 < i_1 < i_2 < \ldots < i_n$ over the wiretap channel. At these times the receiver and the eavesdropper observe symbols $y_1, y_2, \ldots, y_n$ and $z_1, z_2, \ldots, z_n$ respectively. In the remaining times the sender and receiver exchange messages ϕ_t and ψ_t where $1 \leq t \leq k$. For convenience we let $i_{n+1} = k+1$. The eavesdropper observes both ϕ_t and ψ_t. More formally,

- At time 0 the sender and receiver sample random variables m_{x} and m_y respectively from conditional distributions $p_{m_{\mathrm{x}}|u^N}(\cdot|u^N)$ and $p_{m_y|v^N}(\cdot|v^N)$. Note that $m_{\mathrm{x}} \to u^N \to v^N \to m_y$ holds.
- At times $0 < t < i_1$ the sender generates $\phi_t = \Phi_t(m_{\mathrm{x}}, u^N, \psi^{t-1})$ and the receiver generates $\psi_t = \Psi_t(m_y, v^N, \phi^{t-1})$. These messages are exchanged over the public channel.
- At times i_j, $1 \leq j \leq n$, the sender generates $x_j = X_j(m_{\mathrm{x}}, u^N, \psi^{i_j - 1})$ and sends it over the channel. The receiver and eavesdropper observe y_j ad z_j respectively. For these times we set $\phi_{i_j} = \psi_{i_j} = 0$.
- For times $i_j < t < i_{j+1}$, where $1 \leq j \leq n$, the sender and receiver compute $\phi_t = \Phi_t(m_{\mathrm{x}}, u^N, \psi^{t-1})$ and $\psi_t = \Psi_t(m_y, v^N, y^j, \phi^{t-1})$ respectively and exchange them over the public channel.
- At time $k+1$, the sender and receiver compute $k = K_n(m_{\mathrm{x}}, u^N, \psi^k)$ and the receiver computes $l = L_n(m_y, v^N, y^n, \phi^k)$.

We require that for some sequence ε_n that vanishes as $n \to \infty$, $\Pr(k \neq l) \leq \varepsilon_n$ and

$$\frac{1}{n} I(k; z^n, \psi^k, \phi^k) \leq \varepsilon_n. \tag{4}$$

III. Statement of Main Results

It is convenient to define the following quantities which will be used in the sequel. Suppose that t is a random variable such that $t \to u \to v$, and a and b are random variables such that

$b \to a \to x \to (y, z)$ holds and $I(y; b) \leq I(z; b)$. Furthermore define

$$R_{\text{ch}} = I(a; y), \tag{5a}$$
$$R_{\text{eq}}^{-} = I(a; y|b) - I(a; z|b) \tag{5b}$$
$$R_{\text{s}} = I(t; v), \tag{5c}$$
$$R_{\text{wz}} = I(t; u) - I(t; v). \tag{5d}$$
$$R_{\text{eq}}^{+} = I(x; y \mid z). \tag{5e}$$
$$R_{\text{ch}}^{+} = I(x; y), \tag{5f}$$

We establish the following lower and upper bounds on the secret key rate in Section IV and V respectively.

Lemma 1: A lower bound on the secret-key rate is given by

$$R_{\text{key}}^{-} = \beta R_{\text{s}} + R_{\text{eq}}^{-}, \tag{6}$$

where the random variables t, a and b defined above additionally satisfy the condition

$$\beta R_{\text{wz}} \leq R_{\text{ch}} \tag{7}$$

and the quantities R_{wz}, R_{s}, R_{eq}^{-} and R_{ch} are defined in (5d), (5c), (5b) and (5a) respectively. ■

Lemma 2: An upper bound on the secret-key rate is given by,

$$R_{\text{key}}^{+} = \sup_{\{(x,t)\}} \left\{ \beta R_{\text{s}} + R_{\text{eq}}^{+} \right\}, \tag{8}$$

where the supremum is over all distributions over the random variables (x, t) that satisfy $t \to u \to v$, the cardinality of t is at-most the cardinality of u plus one, and

$$\beta R_{\text{wz}} \leq R_{\text{ch}}^{+}. \tag{9}$$

The quantities R_{s}, R_{wz}, R_{eq}^{+} and R_{ch}^{+} are defined in (5c), (5d), (5e) and (5f) respectively.

Furthermore, it suffices to consider only those distributions where (x, t) are independent. ■

A. Reversely degraded parallel independent channels

The bounds in Lemmas 1 and 2 coincide for the case of reversely degraded channels as shown in section VI-A and stated in the following theorem.

Theorem 1: The secret-key-capacity for the reversely degraded parallel independent channels in Def. 2 is given by

$$C_{\text{key}} = \max_{\{(x_1,\ldots,x_M,t)\}} \left\{ \beta I(v; t) + \sum_{i=1}^{M} I(x_i; y_i|z_i) \right\}, \tag{10}$$

where the random variables $(x_1, \ldots, x_M, t)$ are mutually independent, $t \to u \to v$, and

$$\sum_{i=1}^{M} I(x_i; y_i) \geq \beta \{ I(u; t) - I(v; t) \} \tag{11}$$

Furthermore, the cardinality of t obeys the same bounds as in Lemma 2.

■

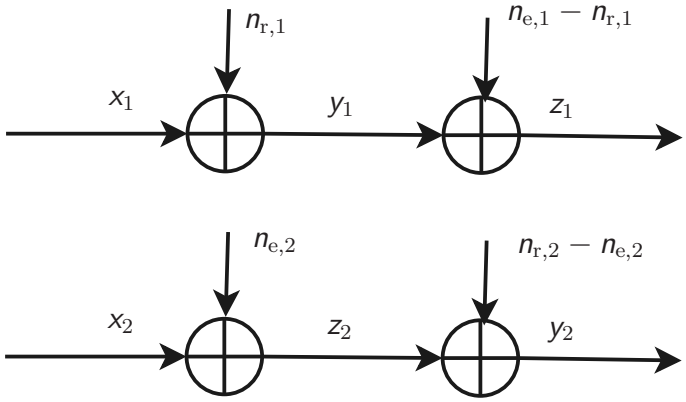

Fig. 2. An example of independent parallel and reversely degraded Gaussian channels. On the first channel, the eavesdropper channel is noisier than the legitimate receiver's channel while on the second channel the order of degradation is reversed.

B. Gaussian Channels and Sources

For the case of Gaussian sources and Gaussian channels, the secret-key capacity can be achieved by Gaussian codebooks as established in section VI-B and stated below.

Corollary 1: The secret-key capacity for the case of Gaussian parallel channels and Gaussian sources in subsection II-A.2 is obtained by optimizing (10) and (11) over independent Gaussian distributions i.e., by selecting $x_i \sim \mathcal{N}(0, P_i)$ and $u = t + d$, for some $d \sim \mathcal{N}(0, D)$, independent of t and $\sum_{i=1}^{n} P_i \leq P$, $P_i \geq 0$, and $0 < D \leq 1$.

$$C_{\text{key}}^{G} = \max_{\{P_i\}_{i=1}^{M}, D} \left\{ \frac{\beta}{2} \log\left(\frac{1+S}{D+S}\right) + \sum_{\substack{i:1\leq i\leq M \\ \sigma_{r,i}\leq\sigma_{e,i}}} \frac{1}{2} \log\left(\frac{1+P_i/\sigma_{r,i}^2}{1+P_i/\sigma_{e,i}^2}\right) \right\}, \tag{12}$$

where $D, P_1, \ldots, P_M$ also satisfy the following relation:

$$\sum_{i=1}^{M} \frac{1}{2} \log\left(1 + \frac{P_i}{\sigma_{r,i}^2}\right) \geq \beta \left\{ \frac{1}{2} \log\left(\frac{1}{D}\right) - \frac{1}{2} \log\left(\frac{1+S}{D+S}\right) \right\} \tag{13}$$

■

C. Remarks

1) Note that the secret-key capacity expression (10) exploits both the source and channel uncertainties at the wiretapper. By setting either uncertainty to zero, one can recover known results. When $I(u; v) = 0$, i.e., there is no secrecy from the source, the secret-key-rate equals the wiretap capacity [19]. If $I(x; y|z) = 0$, i.e., there is no secrecy from the channel, then our result essentially reduces to the result by Csiszar and Narayan [5], that consider the case when the channel is a noiseless bit-pipe with finite rate.
2) In general, the setup of wiretap channel involves a tradeoff between information rate and equivocation. The secret-key generation setup provides an operational significance to this tradeoff. Note that the capacity expression (10) in Theorem 1 involves two terms. The first term $\beta I(t; v)$ is the contribution from the correlated sources. In general, this quantity increases by increasing the information rate $I(x; y)$ as seen from (11). The second term, $I(x; y|z)$ is the equivocation term and increasing this term, often comes at

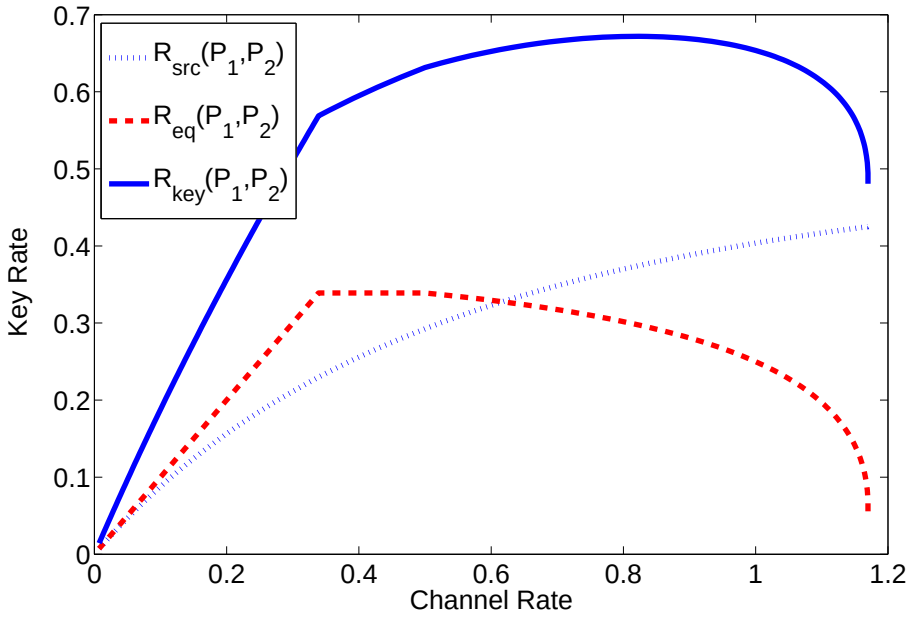

Fig. 3. Tradeoff inherent in the secret-key-capacity formulation. The solid curve is the secret-key-rate, which is the sum of the two other curves. The dotted curve represents the source equivocation, while the dashed curve represents the channel equivocation (18). The secret-key-capacity is obtained at a point between the maximum equivocation and maximum rate.

the expense of the information rate. Maximizing the secret-key rate, involves operating on a certain intermediate point on the rate-equivocation tradeoff curve as illustrated by an example below.

Consider a pair of Gaussian parallel channels,

$$\begin{aligned} y_1 &= a_1 x + n_{r,1}, \quad & z_1 &= b_1 x + n_{e,1} \\ y_2 &= a_2 x + n_{r,2}, \quad & z_2 &= y_2 \end{aligned} \tag{14}$$

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 variables are all sampled from the $\mathcal{CN}(0,1)$ distribution and appropriately correlated so that the users are degraded on each channel. A total power constraint $P = 1$ is selected and the bandwidth expansion factor β equals unity.

From Theorem 1,

$$C_{\text{key}} = \max_{P_1,P_2,D} R_{\text{eq}}(P_1,P_2) + \frac{1}{2}\log\frac{2}{1+D}, \tag{15}$$

such that,

$$R_{\text{wz}}(D) = \frac{1}{2}\log\frac{1}{D} - \frac{1}{2}\log\frac{2}{1+D} \tag{16}$$

$$\leq \frac{1}{2}\left(\log\left(1+a_1^2P_1\right) + \log(1+a_2^2P_2)\right), \tag{17}$$

$$R_{\text{eq}}(P_1,P_2) = \frac{1}{2}\left(\log(1+a_1^2P_1) - \log(1+b_1^2P_1)\right). \tag{18}$$

Fig. 3 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. The optimal

point of operation is between the point of maximum equivocation and maximum rate as indicated by the maximum of the solid line in Fig. 3. This corresponds to a power allocation $(P_1, P_2) \approx (0.29, 0.71)$ and the maximum value is $R_{\text{key}} \approx 0.6719$.

D. Side information at the wiretapper

So far, we have focussed on the case when there is no side information at the wiretapper. This assumption is valid for certain application such as biometrics, when the correlated sources constitute successive measurements of a person's biometric. In other applications, such as sensor networks, it is more realistic to assume that the wiretapper also has access to a side information sequence.

We consider the setup described in Fig. 1, but with a modification that the wiretapper observes a source sequence w^N, obtained by $N-$ independent samples of a random variable w. In this case the secrecy condition takes the form in (1). We only consider the case when the sources and channels satisfy a degradedness condition.

Theorem 2: Suppose that the random variables (u, v, w) satisfy the degradedness condition $u \to v \to w$ and the broadcast channel is also degraded i.e., $x \to y \to z$. Then, the secret-key-capacity is given by

$$C_{\text{key}} = \max_{(x,t)} \left\{ \beta(I(t;v) - I(t;w)) + I(x;y|z) \right\}, \tag{19}$$

where the maximization is over all random variables (t, x) that are mutually independent, $t \to u \to v \to w$ and

$$I(x;y) \geq \beta(I(u;t) - I(v;t)) \tag{20}$$

holds. Furthermore, it suffices to optimize over random variables t whose cardinality does not exceed that of u plus two.

■

E. Secret-key capacity with a public discussion channel

When public interactive communication is allowed as described in section II-B, we have the following upper bound on the secret-key capacity.

Theorem 3: An upper bound on the secret-key capacity for source-channel setup with a public discussion channel is

$$C_{\text{key}} \leq \max_{p_x} I(x;y|z) + \beta I(u;v). \tag{21}$$

The upper bound is tight when channel satisfies either $x \to y \to z$ or $y \to x \to z$.

■

The presence of a public discussion channels allows us to decouple the source and channel codebooks. We generate two separate keys — one from the source component using a Slepian-Wolf codebook and one from the channel component using the key-agreement protocol described in [1], [15].

The upper bound expression (21) in Theorem 3 is established using techniques similar to the proof of the upper bound on the secret-key rate for the channel model [1, Theorem 3]. A derivation is provided in section VIII.

Fig. 4 illustrates the contribution of source and channel coding components for the case of Gaussian parallel channels (14) consisting of (physically) degraded component channels. The term $I(u;v)$ is independent of the channel coding rate, and is shown by the horizontal line.

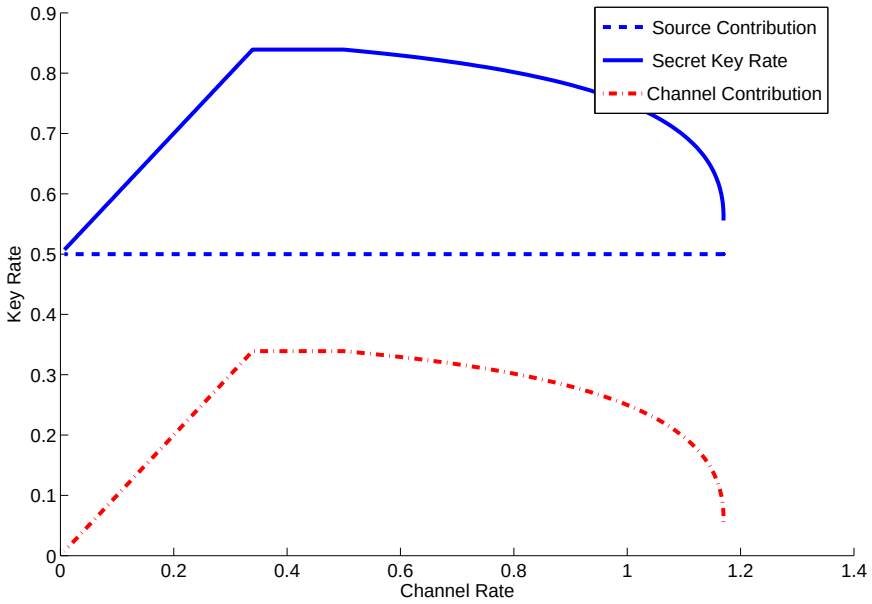

Fig. 4. Secret-key-rate in the presence of a public discussion channel in the Gaussian example (14). The solid curve is the secret-key-rate, which is the sum of the two other curves. The horizontal line is the key rate from the source components. Regardless of the channel rate, the rate is 0.5 bits/symbol. The dashed-dotted curve is the key-rate using the channel $I(x;y|z)$.

The channel equivocation rate $I(x;y|z)$ is maximized at the secrecy capacity. The overall key rate is the sum of the two components. Note that unlike Fig. 3, there is no inherent tradeoff between source and channel coding contributions in the presence of public discussion channel and the design of source and channel codebooks is decoupled.

IV. Achievability: Coding Theorem

We demonstrate the coding theorem in the special case when $a = x$ and $b = 0$ in Lemma 1. Accordingly we have that (5a) and (5b) reduce to

$$R_{\text{ch}} = I(x;y) \tag{22a}$$

$$R_{\text{eq}}^{-} = I(x;y) - I(x;z) \tag{22b}$$

The more general case, can be incorporated by introducing an auxiliary channel $a \to x$ and superposition coding [4] as outlined in Appendix I. Furthermore, in our discussion below we will assume that the distributions $p_{t|u}$ and p_x are selected such that, for a sufficiently small but fixed $\delta > 0$, we have

$$\beta R_{\text{wz}} = R_{\text{ch}} - 3\delta. \tag{23}$$

We note that the optimization over the joint distributions in Lemma 1 is over the region $\beta R_{\text{wz}} \leq R_{\text{ch}}$. If the joint distributions satisfy that $\beta R_{\text{wz}} = \alpha(R_{\text{ch}} - 3\delta)$ for some $\alpha < 1$, one can use the code construction below for a bock-length αn and then transmit an independent message at rate R_{eq}^{-} using a perfect-secrecy wiretap-code. This provides a rate of

$$\alpha\left(\frac{\beta}{\alpha}R_{\text{wz}} + R_{\text{eq}}^{-}\right) + (1-\alpha)R_{\text{eq}}^{-} = R_{\text{eq}}^{-} + \beta R_{\text{wz}},$$

as required.

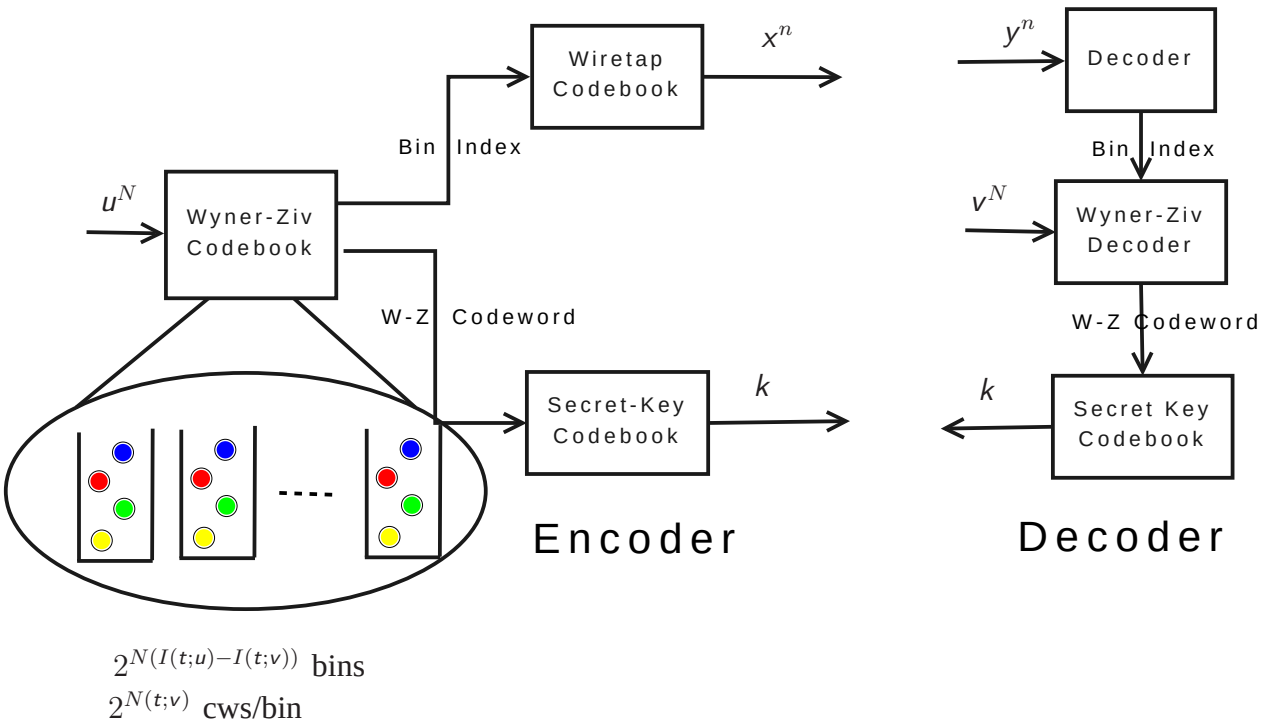

Fig. 5. Source-Channel Code Design for secret-key distillation problem. The source sequence u^N is mapped to a codeword in a Wyner-Ziv codebook. This codeword determines the secret-key via the secret-key codebook. The bin index of the codeword constitutes a message in the wiretap codebook.

A. Codebook Construction

Our codebook construction is as shown in the Fig. 5.

An intuition behind the codebook construction is first described. The wiretap channel carries an ambiguity of $2^{n\{I(a;y|b)-I(a;z|b)\}}$ at the eavesdropper for each transmitted message. Furthermore, each message only reveals the bin index. Hence it carries an additional ambiguity of $2^{NI(v;t)}$ codeword sequences. Combining these two effects the total ambiguity is $2^{n\{I(a;y|b)-I(a;z|b)+\beta I(v;t)\}}$. Thus a secret-key can be produced at the rate $I(a;y|b)-I(a;z|b)+\beta I(v;t)$. This heuristic intuition is made precise below.

The coding scheme consists of three codebooks: Wyner-Ziv codebook, secret-key codebook and a wiretap codebook that are constructed via a random coding construction. In our discussion below we will be using the notion of strong typicality. Given a random variable t, the set of all sequences of length N and type that coincides with the distribution p_t is denoted by T_t^N. The set of all sequences whose empirical type is in an ε-shell of p_t is denoted by $T_{t,\varepsilon}^N$. The set of jointly typical sequences are defined in an analogous manner. Given a sequence u^N of type T_u^N, the set of all sequences v^N that have a joint type of $p_{u,v}()$ is denoted by $T_{u,v}^N(u^N)$. We will be using the following properties of typical sequences

$$|T_{t,\varepsilon}^N| = \exp(N(H(t)+o_\varepsilon(1))) \tag{24a}$$

$$\Pr(t^N = t^N) = \exp(-N(H(t)+o_\varepsilon(1))), \quad \forall\ t^N \in T_{t,\varepsilon}^N \tag{24b}$$

$$\Pr(t^N \in T_{t,\varepsilon}^N) \geq 1-o_\varepsilon(1), \tag{24c}$$

where $o_\varepsilon(1)$ is a term that approaches zero as $N\to\infty$ and $\varepsilon\to 0$.

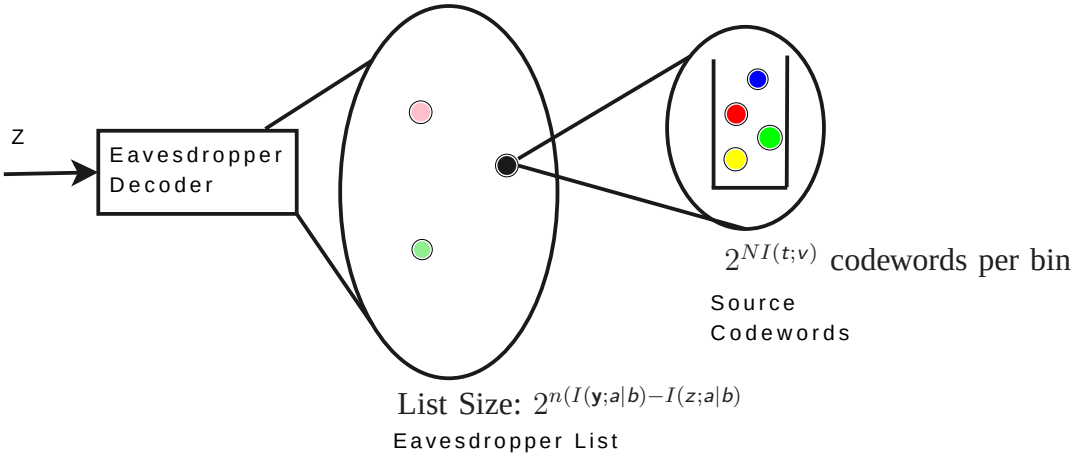

Fig. 6. Equivocation at the eavesdropper through the source-channel codebook. The channel codebook induces an ambiguity of $2^{n(I(a;y|b)-I(a;z|b))}$ among the codeword sequences a^n when the decoder observes z^n. Each sequence a^n only reveals the bin index of the Wyner-Ziv codeword. In induces an ambiguity of $2^{NI(t;v)}$ at the eavesdropper, resulting in a total ambiguity of $2^{n(\beta I(t;v)+I(a;y|b))-I(a;z|b)}$.

For fixed, but sufficiently small constants $\delta > 0$ and $\eta = \delta/\beta > 0$, let,

$$M_{\mathrm{WZ}} = \exp(N(R_{\mathrm{s}} - \eta)) \tag{25a}$$
$$N_{\mathrm{WZ}} = \exp(N(R_{\mathrm{wz}} + 2\eta)) \tag{25b}$$
$$M_{\mathrm{SK}} = \exp(n(I(x;z) - \delta)) \tag{25c}$$
$$N_{\mathrm{SK}} = \exp(n(\beta R_{\mathrm{s}} + R_{\mathrm{eq}}^{-} - \delta)) \tag{25d}$$

Substituting (5a)-(5d) and (23) into (25a)-(25d) we have that

$$N_{\mathrm{tot}} \triangleq M_{\mathrm{SK}} \cdot N_{\mathrm{SK}} = M_{\mathrm{WZ}} \cdot N_{\mathrm{WZ}} = \exp(N(I(t;u) + \eta)) \tag{26}$$

We construct the Wyner-Ziv and secret-key codebooks as follows. Randomly and independently select N_{tot} sequences from the set of $t-$typical sequences T_t^N. Denote this set $\mathcal{T}$. Randomly and independently partition this set into the following codebooks[3]:

- *Wyner-Ziv* codebook with N_{WZ} bins consisting of M_{WZ} sequences. The j^{th} sequence in bin i is denoted by $t_{ij,\mathrm{WZ}}^N$.
- *Secret-key* codebook with N_{SK} bins consisting of M_{SK} sequences. The j^{th} sequence in bin i is denoted by $t_{ij,\mathrm{SK}}^N$.

We define two functions $\Phi_{\mathrm{WZ}} : \mathcal{T} \to \{1, \ldots, N_{\mathrm{WZ}}\}$ and $\Phi_{\mathrm{SK}} : \mathcal{T} \to \{1, \ldots, N_{\mathrm{SK}}\}$ as follows.

Definition 4: Given a codeword sequence t^N, define two mappings

1) $\Phi_{\mathrm{WZ}}(t^N) = i$, if $\exists j \in [1, M_{\mathrm{WZ}}]$, such that $t^N = t_{ij,\mathrm{WZ}}^N$.
2) $\Phi_{\mathrm{SK}}(t^N) = i$, if $\exists j \in [1, M_{\mathrm{SK}}]$ such that $t^N = t_{ij,\mathrm{SK}}^N$.

■

The channel codebook consists of $N_{\mathrm{WZ}} = \exp(n(R_{\mathrm{ch}} - \delta))$ sequences x^n uniformly and independently selected from the set of $x-$typical sequences T_x^n. The channel encoding function maps message i into the sequence x_i^n, i.e., $\Phi_{\mathrm{ch}} : \{1, \ldots, N_{\mathrm{WZ}}\} \to \mathcal{X}^n$ is defined as $\Phi_{\mathrm{ch}}(i) = x_i^n$.

[3]As will be apparent in the analysis, the only pairwise independence is required between the codebooks i.e., $\forall t^N, \hat{t}^N \in \mathcal{T}$, $\Pr\left(\Phi_{\mathrm{WZ}}(t^N) = \Phi_{\mathrm{WZ}}(\hat{t}^N) | \Phi_{\mathrm{SK}}(t^N) = \Phi_{\mathrm{SK}}(\hat{t}^N)\right) = \Pr\left(\Phi_{\mathrm{WZ}}(t^N) = \Phi_{\mathrm{WZ}}(\hat{t}^N)\right) = \frac{1}{N_{\mathrm{WZ}}}$

B. Encoding

Given a source sequence u^N, the encoder produces a secret-key k and a transmit sequence x^N as shown in Fig. 5.

- Find a sequence $t^N \in \mathcal{T}$ such that $(u^N, t^N) \in T^N_{ut,\varepsilon}$. Let $\mathcal{E}_1$ be the even that no such t^N exists.
- Compute $\phi = \Phi_{\rm WZ}(t^N)$ and $k = \Phi_{\rm SK}(t^N)$. Declare k as the secret-key.
- Compute $x_i^n = \Phi_{\rm ch}(\phi)$, and transmit this sequence over $n-$uses of the DMC.

C. Decoding

The main steps of decoding at the legitimate receiver are shown in Fig. 5 and described below.

- Given a received sequence y^n, the sender looks for a unique index i such that $(x_i^n, y^n) \in T^n_{xy,\varepsilon}$. An error event $\mathcal{E}_2$ happens if x_i^n is not the transmitted codeword.
- Given the observed source sequence v^N, the decoder then searches for a unique index $j \in [1, M_{\rm WZ}]$ such that $(t^N_{ij,\rm WZ}, v^N) \in T^N_{tv,\varepsilon}$. An error event $\mathcal{E}_3$ is declared if a unique index does not exist.
- The decoder computes $\hat{k} = \Phi_{\rm SK}(t^N_{ij,\rm WZ})$ and declares $\hat{k}$ as the secret key.

D. Error Probability Analysis

The error event of interest is $\mathcal{E} = \{k \neq \hat{k}\}$. We argue that selecting $n \to \infty$ leads to $\Pr(\mathcal{E}) \to 0$.

In particular, note that $\Pr(\mathcal{E}) = \Pr(\mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3) \leq \Pr(\mathcal{E}_1) + \Pr(\mathcal{E}_2) + \Pr(\mathcal{E}_3)$. We argue that each of the terms vanishes with $n \to \infty$.

Recall that $\mathcal{E}_1$ is the event that the encoder does not find a sequence in $\mathcal{T}$ typical with u^N. Since $\mathcal{T}$ has $\exp(N(I(u;t)+\eta))$ sequences randomly and uniformly selected from the set T_t^N, we have that $\Pr(\mathcal{E}_1) \to 0$.

Since the number of channel codewords equals $N_{\rm WZ} = \exp(n(I(x;y)-\delta))$, and the codewords are selected uniformly at random from the set $T^n_{x,\varepsilon}$, the error event $\Pr(\mathcal{E}_2) \to 0$.

Finally, since the number of sequences in each bin satisfies $M_{\rm WZ} = \exp(N(I(t;v)-\eta))$, joint typical decoding guarantees that $\Pr(\mathcal{E}_3) \to 0$.

E. Secrecy Analysis

In this section, that for the coding scheme discussed above, the equivocation at the eavesdropper is close (in an asymptotic sense) to $R_{\rm key}$.

First we establish some uniformity properties which will be used in the subsequent analysis.

1) Uniformity Properties: In our code construction $\Phi_{\rm WZ}$ satisfies some useful properties which will be used in the sequel.

Lemma 3: The random variable $\Phi_{\rm WZ}$ in Def. 4 satisfies the following relations

$$\frac{1}{n}H(\Phi_{\rm WZ}) = \beta R_{\rm WZ} + o_\eta(1) \tag{27a}$$

$$\frac{1}{n}H(t^N|\Phi_{\rm WZ}) = \beta I(t;v) + o_\eta(1) \tag{27b}$$

$$\frac{1}{n}H(\Phi_{\rm WZ}|z^n) = I(x;y) - I(x;z) + o_\eta(1) \tag{27c}$$

where $o_\eta(1)$ vanishes to zero as we take $\eta \to 0$ and $N \to \infty$ for each η.

Proof: Relations (27a) and (27b) are established below by using the properties of typical sequences (c.f. (24a)-(24c)). Relation (27c) follows from the secrecy analysis of the channel codebook when the message is $\Phi_{\rm WZ}$. The details can be found in e.g., [19].

To establish (27a), define the function $\Gamma_{\rm WZ} : \mathcal{T} \to \{1, \ldots, M_{\rm WZ}\}$ to identify the position of the sequence $t^N \in \mathcal{T}$ in a given bin i.e., $\Gamma_{\rm WZ}(t^N_{ij,{\rm WZ}}) = j$ and note that,

$$\Pr(\Gamma_{\rm WZ} = j, \Phi_{\rm WZ} = i) \leq \sum_{u^N \in T_{u,t,\eta}(t^N_{ij,{\rm WZ}})} \Pr(u^N) \tag{28}$$

$$= \sum_{u^N \in T_{u,t,\eta}(t^N_{ij,{\rm WZ}})} \exp(-N(H(u) + o_\eta(1))) \tag{29}$$

$$= \exp(N(H(u|t) + o_\eta(1))) \exp(-N(H(u) + o_\eta(1))) \tag{30}$$

$$= \exp(-N(I(t;u) + o_\eta(1))) \tag{31}$$

where (28) follows from the construction of the joint-typicality encoder, (29) from (24b) and (30) from (24a). Marginalizing (28), we have that

$$\begin{aligned}\Pr(\Phi_{\rm WZ} = i) &= \sum_{j=1}^{M_{\rm WZ}} \Pr(\Gamma_{\rm WZ} = j, \Phi_{\rm WZ} = i) \\ &\leq M_{\rm WZ} \exp(-N(I(t;u) + o_\eta(1))) \\ &= \exp(-N(I(t;u) - I(t;v) + o_\eta(1))) \\ &= \exp(-N(R_{\rm WZ} + o_\eta(1))) \end{aligned} \tag{32}$$

Eq. (27a) follows from (32) and the continuity of the entropy function. Furthermore, we have from (31) that

$$\frac{1}{N} H(\Phi_{\rm WZ}, \Gamma_{\rm WZ}) = I(t;u) + o_\eta(1). \tag{33}$$

The relation (27b) follows by substituting (27a), since

$$\frac{1}{N} H(t^N|\Phi_{\rm WZ}) = \frac{1}{N} H(\Gamma_{\rm WZ}|\Phi_{\rm WZ}) = \frac{1}{N} H(\Gamma_{\rm WZ}, \Phi_{\rm WZ}) - \frac{1}{N} H(\Phi_{\rm WZ}) = I(t;v) + o_\eta(1). \tag{34}$$

■

Lemma 4: The construction of the secret-key codebook and Wyner-Ziv codebook is such that the eavesdropper can decode the sequence t^N if it is revealed the secret-key $\Phi_{\rm SK} = k$ in addition to its observed sequence z^n. In particular

$$\frac{1}{n} H(t^N|z^n, k) = o_\eta(1). \tag{35}$$

Proof: We show that there exists a decoding function $g : \mathcal{Z}^n \times \{1, 2, \ldots, N_{\rm SK}\} \to \mathcal{T}$ that such that $\Pr(t^N \neq g(z^n, k)) \to 0$ as $n \to \infty$. In particular, the decoding function $g(\cdot, \cdot)$ searches for the sequences in the bin associated with k in the secret-key codebook, whose bin-index in the Wyner-Ziv codebook maps to a sequence x_i^n jointly typical with the received sequence z^n. More formally,

- Given z^n, the decoder constructs a the set of indices $\mathcal{I}_{\rm x} = \{i : (x_i^n, z^n) \in T^n_{xz,\varepsilon}\}$.

- Given k, the decoder constructs a set of sequences, $\mathcal{S} = \left\{ t^N_{kj,\mathrm{SK}} : \Phi_{\mathrm{WZ}}(t^N_{kj,\mathrm{SK}}) \in \mathcal{I}_{\mathrm{x}}, 1 \le j \le M_{\mathrm{SK}}, \right\}$.
- If S contains a unique sequence $\hat{t}^N$, it is declared to be the required sequence. An error event is defined as

$$\begin{aligned} \mathcal{J} &= \{\hat{t}^N \neq t^N\} \\ &= \left\{\exists j, 1 \le j \le M_{\mathrm{SK}}, \Phi_{\mathrm{WZ}}(t^N_{k,j,\mathrm{SK}}) \in \mathcal{I}_{\mathrm{x}}, j \neq j_0\right\}, \end{aligned} \tag{36}$$

  where j_0 is the index of the sequence t^N in bin k of the secret-key codebook, i.e., $t^N_{kj_0,\mathrm{SK}} = t^N$.

It suffices to show that $\Pr(\mathcal{J}) \to 0$ as $n \to \infty$.
We begin by defining the following events:

- The event that the sequence $t^N \notin \mathcal{S}$, which is equivalent to

$$\mathcal{J}_0 = \left\{\Phi_{\mathrm{WZ}}(t^N_{k,j_0,\mathrm{SK}}) \notin \mathcal{I}_{\mathrm{x}}\right\}.$$

  From (24c) we have that $\Pr(\mathcal{J}_0) = o_\eta(1)$.
- For each $j = 1, 2, \ldots M_{\mathrm{SK}}, j \neq j_0$ the event $\mathcal{J}_j$ that the sequence $t^N_{kj\mathrm{SK}} \in \mathcal{S}$,

$$\mathcal{J}_j = \left\{\Phi_{\mathrm{WZ}}(t^N_{k,j,\mathrm{SK}}) \in \mathcal{I}_{\mathrm{x}}\right\}.$$

- For each $j = 1, 2, \ldots M_{\mathrm{SK}}, j \neq j_0$, define the collision event that $t^N_{\mathrm{kj,SK}}$ and $t^N_{\mathrm{kj_0,SK}}$ belong to the same bins in the in the Wyner-Ziv codebook

$$\mathcal{J}_{\mathrm{col,j}} = \left\{\Phi_{\mathrm{WZ}}(t^N_{kj,\mathrm{SK}}) = \Phi_{\mathrm{WZ}}(t^N_{kj_0,\mathrm{SK}})\right\}.$$

Now we upper bound the error probability in terms of these events.

$$\begin{aligned} \Pr(\mathcal{J}) &\le \Pr(\mathcal{J}|\mathcal{J}_0^c) + \Pr(\mathcal{J}_0) \\ &\le \sum_{j=1, j\neq j_0}^{M_{\mathrm{SK}}} \Pr(\mathcal{J}_j|\mathcal{J}_0^c) + o_\eta(1), \end{aligned} \tag{37}$$

Now observe that

$$\begin{aligned} \Pr(\mathcal{J}_j|\mathcal{J}_0^c) &= \Pr(\mathcal{J}_j \cap \mathcal{J}^c_{\mathrm{col,j}}|\mathcal{J}_0^c) + \Pr(\mathcal{J}_j \cap \mathcal{J}_{\mathrm{col,j}}|\mathcal{J}_0^c) && (38) \\ &\le \Pr(\mathcal{J}_j \cap \mathcal{J}^c_{\mathrm{col,j}}|\mathcal{J}_0^c) + \Pr(\mathcal{J}_{\mathrm{col,j}}|\mathcal{J}_0^c) \\ &\le \Pr(\mathcal{J}_j|\mathcal{J}_0^c \cap \mathcal{J}^c_{\mathrm{col,j}}) + \Pr(\mathcal{J}_{\mathrm{col,j}}|\mathcal{J}_0^c). && (39) \end{aligned}$$

We bound each of the two terms in (39). The first term is conditioned on the event that the sequences $t^N_{kj,\mathrm{SK}}$ and $t^N_{kj_0,\mathrm{SK}}$ are assigned to independent bins in the Wyner-Ziv codebook. This event is equivalent to the event that a randomly selected sequence x^N belongs to the typical set $\mathcal{I}_{\mathrm{x}}$. The error event is bounded as [2]

$$\Pr(\mathcal{J}_j|\mathcal{J}_0^c \cap \mathcal{J}^c_{\mathrm{col,j}}) \le \exp(-n(I(x;z) - 3\varepsilon)). \tag{40}$$

To upper bound the second term,

$$\begin{aligned} \Pr(\mathcal{J}_j|\mathcal{J}_0^c) &= \Pr(\mathcal{J}_j) && (41) \\ &= \exp(-n(\beta R_{\mathrm{WZ}} + 2\delta)) && (42) \\ &= \exp(-n(I(x;y) - \delta)) && (43) \end{aligned}$$

where (41) follows from the fact the event $\mathcal{J}_0$ is due to the atypical channel behavior and is independent of the random partitioning event that induces $\mathcal{J}_j$, (42) follows from the fact

that each sequence is independently assigned to one of $\exp\{n(\beta R_{\mathrm{WZ}}+2\delta)\}$ bins in the code construction and (43) follows via relation (23).

Substituting (43) and (40) into (39), we have

$$\begin{aligned}\Pr(\mathcal{J}_j|\mathcal{J}_0^c) &\le \exp(-n(I(x;z)-3\varepsilon)) + \exp(-n(I(x;y)-\delta)) \\ &\le \exp(-n(I(x;z)-4\varepsilon)), \quad n \ge n_0, \end{aligned} \tag{44}$$

where we use the fact that $I(x;y) > I(x;z)$ in the last step so that the required n_0 exists.

Finally substituting (44) into (37) and using relation (25c) for M_{SK}, we have that

$$\Pr(\mathcal{J}) \le \exp(-n(\delta-4\varepsilon)) + o_\eta(1), \tag{45}$$

which vanishes with n, whenever the decoding function selects $\varepsilon < \delta/4$. ■

2) Equivocation Analysis: It remains to show that the equivocation rate at the eavesdropper approaches the secret-key rate as $n \to \infty$, which we do below.

$$\begin{aligned} H(k|z^n) &= H(k,t^N|z^n) - H(t^N|z^n,k) \\ &= H(t^N|z^n) - H(t^N|z^n,k) && (46)\\ &= H(t^N,\Phi_{\mathrm{WZ}}|z^n) - H(t^N|z^n,k) && (47)\\ &= H(t^N|\Phi_{\mathrm{WZ}},z^n) + H(\Phi_{\mathrm{WZ}}|z^n) - H(t^N|z^n,k) \\ &= H(t^N|\Phi_{\mathrm{WZ}}) + H(\Phi_{\mathrm{WZ}}|z^n) - H(t^N|z^n,k), && (48)\\ &= n\beta I(t;v) + n\{I(x;y)-I(x;z)\} + no_\eta(1) && (49)\\ &= n(R_{\mathrm{key}} + o_\eta(1)), && (50)\end{aligned}$$

where (46) and (47) follow from the fact that Φ_{WZ} is a deterministic function of t^N and (48) follows from the fact that $t^N \to \Phi_{\mathrm{WZ}} \to z^n$ holds for our code construction. and (49) step follows from (27b) and (27c) in Lemma 3 and Lemma 4.

V. Proof of the Upper bound (Lemma 2)

Given a sequence of (n,N) codes that achieve a secret-key-rate R_{key}, there exists a sequence ε_n, such that $\varepsilon_n \to 0$ as $n \to \infty$, and

$$\frac{1}{n}H(k|y^n,v^N) \le \varepsilon_n \tag{51a}$$

$$\frac{1}{n}H(k|z^n) \ge \frac{1}{n}H(k) - \varepsilon_n. \tag{51b}$$

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

$$\begin{aligned} nR_{\mathrm{key}} &= H(k) \\ &= H(k|y^n,v^N) + I(k;y^n,v^N) \\ &\le n\varepsilon_n + I(k;y^n,v^N) - I(k;z^n) + I(k;z^n) && (52)\\ &\le 2n\varepsilon_n + I(k;y^n,v^N) - I(k;z^n) && (53)\\ &= 2n\varepsilon_n + I(k;y^n) - I(k;z^n) + I(k;v^N|y^n) \\ &\le 2n\varepsilon_n + I(k;y^n) - I(k;z^n) + I(k,y^n;v^N) && (54)\end{aligned}$$

where (52) and (53) follow from (51a) and (51b) respectively.

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

$$\begin{aligned} I(k, y^n; v^N) &= \sum_{i=1}^{n} I(k, y^n; v_i | v_{i+1}^n) \\ &\le \sum_{i=1}^{N} I(k, y^n, v_{i+1}^n; v_i) \\ &\le \sum_{i=1}^{N} I(k, y^n, v_{i+1}^n, u_1^{i-1}; v_i) \\ &= N I(k, y^n, v_{J+1}^n, u_1^{J-1}; v_J | J) \\ &= N I(k, y^n, v_{J+1}^n, u_1^{J-1}, J; v_J) - I(J; v_J) \\ &= N I(t; v) \end{aligned} \tag{55}$$

where (55) follows from the fact that v_J is independent of J and has the same marginal distribution as v.

Next, we upper bound $I(k; y^n) - I(k; z^n)$ 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.

$$\begin{aligned} I(k; y^n) - I(k; z^n) &\le I(k; y^n | z^n) \\ &\le I(x^n; y^n | z^n) && (56) \\ &\le \sum_{i=1}^{n} I(x_i; y_i | z_i) && (57) \\ &\le n I(x; y | z), && (58) \end{aligned}$$

where (56) follows from the Markov condition $k \to x^n \to (y^n, z^n)$ and (57) follows from the fact that the channel is memoryless and (58) follows from Jensen's inequality since the term $I(x; y|z)$ is concave in the distribution p_x (see e.g., [13, Appendix-I]).

Combining (58) and (55) we have that

$$R_{\mathrm{key}} \le I(x; y|z) + \beta I(v; t), \tag{59}$$

thus establishing the first half of the condition in Lemma 2. It remains to show that the condition

$$\beta\{I(t; u) - I(t; v)\} \le I(x; y)$$

is also satisfied. Since $u^N \to x^n \to y^n$ holds, we have that

$$\begin{aligned} n I(x; y) &\ge I(x^n; y^n) && (60) \\ &\ge I(u^N; y^n) && (61) \\ &\ge I(u^N; y^n, k) - I(v^N; y^n, k) - n\varepsilon_n, && (62) \end{aligned}$$

where the last inequality holds, since

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

where the last step holds via (51a) and the fact that $H(k|y^n,u^N) \ge 0$.

Continuing (62), we have

$$\begin{aligned} nI(x;y) &\ge I(u^N;y^n,k) - I(v^N;y^n,k) - n\varepsilon_n && (63) \\ &= \sum_{i=1}^{N} \{I(u_i;y^n,k,u_1^{i-1}v_{i+1}^n) - I(v_i;y^n,k,u_1^{i-1}v_{i+1}^n)\} + n\varepsilon_n && (64) \\ &= N\{I(u_J;y^n,k,u_1^{J-1}v_{J+1}^n|J) - I(v_J;y^n,k,u_1^{J-1}v_{J+1}^n|J) + \varepsilon_n\} \\ &= N\{I(u_J;t) - I(v_J;t) + I(v_J;J) - I(u_J;J) + \varepsilon_n\} \\ &= N\{I(u;t) - I(v;t) + \varepsilon_n\} && (65) \end{aligned}$$

where (64) follows from the well known chain rule for difference between mutual information expressions (see e.g., [9]), (65) 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.

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. Reversely Degraded Channels

A. Proof of Theorem 1

First we show that the expression is an upper bound on the capacity. From Lemma 2, we have that

$$C_{\text{key}} \le \max_{(x,t)} I(x;y|z) + \beta I(t;v),$$

where we maximize over those distributions where (x,t) are mutually independent, $t \to u \to v$, and

$$I(x;y) \ge \beta(I(t;u) - I(t;v)).$$

For the reversely degraded parallel independent channels, note that

$$\begin{aligned} I(x;y) &\le \sum_{i=1}^{M} I(x_i;y_i) \\ I(x;y|z) &\le \sum_{i=1}^{M} I(x_i;y_i|z_i), \end{aligned}$$

with equality when $(x_1,\ldots,x_M)$ are mutually independent. Thus it suffices to take $(x_1,\ldots,x_M)$ to be mutually independent, which establishes that the proposed expression is an upper bound on the capacity.

For achievability, we propose a choice of auxiliary random variables (a, b) in Lemma 1, such that the resulting expression reduces to the capacity. In particular, assume without loss in generality that for the first P channels we have that $x_i \to y_i \to z_i$ and for the remaining channels we have that $x_i \to z_i \to y_i$. Let $a = (x_1, x_2, \ldots, x_M)$ and $b = (x_{P+1}, \ldots, x_M)$ where the random variables $\{x_i\}$ are mutually independent. It follows from (5a) and (5b) that

$$R_{\text{ch}} = \sum_{i=1}^{M} I(x_i; y_i) \tag{66}$$

$$R_{\text{eq}}^{-} = \sum_{i=1}^{P} I(x_i; y_i|z_i) = \sum_{i=1}^{M} I(x_i; y_i|z_i), \tag{67}$$

where the last equality follows since for $x_i \to z_i \to y_i$, we have that $I(x_i; y_i|z_i) = 0$. Substituting in (6) and (7) we recover the capacity expression.

B. Gaussian Case (Corollary 1)

For the Gaussian case we show that Gaussian codebooks achieve the capacity as in Corollary 1.

Recall that the capacity expression involves maximizing over random variables $\mathbf{x} = (x_1, \ldots, x_M)$, and $t \to u \to v$,

$$C_{\text{key}} = \sum_i I(x_i; y_i|z_i) + \beta I(t; v) \tag{68}$$

subjected to the constraint that $E[\sum_{i=1}^{M} x_i^2] \leq P$ and

$$\sum_i I(x_i; y_i) \geq \beta\{I(t; u) - I(t; v)\}. \tag{69}$$

Let us first fix the distribution $p_{\mathbf{x}}$ and upper bound the objective function (68). Let $R \triangleq \frac{1}{\beta}\sum_{i=1}^{M} I(x_i; y_i)$ and $v = u + s$, where $s \sim \mathcal{N}(0, S)$ is independent of u. We will use the conditional entropy power inequality

$$\exp(2h(u + s|t)) \geq \exp(2h(u|t)) + \exp(2h(s)) \tag{70}$$

for any pair of random variables (t, u) independent of s. The equality happens if (u, t) are jointly Gaussian.

Note that we can express (69) as

$$R + h(v) - h(u) \geq h(v|t) - h(u|t) \tag{71}$$

$$= h(u + s|t) - h(u|t) \tag{72}$$

$$\geq \frac{1}{2}\log\left(\exp(2h(u|t)) + 2\pi e S\right) - h(u|t) \tag{73}$$

Letting

$$h(u|t)) = \frac{1}{2}\log 2\pi e D, \tag{74}$$

we have that

$$D \geq \frac{S}{\exp(2(R + h(v) - h(u))) - 1}. \tag{75}$$

Rearranging we have that

$$\sum_{i=1}^{M} I(x_i; y_i) \geq \frac{\beta}{2}\left[\log\left(1+\frac{S}{D}\right) - \log(1+S)\right]. \tag{76}$$

The term $I(t; v)$ in the objective function (68) can be upper bounded as

$$\begin{aligned} I(t; v) &= h(v) - h(v|t) \\ &= h(v) - h(u+s|t) \\ &\leq h(v) - \frac{1}{2}\log(\exp(2h(u|s)) + 2\pi e S) \qquad (77) \\ &= \frac{1}{2}\log\frac{1+S}{D+S} \qquad (78) \end{aligned}$$

where (77) follows by the application of the EPI (70) and (78) follows via (74). Thus the objective function (68) can be expressed as

$$C_{\text{key}} = \sum_i I(x_i; y_i|z_i) + \frac{\beta}{2}\log\frac{1+S}{D+S}, \tag{79}$$

where D satisfies (75).

It remains to show that the optimal x has a Gaussian distribution. Note that the set of feasible distributions for x is closed and bounded and hence an optimum exists. Also if p_{x} is any optimum distribution, we can increase both R and $I(x_i; y_i|z_i)$ by replacing p_{x} with a Gaussian distribution (see e.g., [14]) with the same second order moment. Since the objective function is increasing in both these terms, it follows that a Gaussian p_{x} also maximizes the objective function (68).

VII. Side information at the Wiretapper

We now provide an achievability and a converse for the capacity stated in Theorem 2

A. Achievability

Our coding scheme is a natural extension of the case when $w = 0$.

Since we are only considering degraded channels note that R_{ch} and R_{eq}^{-} in (5a) and (5b) are defined as

$$R_{\text{ch}} = I(x; y) \tag{80}$$

$$R_{\text{eq}}^{-} = I(x; y) - I(x; z) = I(x; y|z). \tag{81}$$

Furthermore, we replace R_{s} in (5c) with

$$R_{\text{s}} = I(t; v) - I(t; w) \tag{82}$$

and the secret-key rate in (6) is

$$R_{\text{LB}} = \beta\{I(t; v) - I(t; w)\} + I(x; y|z). \tag{83}$$

The construction of Wyner-Ziv codebook and wiretap codebook in Fig. 5 is as discussed in section IV-A, IV-B,and IV-C. The Wyner-Ziv codebook consists of $\approx 2^{NI(t;u)}$ codeword sequences sampled uniformly from the set T_t^N. These sequences are uniformly and randomly partitioned into $\approx 2^{N\{I(t;u)-I(t;v)\}}$ bins so that there are $\approx 2^{NI(t;v)}$ sequences in each bin. The bin index of a codeword sequence, Φ_{WZ}, forms a message for the wiretap codebook as

before. The construction of the secret key codebook is modified to reflect the side information sequence at the eavesdropper. In particular we construct the secret-key codebook with parameters

$$M_{\mathrm{SK}} = \exp\left(n(I(x;z) + \beta I(w;t)) - \delta\right) \tag{84}$$

$$N_{\mathrm{SK}} = \exp\left(n(\beta R_{\mathrm{s}} + R_{\mathrm{eq}}^{-} - \delta)\right) \tag{85}$$

and R_{s} is defined in (82).

B. Secrecy Analysis

We show that the equivocation condition at the eavesdropper (1) holds for the code construction. This is equivalent to showing that

$$\frac{1}{n}H(k|w^N, z^n) = \beta(I(t;v) - I(t;w)) + I(x;y|z) + o_\eta(n), \tag{86}$$

which we will now do.

We first provide an alternate expression for the left hand side in (86).

$$\begin{aligned} H(k|w^N, z^n) &= H(k, t^N|w^N, z^n) - H(t^N|k, w^N, z^n) && (87)\\ &= H(t^N|w^N, z^n) - H(t^N|k, w^N, z^n) \\ &= H(t^N, \Phi_{\mathrm{WZ}}|w^N, z^n) - H(t^N|k, w^N, z^n) && (88)\\ &= H(\Phi_{\mathrm{WZ}}|w^N, z^n) + H(t^N|\Phi_{\mathrm{WZ}}, w^N) - H(t^N|k, w^N, z^n) && (89) \end{aligned}$$

where (88) follows from the fact that Φ_{WZ} is a deterministic function of t^N, while (89) follows from the fact that $t^N \to (w^N, \Phi_{\mathrm{WZ}}) \to z^n$ forms a Markov chain. The right hand side in (86) is established by showing that

$$\frac{1}{n}H(\Phi_{\mathrm{WZ}}|w^N, z^n) \geq I(x;y|z) + o_\eta(1) \tag{90a}$$

$$\frac{1}{n}H(t^N|\Phi_{\mathrm{WZ}}, w^N) = \beta(I(t;v) - I(t;w)) + o_\eta(1) \tag{90b}$$

$$\frac{1}{n}H(t^N|k, w^N, z^n) = o_\eta(1). \tag{90c}$$

To interpret (90a), recall that Φ_{WZ} is the message to the wiretap codebook. The equivocation introduced by the wiretap codebook $\frac{1}{n}H(\Phi_{\mathrm{WZ}}|z^n)$ equals $I(x;y|z)$. Eq. (90a) shows that if in addition to z^n, the eavesdropper has access to w^N, a degraded source, the equivocation still does not decrease (except for a negligible amount). The intuition behind this claim is that since the bin index Φ_{WZ} is almost independent of v^N (see Lemma 5 below), it is also independent of w^N due to the Markov condition.

Eq. (90b) shows that the knowledge of w^N reduces the list of t^N sequences in any bin from $\exp(N(I(t;v)))$ to $\exp(N(I(t;v) - I(t;w)))$, while (90c) shows that for the code construction, the eavesdropper, if revealed the secret-key, can decode t^N with high probability.

To establish (90a),

$$\begin{aligned} \frac{1}{n}H(\Phi_{\mathrm{WZ}}|w^N, z^n) &\geq \frac{1}{n}H(\Phi_{\mathrm{WZ}}|z^n, v^N) && (91)\\ &= \frac{1}{n}H(\Phi_{\mathrm{WZ}}|z^n) - \frac{1}{n}I(\Phi_{\mathrm{WZ}}; v^N|z^n) \\ &\geq I(x;y|z) + o_\eta(1) - \frac{1}{n}I(\Phi_{\mathrm{WZ}}; v^N|z^n), && (92)\\ &\geq I(x;y|z) + o_\eta(1) - \frac{1}{n}I(\Phi_{\mathrm{WZ}}; v^N), && (93) \end{aligned}$$

where (91) follows from the fact that $w^N \to v^N \to (\Phi_{\rm WZ}, z^n)$, (92) from Lemma 3 and (93) from the fact that $v^N \to \Phi_{\rm WZ} \to z^n$ so that

$$\frac{1}{n} I(\Phi_{\rm WZ}; v^N | z^n) \leq \frac{1}{n} I(\Phi_{\rm WZ}; v^N). \tag{94}$$

Thus we need to show the following.

Lemma 5:

$$\frac{1}{n} I(\Phi_{\rm WZ}; v^N) \leq o_\eta(1). \tag{95}$$

Proof: From Lemma 3 note that

$$\frac{1}{N} H(\Phi_{\rm WZ}) = I(t; u) - I(t; v) + o_\eta(1)$$

and hence we need to show that

$$\frac{1}{N} H(\Phi_{\rm WZ} | v^N) = I(t; u) - I(t; v) + o_\eta(1)$$

as we do below.

$$\begin{aligned} \frac{1}{N} H(\Phi_{\rm WZ} | v^N) &= \frac{1}{N} H(\Phi_{\rm WZ}, t^N | v^N) - \frac{1}{N} H(t^N | v^N, \Phi_{\rm WZ}) \\ &= \frac{1}{N} H(t^N | v^N) + o_\eta(1) \end{aligned} \tag{96}$$

Where (96) follows since each bin has $M_{\rm WZ} = \exp\left(N(I(t; v) - \eta)\right)$ sequences, (from standard joint typicality arguments) we have that

$$\frac{1}{N} H(t^N | v^N, \Phi_{\rm WZ}) = o_\eta(1). \tag{97}$$

Finally by substituting $a = v$, $b = u$ and $c = t$ and $R = I(t; u) + \eta$, in Lemma 6 in Appendix II we have that

$$\frac{1}{N} H(t^N | v^N) = I(t; u) - I(t; v) + o_\eta(1).$$

This completes the derivation of (95).

■

To establish (90b), we again use Lemma 6 in Appendix II, with $a = w$, $b = u$ and $c = t$ and $R = I(t; v) - \eta$. Finally, to establish (90c), we construct a decoder as in section IV-E that searches for a sequence t_{kj}^N such that $\Phi_{\rm WZ}(t_{kj}^N) \in \mathcal{I}_{\rm x}$ and which is also jointly typical with w^N. Since there are $\exp\{n(\beta I(w; t) + I(x; z) - \eta)\}$ sequences in the set, we can show along the same lines as in the proof of Lemma 4 that t^N can be decoded with high probability given (k, z^n, w^N). The details will be omitted.

C. Converse

Suppose there is a sequences of (n, N) codes that achieves a secret key (k) rate of R, and $\beta = N/n$. Then from Fano's inequality,

$$H(k|y^n, v^N) \leq n\varepsilon_n,$$

and from the secrecy constraint.

$$\frac{1}{n} I(k; z^n, w^N) \leq \varepsilon_n.$$

Combining these inequalities, we have that,

$$\begin{aligned}
nR_{\text{key}} &\leq I(k; y^n, v^N) - I(k; z^n, w^N) + 2n\varepsilon_n \\
&\leq I(k; y^n, v^N \mid z^n, w^N) + 2n\varepsilon_n \\
&\leq h(y^n \mid z^n) + h(v^N \mid w^N) - h(y^n \mid z^n, w^N, k) - h(v^N \mid y^n, z^n, w^N, k) + 2n\varepsilon_n \\
&\leq h(y^n \mid z^n) + h(v^N \mid w^N) - h(y^n \mid z^n, w^N, k, x^n) - h(v^N \mid y^n, z^n, w^N, k,) + 2n\varepsilon_n \\
&= h(y^n \mid z^n) + h(v^N \mid w^N) - h(y^n \mid z^n, x^n) - h(v^N \mid y^n, z^n, w^N, k,) + 2n\varepsilon_n \qquad (98) \\
&\leq \sum_{i=1}^{n} I(x_i; y_i \mid z_i) + h(v^N \mid w^N) - h(v^N|y^n, w^N, k) + 2n\varepsilon_n \qquad (99) \\
&\leq nI(x; y \mid z) + h(v^N \mid w^N) - h(v^N|y^n, w^N, k) + 2n\varepsilon_n \qquad (100)
\end{aligned}$$

where the (98) follows from the fact that $(w^N, k) \to (z^n, x^n) \to y^n$, and (99) follows from the Markov condition $z^n \to (y^n, w^n, k) \to v^N$ that holds for the degraded channel, while (100) follows from the fact that $I(x; y|z)$ is a concave function of p_{x_i} (see e.g., [13, Appendix-I]) and we select $p_x(\cdot) = \frac{1}{n}\sum_{i=1}^{n} p_{x_i}(\cdot)$. Now, let $t_i = (k, u_{i+1}^n v^{i-1}, y^n)$, J be a random variable uniformly distributed over the set $[1, 2, \ldots n]$ and $t = (J, k, u_{J+1}^n v^{J-1}, y^n)$ we have that

$$\begin{aligned}
h(v^N|y^n, w^N, k) &= \sum_{i=1}^{N} h(v_i|v^{i-1}, y^n, w^N, k) \\
&\geq \sum_{i=1}^{N} h(v_i|v^{i-1}, y^n, w^N, u_{i+1}^N, k) \\
&= \sum_{i=1}^{N} h(v_i|v^{i-1}, y^n, w_i, u_{i+1}^N, k) \qquad (101) \\
&= N \cdot h(v_J|t, w_J)
\end{aligned}$$

where we have used the fact that $(w^{i-1}, w_{i+1}^N) \to (v^{i-1}, y^n, w_i, u_{i+1}^N, k) \to v_i$ which can be verified as follows

$$\begin{aligned}
&p\left(v_i \mid w_i, w^{i-1}, w_{i+1}^N, v^{i-1}, u_{i+1}^N, y^n, k\right) \\
=&\sum_{u_i=u} p\left(v_i \mid w_i, u_i = u, w^{i-1}, w_{i+1}^N, v^{i-1}, u_{i+1}^N, y^n, k\right) p\left(u_i = u \mid w_i, w^{i-1}, w_{i+1}^N, v^{i-1}, u_{i+1}^N, y^n, k\right) \\
=&\sum_{u_i=u} p\left(v_i \mid w_i, u_i = u\right) p\left(u_i = u \mid w_i, v^{i-1}, u_{i+1}^N, y^n, k\right) \qquad (102) \\
=&p\left(v_i \mid w_i, v^{i-1}, u_{i+1}^N, y^n, k\right),
\end{aligned}$$

where (102) follows from the fact that since the sequence v^N is sampled i.i.d. , we have that

$$v_i \to (u_i, w_i) \to (w^{i-1}, w_{i+1}^N, v^{i-1}, u_{i+1}^N, y^n, k)$$

and since $u \to v \to w$, it follows that

$$u_i \to (v^{i-1}, u_{i+1}^N, y^n, w_i, k) \to (w^{i-1}, w_{i+1}^N).$$

Since, v_J and w_J are both independent of J, we from (100) that

$$R_{\text{key}} \leq I(x; y|z) + \beta I(t; v|w) + 2\varepsilon_n.$$

Finally, using the steps between (63)-(65) as in the converse for the case when $w = 0$, we have that

$$I(x; y) \geq \beta(I(t; u) - I(t; v)), \tag{103}$$

which completes the proof.

VIII. Public discussion channel

We establish the upper bound on the secret key capacity in the presence of interactive communication over a public discussion channel.

Proof:

First from Fano's inequality we have the following,

$$\begin{aligned} nR &= H(k) && (104)\\ &= H(k|l) + I(k; l) && (105)\\ &\leq n\varepsilon_n + I(k; l) && (106) \end{aligned}$$

where the last inequality follows from Fano's inequality. Also from the secrecy constraint we have that

$$\frac{1}{n} I(k; \phi^k, \psi^k, z^n) \leq \varepsilon_n,$$

which results in the following

$$\begin{aligned} nR &\leq n\varepsilon_n + I(k; l, \psi^k, \phi^k, z^n) && (107)\\ &\leq 2n\varepsilon_n + I(k; l|\psi^k, \phi^k, z^n) && (108)\\ &\leq 2n\varepsilon_n + I(m_x, u^N; m_y, v^N, y^n|\psi^k, \phi^k, z^n), && (109) \end{aligned}$$

where the last step follows from the data-processing inequality since $k = K(m_x, u^N, \psi^k)$ and $l = L(m_y, v^N, y^n, \phi^k)$. ■

Using the chain rule, we have that

$$\begin{aligned} &I(m_x, u^N; m_y, v^N, y^n|\psi^k, \phi^k, z^n) && (110)\\ &= I(m_x, u^N; m_y, v^N, y^n, \psi^k, \phi^k, z^n) - I(m_x, u^N; \psi^k, \phi^k, z^n) && (111)\\ &= I(m_x, u^N; m_y, v^N, \psi^{i_1-1}, \phi^{i_1-1}) + \sum_{j=1}^{n} F_j + G_j \\ &\quad - I(m_x, u^N; \psi^{i_1-1}, \phi^{i_1-1}) - \sum_{j=1}^{n} \hat{F}_j + \hat{G}_j, && (112) \end{aligned}$$

where for each $j = 1, 2, \ldots, n$ we define $F_j = I(m_{\mathrm{x}}, u^N; y_j, z_j | m_y, v^N, y^{j-1}, z^{j-1}, \phi^{i_j-1}, \psi^{i_j-1})$, $G_j = I(m_{\mathrm{x}}, u^N; \phi_{i_j+1}, \ldots, \phi_{i_{j+1}-1}, \psi_{i_j+1}, \ldots, \psi_{i_{j+1}-1} | m_y, v^N, y^j, z^j, \phi^{i_j-1}, \psi^{i_j-1})$, and $\hat{F}_j = I(m_{\mathrm{x}}, u^N; z_j | z^{j-1}, \psi^{i_j-1}, \phi^{i_j-1})$, $\hat{G}_j = I(m_{\mathrm{x}}, u^N; \phi_{i_j+1}, \ldots, \phi_{i_{j+1}-1}, \psi_{i_j+1}, \ldots, \psi_{i_{j+1}-1} | z^j, \phi^{i_j-1}, \psi^{i_j-1})$.

We now bound the expression in (112). First note that

$$\begin{aligned}
&I(m_{\mathrm{x}}, u^N; m_y, v^N, \psi^{i_1-1}, \phi^{i_1-1}) - I(m_{\mathrm{x}}, u^N; \psi^{i_1-1}, \phi^{i_1-1}) \\
&= I(m_{\mathrm{x}}, u^N; m_y, v^N | \psi^{i_1-1}, \phi^{i_1-1}) \\
&\leq I(m_{\mathrm{x}}, u^N, \psi_{i_1-1}; m_y, v^N | \psi^{i_1-2}, \phi^{i_1-1}) \\
&= I(m_{\mathrm{x}}, u^N; m_y, v^N | \psi^{i_1-2}, \phi^{i_1-1}) \\
&\leq I(m_{\mathrm{x}}, u^N; m_y, v^N, \phi_{i_1-1} | \psi^{i_1-2}, \phi^{i_1-2}) \\
&= I(m_{\mathrm{x}}, u^N; m_y, v^N | \psi^{i_1-2}, \phi^{i_1-2})
\end{aligned}$$

where the third and fifth step follow from the fact that $\psi_{i_1-1} = \Psi_{i_1-1}(m_{\mathrm{x}}, u^N, \phi^{i_1-2})$ and $\phi_{i_1-1} = \Phi_{i_1-1}(m_y, v^N, \psi^{i_1-2})$. Recursively continuing we have that

$$I(m_{\mathrm{x}}, u^N; m_y, v^N | \psi^{i_1-1}, \phi^{i_1-1}) \leq I(m_{\mathrm{x}}, u^N; m_y, v^N) = I(u^N; v^N) = NI(u; v) \tag{113}$$

where we use the facts that $m_{\mathrm{x}} \to u^N \to v^N \to m_y$ and that (u^N, v^N) are discrete and memoryless.

Also note that

$$\begin{aligned}
&F_j - \hat{F}_j && (114)\\
&= I(m_{\mathrm{x}}, u^N; y_j, z_j | m_y, v^N, y^{j-1}, z^{j-1}, \phi^{i_j-1}, \psi^{i_j-1}) - I(m_{\mathrm{x}}, u^N; z_j | z^{j-1}, \psi^{i_j-1}, \phi^{i_j-1}) \\
&= H(y_j, z_j | m_y, v^N, y^{j-1}, z^{j-1}, \phi^{i_j-1}, \psi^{i_j-1}) - H(y_j, z_j | m_y, v^N, y^{j-1}, z^{j-1}, \phi^{i_j-1}, \psi^{i_j-1}, m_{\mathrm{x}}, u^N) \\
&\quad - H(z_j | z^{j-1}, \psi^{i_j-1}, \phi^{i_j-1}) + H(z_j | z^{j-1}, \psi^{i_j-1}, \phi^{i_j-1}, m_{\mathrm{x}}, u^N) \\
&= H(y_j, z_j | m_y, v^N, y^{j-1}, z^{j-1}, \phi^{i_j-1}, \psi^{i_j-1}) - H(y_j, z_j | x_j) - H(z_j | z^{j-1}, \psi^{i_j-1}, \phi^{i_j-1}) + H(z_j | x_j) && (115)\\
&\leq H(y_j | z^j, \psi^{i_j-1}, \phi^{i_j-1}) - H(y_j | z_j, x_j) \\
&\leq I(x_j; y_j | z_j), && (116)
\end{aligned}$$

where (115) follows from the fact that $x_j = X_j(m_{\mathrm{x}}, u^N, \psi^{i_j-1})$ and that since the channel is memoryless $(m_{\mathrm{x}}, m_y, u^N, v^N, \phi^{i_j-1}, \psi^{i_j-1}, y^{j-1}, z^{j-1}) \to x_j \to (y_j, z_j)$ holds. The last two steps follow from the fact that conditioning reduces entropy.

Finally to upper bound $G_j - \hat{G}_j$,

$$\begin{aligned}
&G_j - \hat{G}_j \\
&= I(m_{\mathrm{x}}, u^N; \phi_{i_j+1}, \ldots, \phi_{i_{j+1}-1}, \psi_{i_j+1}, \ldots, \psi_{i_{j+1}-1} | m_y, v^N, y^j, z^j, \phi^{i_j-1}, \psi^{i_j-1}) \\
&\quad - I(m_{\mathrm{x}}, u^N; \phi_{i_j+1}, \ldots, \phi_{i_{j+1}-1}, \psi_{i_j+1}, \ldots, \psi_{i_{j+1}-1} | z^j, \phi^{i_j-1}, \psi^{i_j-1}) \\
&= I(m_{\mathrm{x}}, u^N; m_y, v^N, y^j, \phi_{i_j+1}, \ldots, \phi_{i_{j+1}-1}, \psi_{i_j+1}, \ldots, \psi_{i_{j+1}-1} | z^j, \phi^{i_j-1}, \psi^{i_j-1}) \\
&- I(m_{\mathrm{x}}, u^N; m_y, v^N, y^j | z^j, \phi^{i_j-1}, \psi^{i_j-1}) - I(m_{\mathrm{x}}, u^N; \phi_{i_j+1}, \ldots, \phi_{i_{j+1}-1}, \psi_{i_j+1}, \ldots, \psi_{i_{j+1}-1} | z^j, \phi^{i_j-1}, \psi^{i_j-1}) \\
&= I(m_{\mathrm{x}}, u^N; m_y, v^N, y^j | \phi^{i_{j+1}-1}, \psi^{i_{j+1}-1}, z^j) - I(m_{\mathrm{x}}, u^N; m_y, v^N, y^j | \phi^{i_j-1}, \psi^{i_j-1}, z^j)
\end{aligned}$$

Furthermore since $\phi_{i_{j+1}-1} = \Phi_{i_{j+1}-1}(m_{\rm x}, u^N, \psi^{i_{j+1}-2})$ and $\psi_{i_{j+1}-1} = \Psi_{i_{j+1}-1}(m_y, v^N, \phi^{i_{j+1}-2})$ we have that

$$\begin{aligned}
&I(m_{\rm x}, u^N; m_y, v^N, y^j|\phi^{i_{j+1}-1}, \psi^{i_{j+1}-1}, z^j) \\
&\leq I(m_{\rm x}, u^N, \phi_{i_{j+1}-1}; m_y, v^N, y^j|\phi^{i_{j+1}-2}, \psi^{i_{j+1}-1}, z^j) \\
&= I(m_{\rm x}, u^N; m_y, v^N, y^j|\phi^{i_{j+1}-2}, \psi^{i_{j+1}-1}, z^j) \\
&\leq I(m_{\rm x}, u^N; m_y, v^N, y^j, \psi_{i_{j+1}-1}|\phi^{i_{j+1}-2}, \psi^{i_{j+1}-2}, z^j) \\
&= I(m_{\rm x}, u^N; m_y, v^N, y^j, |\phi^{i_{j+1}-2}, \psi^{i_{j+1}-2}, z^j)
\end{aligned}$$

Continuing this process we have that

$$I(m_{\rm x}, u^N; m_y, v^N, y^j|\phi^{i_{j+1}-1}, \psi^{i_{j+1}-1}, z^j) \leq I(m_{\rm x}, u^N; m_y, v^N, y^j|\phi^{i_j-1}, \psi^{i_j-1}, z^j)$$

and thus

$$G_j - \hat{G}_j \leq 0. \tag{117}$$

Substituting (113), (116) and (117) into (112) we have that

$$nR \leq \sum_{j=1}^{n} I(x_j; y_j|z_j) + NI(u; v) + 2n\varepsilon_n \tag{118}$$

$$\leq \max_{p_x} nI(x; y|z) + NI(u; v) + 2n\varepsilon_n \tag{119}$$

thus yielding the stated upper bound.

IX. Conclusions

In this paper we introduced a secret-key agreement technique that harnesses uncertainties from both sources and channels. Applications of sensor networks and biometric systems motivated this setup.

We first consider the case when the legitimate terminals observe a pair of correlated sources and communicate over a wiretap channel for generating secret keys. The secret-key capacity is bounded by establishing upper and lower bounds. The lower bound is established by providing a coding theorem that combines ideas from source and channel coding. Its optimality is established when the wiretap channel consists of parallel, independent and degraded channels. The lower bound in general involves us to operate at a point on the wiretap channel that balances the contribution of source and channel contributions and this illustrated for the Gaussian channels.

In addition we also establish the capacity when the wiretapper has access to a source sequence which is a degraded version of the source sequence of the legitimate receiver. Furthermore the case when a public discussion channel is available for interactive communication is also studied and an upper bound on the secret-key capacity is provided. For the practically important case, when the wiretap channel consists of "independent noise" for the legitimate receiver and the discussion channel allows us to separately generate keys from source and channel components without loss of optimality.

In terms of future work, there can be many fruitful avenues to explore for secret-key distillation in a joint-source-channel setup. One can consider multi-user extensions of the secret-key generation problem along the lines of [6] and also consider more sophisticated channel models such as the compound wiretap channels, MIMO wiretap channels and wiretap channels with feedback and/or side information. Connections of this setup to wireless channels, biometric systems and other applications can also be interesting.

APPENDIX I
EXTENSION OF LEMMA 1 TO GENERAL (a, b)

We extend the coding theorem in section IV for Lemma 1 to the case of general (a, b).

We focus on the case when $a = x$. The general case then follows by further considering the auxiliary channel $a \to x$, sampling the codewords from the typical set T_a^n and then passing each symbol of a^n through an auxiliary channel $p_{x|a}(\cdot)$.

Our extension involves using a superposition code as discussed below. Let us define $R_{\rm a} = I(x; y|b)$ and $R_{\rm b} = I(b; y)$. Since $b \to x \to y$, we have that $R_{\rm b} + R_{\rm a} = I(x; y)$. We first generate a codebook $\mathcal{C}_{\rm b}$ with $N_{\rm b} = \exp\left(n(R_{\rm b} - \delta_b)\right)$ sequences sampled uniformly from the set T_b^n. For each sequence $b_i^n \in \mathcal{C}_{\rm b}$, we generate a codebook $\mathcal{C}_{\rm a}(b_i^n)$ by selecting $N_{\rm a} = \exp(n(I(x; y|b) - \delta_a))$ sequences uniformly at random from the set $T_{x,b}^n(b_i^n)$.

Select $\delta_a > 0$ and $\delta_{\rm b} > 0$ as arbitrary constants such that $\delta_{\rm a} + \delta_{\rm b} = \delta$, which satisfies (23). Note that we have $N_{\rm WZ} = N_{\rm a} \cdot N_{\rm b}$. We define an encoding functions: $\Phi_{{\rm WZ},b} : \{1, 2, \ldots, N_{\rm b}\} \to \mathcal{C}_b$ and $\Phi^i_{{\rm WZ},a} : \{1, 2, \ldots, N_{\rm a}\} \to \mathcal{C}_a(b_i^n)$ as a mapping from the messages to respective codewords in the codebooks.

The construction of the Wyner-Ziv codebook and the secret-key codebook is via random partitioning along the lines in section IV-A — the constants $M_{\rm WZ}$ and $N_{\rm WZ}$ are as given in (25a) and (25b) respectively while

$$M_{\rm SK} = \exp\left(n(I(b; y) + I(x; z|b) - \delta)\right), \tag{120a}$$

$$N_{\rm SK} = \exp\left(n(\beta I(t; v) + I(x; y|b) - I(x; z|b) - \delta)\right). \tag{120b}$$

The encoding function is defined as follows: given a sequence u^N, as in section IV-B, a jointly typical sequence $t^N \in \mathcal{T}$ is selected and the bin index and secret-key are computed via the mappings $\Phi_{\rm WZ}(t^N)$ and $\Phi_{\rm SK}(t^N)$ respectively in Def. 4. The bin index is split into two indices $\Phi_{\rm a} \in \{1, 2, \ldots, N_{\rm a}\}$ and $\Phi_{\rm b} \in \{1, \ldots, N_{\rm b}\}$, which form messages for the channel codebooks constructed above and the resulting sequence x^n is transmitted.

The decoder upon observing y^n searches for sequences $b_i^n \in \mathcal{C}_{\rm b}$ and $x^n \in \mathcal{C}_{\rm a}(b_i^n)$ that are jointly typical i.e., $(y^n, x^n, b_i^n) \in T^n_{y,x,b,\eta}$. By our choice of $N_{\rm b}$ and $N_{\rm a}$ this succeeds with high probability. It then reconstructs the bin index $\Phi_{\rm WZ}$ and searches for a sequence $t^N \in \mathcal{T}$ that lies in this bin and is jointly typical with v^N. As in section IV-C, this step succeeds with high probability. The secret-key is then computed as $\hat{k} = \Phi_{\rm SK}(t^N)$.

We need to show the secrecy condition that

$$\frac{1}{n} H(k|z^n) = \{I(x; y|b) - I(x; z|b)\} + \beta I(t; v) + o_\eta(1). \tag{121}$$

By expressing $H(k|z^n)$ as in (48) in section IV-E.2

$$H(k|z^n) = H(\Phi_{\rm WZ}|z^n) + H(t^N|\Phi_{\rm WZ}) - H(t^N|k, z^n). \tag{122}$$

For the superposition codebook, since $\Phi_{\rm WZ}$ is the transmitted message we have from [4]

$$\frac{1}{n} H(\Phi_{\rm WZ}|z^n) = I(x; y|b) - I(x; z|b) + o_\eta(1), \tag{123}$$

and from (27b) in Lemma 3,

$$\frac{1}{N} H(t^N|\Phi_{\rm WZ}) = I(t; v) + o_\eta(1). \tag{124}$$

To show that

$$\frac{1}{N} H(t^N|z^n, k) = o_\eta(1) \tag{125}$$

we use a decoder analogous to that in the proof of Lemma 4 in Section IV-E. Upon observing z^n, the decoder searches for a sequence $b_i^n \in \mathcal{C}_{\rm b}$ that is jointly typical. This event succeeds with high probability since $I(b;z) \geq I(b;y) = R_{\rm b}$. Let the set of conditionally typical sequences x^n be

$$\mathcal{I}_{\rm x} = \{j | x_j^n \in \mathcal{C}_{\rm b}(b_i^n), (x_j^n, z^n) \in T_{x,z,\eta}^n\}. \tag{126}$$

The eavesdropper searches for all sequences $t_{kj,\rm SK}^N$ such that $\Phi_{\rm a}(t_{kj,\rm SK}^N) \in \mathcal{I}_{\rm x}$ and $\Phi_{\rm b}(t_{kj,\rm SK}^N) = i$. Since the number of sequences $t_{kj,\rm SK}^N$ is $M_{\rm SK} = \exp\left(n(I(x;z|b) + I(b;y) - \delta)\right)$, along the lines of Lemma 4, it follows that the codeword sequence is decoded with high probability.

Note that (121) follows from (122), (123), (124) and (125).

Appendix II
Conditional Entropy Lemma

Lemma 6: Suppose that the random variables a, b, and c are finite valued with a joint distribution $p_{a,b,c}(\cdot)$ that satisfies $a \to b \to c$. Suppose that a set $\mathcal{C}_c$ is selected by drawing $\exp(NR)$ sequences $\{c_i^N\}$ uniformly and at random from the set of typical sequences T_c^N where $R < H(c)$. Suppose that the pair of length-N sequences (a^N, b^N) are drawn i.i.d. from the distribution $p_{a,b}$ and a sequence $c_i^N \in \mathcal{C}_c$ is selected uniformly at random from the set of all possible sequences such that $(c_i^N, b^N) \in T_{cb,\eta}^N$. Then for $R > I(c;a)$, we have that

$$\frac{1}{N} H(c_i^N | a^N) = R - I(c;a) + o_\eta(1), \tag{127}$$

where the term $o_\eta(1)$ vanishes to zero as $N \to \infty$ and $\eta \to 0$.

Proof: From (24c), for all pair of sequences (a^N, b^N), except a set whose probability is $o_\eta(1)$, we have that $(a^N, b^N) \in T_{ab,\eta}^N$. For each such typical pair, since $a \to b \to c$ and $(b^N, c_i^N) \in T_{bc,\eta}^N$ from the Markov Lemma it follows that $(a^N, c_i^N) \in T_{ac,\eta}^N$.

To establish (127) it suffices to show that for all sequences $a^N \in T_{a,\eta}^N$, except a set whose probability is at most $o_\eta(1)$

$$\Pr(c^N = c_i^N | a^N = a^N) = \exp(-N(R - I(c;a) + o_\eta(1))). \tag{128}$$

The expression in (127) then immediately follows by due to the continuity of the $\log$ function. To establish (128),

$$\Pr(c^N = c_i^N | a^N = a^N) = \frac{p(a^N | c_i^N) \Pr(c^N = c_i^n)}{p(a^N)}. \tag{129}$$

From property (24b) of typical sequences $p(a^N) = \exp(-N(H(a) + o_\eta(1)))$, $p(a^N | c_i^N) = \exp(-N(H(a|c) + o_\eta(1)))$ and since the sequence c^N is uniformly selected from 2^{nR} sequences, we have that $\Pr(c^N = c_i^N) = \exp(-NR)$. Substituting these quantities in (129) establishes (128). ■

References

[1] 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, Jul. 1993.

[2] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley and Sons, 1991.

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

[4] ——, *Information Theory, Coding Theorems for Discrete Memoryless Systems*. Akadémiai Kiadó, 1981.

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

[6] ——, "Secrecy capacities for multiple terminals," *IEEE Trans. Inform. Theory*, vol. 50, pp. 3047–3061, 2004.

[7] 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.
[8] A. A. El Gamal, "Capacity of the product and sum of two un-matched broadcast channels," *Probl. Information Transmission*, pp. 3–23, 1980.
[9] ——, "Course notes in multiuser information theory, Stanford university," 2003.
[10] D. Gunduz, E. Erkip, and H. V. Poor, "Lossless compression with security constraints," in *Proc. Int. Symp. Inform. Theory*, Toronto, Jul. 2008.
[11] A. Khisti, "Secret key generation using correlated sources and noisy channels," in *Presentation at the Information Theory and its Applications (ITA) Workshop*, San Diego, Jan. 2008.
[12] A. Khisti, S. N. Diggavi, and G. W. Wornell, "Secret key generation using correlated sources and noisy channels," in *Proc. Int. Symp. Inform. Theory*, Toronto, Jun. 2008.
[13] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure Broadcasting," *IEEE Trans. Inform. Theory, Special Issue on Information Theoretic Security*, 2008.
[14] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," *Submitted Aug. 2007, IEEE Trans. Inform. Theory, available online, http://arxiv.org/abs/0708.4219*.
[15] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, pp. 733–742, Mar. 1993.
[16] 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.
[17] V. Prabhakaran, K. Eswaran, and K. Ramchandran, "Secrecy via sources and channels – a secret key - secret message rate trade-off region," *Online (07/07/08) http://arxiv.org/abs/0708.4219*.
[18] V. Prabhakaran and K. Ramachandran, "A separation result for secure communication," in *talk presented at the 45th Allerton Conf. Commun., Contr., Computing*, Oct. 2007.
[19] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–87, 1975.
[20] H. Yamamoto, "Rate distortion theory for the shannon cipher system," *IEEE Trans. Inform. Theory*, vol. 43, May 1997.