Secret-Key Generation using Correlated Sources and Channels

Ashish Khisti, *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 terminals communicate 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, thus establishing the capacity, when the underlying channel consists of a set of independent, parallel and reversely degraded wiretap channels. In the lower bound expression, 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 case of parallel Gaussian channels and jointly Gaussian sources 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.

Index Terms

Information theoretic security, secret-key agreement, wiretap channel, joint source-channel coding, public discussion

I. Introduction

Several applications 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 [31]. 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. Several extensions of this channel have been studied recently. See e.g., [3], [11], [16], [20], [22]–[24], [30].

Part of the material in this paper was presented at the 2008 Information Theory and its Application Workshop [17] and the 2008 International Symposium on Information Theory [18]. Ashish Khisti is with ECE Department, University of Toronto, Toronto, ON, Canada (akhisti@comm.utoronto.ca). Suhas Diggavi is with the Department of Electrical Engineering, University of California, Los Angeles (UCLA) as well as with the School of Computer and Communication Sciences at EPFL (suhas@ee.ucla.edu). Gregory Wornell is with the faculty of EECS Dept., MIT (gww@mit.edu).

In the source coding setup [1], [26], 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 rate asymptotically equals the secret-key rate. Several multiuser extensions of this problem have been subsequently studied. See e.g., [9], [10].

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 in secret key generation across sensors in a body area network [4], [5]. Sensors placed at different locations on a human body measure correlated biological signals which can be used to generate a secret key. Further they need to communicate over a wireless medium, in the presence of potential eavesdropping sensors which would naturally be further away. While earlier works only exploit signal correlation across sensors for key generation, our information theoretic results suggest that both signal correlation as well as channel equivocation must be used to maximize the secret key rate.

How to simultaneously exploit both the source correlation and channel equivocation in generating a common secret key? Our proposed approach is a joint design of source and channel codebooks. The source sequence is quantized using a Wyner-Ziv like codebook and the corresponding bin index constitutes a message for a channel codebook. The secret key is generated by jointly exploiting the source and channel uncertainties at the eavesdropper. When the conditional entropy of the source sequences is not sufficiently high, we only reserve a certain fraction of the total channel uses for this scheme. In the remaining time we transmit an independent secret message over over channel. Optimality of our scheme is established 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 [7]. 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 [15], [27], [32] 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, [29], 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 [28] 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 [28] appears consistent with the expression in this paper, the optimality claims in [28] 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. The channel from sender to receiver and

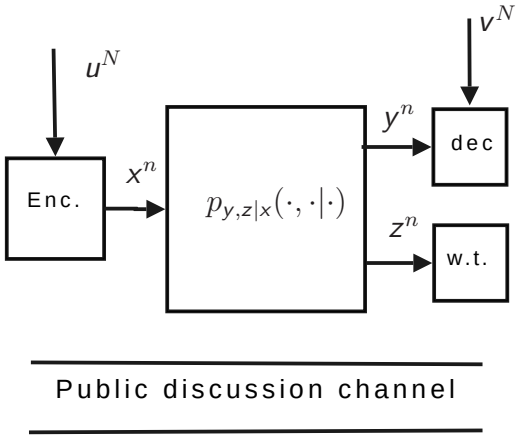

Fig. 1. Secret-key agreement over the wiretap channel with correlated sources. The sender and receiver communicate over a wiretap channel and have access to correlated sources. They communicate interactively over a public discussion channel of rate R, if it is available.

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. Throughout this paper assume that the source and channels are independent i.e., $(u,v) \to x \to (y,z)$ holds. Further the source sequences are known to the terminals before the communication begins i.e., non-causally. 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 $p_{\mathsf{m}_x|u^N}(\cdot|u^N)$. 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[2] 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 [12] 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[3]. 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]Throughout this work we only require that the normalized mutual information between the key and the eavesdropper output vanish as the block-length goes to infinity. A stronger notion of secrecy can also be considered, which requires that the mutual information approach zero as the block length increases (see e.g., [6], [25]). We do not pursue this extension.

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

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], [26]. 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. We consider a total of k rounds of exchanges i.e., $1 \leq t \leq k$ and define $i_{n+1} = k+1$. Note that k is an arbitrary integer in this setup.The eavesdropper observes $\{\phi_t, \psi_t\}_{t=1}^{k+1}$. 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

Below we consider the case when a public discussion channel is not available. The results for the case of public discussion are stated in section III-E.

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 $I(y; b) \leq I(z; b)$ and[4]

$$I(a; y|b) \geq I(a; z|b). \tag{5}$$

Furthermore define

$$R_{\rm ch} = I(a; y), \tag{6a}$$
$$R_{\rm eq}^{-} = I(a; y|b) - I(a; z|b) \tag{6b}$$
$$R_{\rm s} = I(t; v), \tag{6c}$$
$$R_{\rm wz} = I(t; u) - I(t; v). \tag{6d}$$
$$R_{\rm eq}^{+} = I(x; y \mid z). \tag{6e}$$
$$R_{\rm ch}^{+} = I(x; y), \tag{6f}$$

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

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

$$R_{\rm key}^{-} = \beta R_{\rm s} + R_{\rm eq}^{-}, \tag{7}$$

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

$$\beta R_{\rm wz} \leq R_{\rm ch} \tag{8}$$

and the quantities $R_{\rm wz}$, $R_{\rm s}$, $R_{\rm eq}^{-}$ and $R_{\rm ch}$ are defined in (6d), (6c), (6b) and (6a) respectively. ■

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

$$R_{\rm key}^{+} = \max_{\{(x,t)\}} \left\{ \beta R_{\rm s} + R_{\rm eq}^{+} \right\}, \tag{9}$$

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

$$\beta R_{\rm wz} \leq R_{\rm ch}^{+}. \tag{10}$$

The quantities $R_{\rm s}$, $R_{\rm wz}$, $R_{\rm eq}^{+}$ and $R_{\rm ch}^{+}$ are defined in (6c), (6d), (6e) and (6f) respectively.

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

As suggested to us by an anonymous reviewer, the upper bound in Theorem 2 can be further tightened as stated below.

Proposition 1: An upper bound on the secret-key rate is given by,

$$R_{\rm key}^{+} = \inf_{p_{g,y,z|x}} \max_{\{(x,t)\}} \left\{ \beta I(t; v) + I(x; y|g) + I(x; g|z) \right\}, \tag{11}$$

where the infimum is over three-receiver memoryless channels of the form $p_{g,y,z|x}(\cdot)$ for which the distribution $p_{y,z|x}(\cdot)$ coincides with the given channel whereas the maximization is over independent random variables (x, t) that satisfy (10).

[4]The condition in (5) will be satisfied even if not explicitly enforced in the optmization of Theorem 1. Suppose that (a, b) are such that the expression in (5) is violated. We note that such a choice cannot be the optimal choice in Theorem 1. Define $a' = b' = (a, b)$. Observe that $I(a; y) = I(a'; y)$ and hence the expression for $R_{\rm key}^{-}$ in (7) increases whereas the constraint set in (8) remains unchanged with this new choice of variables.

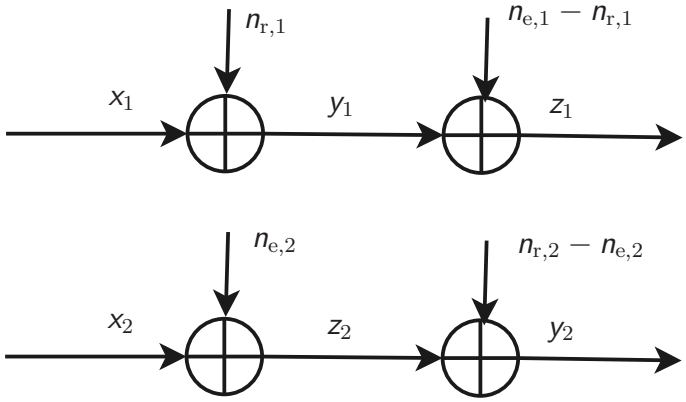

Fig. 2. An example of independent parallel and reversely degraded Gaussian channels. On the first channel, the eavesdropper channel is noisier than the legitimate receiver's channel while on the second channel the order of degradation is reversed.

A. Reversely degraded parallel independent channels

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

Theorem 3: The secret-key-capacity for the reversely degraded parallel independent channels in Def. 2 is given by

$$C_{\text{key}} = \max_{\{(x_1,\ldots,x_M,t)\}} \left\{ \beta I(v;t) + \sum_{i=1}^{M} I(x_i;y_i|z_i) \right\}, \tag{12}$$

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

$$\sum_{i=1}^{M} I(x_i;y_i) \geq \beta\{I(u;t) - I(v;t)\} \tag{13}$$

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

■

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-A2 is obtained by optimizing (12) and (13) 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 $\sum_{i=1}^{M} P_i \leq P$, $P_i \geq 0$, and $0 < D \leq 1$.

$$C^G_{\text{key}} = \max_{\{P_i\}_{i=1}^{M},D} \left\{ \frac{\beta}{2}\log\left(\frac{1+S}{D+S}\right) + \sum_{\substack{i:1\leq i\leq M \\ \sigma_{r,i}\leq\sigma_{e,i}}} \frac{1}{2}\log\left(\frac{1+P_i/\sigma^2_{r,i}}{1+P_i/\sigma^2_{e,i}}\right) \right\}, \tag{14}$$

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

$$\sum_{i=1}^{M} \frac{1}{2}\log\left(1+\frac{P_i}{\sigma^2_{r,i}}\right) \geq \beta\left\{\frac{1}{2}\log\left(\frac{1}{D}\right) - \frac{1}{2}\log\left(\frac{1+S}{D+S}\right)\right\} \tag{15}$$

■

C. Remarks

1) Note that the secret-key capacity expression (12) 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 [31]. 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 [9], 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 (12) in Theorem 3 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 (13). The second term, $I(x;y|z)$ is the equivocation term and increasing this term, often comes at 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 in section III-F.

D. Side information at the wiretapper

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 4: 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

$$C_{\text{key}}=\max_{(x,t)}\left\{\beta(I(t;v)-I(t;w))+I(x;y|z)\right\}, \tag{16}$$

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

$$I(x;y)\geq\beta(I(u;t)-I(v;t)) \tag{17}$$

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

In the presence of public interactive communication we have the following result.

Theorem 5: An secret-key capacity for source-channel setup with a public discussion channel and a wiretap channel $p_{y,z|x}(\cdot)$ that satisfies either $x\to y\to z$ or $y\to x\to z$ is

$$C_{\text{key}}\leq\max_{p_x} I(x;y|z)+\beta I(u;v). \tag{18}$$

The expression (18) continues to be an upper bound even when the wiretap channel does not satisfy either of the upper bounds.

■

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], [26].

The upper bound expression (18) in Theorem 5 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.

F. Example: Gaussian Channels with and without public discussion

Consider a pair of Gaussian parallel channels,

$$\begin{aligned} y_1 &= a_1 x + n_{r,1}, \quad z_1 = b_1 x + n_{e,1} \\ y_2 &= a_2 x + n_{r,2}, \quad z_2 = y_2 \end{aligned} \tag{19}$$

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.

1) Without Public Discusion: From Theorem 1, in absence of the public discussion channel,

$$C_{\text{key}} = \max_{P_1,P_2,D} R_{\text{eq}}(P_1,P_2) + \frac{1}{2}\log\frac{2}{1+D}, \tag{20}$$

such that,

$$R_{\text{wz}}(D) = \frac{1}{2}\log\frac{1}{D} - \frac{1}{2}\log\frac{2}{1+D} \tag{21}$$

$$\leq \frac{1}{2}\left(\log\left(1+a_1^2P_1\right) + \log(1+a_2^2P_2)\right), \tag{22}$$

$$R_{\text{eq}}(P_1,P_2) = \frac{1}{2}\left(\log(1+a_1^2P_1) - \log(1+b_1^2P_1)\right). \tag{23}$$

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 $R_{\text{key}} \approx 0.6719$.

2) With Public Discussion: Fig. 4 illustrates the contribution of source and channel coding components for the case of Gaussian parallel channels (19) 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. 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: Proof of Theorem 1

We demonstrate the coding theorem in the special case when $a = x$ and $b = 0$ in Theorem 1. Furthermore via (5) we require that

$$I(x;y) \geq I(x;z) \tag{24}$$

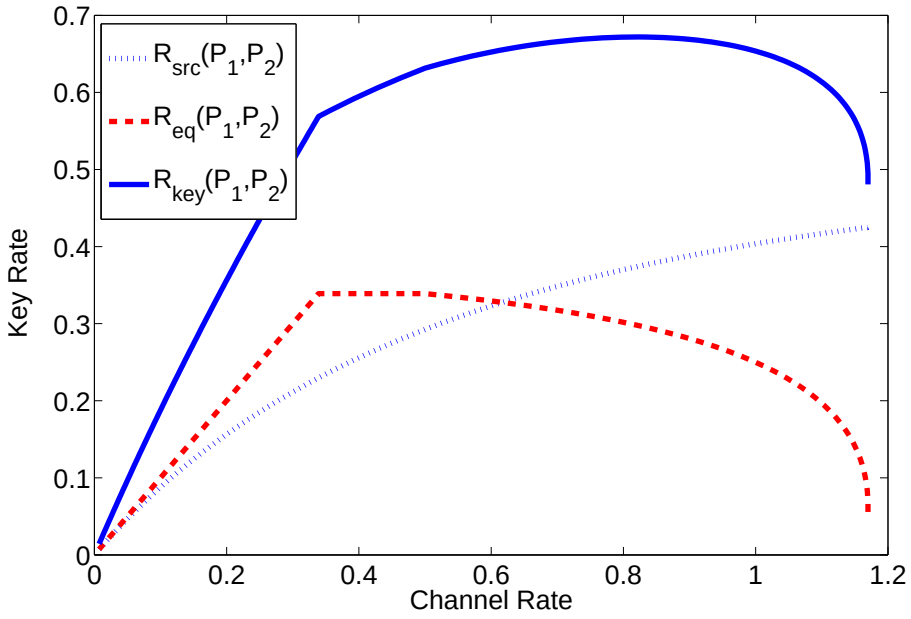

Fig. 3. Tradeoff inherent in the secret-key-capacity formulation. The solid curve is the secret-key-rate, which is the sum of the two other curves. The dotted curve represents the source equivocation, while the dashed curve represents the channel equivocation (23). The secret-key-capacity is obtained at a point between the maximum equivocation and maximum rate.

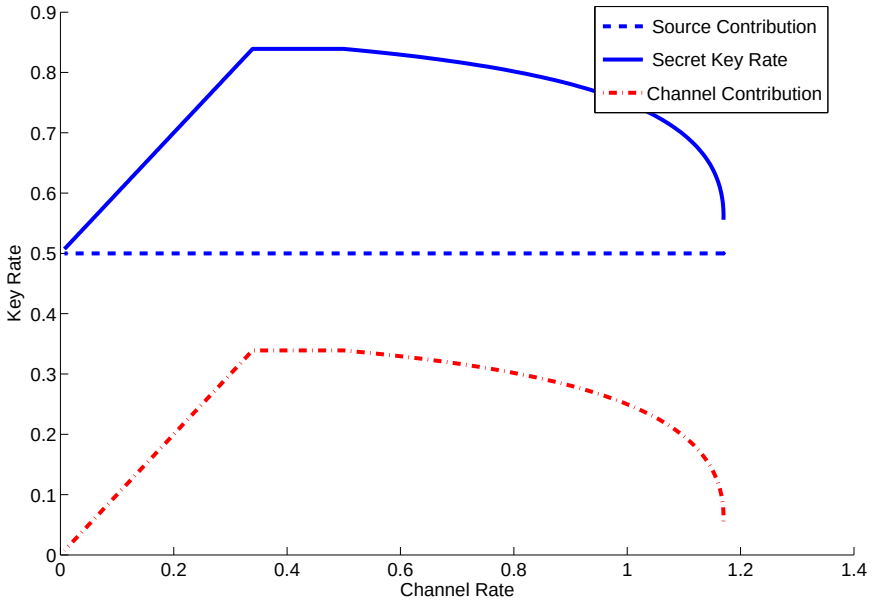

Fig. 4. Secret-key-rate in the presence of a public discussion channel in the Gaussian example (19). The solid curve is the secret-key-rate, which is the sum of the two other curves. The horizontal line is the key rate from the source components. Regardless of the channel rate, the rate is 0.5 bits/symbol. The dashed-dotted curve is the key-rate using the channel $I(x;y|z)$.

Accordingly we have that (6a) and (6b) reduce to

$$R_{\rm ch} = I(x;y) \tag{25a}$$

$$R_{\rm eq}^{-} = I(x;y) - I(x;z) \tag{25b}$$

The more general case, can be incorporated by introducing an auxiliary channel $a \to x$ and superposition coding [8] as outlined in Appendix A. 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

$$\beta R_{\rm wz} = R_{\rm ch} - 3\delta. \tag{26}$$

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

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

as required.

Remark 2: The region in Theorem 1 is achieved as we take the limit $\delta \to 0$. Note that the set of joint distribution is compact. Hence the sequence of maximizing distributions converges to a limit as $\delta \to 0$. By continuity, this limit converges to the maximizing distribution in Theorem 1.

The rest of the proof is structured as follows. In section IV-E—IV-D we describe an ensemble of codebooks as illustrated in Fig. 5 and the associated encoding and decoding schemes at the receiver and at the eavesdropper (with appropriate side information) for each such codebook. We then show in section IV-E that the error probability averaged over the ensemble of these codebooks can be made arbitrarily small. This implies the existence of at-least one codebook with the desired error probability. Finally our secrecy analysis in section IV-F for this particular codebook completes the proof.

A. Codebook Construction

Throughout $\delta > 0$ and $\eta = \delta/\beta > 0$ are constants. Let[5],

$$M_{\rm WZ} = \exp_2(N(R_{\rm s} - \eta)) \tag{27a}$$

$$N_{\rm WZ} = \exp_2(N(R_{\rm wz} + 2\eta)) \tag{27b}$$

$$M_{\rm SK} = \exp_2(n(I(x;z) - \delta)) \tag{27c}$$

$$N_{\rm SK} = \exp_2(n(\beta R_{\rm s} + R_{\rm eq}^{-} - \delta)) \tag{27d}$$

Substituting (6a)-(6d) and (26) into (27a)-(27d) we have that

$$N_{\rm tot} \triangleq M_{\rm SK} \cdot N_{\rm SK} = M_{\rm WZ} \cdot N_{\rm WZ} = \exp_2\left(N(I(t;u) + \eta)\right) \tag{28}$$

- **Selection of $\mathcal{T}$**: Construct a set $\mathcal{T}$ consisting of $N_{\rm tot}$ sequences, each sampled uniformly from the set T_t^n of typical sequences[6].

[5]We use the notation $\exp_2(x) = 2^x$ throughout the paper.

[6]Throughout we use the notion of strong typicality. See e.g., [13, Chapter 2].

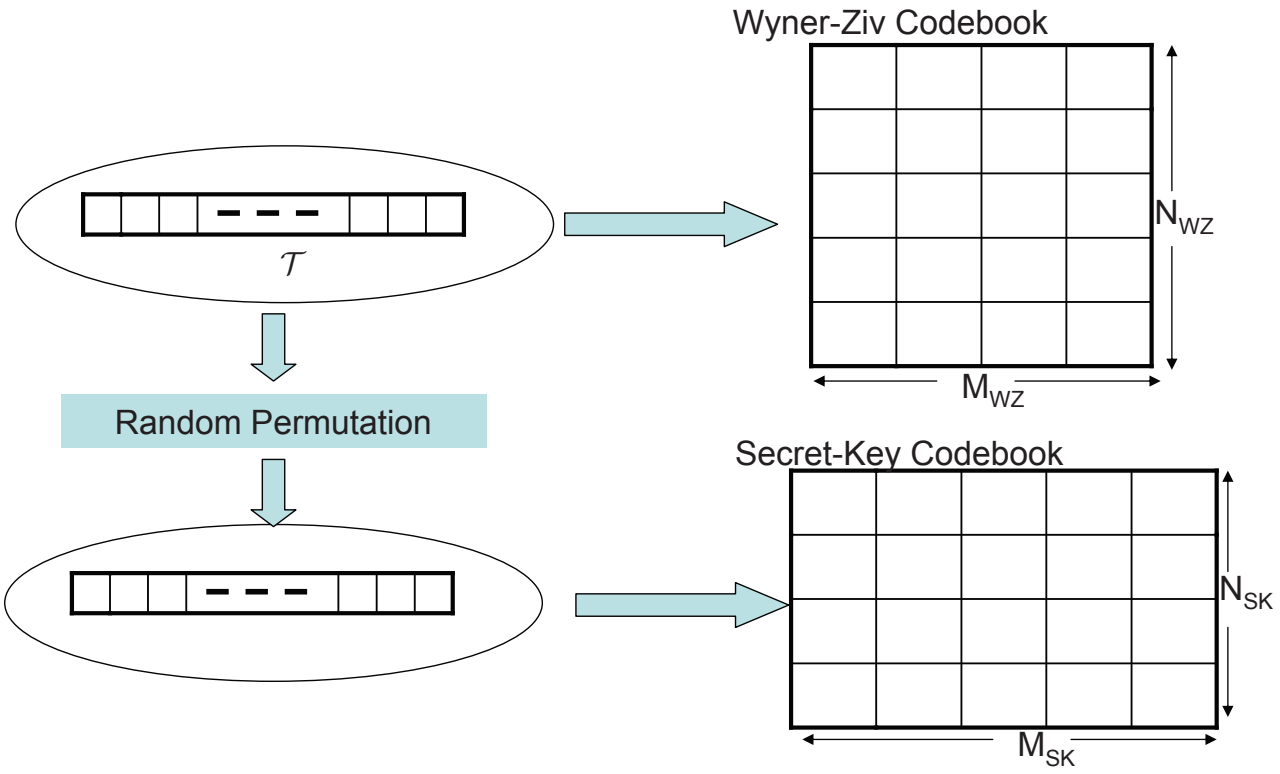

Fig. 5. Construction of the codebook ensemble. The set $\mathcal{T}$ consists of $\approx 2^{NI(u;t)}$ sequences, each sampled uniformly from the set T_t^n of typical sequences. The Wyner-Ziv codebook is formed by arranging these sequences into $N_{\rm WZ}$ bins, each consisting of $M_{\rm WZ}$ sequences. The elements of set $\mathcal{T}$ are then randomly permuted to form the set $\Pi(\mathcal{T})$. The elements of $\Pi(\mathcal{T})$ are then arranged to form the secret-key codebook as shown.

- **Wyner-Ziv Codebook**: Construct $\mathcal{C}^{\rm WZ}$ as follows. Partition the set $\mathcal{T}$ into N_{WZ} bins, $\mathcal{B}_1^{\rm WZ}, \ldots, \mathcal{B}_{N_{\rm WZ}}^{\rm WZ}$ each consisting of $M_{\rm WZ}$ codeword sequences so that bin $\mathcal{B}_i^{\rm WZ}$ consists of sequences numbered $(i-1)\cdot M_{\rm WZ}+1$ to $i\cdot M_{\rm WZ}$ in $\mathcal{T}$. The sequences in bin $\mathcal{B}_i^{\rm WZ}$ are enumerated as
$$\mathcal{B}_i^{\rm WZ} = \left\{ t_{i1}^{N,{\rm WZ}}, \ldots, t_{iM_{\rm WZ}}^{N,{\rm WZ}} \right\}. \tag{29}$$
- **Secret-Key Codebook**: Construct $\mathcal{C}^{\rm SK}$ as follows. Randomly permute the elements of $\mathcal{T}$ to construct another set $\Pi(\mathcal{T})$. Partition the elements of $\Pi(\mathcal{T})$ into $N_{\rm SK}$ bins $\mathcal{B}_1^{\rm SK}, \ldots, \mathcal{B}_{N_{\rm SK}}^{\rm SK}$, each consisting of $M_{\rm SK}$ sequences. The bin $\mathcal{B}_i^{\rm SK}$ consists of sequences that are numbered $(i-1)M_{\rm SK}+1, \ldots, iM_{\rm SK}$ in $\Pi(\mathcal{T})$. The sequences in bin $\mathcal{B}_i^{\rm SK}$ are enummerated as
$$\mathcal{B}_i^{\rm SK} = \left\{ t_{i1}^{N,{\rm SK}}, \ldots, t_{iM_{\rm SK}}^{N,{\rm SK}} \right\}. \tag{30}$$
- **Channel Codebook** Construct $\mathcal{C}^{\rm CH}$ consisting of $N_{\rm WZ}$ sequences $\left\{ x_1^n, \ldots, x_{N_{\rm WZ}}^n \right\}$ each of which is sampled from the typical set T_x^n.
Remark 3: We note that our codebook construction does not require binning as in the wiretap codebook construction [31]. The analysis of the error probability however reveals that our source-channel codebook should also constitute a good code for an eavesdropper when revealed the secret-key (36), analogous to the wiretap codebook.

The codebooks are revealed to all the three terminals. As illustrated in Fig. 5, note that while the Wyner-Ziv codebook is obtained by arranging the elements of $\mathcal{T}$ in a $N_{\rm WZ}\times M_{\rm WZ}$ table,

the secret-key codebook is obtained by first randomly permuting the elements of $\mathcal{T}$ and then arranging these elements into a $N_{\rm SK} \times M_{\rm SK}$ table. In the analysis of the error probability, averaged over the ensemble of codebooks, this construction guarantees that two sequences belonging to the same bin in the secret-key codebook are independently assigned to the bins of the Wyner-Ziv codebook (c.f. 185).

B. Encoding

- Given a sequence u^N, the encoder searches for an element $t^N \in \mathcal{T}$ such that $(u^N, t^N) \in T^N_{ut,\varepsilon}$. If no such sequence exists then an error event $\mathcal{E}_1$ is declared
- The encoder computes the Wynzer-Ziv bin index $\phi = \Phi_{\rm WZ}(t^N)$. The function $\Phi_{\rm WZ} : \mathcal{T} \to \{1, 2, \ldots, N_{\rm WZ}\}$ is defined as follows

$$\Phi_{\rm WZ}(t^N) = i, \quad \text{if } t^N \in \mathcal{B}_i^{\rm WZ}. \tag{31}$$

- The encoder then selects the codeword x^n_ϕ and transmits it over n uses of the discrete memoryless channel.
- The encoder computes the Secret-key $k = \Phi_{\rm SK}(t^N)$. The function $\Phi_{\rm SK} : \mathcal{T} \to \{1, \ldots, N_{\rm SK}\}$ is defined as follows

$$\Phi_{\rm SK}(t^N) = i, \quad \text{if } t^N \in \mathcal{B}_i^{\rm SK}. \tag{32}$$

C. Decoding at legitimate receiver

The main steps of decoding at the legitimate receiver are as follows.

- Given a received sequence y^n, the receiver 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 or no such x_i^n is found.
- Given the observed source sequence v^N, the decoder then searches for a unique index $j \in \{1, \ldots, M_{\rm WZ}\}$ such that $(t_{ij}^{N,{\rm WZ}}, v^N) \in T^N_{tv,\varepsilon}$. An error event $\mathcal{E}_3$ is declared if a unique index does not exist.
- The decoder computes $\hat{k} = \Phi_{\rm SK}(t_{ij}^{N,{\rm WZ}})$ and declares $\hat{k}$ as the secret key.

The encoding and decoding steps are illustrated in Fig. 6.

D. Decoding with side-information at the eavesdropper

We construct a decoder at the eavesdropper when the secret-key is revealed as side information i.e., the decoder produces t^N when given (k, z^n) via the following steps:

- The eavesdropper constructs a set $\mathcal{I} = \{i \mid (x_i^n, z^n) \in T^n_{xy,\varepsilon}\}$.
- It searches for all sequences in $\mathcal{B}_k^{\rm SK}$, whose Wyner-Ziv bin index belongs to $\mathcal{I}$ i.e.,

$$\mathcal{T}_e = \left\{ t^N | t^N \in \mathcal{B}_k^{\rm SK}, \Phi_{\rm WZ}(t^N) \in \mathcal{I} \right\} \tag{33}$$

Let $\mathcal{E}_4$ be the event that the set $\mathcal{T}_e$ does not contain the sequence t^N selected by the sender or contains more than one sequence.

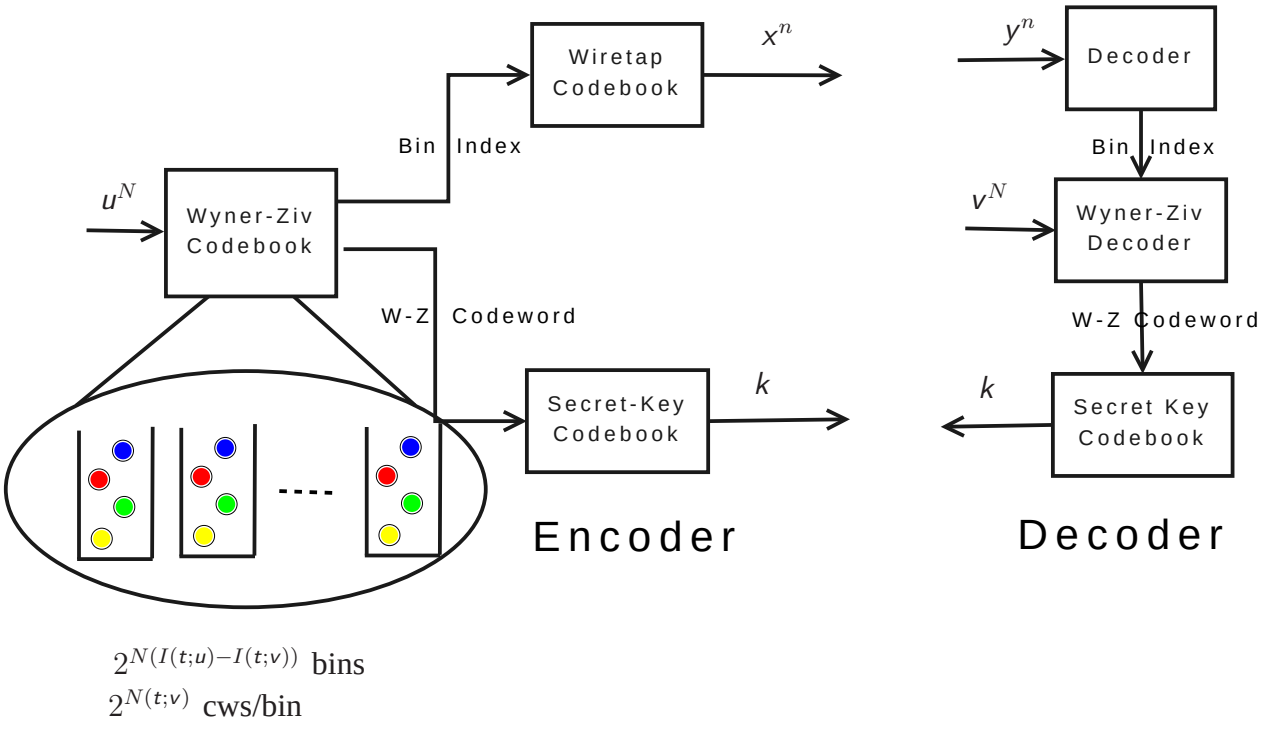

Fig. 6. Source-Channel Code Design for secret-key distillation problem. The source sequence u^N is mapped to a codeword in a Wyner-Ziv codebook. This codeword determines the secret-key via the secret-key codebook. The bin index of the codeword constitutes a message in the channel codebook.

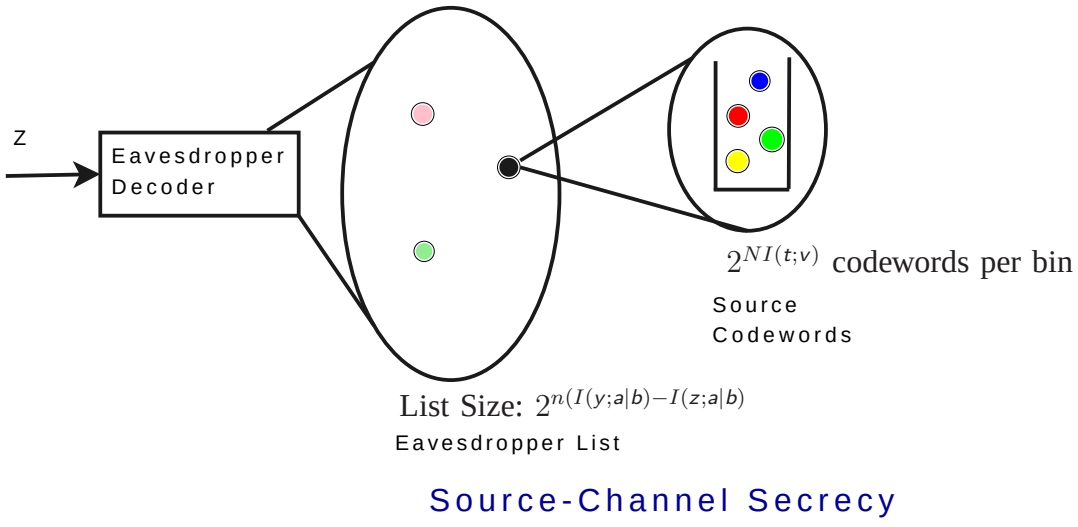

Fig. 7. Equivocation at the eavesdropper through the source-channel codebook. The channel codebook induces an ambiguity of $2^{n(I(a;y|b)-I(a;z|b))}$ among the codeword sequences a^n when the decoder observes z^n. Each sequence a^n only reveals the bin index of the Wyner-Ziv codeword. In induces an ambiguity of $2^{NI(t;v)}$ at the eavesdropper, resulting in a total ambiguity of $2^{n(\beta I(t;v)+I(a;y|b))-I(a;z|b)}$.

E. Error Probability Analysis

We show that averaged over the ensemble of codebooks

$$\Pr(\mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3 \cup \mathcal{E}_4) \to 0 \tag{34}$$

as $n \to \infty$. This implies the existence of at-least one codebook in ensemble with this property. Since

$$\Pr(\mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3 \cup \mathcal{E}_4) \leq \sum_{i=1}^{4} \Pr(\mathcal{E}_i),$$

it suffices to show that $\Pr(\mathcal{E}_i) \to 0$ for each $i = 1, \ldots, 4$.

Recall that $\mathcal{E}_1$ is the event that the encoder does not find a typical codeword in the Wyner-Ziv codebook. Since the number of sequences $N_{\text{tot}} = 2^{NI(t;u)+N\eta}$ it follows from standard arguments that this event happens with vanishing probability. Since the number of channel codewords equals $N_{\text{WZ}} = 2^{n(I(x;y)-\delta)}$, the error event $\mathcal{E}_2$ which denotes the failure at the legitimate receiver to decode the channel codeword satisfies $\Pr(\mathcal{E}_2) \to 0$. Since the number of sequences in each bin satisfies $M_{\text{WZ}} = 2^{N(I(t;v)-\eta)}$, the event $\mathcal{E}_3$ that the decoder fails to uniquely decode t^N satisfies $\Pr(\mathcal{E}_3) \to 0$.

A proof for the fact that the error event $\mathcal{E}_4$ also happens with a vanishing probability when $\varepsilon < \delta/4$ i.e.,

$$\Pr(\mathcal{E}_4) \to 0 \tag{35}$$

as $n \to \infty$ is provided in Appendix B.

Now consider a codebook $\mathcal{C}$ for which the error events have vanishing probability. For this codebook the legitimate receiver will be able to decode the secret-key k with high probability. Also since $\Pr(\mathcal{E}_4) \to 0$, applying Fano's lemma,

$$\frac{1}{n} H(t^N | k, z^n) = o_\eta(1). \tag{36}$$

F. Secrecy Analysis

In this section, we show that for the codebook selected above, the equivocation at the eavesdropper is close (in an asymptotic sense) to R_{key}.

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

1) Uniformity Properties:

Lemma 1: For any code $\mathcal{C}$ in the random codebook ensemble, the resulting random variable Φ_{WZ} satisfies the following,

$$\frac{1}{n} H(\Phi_{\text{WZ}}) = \beta R_{\text{WZ}} + o_\eta(1) \tag{37a}$$

$$\frac{1}{n} H(t^N | \Phi_{\text{WZ}}) = \beta I(t; v) + o_\eta(1) \tag{37b}$$

$$\frac{1}{n} H(\Phi_{\text{WZ}} | z^n) = I(x; y) - I(x; z) + o_\eta(1). \tag{37c}$$

Remark 4: The relation (37a) states that the Wyner-Ziv bin index produced, is nearly uniformly distributed over $\{1, \ldots, N_{\text{WZ}}\}$. The second condition (37b) states that in given a bin $\mathcal{B}_i^{\text{WZ}}$ all the codeword sequences in this bin are selected with a nearly uniform probability. To interpret the last relation, recall that the Wyner-Ziv bin index is a message for the channel

codebook. Hence (37c) states that the equivocation rate of the message at the eavesdropper is governed by the channel equivocation in [31].

Proof:

To establish (37a), define the function $\Gamma_{\mathrm{WZ}} : \mathcal{T} \to \{1, \ldots, M_{\mathrm{WZ}}\}$ which identifies the position of the sequence $t^N \in \mathcal{T}$ in a given bin i.e., $\Gamma_{\mathrm{WZ}}(t_{ij}^{N,\mathrm{WZ}}) = j$ and note that,

$$\begin{aligned}
&\Pr(\Gamma_{\mathrm{WZ}} = j, \Phi_{\mathrm{WZ}} = i) = \Pr(t_{ij}^{N,\mathrm{WZ}}) \\
&\leq \sum_{u^N \in T_{u,t,\eta}(t_{ij}^{N,\mathrm{WZ}})} \Pr(u^N) && (38)\\
&= \sum_{u^N \in T_{u,t,\eta}(t_{ij}^{N,\mathrm{WZ}})} 2^{-N(H(u)+o_\eta(1))} && (39)\\
&= 2^{N(H(u|t)+o_\eta(1))} 2^{-N(H(u)+o_\eta(1))} && (40)\\
&= 2^{-N(I(t;u)+o_\eta(1))} && (41)
\end{aligned}$$

where (38) follows from the construction of the joint-typicality encoder, and (39) from the fact that the number of sequences u^N jointly typical with $t_{ij}^{N,\mathrm{WZ}}$ is equal to $2^{N(H(u|t)+o_\eta(1))}$. Since there are a total of $2^{N(I(u;t))+\eta}$ codewords sequences, it follows from (41) that

$$\frac{1}{N} H(\Phi_{\mathrm{WZ}}, \Gamma_{\mathrm{WZ}}) = I(t; u) + o_\eta(1). \tag{42}$$

Furthermore, marginalizing (38), we have that

$$\begin{aligned}
\Pr(\Phi_{\mathrm{WZ}} = i) &= \sum_{j=1}^{M_{\mathrm{WZ}}} \Pr(\Gamma_{\mathrm{WZ}} = j, \Phi_{\mathrm{WZ}} = i) \\
&\leq M_{\mathrm{WZ}} 2^{-N(I(t;u)+o_\eta(1))} \\
&= 2^{-N(I(t;u)-I(t;v)+o_\eta(1))} \\
&= 2^{-N(R_{\mathrm{WZ}}+o_\eta(1))} && (43)
\end{aligned}$$

Since $\Phi_{\mathrm{WZ}} \in \{1, \ldots, 2^{N(R_{\mathrm{WZ}}+2\eta)}\}$ it follows that

$$\frac{1}{N} H(\Phi_{\mathrm{WZ}}) = R_{\mathrm{WZ}} + o_\eta(1). \tag{44}$$

Furthermore,

$$\frac{1}{N} H(t^N|\Phi_{\mathrm{WZ}}) = \frac{1}{N} H(\Gamma_{\mathrm{WZ}}|\Phi_{\mathrm{WZ}}) = \frac{1}{N} H(\Gamma_{\mathrm{WZ}}, \Phi_{\mathrm{WZ}}) - \frac{1}{N} H(\Phi_{\mathrm{WZ}}) = I(t; v) + o_\eta(1). \tag{45}$$

To establish (37c) note that in our construction there is a one-to-one correspondence between Φ_{WZ} and x^n. Hence we have that

$$\begin{aligned}
&\frac{1}{n} H(\Phi_{\mathrm{WZ}}|z^n) \\
&= \frac{1}{n} H(\Phi_{\mathrm{WZ}}) + \frac{1}{n} H(z^n|\Phi_{\mathrm{WZ}}) - \frac{1}{n} H(z^n) && (46)\\
&= \beta R_{\mathrm{WZ}} + o_\eta(1) + \frac{1}{n} H(z^n|x^n) - \frac{1}{n} H(z^n) && (47)\\
&= I(x; y) - 3\delta + o_\eta(1) + \frac{1}{n} H(z^n|x^n) - \frac{1}{n} H(z^n) && (48)
\end{aligned}$$

where (47) follows from (43) which provides a bound on the probability of $\Phi_{\rm WZ}$ and the fact that there is a one-to-one correspondence between $\Phi_{\rm WZ}$ and x^n, and (48) follows by substituting the expression for $R_{\rm WZ}$ in the relation (26).

To simplify the remaining two expressions let J denote the indicator variable, which equals 1 if $(z^n, x^n) \in T^n_{zx,\eta}$ and zero otherwise. Recall that each x^n is sampled uniformly from the set T^n_x and since the channel $p_{z|x}(\cdot)$ is memoryless it follows from the conditional typicality lemma that $\Pr(J=1) = 1 - o_\eta(1)$ and also that

$$\begin{aligned}\frac{1}{n}H(z^n|x^n) &\geq \frac{1}{n}H(z^n|x^n, J=1)\Pr(J=1) &(49)\\ &\geq H(z|x) - o_\eta(1) &(50)\end{aligned}$$

and furthermore

$$\begin{aligned}\frac{1}{n}H(z^n) &\leq \frac{1}{n}H(z^n|J=1)\Pr(J=1) + \frac{1}{n}H(J) &(51)\\ &\leq H(z) + o_\eta(1). &(52)\end{aligned}$$

Substituting (50) and (52) in (48) establishes (37c).
■

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

$$\begin{aligned}H(k|z^n) &= H(k, t^N|z^n) - H(t^N|z^n, k)\\ &= H(t^N|z^n) - H(t^N|z^n, k) &(53)\\ &= H(t^N, \Phi_{\rm WZ}|z^n) - H(t^N|z^n, k) &(54)\\ &= H(t^N|\Phi_{\rm WZ}, z^n) + H(\Phi_{\rm WZ}|z^n) - H(t^N|z^n, k)\\ &= H(t^N|\Phi_{\rm WZ}) + H(\Phi_{\rm WZ}|z^n) - H(t^N|z^n, k), &(55)\\ &= n\beta I(t; v) + n\{I(x; y) - I(x; z)\} + o_\eta(1) &(56)\\ &= n\{R_{\rm key} + o_\eta(1)\}, &(57)\end{aligned}$$

where (53) and (54) follow from the fact that $\Phi_{\rm WZ}$ is a deterministic function of t^N and (55) follows from the fact that $t^N \to \Phi_{\rm WZ} \to z^n$ holds for our code construction. and (56) follows from (37b) and (37c) in Lemma 1 and (36).

Thus we have that

$$\frac{1}{n}H(k|z^n) = R_{\rm key} + o_\eta(1),$$

as required.

V. Converse: Proof of theTheorem 2

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

$$\begin{aligned}\frac{1}{n}H(k|y^n, v^N) &\leq \varepsilon_n &(58a)\\ \frac{1}{n}H(k|z^n) &\geq \frac{1}{n}H(k) - \varepsilon_n. &(58b)\end{aligned}$$

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

$$\begin{aligned} nR_{\text{key}} &= H(k) \\ &= H(k|y^n, v^N) + I(k; y^n, v^N) \\ &\le n\varepsilon_n + I(k; y^n, v^N) - I(k; z^n) + I(k; z^n) && (59) \\ &\le 2n\varepsilon_n + I(k; y^n, v^N) - I(k; z^n) && (60) \\ &= 2n\varepsilon_n + I(k; y^n) - I(k; z^n) + I(k; v^N|y^n) \\ &\le 2n\varepsilon_n + I(k; y^n) - I(k; z^n) + I(k, y^n; v^N) && (61) \end{aligned}$$

where (59) and (60) follow from (58a) and (58b) 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 $t \to u_{\text{J}} \to v_{\text{J}}$ holds since the source sequences are memoryless.

$$\begin{aligned} I(k, y^n; v^N) &= \sum_{i=1}^{n} I(k, y^n; v_i|v_{i+1}^N) \\ &\le \sum_{i=1}^{N} I(k, y^n, v_{i+1}^N; v_i) \\ &\le \sum_{i=1}^{N} I(k, y^n, v_{i+1}^N, u_1^{i-1}; v_i) \\ &= NI(k, y^n, v_{J+1}^N, u_1^{J-1}; v_J|J) \\ &= NI(k, y^n, v_{J+1}^N, u_1^{J-1}, J; v_J) - I(J; v_J) \\ &= NI(t; v) && (62) \end{aligned}$$

where (62) 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.

$$\begin{aligned} I(k; y^n) - I(k; z^n) &\le I(k; y^n|z^n) \\ &\le I(x^n; y^n|z^n) && (63) \\ &\le \sum_{i=1}^{n} I(x_i; y_i|z_i) && (64) \\ &\le nI(x; y|z), && (65) \end{aligned}$$

where (63) follows from the Markov condition $k \to x^n \to (y^n, z^n)$ and (64) follows from the fact that the channel is memoryless and (65) follows from Jensen's inequality since the term $I(x; y|z)$ is concave in the distribution p_x (see e.g., [19, Appendix-I]).

Combining (65) and (62) we have that

$$R_{\text{key}} \le I(x; y|z) + \beta I(v; t), \tag{66}$$

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

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

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

$$\begin{aligned} nI(x;y) &\geq I(x^n;y^n) && (67)\\ &\geq I(u^N;y^n) && (68)\\ &\geq I(u^N;y^n,k) - I(v^N;y^n,k) - n\varepsilon_n, && (69)\end{aligned}$$

where the last inequality holds, since

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

where the last step holds via (58a) and the fact that $H(k|y^n,u^N) \geq 0$.

Continuing (69), we have

$$\begin{aligned} nI(x;y) &\geq I(u^N;y^n,k) - I(v^N;y^n,k) - n\varepsilon_n && (70)\\ &= \sum_{i=1}^{N}\{I(u_i;y^n,k|u_1^{i-1}v_{i+1}^N) - I(v_i;y^n,k|u_1^{i-1}v_{i+1}^N)\} + n\varepsilon_n && (71)\\ &= \sum_{i=1}^{N}\{I(u_i;y^n,k,u_1^{i-1}v_{i+1}^N) - I(v_i;y^n,k,u_1^{i-1}v_{i+1}^N)\} + n\varepsilon_n && (72)\\ &= N\{I(u_J;y^n,k,u_1^{J-1}v_{J+1}^N|J) - I(v_J;y^n,k,u_1^{J-1}v_{J+1}^N|J) + \varepsilon_n\}\\ &= N\{I(u_J;t) - I(v_J;t) + I(v_J;J) - I(u_J;J) + \varepsilon_n\}\\ &= N\{I(u;t) - I(v;t) + \varepsilon_n\} && (73)\end{aligned}$$

where (71) follows from Csiszar's Lemma (see e.g., [8, Section V]) which states that for any triple (M,y^n,z^n) with an arbitrary joint distribution $p(M,y^n,z^n)$ and any $n \geq 1$ we have that

$$I(M;y^n) - I(M;z^n) = \sum_{i=1}^{n} I(M;y_i|y^{i-1},z_{i+1}^n) - I(M;z_i|y^{i-1},z_{i+1}^n). \quad (74)$$

Furthermore (72) follows from the fact that (u_i,v_i) is independent of (u^{i-1},v_{i+1}^n) and (73) 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 is shown in Appendix C.

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.

A. Proof of Proposition 1

Following [14] we introduce a fictitious memoryless channel $p_{g,y,z|x}(\cdot)$ whose marginal distribution $p_{y,z|x}(\cdot)$ coincides with the original channel transition probability.

$$\begin{aligned} nR_{\text{key}} &= H(k) \\ &= H(k|y^n, v^N) + I(k; y^n, v^N) \\ &\leq n\varepsilon_n + I(k; y^n, v^N) - I(k; g^n) + I(k; g^n) \qquad (75) \\ &= n\varepsilon_n + I(k; y^n) - I(k; g^n) + I(k; v^N|y^n) + I(k; g^n) \\ &\leq n\varepsilon_n + I(k; y^n) - I(k; g^n) + I(k, y^n; v^N) + I(k; g^n). \qquad (76) \end{aligned}$$

Following the steps leading to (65) we can establish that

$$I(k; y^n) - I(k; g^n) \leq nI(x; y|g) \qquad (77)$$

and with $t = (k, y^n, v_{J+1}^N, u_1^{J-1}, J)$ we have via (62) that

$$I(k, y^n; v^N) \leq NI(t; v) \qquad (78)$$

and finally

$$\begin{aligned} I(k; g^n) &\leq I(k; g^n) - I(k; z^n) + I(k; z^n) \\ &\leq I(k; g^n) - I(k; z^n) + n\varepsilon_n \qquad (79) \\ &\leq nI(x; g|z) + n\varepsilon_n \qquad (80) \end{aligned}$$

where (79) follows from the secrecy constraint with respect to the receiver who observes z^n (c.f. (58b)) and the last step can be established in a manner analogous to that in (65). Substituting (77), (78) and (80) into (76) and normalizing by n we have that

$$R_{\text{key}} \leq \beta I(t; v) + I(x; y|g) + I(x; g|z). \qquad (81)$$

The remaining constraint does not involve g and directly follows from (73).

Following the discussion in [14] we can interpret the bound (81) as follows. We split the total secret-key into two parts. The first part is kept secret from the fictitious user only and its rate is upper bounded by $I(x; y|g)$ whereas the second part is shared with the fictitious user and kept secret from the eavesdropper. Its rate is upper bounded by $I(x; g|z)$. The claim is that the secret-key capacity in the original problem cannot exceed the sum of two rates split in this way.

VI. Reversely Degraded Channels

A. Proof of Theorem 3

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

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

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

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

For the reversely degraded parallel independent channels, note that

$$I(x;y) \leq \sum_{i=1}^{M} I(x_i;y_i)$$
$$I(x;y|z) \leq \sum_{i=1}^{M} I(x_i;y_i|z_i),$$

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 Theorem 1, such that the resulting expression reduces to the capacity. In particular, assume without loss in generality that for the first M^+ 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 $b = (x_{M^+ +1}, \ldots, x_M)$ where the random variables $\{x_i\}$ are mutually independent. Note that this choice of (a,b) is feasible i.e., it satisfies $I(b;z) \leq I(b;y)$ and $I(a;y|b) \geq I(a;z|b)$. It follows from (6a) and (6b) that

$$R_{\text{ch}} = \sum_{i=1}^{M} I(x_i;y_i) \tag{82}$$
$$R_{\text{eq}}^{-} = \sum_{i=1}^{M^+} I(x_i;y_i) - I(x_i;z_i) \tag{83}$$
$$= \sum_{i=1}^{M^+} I(x_i;y_i|z_i) = \sum_{i=1}^{M} I(x_i;y_i|z_i), \tag{84}$$

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 (7) and (8) 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 $t \to u \to v$,

$$C_{\text{key}} = \sum_i I(x_i;y_i|z_i) + \beta I(t;v) \tag{85}$$

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

$$\sum_i I(x_i;y_i) \geq \beta\{I(t;u) - I(t;v)\}. \tag{86}$$

Let us first fix the distribution $p_{\mathbf{x}}$ and upper bound the objective function (85). 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 due to Bergmans [2],

$$\exp(2h(u+s|t)) \geq \exp(2h(u|t)) + \exp(2h(s)) \tag{87}$$

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 (86) as

$$\begin{aligned} R + h(v) - h(u) &\geq h(v|t) - h(u|t) && (88)\\ &= h(u+s|t) - h(u|t) && (89)\\ &\geq \frac{1}{2}\log\left(\exp(2h(u|t)) + 2\pi e S\right) - h(u|t) && (90)\end{aligned}$$

Letting

$$h(u|t)) = \frac{1}{2}\log 2\pi e D, \tag{91}$$

we have that

$$D \geq \frac{S}{\exp(2(R + h(v) - h(u))) - 1}. \tag{92}$$

Rearranging we have that

$$\sum_{i=1}^{M} I(x_i; y_i) \geq \frac{\beta}{2}\left[\log\left(1 + \frac{S}{D}\right) - \log(1+S)\right]. \tag{93}$$

The term $I(t; v)$ in the objective function (85) can be upper bounded as

$$\begin{aligned} I(t; v) &= h(v) - h(v|t)\\ &= h(v) - h(u+s|t)\\ &\leq h(v) - \frac{1}{2}\log(\exp(2h(u|s)) + 2\pi e S) && (94)\\ &= \frac{1}{2}\log\frac{1+S}{D+S} && (95)\end{aligned}$$

where (94) follows by the application of the EPI (87) and (95) follows via (91). Thus the objective function (85) can be expressed as

$$C_{\text{key}} = \sum_i I(x_i; y_i|z_i) + \frac{\beta}{2}\log\frac{1+S}{D+S}, \tag{96}$$

where D satisfies (92).

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., [21]) 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 (85).

VII. Side information at the Wiretapper

We now provide an achievability and a converse for the capacity stated in Theorem 4

A. Achievability

The coding scheme is a natural extension of the case when $w = 0$. In particular the construction involves a subset $\mathcal{T}$ of T_t^N partitioned into a Wyner-Ziv codebook $\mathcal{C}^{\mathrm{WZ}}$ and a secret-key codebook $\mathcal{C}^{\mathrm{SK}}$. In addition the channel codebook $\mathcal{C}^{\mathrm{ch}}$ is a subset of the set T_x^n. As before the Wynzer-Ziv codebook consists of N_{WZ} bins, each consisting of a total of M_{WZ} codewords, where we select $M_{\mathrm{WZ}} = \exp_2(N(I(t;v) - \eta))$ and $N_{\mathrm{WZ}} = \exp_2(N(R_{\mathrm{wz}} + 2\eta))$. However the parameters of the secret-key codebook are selected to reflect the side information at the eavesdropper. The secret-key codebook consists of a total of N_{SK} bins, each consisting of M_{SK} sequences, where

$$M_{\mathrm{SK}} = \exp_2\left(n(I(x;z) + \beta I(w;t)) - \delta\right) \tag{97}$$

$$N_{\mathrm{SK}} = \exp_2\left(n(\beta R_{\mathrm{s}} + R_{\mathrm{eq}}^{-} - \delta)\right) \tag{98}$$

reflect the increase in number of codewords in each bin to account for the side information at the eavesdropper. Furthermore we replace R_{s} in (6c) with

$$R_{\mathrm{s}} = I(t;v) - I(t;w) \tag{99}$$

and the resulting secret-key rate in (7) is

$$R_{\mathrm{LB}} = \beta R_{\mathrm{s}} + R_{\mathrm{eq}}^{-}. \tag{100}$$

as reflected in the exponent of N_{SK}. Finally since the channels are assumed to be degraded note that R_{ch} and R_{eq}^{-} in (6a) and (6b) are defined as

$$R_{\mathrm{ch}} = I(x;y) \tag{101}$$

$$R_{\mathrm{eq}}^{-} = I(x;y) - I(x;z) = I(x;y|z). \tag{102}$$

The channel codebook consists of a total of $\exp(nR_{\mathrm{ch}} - n\delta)$ codewords as in the no-side information case. Furthermore as in (26), we present the coding scheme for

$$R_{\mathrm{WZ}} = R_{\mathrm{ch}} - 3\delta, \tag{103}$$

and the case when $R_{\mathrm{WZ}} < R_{\mathrm{ch}} - 3\delta$ follows by a time-sharing argument. Thus the total number of codewords is

$$N_{\mathrm{tot}} = N_{\mathrm{WZ}} M_{\mathrm{WZ}} = N_{\mathrm{SK}} M_{\mathrm{SK}} = \exp_2\left(N(I(u;t) + \eta)\right) \tag{104}$$

The encoder is analogous to the case without side information described in section IV-B. The transmitter upon observing u^N finds a sequence $t^N \in \mathcal{T}$ that is jointly typical. If there is more than one sequence, any one of the candidates is selected at random. The encoder declares the bin index of t^N in the $\mathcal{C}^{\mathrm{SK}}$ as the secret-key codebook whereas the bin index of t^N in $\mathcal{C}^{\mathrm{WZ}}$ is used as the message for the channel codebook. The resulting codeword x^n is then transmitted over n channel uses. The decoder at the legitimate receiver is as described in section IV-C. We summarize the main steps below

- The decoder searches for a unique sequence in $\mathcal{C}^{\mathrm{ch}}$ that is jointly typical with y^n. If successful, it obtains the bin-index of the Wyner-Ziv codebook.
- It then searches for a unique sequence in this bin jointly typical with v^N.
- It declares the bin-index of the resulting sequence in the secret-key codebook to be the secret key.

The decoding at the eavesdropper, with the knowledge of the key as described in section IV-D, needs to be modified to take into account the additional side information w^N. The decoder

searches for a sequence in the set $\mathcal{B}_k^{\mathrm{SK}}$ that is (a) jointly typical with w^N i.e., $(w^N, t_{kj}^n) \in T_{wt,\varepsilon}^N$and (b) the Wyner-Ziv bin index $h_j = \Phi_{\mathrm{WZ}}(t_{kj}^{N,\mathrm{SK}})$ is such that $x_{h_j}^n$ is jointly typical with the received sequence z^n i.e., $(x_{h_j}^N, z^n) \in T_{xz,\varepsilon}^n$.

The probability of error analysis at the encoder and the legitimate decoder follows from the no-side information case as there are no modifications in the Wyner-Ziv codebook and the channel codebook whereas the secret-key codebook is only used for a lookup. To compute the error probability at the modified eavesdropper, note that the failure event can be expressed as:

$$\mathcal{F} = \mathcal{F}_0 \bigcup_{j=1, j\neq j_0}^{M_{\mathrm{SK}}} \mathcal{F}_j \tag{105}$$

where j_0 denotes the index of the secret-key in $\mathcal{B}_k^{\mathrm{SK}}$ i.e., $t^N = t_{kj_0}^{N,\mathrm{SK}}$ and $\mathcal{F}_0$ denotes the event that the sequence selected by the transmitter fails to be in the typical set of the eavesdropper while $\mathcal{F}_j$ denotes the event that the sequence $t_{kj}^{N,\mathrm{SK}}$ for $j \neq j_0$ appears in the typical set of the eavesdropper. Thus we have that

$$\Pr(\mathcal{F}) \leq \Pr(\mathcal{F}_0) + \sum_{j\neq j_0} \Pr(\mathcal{F}_j). \tag{106}$$

From the law of large numbers it follows that $\Pr(\mathcal{F}_0) \to 0$. Furthermore we can express

$$\mathcal{F}_j = \mathcal{J}_j \bigcap \mathcal{I}_j, \qquad j \neq j_0 \tag{107}$$

where $\mathcal{J}_j$ denotes the event that $x_{h_j}^n$ is jointly typical with z^n and $\mathcal{I}_j$ is the event that $(t_{ij}^{N,\mathrm{SK}}, w^N) \in T_{tw,\varepsilon}^N$. Following the analysis in Appendix B leading to (187) we have that

$$\Pr(\mathcal{J}_j) \leq \exp_2(-n(I(x;z) - 4\varepsilon)) \tag{108}$$

and furthermore since $t_{kj}^{N,\mathrm{SK}}$ is selected independent of w^N for $j \neq j_0$ we have that $\Pr(\mathcal{I}_j) \leq \exp_2(-N(I(t;w) - 3\varepsilon))$. Since the events $\mathcal{J}_i$ and $\mathcal{I}_i$ are due to atypical channel and source events respectively they are mutually independent and hence

$$\Pr(\mathcal{F}_j) = \Pr(\mathcal{I}_j)\Pr(\mathcal{J}_j) = \exp_2\left\{-n(I(x;z) + \beta I(t;w) - \varepsilon')\right\} \tag{109}$$

where $\varepsilon' = 3\beta\varepsilon + 4\varepsilon$. Using (97) we have that

$$\Pr(\mathcal{F}) \leq \Pr(\mathcal{F}_0) + M_{\mathrm{SK}} \Pr(\mathcal{F}_j) \tag{110}$$

$$= \Pr(\mathcal{F}_0) + \exp_2(-n(\delta - \varepsilon')), \tag{111}$$

which vanishes as $n \to \infty$. In the secrecy analysis in the next subsection we use the fact that any codebook satisfying (111) as satisfies, from Fano's lemma,

$$\frac{1}{N} H(t^N | k, w^n, z^n) = o_\eta(1). \tag{112}$$

B. Secrecy Analysis

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

$$\frac{1}{n}H(k|w^N, z^n) = \beta(I(t;v) - I(t;w)) + I(x;y|z) + o_\eta(1), \tag{113}$$

which we will now do.

We first provide an alternate expression for the left hand side in (113).

$$\begin{aligned} H(k|w^N, z^n) &= H(k, t^N|w^N, z^n) - H(t^N|k, w^N, z^n) && (114)\\ &= H(t^N|w^N, z^n) - H(t^N|k, w^N, z^n) \\ &= H(t^N|w^N, z^n) - No_\eta(1) && (115)\\ &= H(t^N, \Phi_{\mathrm{WZ}}|w^N, z^n) - No_\eta(1) && (116)\\ &= H(\Phi_{\mathrm{WZ}}|w^N, z^n) + H(t^N|\Phi_{\mathrm{WZ}}, w^N) - No_\eta(1) && (117)\end{aligned}$$

where (115) follows from (112), (116) follows from the fact that Φ_{WZ} is a deterministic function of t^N, while (117) 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 (113) is established by showing that

$$\frac{1}{n}H(\Phi_{\mathrm{WZ}}|w^N, z^n) \geq I(x;y|z) + o_\eta(1) \tag{118a}$$

$$\frac{1}{n}H(t^N|\Phi_{\mathrm{WZ}}, w^N) = \beta(I(t;v) - I(t;w)) + o_\eta(1) \tag{118b}$$

To interpret (118a), recall that Φ_{WZ} is the message to the channel codebook. The equivocation introduced by the channel codebook $\frac{1}{n}H(\Phi_{\mathrm{WZ}}|z^n)$ equals $I(x;y|z)$. Eq. (118a) 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 2 below), it is also independent of w^N due to the Markov condition. Eq. (118b) shows that the knowledge of w^N reduces the list of t^N sequences in any bin from $\exp_2(N(I(t;v)))$ to $\exp_2(N(I(t;v) - I(t;w)))$.

To establish (118a),

$$\begin{aligned} \frac{1}{n}H(\Phi_{\mathrm{WZ}}|w^N, z^n) &\geq \frac{1}{n}H(\Phi_{\mathrm{WZ}}|z^n, v^N) && (119)\\ &= \frac{1}{n}H(\Phi_{\mathrm{WZ}}|z^n) - \frac{1}{n}I(\Phi_{\mathrm{WZ}}; v^N|z^n) \\ &\geq I(x;y|z) + o_\eta(1) - \frac{1}{n}I(\Phi_{\mathrm{WZ}}; v^N|z^n), && (120)\\ &\geq I(x;y|z) + o_\eta(1) - \frac{1}{n}I(\Phi_{\mathrm{WZ}}; v^N), && (121)\end{aligned}$$

where (119) follows from the fact that $w^N \to v^N \to (\Phi_{\mathrm{WZ}}, z^n)$, (120) from Lemma 1 and (121) from the fact that $v^N \to \Phi_{\mathrm{WZ}} \to z^n$ so that

$$\frac{1}{n}I(\Phi_{\mathrm{WZ}}; v^N|z^n) \leq \frac{1}{n}I(\Phi_{\mathrm{WZ}}; v^N). \tag{122}$$

Thus we need to show the following.

Lemma 2:

$$\frac{1}{N}I(\Phi_{\mathrm{WZ}}; v^N) = o_\eta(1). \tag{123}$$

Proof: From Lemma 1 note that

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

and hence we need to show that

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

as we do below.

$$\begin{aligned}\frac{1}{N}H(\Phi_{\mathrm{WZ}}|v^N) &= \frac{1}{N}H(\Phi_{\mathrm{WZ}}, t^N|v^N) - \frac{1}{N}H(t^N|v^N, \Phi_{\mathrm{WZ}}) \\ &= \frac{1}{N}H(t^N|v^N) + o_\eta(1) \qquad (124)\end{aligned}$$

Where (124) follows since each bin has $M_{\mathrm{WZ}} = \exp_2\left(N(I(t;v)-\eta)\right)$ sequences, (from standard joint typicality arguments) we have that

$$\frac{1}{N}H(t^N|v^N, \Phi_{\mathrm{WZ}}) = o_\eta(1). \qquad (125)$$

Furthermore,

$$\begin{aligned}\frac{1}{N}H(t^N|v^N) &= \frac{1}{N}H(v^N|t^N) + \frac{1}{N}H(t^N) - \frac{1}{N}H(v^N) \qquad (126)\\ &= \frac{1}{N}H(v^N|t^N) + \frac{1}{N}H(t^N) - H(v) \qquad (127)\\ &= \frac{1}{N}H(v^N|t^N) + I(u;t) - H(v) + o_\eta(1) \qquad (128)\end{aligned}$$

where (127) follows from the fact v^N is an i.i.d. sequence whereas (128) follows via (41) since we have that $H(t^N) = H(\Gamma_{\mathrm{WZ}}, \Phi_{\mathrm{WZ}})$. Furthermore define J to be an indicator variable that equals 1 if $(v^N, t^N) \in T^N_{vt,\eta}$ and zero otherwise. From standard typicality arguments, $\Pr(J=1) = 1 - o_\eta(1)$ and $\Pr(J=0) = o_\eta(1)$ and by counting the number of jointly typical sequences in $T^n_{v,\varepsilon}$ for each $t^N \in \mathcal{T}^n_{t,\varepsilon}$ we can show (see e.g., [13, pp. 2.32—2.34])

$$\frac{1}{N}H(v^N|t^N, J=1) = H(v|t) + o_\eta(1) \qquad (129)$$

Hence,

$$\begin{aligned}\frac{1}{N}H(v^N|t^N) &= \frac{1}{N}H(v^N|t^N, J) + \frac{1}{N}I(J; v^N|t^N)\\ &= \frac{1}{N}H(v^N|t^N, J) + o_\eta(1) \qquad (130)\\ &= \frac{1}{N}H(v^N|t^N, J=1)\Pr(J=1) + \frac{1}{N}H(v^N|t^N, J=0)\Pr(J=0) + o_\eta(1)\\ &= \frac{1}{N}H(v^N|t^N, J=1) + o_\eta(1) \qquad (131)\\ &= H(v|t) + o_\eta(1), \qquad (132)\end{aligned}$$

where (130) follows from the fact that $H(J) \leq 1$, since J is a binary random variable, and (131) follows from the fact that $\Pr(J=0) = o_\eta(1)$ and the last step follows from (129). Combining (132), (128) and (124) completes the proof. ■

To establish (118b), we begin by observing that,

$$\frac{1}{n}H(t^N|\Phi_{\rm WZ}, w^N) = \frac{1}{n}H(w^N|t^N, \Phi_{\rm WZ}) + \frac{1}{n}H(t^N|\Phi_{\rm WZ}) - \frac{1}{n}H(w^N|\Phi_{\rm WZ}) \tag{133}$$

$$= \frac{1}{n}H(w^N|t^N) + \frac{1}{n}H(t^N|\Phi_{\rm WZ}) - \frac{1}{n}H(w^N|\Phi_{\rm WZ}) \tag{134}$$

$$= \beta H(w|t) + \frac{1}{n}H(t^N|\Phi_{\rm WZ}) - \frac{1}{n}H(w^N|\Phi_{\rm WZ}) + o_\eta(1) \tag{135}$$

$$= \beta H(w|t) + \beta I(t;v) - \frac{1}{n}H(w^N|\Phi_{\rm WZ}) + o_\eta(1) \tag{136}$$

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

$$= \beta H(w|t) + \beta I(t;v) - \frac{1}{n}H(w^N) + o_\eta(1) \tag{137}$$

$$= \beta H(w|t) + \beta I(t;v) - \beta H(w) + o_\eta(1) \tag{138}$$

$$= \beta I(t;v) - \beta I(t;w) + o_\eta(1) \tag{139}$$

$$\tag{140}$$

where (134) follows from the fact that $\Phi_{\rm WZ}$ is a deterministic function of t^N, and (135) follows through an argument analogous to that used to establish (132) and (136) follows from (37b), is established in Lemma 1, and (137) follows from Lemma 2 since $\Phi_{\rm WZ} \to v^N \to w^N$ and (139) follows from the fact that the sequence w^N is i.i.d.

C. Converse

Consider a sequences of (n, N) codes that achieves a secret key rate of R. Let $\beta = N/n$. Then from Fano's Lemma,

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

and from the secrecy constraint.

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

Combining these inequalities, we have that,

$$\begin{aligned}
nR_{\rm key} &\leq I(k; y^n, v^N) - I(k; z^n, w^N) + 2n\varepsilon_n \\
&\leq I(k; y^n, v^N \mid z^n, w^N) + 2n\varepsilon_n \\
&\leq H(y^n \mid z^n) + H(v^N \mid w^N) - H(y^n \mid z^n, w^N, k) - H(v^N \mid y^n, z^n, w^N, k) + 2n\varepsilon_n \\
&\leq H(y^n \mid z^n) + H(v^N \mid w^N) - H(y^n \mid z^n, w^N, k, x^n) - H(v^N \mid y^n, z^n, w^N, k) + 2n\varepsilon_n \\
&= H(y^n \mid z^n) + H(v^N \mid w^N) - H(y^n \mid z^n, x^n) - H(v^N \mid y^n, z^n, w^N, k) + 2n\varepsilon_n
\end{aligned} \tag{141}$$

$$\leq \sum_{i=1}^{n} I(x_i; y_i \mid z_i) + H(v^N \mid w^N) - H(v^N|y^n, w^N, k) + 2n\varepsilon_n \tag{142}$$

$$\leq nI(x; y \mid z) + H(v^N \mid w^N) - H(v^N|y^n, w^N, k) + 2n\varepsilon_n \tag{143}$$

where the (141) follows from the fact that $(w^N, k) \to (z^n, x^n) \to y^n$, and (142) follows from the Markov condition $z^n \to (y^n, w^N, k) \to v^N$ that holds for the degraded channel, while (143) follows from the fact that $I(x; y|z)$ is a concave function of p_{x_i} (see e.g., [19, 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 $[1, 2, \dots N]$ and $t = (J, k, u_{J+1}^N v^{J-1}, y^n)$ we have that

$$\begin{aligned} H(v^N|y^n, w^N, k) &= \sum_{i=1}^{N} H(v_i|v^{i-1}, y^n, w^N, k) \\ &\geq \sum_{i=1}^{N} H(v_i|v^{i-1}, y^n, w^N, u_{i+1}^N, k) \\ &= \sum_{i=1}^{N} H(v_i|v^{i-1}, y^n, w_i, u_{i+1}^N, k) \qquad (144) \\ &= N \cdot H(v_J|t, w_J) \end{aligned}$$

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

$$\begin{aligned} & p\left(v_i \mid w_i, w^{i-1}, w_{i+1}^N, v^{i-1}, u_{i+1}^N, y^n, k\right) \\ =& \sum_{u_i=u} p\left(v_i \mid w_i, u_i = u, w^{i-1}, w_{i+1}^N, v^{i-1}, u_{i+1}^N, y^n, k\right) p\left(u_i = u \mid w_i, w^{i-1}, w_{i+1}^N, v^{i-1}, u_{i+1}^N, y^n, k\right) \\ =& \sum_{u_i=u} p\left(v_i \mid w_i, u_i = u\right) p\left(u_i = u \mid w_i, v^{i-1}, u_{i+1}^N, y^n, k\right) \qquad (145) \\ =& p\left(v_i \mid w_i, v^{i-1}, u_{i+1}^N, y^n, k\right), \end{aligned}$$

where (145) 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 (143) that

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

Finally, using the steps between (70)-(73) as in the converse for the case when $w = 0$, we have that

$$I(x; y) \geq \beta(I(t; u) - I(t; v)), \qquad (146)$$

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 lemma we have the following,

$$\begin{aligned} nR &= H(k) && (147) \\ &= H(k|l) + I(k; l) && (148) \\ &\leq n\varepsilon_n + I(k; l) && (149) \end{aligned}$$

where the last inequality follows from Fano's lemma. 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

$$\begin{aligned}nR &\leq n\varepsilon_n + I(k;l,\psi^k,\phi^k,z^n) &(150)\\ &\leq 2n\varepsilon_n + I(k;l|\psi^k,\phi^k,z^n) &(151)\\ &\leq 2n\varepsilon_n + I(m_{\mathrm{x}},u^N;m_y,v^N,y^n|\psi^k,\phi^k,z^n), &(152)\end{aligned}$$

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

Using the chain rule, we have that

$$\begin{aligned}&I(m_{\mathrm{x}},u^N;m_y,v^N,y^n|\psi^k,\phi^k,z^n) &(153)\\ &= I(m_{\mathrm{x}},u^N;m_y,v^N,y^n,\psi^k,\phi^k,z^n) - I(m_{\mathrm{x}},u^N;\psi^k,\phi^k,z^n) &(154)\\ &= I(m_{\mathrm{x}},u^N;m_y,v^N,\psi^{i_1-1},\phi^{i_1-1}) + \sum_{j=1}^{n} F_j + G_j\\ &\quad - I(m_{\mathrm{x}},u^N;\psi^{i_1-1},\phi^{i_1-1}) - \sum_{j=1}^{n}\hat{F}_j+\hat{G}_j, &(155)\end{aligned}$$

where for each $j=1,2,\ldots,n$ we define

$$\begin{aligned}F_j &= I(m_{\mathrm{x}},u^N;y_j,z_j|m_y,v^N,y^{j-1},z^{j-1},\phi^{i_j-1},\psi^{i_j-1}) &(156)\\ G_j &= I(m_{\mathrm{x}},u^N;\phi_{i_j+1},\ldots,\phi_{i_{j+1}-1},\psi_{i_j+1},\ldots,\psi_{i_{j+1}-1}|m_y,v^N,y^j,z^j,\phi^{i_j-1},\psi^{i_j-1}) &(157)\\ \hat{F}_j &= I(m_{\mathrm{x}},u^N;z_j|z^{j-1},\psi^{i_j-1},\phi^{i_j-1}) &(158)\\ \hat{G}_j &= I(m_{\mathrm{x}},u^N;\phi_{i_j+1},\ldots,\phi_{i_{j+1}-1},\psi_{i_j+1},\ldots,\psi_{i_{j+1}-1}|z^j,\phi^{i_j-1},\psi^{i_j-1}). &(159)\end{aligned}$$

We now bound the expression in (155). 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

$$I(m_{\mathrm{x}},u^N;m_y,v^N|\psi^{i_1-1},\phi^{i_1-1})\leq I(m_{\mathrm{x}},u^N;m_y,v^N)=I(u^N;v^N)=NI(u;v) \qquad (160)$$

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

$$
\begin{aligned}
&F_j - \hat{F}_j && (161)\\
&= I(m_{\mathrm{x}}, u^N; y_j, z_j | m_y, v^N, y^{j-1}, z^{j-1}, \phi^{i_j-1}, \psi^{i_j-1}) - I(m_{\mathrm{x}}, u^N; z_j | z^{j-1}, \psi^{i_j-1}, \phi^{i_j-1})\\
&= H(y_j, z_j | m_y, v^N, y^{j-1}, z^{j-1}, \phi^{i_j-1}, \psi^{i_j-1}) - H(y_j, z_j | m_y, v^N, y^{j-1}, z^{j-1}, \phi^{i_j-1}, \psi^{i_j-1}, m_{\mathrm{x}}, u^N)\\
&\quad - H(z_j | z^{j-1}, \psi^{i_j-1}, \phi^{i_j-1}) + H(z_j | z^{j-1}, \psi^{i_j-1}, \phi^{i_j-1}, m_{\mathrm{x}}, u^N)\\
&= H(y_j, z_j | m_y, v^N, y^{j-1}, z^{j-1}, \phi^{i_j-1}, \psi^{i_j-1}) - H(y_j, z_j | x_j) - H(z_j | z^{j-1}, \psi^{i_j-1}, \phi^{i_j-1}) + H(z_j | x_j) && (162)\\
&\leq H(y_j | z^j, \psi^{i_j-1}, \phi^{i_j-1}) - H(y_j | z_j, x_j)\\
&\leq I(x_j; y_j | z_j), && (163)
\end{aligned}
$$

where (162) 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 $\phi_{i_{j+1}-1} = \Phi_{i_{j+1}-1}(m_{\mathrm{x}}, u^N, \psi^{i_{j+1}-2})$ and $\psi_{i_{j+1}-1} = \Psi_{i_{j+1}-1}(m_y, v^N, \phi^{i_{j+1}-2})$ we have that

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

Continuing this process we have that

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

and thus

$$
G_j - \hat{G}_j \leq 0. \tag{164}
$$

Substituting (160), (163) and (164) into (155) we have that

$$
\begin{aligned}
nR &\leq \sum_{j=1}^{n} I(x_j; y_j | z_j) + NI(u; v) + 2n\varepsilon_n && (165)\\
&\leq \max_{p_x} nI(x; y | z) + NI(u; v) + 2n\varepsilon_n && (166)
\end{aligned}
$$

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. 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, of "independent noise" channels we show that it suffices to separately treat 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 [10] 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.

Acknowledgement

Ashish Khisti thanks Matthieu Bloch for detailed comments and also spotting an error in an earlier version of this paper. The authors work was supported by Natural Science and Engineering Research Council of Canada (NSERC) discovery grant program, NSF Grant No. CCF-0515109 and Swiss National Science Foundation through NCCR-MICS.

Appendix A
Extension of Theorem 1 to general (a, b)

In section IV the coding theorem was derived for the case when $a = x$ and $b =$ const. In this section we complete the proof of the general case. We will only consider the case when $a = x$, since the general case follows by sampling the codewords from the typical set T_a^n and then passing each symbol of a^n through an auxiliary channel $p_{x|a}(\cdot)$.

A. Codebook Construction

We describe the construction of an ensemble of codebooks and by computing the error probability averaged over this ensemble, show that there exists one codebook with the desired property.

1) Channel Codebook: Define $R_a = I(x; y|b)$ and $R_b = I(b; y)$ and recall that since $b \to x \to y$ we have that $R_a + R_b = I(x; y)$. We construct a *base* codebook $\mathcal{C}_b$ consisting of $N_b = \exp_2(nR_b - n\delta_b)$ sequences, which forms the could center of a superposition code. For each sequence $b_i^n \in \mathcal{C}_b$ we generate a codebook $\mathcal{C}_a(b_i^n)$ consisting of $N_a = \exp_2(nI(x; y|b) - n\delta_a)$ sequences. All sequences in $\mathcal{C}_b$ are sampled uniformly at random from the set T_b^n while all sequences in $\mathcal{C}_a(b_i^n)$ are sampled uniformly at random from the

conditionally typical set $T_x^n(b_i^n)$. Here $\delta_a > 0$ and $\delta_{\rm b} > 0$ as arbitrary constants such that $\delta_{\rm a} + \delta_{\rm b} = \delta$, which satisfies (26). If this condition is not satisfied, as discussed in section IV, time-sharing between transmitting an independent message and the source coding approach discussed here is necessary.

2) Source Codebooks: The Wyner-Ziv codebook $\mathcal{C}^{\rm WZ}$ is constructed as in section IV. A set $\mathcal{T}$ consisting of $N_{\rm tot}$ sequences is constructed by selecting the sequences uniformly at random from the set T_t^N. These sequences are partitioned into $N_{\rm WZ}$ bins, each consistnig of $M_{\rm WZ}$ sequences where the constants $M_{\rm WZ}$ and $N_{\rm WZ}$ are defined in (27a) and (27b) respectively. The secret-key codebook $\mathcal{C}^{\rm SK}$ consists of a total of $N_{\rm SK}$ bins, each with $M_{\rm SK}$ codewords, where

$$M_{\rm SK} = \exp_2\left(n(I(b;y) + I(x;z|b) - \delta)\right), \tag{167a}$$

$$N_{\rm SK} = \exp_2\left(n(\beta I(t;v) + I(x;y|b) - I(x;z|b) - \delta)\right). \tag{167b}$$

Via (26), note that,

$$N_{\rm tot} = N_{\rm SK} M_{\rm SK} = N_{\rm WZ} M_{\rm WZ} = N_a N_b = \exp_2(nI(x;y) - n\delta). \tag{168}$$

B. Encoding

The encoder finds a sequence t^N jointly typical with u^N and declares its bin index in the secret-key codebook as the secret-key. The bin index in the Wyner-Ziv codebook is the message that is transmitted to the receiver. The bin index $\Phi_{\rm WZ}$ 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 two channel codebooks $\mathcal{C}_a(\cdot)$ and $\mathcal{C}_b$ respectively. Thus the encoder first maps $\Phi_{\rm b}$ to a codeword b^n in $\mathcal{C}_b$ and then maps the message $\Phi_{\rm a}$ to the codeword x^n in $\mathcal{C}_a(b^n)$. The sequence x^n is transmitted over n channel uses.

C. Decoding

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 $\hat{k} = \Phi_{\rm SK}(t^N)$.

D. Decoding with side information at the eavesdropper

The eavesdropper, when revealed k in addition to z^n, can reconstruct t^N as follows. 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 $I(b;z) \geq I(b;y) = R_{\rm b}$. Thereafter it searches for sequences in $\mathcal{B}_k^{\rm SK} = \{t_{k1}^{N,{\rm SK}}, \ldots, t_{kM_{\rm SK}}^{N,{\rm SK}}\}$ such that $[\Phi_{aj}, \Phi_{bj}] = \Phi_{\rm WZ}(t_{kj}^{N,{\rm SK}})$ satisfies: (1) $\Phi_{bj} = i$ and (2) $x^n_{\Phi_{aj}} \in \mathcal{C}_a(b_i^n)$ is jointly $\varepsilon-$ typical with z^n.

The probability that a false sequence in $\mathcal{B}_k^{\rm SK}$ satisfies these conditions is

$$\Pr(e) = \exp_2\left\{-n(I(x;z|b) + I(b;y) - \varepsilon)\right\} \tag{169}$$

and hence the choice of $M_{\rm SK}$ in (167a) guarantees that the error probability approaches zero provided $\varepsilon < \delta$.

Thus by Fano's lemma, there exists one particular codebook that satisfies

$$\frac{1}{N} H(t^N|z^n, k) = o_\eta(1) \tag{170}$$

E. Secrecy Analysis

Following the steps leading to (55) we have

$$H(\mathsf{k}|\mathsf{z}^n) = H(\Phi_{\rm WZ}|\mathsf{z}^n) + H(\mathsf{t}^N|\Phi_{\rm WZ}) - H(\mathsf{t}^N|\mathsf{k},\mathsf{z}^n) \tag{171}$$

$$= H(\Phi_{\rm WZ}|\mathsf{z}^n) + H(\mathsf{t}^N|\Phi_{\rm WZ}) - No_\eta(1) \tag{172}$$

where the second step follows from (170).

For the superposition codebook, since $\Phi_{\rm WZ}$ is the transmitted message we have from [8, Corollary 2, pp. 341]

$$\frac{1}{n}H(\Phi_{\rm WZ}|\mathsf{z}^n) = I(\mathsf{x};\mathsf{y}|\mathsf{b}) - I(\mathsf{x};\mathsf{z}|\mathsf{b}) + o_\eta(1), \tag{173}$$

and from (37b) in Lemma 1,

$$\frac{1}{N}H(\mathsf{t}^N|\Phi_{\rm WZ}) = I(\mathsf{t};\mathsf{v}) + o_\eta(1). \tag{174}$$

Substituting these relations into (172) we have that

$$\frac{1}{n}H(\mathsf{k}|\mathsf{z}^n) = \{I(\mathsf{x};\mathsf{y}|\mathsf{b}) - I(\mathsf{x};\mathsf{z}|\mathsf{b})\} + \beta I(\mathsf{t};\mathsf{v}) + o_\eta(1). \tag{175}$$

as required.

APPENDIX B
PROOF OF (35)

We can express

$$\mathcal{E}_4 = \mathcal{J}_0 \bigcup \mathcal{J}_1 \bigcup \ldots \mathcal{J}_{j_0-1} \bigcup \mathcal{J}_{j_0+1} \ldots \bigcup \mathcal{J}_{M_{\rm SK}} \tag{176}$$

where j_0 is the index of the sequence t^N selected by the sender in bin $\mathcal{B}_k^{\rm SK}$ of $\mathcal{C}^{\rm SK}$, and where the event $\mathcal{J}_0$ is defined as the event,

$$\mathcal{J}_0 = \{\Phi_{\rm WZ}(t_{kj_0}^{N,{\rm SK}}) \notin \mathcal{I}\} \tag{177}$$

and $\mathcal{J}_j$ for $1 \le j \le M_{\rm SK}$, $j \ne j_0$ is

$$\mathcal{J}_j = \left\{\Phi_{\rm WZ}(t_{kj}^{N,{\rm SK}}) \in \mathcal{I}\right\} \tag{178}$$

It follows that

$$\Pr(\mathcal{E}_4) \le \Pr(\mathcal{J}_0) + \sum_{j=1, j\ne j_0}^{M_{\rm SK}} \Pr(\mathcal{J}_j|\mathcal{J}_0^c). \tag{179}$$

where $\mathcal{J}_0^c$ denotes the compliment of the event $\mathcal{J}_0$.

By law of large numbers it follows that $\Pr(\mathcal{J}_0) \to 0$. To evaluate $\Pr(\mathcal{J}_j|\mathcal{J}_0^c)$ we define the event $\mathcal{J}_j^{\rm col}$ as the event that the Wyner-Ziv bin indices of the sequences $t_{kj}^{N,{\rm SK}}$ and $t_{kj_0}^{N,{\rm SK}}$ are identical i.e.,

$$\mathcal{J}_j^{\rm col} = \left\{\Phi_{\rm WZ}(t_{kj}^{N,{\rm SK}}) = \Phi_{\rm WZ}(t_{kj_0}^{N,{\rm SK}})\right\} \tag{180}$$

Using $\mathcal{J}_j^{\rm col}$ we can upper bound the error event as

$$\Pr(\mathcal{J}_j|\mathcal{J}_0^c) \le \Pr(\mathcal{J}_j^{\rm col}|\mathcal{J}_0^c) + \Pr(\mathcal{J}_j|\mathcal{J}_j^{{\rm col},c} \cap \mathcal{J}_0^c) \tag{181}$$

where the first term is the error probability due to a collision event and the second term is the error probability when there is no collision.

The first term can be upper bounded as follows

$$\Pr(\mathcal{J}_j^{\text{col}}|\mathcal{J}_0^c) = \Pr(\mathcal{J}_j^{\text{col}}) \tag{182}$$
$$= \exp_2(-n(\beta R_{\text{WZ}} + 2\delta)) \tag{183}$$
$$= \exp_2(-n(I(\mathsf{x};\mathsf{y}) - \delta)) \tag{184}$$

where (182) follows from the fact the event $\mathcal{J}_0$ is due to the atypical channel behaviour and is independent of the random partitioning event $\mathcal{J}_j^{\text{col}}$, (183) follows from the fact that since both the codebooks $\mathcal{C}^{\text{WZ}}$ and $\mathcal{C}^{\text{SK}}$ are obtained by partitioning the set $\mathcal{T}$ after a random permutation, we have for any $t_1^N, t_2^N \in \mathcal{T}$

$$\Pr\left(\Phi_{\text{WZ}}(t_1^N) = \Phi_{\text{WZ}}(t_2^N)|\Phi_{\text{SK}}(t_1^N) = \Phi_{\text{SK}}(t_2^N)\right) = \Pr\left(\Phi_{\text{WZ}}(t_1^N) = \Phi_{\text{WZ}}(t_2^N)\right) = \frac{1}{N_{\text{WZ}}} \tag{185}$$

and $N_{\text{WZ}} = \exp_2\{n(\beta R_{\text{WZ}} + 2\delta)\}$ and (184) follows via relation (26). The second term reduces to an event that $\mathsf{x}^n \in \mathcal{C}^{\text{ch}}$, sampled independent of $\mathsf{x}_{j_0}^n$ satisfies $(\mathsf{x}^n, \mathsf{z}^n) \in T_{\mathsf{x},\mathsf{z},\varepsilon}^n$. Hence we have

$$\Pr(\mathcal{J}_j|\mathcal{J}_0^c \cap \mathcal{J}_j^{\text{col,c}}) \leq \exp_2(-n(I(\mathsf{x};\mathsf{z}) - 3\varepsilon)). \tag{186}$$

Combining (184) and (186) we have

$$\begin{aligned}\Pr(\mathcal{J}_j|\mathcal{J}_0^c) &\leq \exp_2(-n(I(\mathsf{x};\mathsf{z}) - 3\varepsilon)) + \exp_2(-n(I(\mathsf{x};\mathsf{y}) - \delta)) \\ &\leq \exp_2(-n(I(\mathsf{x};\mathsf{z}) - 4\varepsilon)), \quad n \geq n_0,\end{aligned} \tag{187}$$

where we use the fact that $I(\mathsf{x};\mathsf{y}) \geq I(\mathsf{x};\mathsf{z})$ from (24) in the last step so that the required n_0 exists. Finally using relation (27c) for M_{SK}, we have that

$$\sum_{j=1, j\neq j_0}^{M_{\text{SK}}} \Pr(\mathcal{J}_j) \leq \exp_2(-n(\delta - 4\varepsilon)) + o_\eta(1), \tag{188}$$

which vanishes with n, whenever the decoding function selects $\varepsilon < \delta/4$. Thus we have that $\Pr(\mathcal{E}_4) \to 0$ as $n \to \infty$.

Appendix C
Cardinality Bounds on t in Theorem 1

Let the alphabet of u be denoted by $\{1, \ldots, |\mathcal{U}|\}$ and let $p_{\mathsf{u}|\mathsf{t}}(\cdot|t)$ be a probability mass function indexed by t. Define the following functions of the $p_{\mathsf{u}|\mathsf{t}}(\cdot|t)$:

$$g_j(p_{\mathsf{u}|\mathsf{t}}(\cdot|t)) = \begin{cases} p_{\mathsf{u}|\mathsf{t}}(j|t), & j = 1, \ldots, |\mathcal{U}| - 1 \\ H(\mathsf{u}|\mathsf{t} = t), & j = |\mathcal{U}| \\ H(\mathsf{v}|\mathsf{t} = t) & j = |\mathcal{U}| + 1 \end{cases} \tag{189}$$

The first $|\mathcal{U}| - 1$ functions are conditional probabilities $p\{\mathsf{u} = j|\mathsf{t} = t\}$, each of which is a continuous function of the conditional pmf $p(u|t)$. The function $H(\mathsf{u}|\mathsf{t} = t)$ is also continuous in $p(u|t)$ by virtue of the continuity of the entropy function. Finally the function $H(\mathsf{v}|\mathsf{t} = t)$ is a continuous function of $p(u|t)$ due to the linear relation $p(v|t) = \sum_u p(v|u)p(u|t)$. Hence

by the Caratheodry theorem (see e.g., [13, Appendix C]) there exists another random variable t' taking no more than $|\mathcal{U}|+1$ values such that

$$H(u|t) = H(u|t') \tag{190}$$
$$H(v|t) = H(v|t'), \tag{191}$$
$$E_t[p(u|t)] = p(u) = E_{t'}[p(u|t')], \qquad u \in \{1, \ldots, |\mathcal{U}|-1\} \tag{192}$$
$$\tag{193}$$

Since the sum of the probability mass functions is 1 the last relation also holds for $u = |\mathcal{U}|$. It is thus easy to see that any point that can be achieved in Theorem 1 can also be achieved by restricting t to have cardinality no more than $|\mathcal{U}|+1$. This completes the argument.

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] P. Bergmans, "A simple converse for broadcast channels with additive white Gaussian noise (corresp.)," *IEEE Trans. Inform. Theory*, vol. 20, pp. 279–280, 1974.

[3] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information theoretic security," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2515–2534, Jun. 2008.

[4] F. Bui and D. Hatzinakos, "Biometric methods for secure communications in body sensor networks: Resource-efficient key management and signal-level data scrambling," *EURASIP Journal on Advances in Signal Processing, Special Issue on Advanced Signal Processing and Pattern Recognition Methods for Biometrics*, pp. 1–16, Jan 2008.

[5] S. Cherukuri, K. Venkatsubramanian, and S. Gupta, "Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Workshop on Wireless Security and Privacy (WiSPr), International Conference on Parallel Processing Workshops*, Oct. 2003, pp. 432–439.

[6] I. Csiszár, "Almost independence and secrecy capacity (in russian)," *Probl. Inform. Transmission*, vol. 32, pp. 48–57, 1996.

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

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

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

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

[11] E. Ekrem and S. Ulukus, "The secrecy capacity region of the gaussian mimo multi-receiver wiretap channel," *IEEE Trans. Inform. Theory*, submitted. [Online]. Available: http://arxiv.org/abs/0903.3096

[12] A. A. El Gamal, "Capacity of the product and sum of two un-matched broadcast channels," *Probl. Information Transmission*, pp. 3–23, Jan-March 1980.

[13] A. A. El Gamal and Y. H. Kim, "Lecture notes on network information theory," CoRR abs/1001.3404, (2010).

[14] A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals - Part I," *IEEE Trans. Inform. Theory*, vol. 56, pp. 3973–3996, Jun. 2010.

[15] D. Gunduz, E. Erkip, and H. V. Poor, "Lossless compression with security constraints," in *Proc. Int. Symp. Inform. Theory*, Toronto, Jul. 2008.

[16] X. He and A. Yener, "Secure degrees of freedom for Gaussian channels with interference: Structured codes outperform Gaussian signaling," *IEEE Trans. Inform. Theory*, submitted. [Online]. Available: http://arxiv.org/abs/0907.5388

[17] 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.

[18] 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.

[19] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure Broadcasting over fading channels," *IEEE Trans. Inform. Theory, Special Issue on Information Theoretic Security*, vol. 54, pp. 2453–2469, Jun. 2008.

[20] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MIMOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, pp. 5515–5532, Nov. 2010.

[21] ——, "Secure transmission with multiple antennas: The MISOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, pp. 3088–3104, Jul. 2010.

[22] O. O. Koyluoglu, H. E. Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inform. Theory*. [Online]. Available: http://arxiv.org/abs/0810.1187

[23] L. Lai and H. E. Gamal, "The Relay Eavesdropper channel: Cooperation for Secrecy," *IEEE Trans. Inform. Theory*, vol. 54, pp. 4005–4019, Sep. 2008.

[24] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inform. Theory*, vol. 55, pp. 2547–2553, Jun. 2009.
[25] 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.
[26] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, pp. 733–742, Mar. 1993.
[27] N. Merhav, "Shannon's secrecy system with informed receivers an its application to systematic coding for wiretapped channels," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2723–2734, 2008.
[28] 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*.
[29] V. Prabhakaran and K. Ramachandran, "A separation result for secure communication," in *talk presented at the 45th Allerton Conf. Commun., Contr., Computing*, Oct. 2007.
[30] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative Jamming," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2735–2751, Jun. 2008.
[31] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–87, 1975.
[32] H. Yamamoto, "Rate distortion theory for the shannon cipher system," *IEEE Trans. Inform. Theory*, vol. 43, May 1997.

Ashish Khisti Ashish Khisti is an assistant professor in the Electrical and Computer Engineering (ECE) department at the University of Toronto, Toronto, Ontario Canada. He received his BASc degree in Engineering Sciences from University of Toronto and his S.M and Ph.D. Degrees from the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA. His research interests span the areas of information theory, wireless physical layer security and streaming in multimedia communication systems. At the University of Toronto, he heads the signals, multimedia and security laboratory. For his graduate studies he was a recipient of the NSERC postgraduate fellowship, HP/MIT alliance fellowship, Harold H. Hazen Teaching award and the Morris Joseph Levin Masterworks award.

Suhas N. Diggavi Suhas N. Diggavi (M99) received the B.Tech. degree in electrical engineering from the Indian Institute of Technology, Delhi, and the Ph.D. degree in electrical engineering from Stanford University, Stanford, CA, in 1998. After completing the Ph.D. degree, he was a Principal Member Technical Staff in the Information Sciences Center,AT&T Shannon Laboratories, Florham Park, NJ. After that, he was on the faculty at the School of Computer and Communication Sciences, Ecole Polytechnique Fdrale de Lausanne (EPFL), Lausanne, Switzerland, where he directed the Laboratory for Information and Communication Systems (LICOS). He is currently a Professor in the Department of Electrical Engineering, University of California, Los Angeles. His research interests include wireless communications networks, information theory, network data compression and network algorithms. He has 8 issued patents. Dr. Diggavi is a recipient of the 2006 IEEE Donald Fink prize paper award, 2005 IEEE Vehicular Technology Conference Best Paper Award, and the Okawa Foundation Research Award. He is currently an editor for ACM/IEEE TRANSACTIONS ON NETWORKING and the IEEE TRANSACTIONS ON INFORMATION THEORY.

Gregory W. Wornell Gregory W. Wornell received the B.A.Sc. degree (with honors) from the University of British Columbia, Canada, and the S.M. and Ph.D. degrees from the Massachusetts Institute of Technology, all in Electrical Engineering and Computer Science, in 1985, 1987 and 1991, respectively. Since 1991 he has been on the faculty at MIT, where he is Professor of Electrical Engineering and Computer Science. At MIT he leads the Signals, Information, and Algorithms Laboratory within the Research Laboratory of Electronics, and co-directs the MIT Center for Wireless Networking. He is also chair of Graduate Area I (Systems, Communication, Control, and Signal Processing) within the EECS department's doctoral program, and a member of the MIT Computational and Systems Biology Initiative. He has held visiting appointments at the Department of Electrical Engineering and Computer Science at the University of California, Berkeley, CA, in 1999-2000, at Hewlett-Packard Laboratories, Palo Alto, CA, in 1999, and at AT&T Bell Laboratories, Murray Hill, NJ, in 1992-3. His research interests and publications span the areas of signal processing, digital communication, and information theory, and include algorithms and architectures for wireless and sensor networks, broadband systems, and multimedia environments. He has been involved in the Signal Processing and Information Theory societies of the IEEE in a variety of capacities, and maintains a number of close industrial relationships and activities. He has won a number of awards for both his research and teaching, and is a Fellow of the IEEE.