

Discriminatory Source Coding for a Noiseless Broadcast Channel

Leonard Gropop
 Dept. of EECS
 U.C. Berkeley
 Berkeley, CA 94720, USA
 Email: lgropop@eecs.berkeley.edu

Anant Sahai
 Dept. of EECS
 U.C. Berkeley
 Berkeley, CA 94720, USA
 Email: sahai@eecs.berkeley.edu

Michael Gastpar
 Dept. of EECS
 U.C. Berkeley
 Berkeley, CA 94720, USA
 Email: gastpar@eecs.berkeley.edu

Abstract—We introduce a new problem of broadcast source coding with a discrimination requirement — there is an eavesdropping user from whom we wish to withhold the true message in an entropic sense. Binning can achieve the Slepian-Wolf rate, but at the cost of full information leakage to the eavesdropper. Our main result is a lower bound that implies that *any* entropically efficient broadcast scheme must be “like binning” in that it also must leak significant information to eavesdroppers

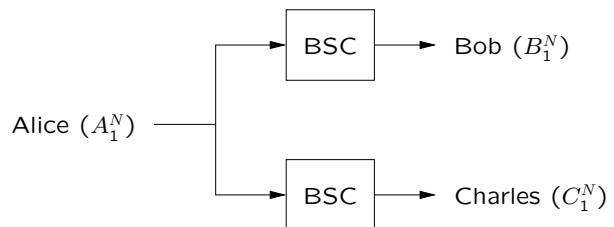


Fig. 1. Setup for introductory problem

I. INTRODUCTION

At a recent CISS talk the following intriguing problem was posed by Wolf [1]: Alice possesses a file modeled as a random binary string A_1^N and Bob possesses a corrupted version of the file, B_1^N , modeled as passing A_1^N through a BSC with crossover probability γ . Suppose Alice knows Bob’s corrupted version, and she wishes to inform Bob of A_1^N using a short message. Alice could simply compute the difference sequence $A_1^N \oplus B_1^N$ (where \oplus denotes addition modulo 2), compress it losslessly, and send this to Bob, requiring $N\mathcal{H}(\gamma)$ bits, where $\mathcal{H}(\cdot)$ denotes the binary entropy function. Alternatively, Alice could ignore her knowledge of B_1^N , and simply perform Slepian-Wolf binning of A_1^N and send the bin index. This *also* requires $N\mathcal{H}(\gamma)$ bits in the large- N limit [2]. While both strategies are equally efficient from a rate perspective, the latter will require a significantly higher decoding complexity.

Wolf then went on to add a third user, Charles, who also has an independently corrupted version C_1^N of the original string A_1^N , as illustrated in Figure 1. Again, it is assumed that Alice knows the sequence C_1^N (as well as B_1^N), and the problem is now for Alice to inform both Bob and Charles of A_1^N in an efficient way using a single broadcast that everyone can hear noiselessly. She could send Bob’s error sequence $A_1^N \oplus B_1^N$ over the broadcast channel followed by Charles’ error sequence $A_1^N \oplus C_1^N$ using a total of $2N\mathcal{H}(\gamma)$ bits. Or as before, she could broadcast the Slepian-Wolf bin index of A_1^N , requiring $N\mathcal{H}(\gamma)$ bits. The latter scheme is now twice as efficient as the former, but still requires a significant increase in decoding complexity. The question posed by Wolf is: Is there a third strategy that has the efficiency of binning, but the “coding

complexity” of merely sending the difference sequence?¹

The deep underlying question that we feel Wolf is asking is whether there is any strategy that makes explicit and non-trivial use of Alice’s knowledge of the sequences B_1^N and C_1^N . We attempt to formalize this indirectly by a secrecy requirement. Suppose Alice’s broadcast channel has been wiretapped so that anything transmitted across it is noiselessly received by an eavesdropper, Eve. Like Bob and Charles, Eve possesses some side information E_1^N about A_1^N . What is the minimum number of bits Alice must now use if she wishes to deny Eve access to any more information about the message? Is $N\mathcal{H}(\gamma)$ enough? ²

We will concentrate on two specific cases. In the first Eve knows nothing about A_1^N a-priori. This setup can be viewed as a generalization of the Shannon secrecy system [3] to multiple recipients. Each recipient’s side information plays the role of the key source Alice may use to communicate to them in “perfect-secrecy”. In the second case, E_1^N is generated from A_1^N in the same fashion as B_1^N and C_1^N .

¹There is a simple solution to the problem from the point of view of computational complexity. Alice can “bin” the message A by breaking it up into moderately sized blocks and using an LDPC syndrome as a part of the broadcast message X . Then, Alice can simulate the LDPC decoding from both Bob’s and Charles’s points of view and use bit doping in the style of [7] separately for each one. This will exploit Alice’s knowledge of the side information and add only a tiny increment of rate. In effect, bit doping allows us to trade a little extra rate to back off the large N asymptotics. But this is clearly not the answer to Wolf’s underlying question in that this is simply an efficient way to do binning, not anything truly different.

²Notice that in the LDPC+“bit doping” construction given earlier, Eve will end up learning most of the bits of A using her side information to decode the LDPC. The intuition behind our problem is that if the message had truly been targeted to Bob and Charles, it should not be significantly helpful to Eve.

These problems are interesting in their own right as they closely relate to Wyner's problem of communicating over a wiretap channel [4], generalized by Csiszár and Körner [5] and further generalized by means of interaction between the recipients and sender, by Maurer [6].

We formulate the problem in more generality in section II. In section III we present a lower bound to the minimum number of bits required, which constitutes the main result of this paper. This bound is then used to investigate the two specific cases detailed above. Upper bounds are also presented. In section IV we prove the main result and in section V we discuss the motivation behind this bound and the difficulties associated with attaining a conjectured tighter bound.

II. PROBLEM SETUP

Alice has access to an N -length random string A_1^N and wishes to broadcast a short message X_1^M of length M to K recipients. The k th recipient has access to $B_1^N(k)$. Eve has side information E_1^N and Alice does not wish her to gain any new information about A_1^N from the broadcast. We initially assume Alice knows the realizations of all r.v.'s involved, but the case where she doesn't know E_1^N will also be discussed later on. Lastly the random variables $B_1^N(1), \dots, B_1^N(K), E_1^N$ are assumed to be conditionally independent of each other given A_1^N .

Definition 2.1: An (M, N) discrimination code for the source A_1^N consists of an encoder map,

$$f : \{0, 1\}^N \times \{0, 1\}^{N \times K} \times \{0, 1\}^N \rightarrow \{0, 1\}^M$$

and K decoder maps,

$$g_k : \{0, 1\}^M \times \{0, 1\}^N \rightarrow \{0, 1\}^N, \quad k = 1, \dots, K$$

The encoding function

$$f(A_1^N, B_1^N(1), \dots, B_1^N(K), E_1^N)$$

outputs the update X_1^M . The decoding functions

$$g_1(X_1^M, B_1^N(1)), \dots, g_K(X_1^M, B_1^N(K))$$

output estimates $\hat{A}_1^N(1), \dots, \hat{A}_1^N(K)$ of A_1^N . \square

Alice wishes to leak no more than $N\Delta$ new bits of information about A_1^N to Eve. Accordingly we have

Definition 2.2: R_S is said to be an achievable Δ -secrecy rate if there exists a sequence of (NR_S, N) discrimination codes such that

- (i) $P(\hat{A}_1^N(k) \neq A_1^N) \rightarrow 0$ as $N \rightarrow \infty, \forall k$
- (ii) $H(A_1^N | E_1^N, X_1^M) \geq H(A_1^N | E_1^N) - \Delta N.$ \square

We will discuss two specific cases of the problem:

A. Perfect-Secrecy

In this problem Alice's file is modelled as an N -length sequence

$$A_1^N \triangleq \{A_1, \dots, A_N\}$$

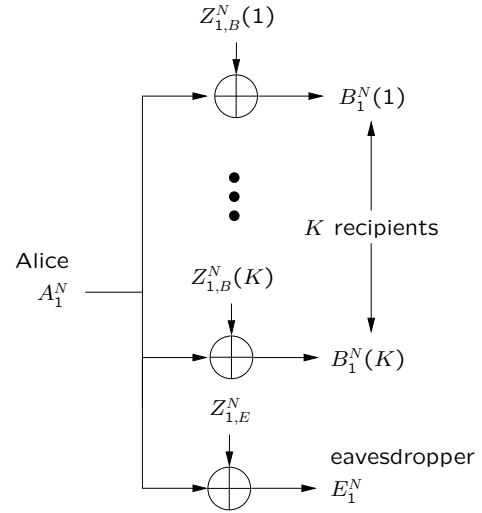


Fig. 2. Dependence structure between $A_1^N, B_1^N(1), \dots, B_1^N(K), E_1^N$

The $A_i \in \{0, 1\}$ are i.i.d. Bernoulli(1/2) distributed, for $i = 1, \dots, N$. The recipients' side information random variables are generated by passing A_1^N through independent BSCs with crossover probability γ . Denote the noise sequences as $Z_{1,B}^N(1), \dots, Z_{1,B}^N(K)$. That is, the corrupted files are given by

$$B_1^N(k) = A_1^N \oplus Z_{1,B}^N(k)$$

for $k = 1, \dots, K$, where \oplus denotes the bit-wise XOR operation. In this problem, the eavesdropper is given no side information about A_1^N . Thus Alice's broadcasted message must be conveyed to each recipient in "perfect-secrecy" (in the Shannon sense [3]). We can treat this as a specific case of the general problem by setting E_1^N to zero.

B. I.I.D. BSCs

This problem is similar to the one above except we give the eavesdropper side information about A_1^N . E_1^N is generated by passing A_1^N through independent BSCs with the same crossover probability, γ . Denote the noise sequence $Z_{1,E}^N$ (see figure 2). So

$$E_1^N = A_1^N \oplus Z_{1,E}^N$$

III. RESULTS

A. General Lower Bound

For the general problem with K recipients and one eavesdropper the following lower bound holds.

Theorem 3.1: If R_S is an achievable Δ -secrecy rate then

$$R_S \geq \lim_{N \rightarrow \infty} \frac{1}{N} \left[\sum_{k=1}^K H(A_1^N | B_1^N(k), E_1^N) + \max_{l \in \{1, \dots, K\}} I(A_1^N; E_1^N | B_1^N(l)) \right] - (K-1)\Delta \quad \square$$

B. Perfect-Secrecy

We can apply theorem 3.1 to this problem by setting E_1^N to zero. It turns out this bound is tight.

Theorem 3.2: For the perfect-secrecy problem, the minimum achievable Δ -secrecy rate, R_S^* satisfies

$$R_S^* = \Delta + K(\mathcal{H}(\gamma) - \Delta). \quad \square$$

Thus in the case of perfect secrecy where Alice wishes to leak no information about A_1^N to the eavesdropper ($\Delta = 0$), she cannot do better than transmitting each recipient's error sequence. Alternatively, if Alice broadcasts at a rate $R < R_S^*$ such that all recipients are able to decode A_1^N from her message, she must leak information to Eve at a rate greater than $\mathcal{H}(\gamma) - (R - \mathcal{H}(\gamma))/K$. In particular, for the case considered in the introduction—where $\Delta = 0$ and there are at least two recipients—this secrecy requirement prohibits Alice from using a short message of length $NH(\gamma)$ bits.

C. I.I.D. BSCs Problem

The scheme used in the case of perfect-secrecy may be used in this one, however the lower bound of theorem 3.1 no longer matches.

Corollary 3.3: For the I.I.D. BSCs problem, the minimum achievable Δ -secrecy rate R_S^* satisfies

$$(2K - 1)\mathcal{H}(\gamma) - (K - 1)\mathcal{H}(2\gamma(1 - \gamma)) - (K - 1)\Delta \leq R_S^* \leq K\mathcal{H}(\gamma) - (K - 1)\Delta \quad (1)$$

and so for $\Delta = 0$,

$$R_S^* > K\mathcal{H}(\gamma). \quad \square$$

These bounds are plotted in figure 3 for $K = 2$ and $\Delta = 0$. The region between the bounds of equation (1) is shaded. Corollary 3.3 tells us that if Alice broadcasts at a rate $R < (2K - 1)\mathcal{H}(\gamma) - (K - 1)\mathcal{H}(2\gamma(1 - \gamma))$ such that all recipients are able to decode A_1^N from her message, she must leak information to Eve at a rate greater than

$$\frac{R - (2K - 1)\mathcal{H}(\gamma) + (K - 1)\mathcal{H}(2\gamma(1 - \gamma))}{K - 1}.$$

For the case considered in the introduction we see that if Alice uses an entropically efficient message of length $NH(\gamma)$ she must end up leaking information to the eavesdropper.

IV. PROOFS

A. General Problem – Proof of Theorem 3.1

The bound is essentially a genie-aided one. The main idea is to give additional side information to the recipients. Specifically we suppose all recipients except one have knowledge of E_1^N , in addition to their original side-information. See figure 4. This provides a bound to the general problem as the recipients are no worse off given this additional information. We then optimize the bound by choosing the appropriate recipient to deny the additional side information to. The motivation for using such a bound is discussed in the next section.

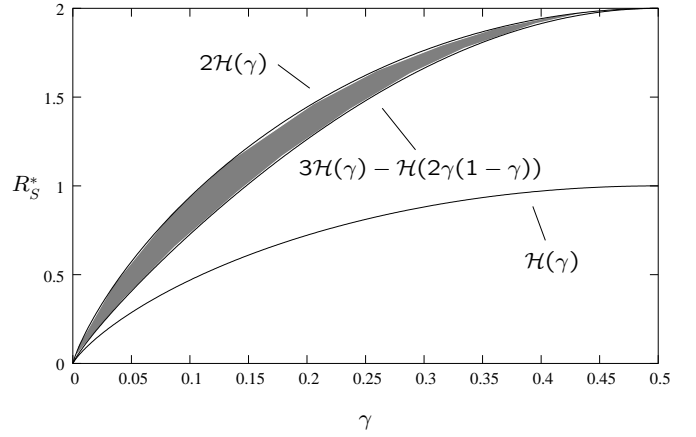


Fig. 3. For the I.I.D. BSCs problem with 2 recipients and $\Delta = 0$, the minimum achievable secrecy rate lies strictly above $\mathcal{H}(\gamma)$, somewhere between $2\mathcal{H}(\gamma)$ and $3\mathcal{H}(\gamma) - \mathcal{H}(2\gamma(1 - \gamma))$.

Denote the recipient that is denied access to the additional side-information as recipient l . Applying Fano's inequality to property (i) of definition 2.2 we have

$$H(A_1^N | B_1^N(k), X_1^M) \leq NP(\hat{A}_1^N(k) \neq A_1^N) + 1 \triangleq N\epsilon_N(k)$$

for all $k \in \{1, \dots, K\}$, where $\epsilon_N(k) \rightarrow 0$ as $N \rightarrow \infty$. We can now write a sequence of inequalities. For notational simplicity we denote A_1^N as simply A in this section and likewise for all other r.v.s. We also use the convention that summations are only taken over the term directly following.

$$\begin{aligned} & KH(A) - N \sum_{k=1}^K \epsilon_N(k) \\ &= \sum_{k \neq l} H(A|B(k), E) + H(A|B(l)) + \sum_{k \neq l} I(A; B(k), E) \\ &\quad + I(A; B(l)) \\ &\geq \sum_{k \neq l} H(A|B(k), E) - \sum_{k \neq l} H(A|B(k), E, X) + H(A|B(l)) \\ &\quad - H(A|B(l), X) + \sum_{k \neq l} I(A; B(k), E) + I(A; B(l)) \\ &= \sum_{k \neq l} I(A; X|B(k), E) + I(A; X|B(l)) + \sum_{k \neq l} I(A; B(k), E) \\ &\quad + I(A; B(l)) \\ &= \sum_{k \neq l} H(X|B(k), E) + H(X|B(l)) - \sum_{k \neq l} H(X|B(k), E, A) \\ &\quad - H(X|B(l), A) + \sum_{k \neq l} I(A; B(k), E) + I(X; B(l)) \end{aligned}$$

Concentrating on the 3rd and 4th terms in the previous

expression

$$\begin{aligned}
& \sum_{k \neq l} H(X|B(k), E, A) + H(X|B(l), A) \\
&= \sum_{k \neq l} H(X, A, B(k), E) + H(X, A, B(l)) \\
&\quad - \sum_{k \neq l} H(A, B(k), E) - H(A, B(l)) \\
&\geq (K-1)H(X, A) + H(X, A, B(1), \dots, B(K), E) \\
&\quad - \sum_{k \neq l} H(A, B(k), E) - H(A, B(l)) \\
&= (K-1)H(X|A) + H(X|A, B(1), \dots, B(K), E) \\
&\quad + H(A, B(1), \dots, B(K), E) + (K-1)H(A) \\
&\quad - \sum_{k \neq l} H(A, B(k), E) - H(A, B(l)).
\end{aligned}$$

In the second step we have used a polymatroidal theorem ([8] p297) for brevity. Thus

$$\begin{aligned}
& KH(A) - N \sum_{k=1}^K \epsilon_N(k) \\
&\leq \sum_{k \neq l} H(X|B(k), E) + H(X|B(l)) - (K-1)H(X|A) \\
&\quad - H(X|A, B(1), \dots, B(K), E) \\
&\quad - H(A, B(1), \dots, B(K), E) \\
&\quad - (K-1)H(A) + \sum_{k \neq l} H(A, B(k), E) + H(A, B(l)) \\
&\quad + \sum_{k \neq l} I(A; B(k), E) + I(A; B(l)) \\
&= \sum_{k \neq l} H(X|B(k), E) + H(X|B(l)) - (K-1)H(X|A) \\
&\quad - H(X|A, B(1), \dots, B(K), E) + KH(A) \\
&\quad - \sum_{k \neq l} H(A|B(k), E) - H(A|B(l))
\end{aligned}$$

where we have made use of the fact that $B(k), B(l)$ and E are conditionally independent given A . Now

- i) $\sum_{k \neq l} H(X|B(k), E) \leq (K-1)H(X|E)$,
- ii) $H(X|B(l)) \leq H(X)$,
- iii) $H(X|A) \geq H(X|A, E) \geq H(X|E) - N\Delta$, and
- iv) $H(X|A, B(1), \dots, B(K), E) \geq 0$.

Using these inequalities we arrive at

$$\begin{aligned}
H(X_1^M) &\geq \sum_{k \neq l} H(A_1^N | B_1^N(k), E_1^N) + H(A_1^N | B_1^N(l)) \\
&\quad - N \left((K-1)\Delta + \sum_{k=1}^K \epsilon_N(k) \right).
\end{aligned}$$

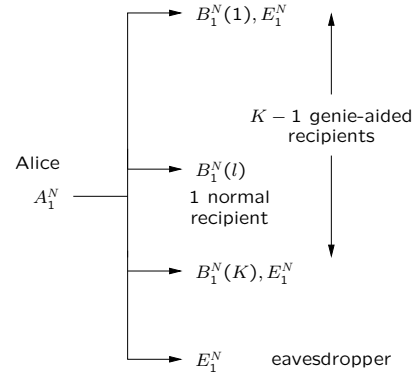


Fig. 4. Setup

Thus we have

$$\begin{aligned}
R_S &\geq \frac{1}{N} H(X_1^M) \\
&\geq \frac{1}{N} \sum_{k=1}^K H(A_1^N | B_1^N(k), E_1^N) + \frac{1}{N} I(A_1^N; E_1^N | B_1^N(l)) \\
&\quad - (K-1)\Delta - \sum_{k=1}^K \epsilon_N(k)
\end{aligned}$$

Taking the limit $N \rightarrow \infty$ forces $\sum_{k=1}^K \epsilon_N(k) \rightarrow 0$. Maximizing over l yields the desired bound.

B. Perfect-Secrecy – Proof of Theorem 3.2

Setting E_1^N to zero in theorem 3.1 we have

$$\begin{aligned}
R_S^* &\geq \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{k=1}^K H(A_1^N | B_1^N(k)) - (K-1)\Delta \\
&= K\mathcal{H}(\gamma) - (K-1)\Delta.
\end{aligned}$$

One way of achieving this bound is the following: Alice first performs Slepian-Wolf binning of the string $A_1, \dots, A_{N\Delta/\mathcal{H}(\gamma)}$ using $N\Delta$ bits (ignoring integer effects) and broadcasts the bin index. This leaks $N\Delta$ bits of information to Eve –just enough to satisfy property (ii) of definition 2.2. From the Slepian-Wolf theorem, we know it will also enable the recipients to decode the first $N\Delta/\mathcal{H}(\gamma)$ bits of the message as $N \rightarrow \infty$, satisfying property (i). Alice then performs individual Slepian-Wolf binning of each recipients noise sequence using $N(\mathcal{H}(\gamma) - \Delta)$ bits per recipient. These K bin indices are also broadcast. In the same way this information enables the recipients to decode the rest of the message. The scheme achieves a Δ -secrecy rate of $R_S = \Delta + K(\mathcal{H}(\gamma) - \Delta)$ which matches the bound.

C. I.I.D. BSCs – Proof of Corollary 3.3

Evaluating the lower bound of theorem 3.1 yields

$$\begin{aligned}
R_S^* &\geq \lim_{N \rightarrow \infty} \frac{1}{N} \left[N\mathcal{H}(\gamma) + \sum_{k=1}^K N(2\mathcal{H}(\gamma) - \mathcal{H}(2\gamma(1-\gamma))) \right] \\
&\quad - (K-1)\Delta \\
&= (2K-1)\mathcal{H}(\gamma) - (K-1)\mathcal{H}(2\gamma(1-\gamma)) - (K-1)\Delta.
\end{aligned}$$

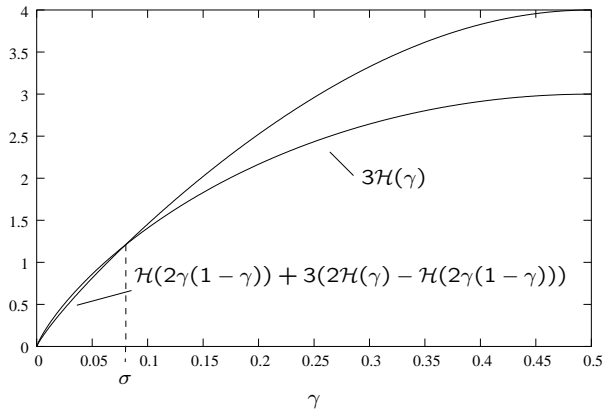


Fig. 5. $\mathcal{H}(2\gamma(1-\gamma)) + 3(2\mathcal{H}(\gamma) - \mathcal{H}(2\gamma(1-\gamma)))$ is strictly less than $3\mathcal{H}(\gamma)$ for $0 < \gamma < \sigma$.

To see that $R_S > K\mathcal{H}(\gamma)$ for $\Delta = 0$ and $\gamma > 0$, note the function $\mathcal{H}(\gamma) = \gamma \log_2 \gamma - (1-\gamma) \log_2 (1-\gamma)$ is monotonically increasing for $0 < \gamma < 1/2$ and $2\gamma(1-\gamma) < 2\gamma$ for $\gamma > 0$. Thus for $\gamma > 0$, $\mathcal{H}(2\gamma(1-\gamma)) < 2\mathcal{H}(\gamma)$ and $(2K-1)\mathcal{H}(\gamma) - (K-1)\mathcal{H}(2\gamma(1-\gamma)) > H(\gamma)$.

V. DISCUSSION

We discuss the motivation behind the genie-aided bound of theorem 3.1. For simplicity assume $\Delta = 0$. Consider the I.I.D. BSCs problem with three recipients. If the perfect-secrecy strategy is used, that is if Alice merely bins the three error sequences and transmits their indices, the secrecy rate achieved is $3\mathcal{H}(\gamma)$. There is an alternative: Since Alice has knowledge of the eavesdroppers side information, she can first broadcast the Slepian-Wolf bin index of E_1^N using $H(E_1^N|B_1^N(k))$ bits and follow this by sending the bin indices of the three error sequences using a reduced number of bins $H(A_1^N|B_1^N(k), E_1^N)$ instead of $H(A_1^N|B_1^N(k))$. More precisely Alice sends

$$X_1^M = (g(D_1^N), h(Z_{1,B}^N), h(Z_{1,C}^N), h(Z_{1,E}^N))$$

using random binning functions

$$\begin{aligned} g : \{0, 1\}^N &\rightarrow \{0, 1\}^{N\mathcal{H}(2\gamma(1-\gamma))} \\ h : \{0, 1\}^N &\rightarrow \{0, 1\}^{N(2\mathcal{H}(\gamma) - \mathcal{H}(2\gamma(1-\gamma)))}. \end{aligned}$$

As E_1^N is already known by Eve, broadcasting it reveals no new information to her. The secrecy rate achieved by this scheme is $\mathcal{H}(2\gamma(1-\gamma)) + 3(2\mathcal{H}(\gamma) - \mathcal{H}(2\gamma(1-\gamma)))$. Indeed figure 4 illustrates that this is strictly less than the secrecy rate achieved by the perfect-secrecy scheme over some range of γ .

This suggests Alice may be better off sending an update that gives the recipients a better idea of E_1^N . Doing so essentially kills several birds with one stone –any information about E_1^N broadcasted by Alice is useful to *all* recipients. Whereas for perfect-secrecy this is a luxury she is prohibited from indulging in, it may benefit her here. It is this phenomenon that makes a precise characterization of $R_S^*(\gamma)$ tricky.

The idea of the genie-aided bound is to give the message recipients enough side information about E_1^N to remove Alices incentive to transmit an update that depends directly on E_1^N .

The simplest way of achieving this is to give all recipients genie-access to E_1^N . We can do better though –knowledge of E_1^N need only be giving to $K-1$ of them, as this is sufficient to remove Alices desire to broadcast some component of E_1^N in that doing so will only benefit a single recipient.

The update scheme described above can generalized and used to tighten the upper bound of corollary 5.1, i.e. Alice first broadcasts $N\Delta$ bits of A_1^N , then E_1^N using $NH(2\gamma(1-\gamma))$ bits, then transmits each recipients error sequence to them individually using $KN(2\mathcal{H}(\gamma) - H(2\gamma(1-\gamma)) - \Delta)$ bits. Thus

Theorem 5.1: For the I.I.D. BSCs problem where Alice knows E_1^N ,

$$R_S^* \leq 2K\mathcal{H}(\gamma) - (K-1)\mathcal{H}(2\gamma(1-\gamma)) - (K-1)\Delta$$

and so the minimum achievable Δ -secrecy rate per user $R_S^*(K)/K$ satisfies

$$\lim_{K \rightarrow \infty} R_S^*(K)/K = 2\mathcal{H}(\gamma) - \mathcal{H}(2\gamma(1-\gamma)) - \Delta. \quad \square$$

An interesting variant of the problem arises when we deny Alice knowledge of E_1^N . One would expect she cannot do better than in the case of perfect-secrecy. This turns out to be difficult to prove. The only additional thing we can say is $I(E_1^N; X_1^M|A_1^N) = 0$. Combining this with the zero leakage requirement ($I(A_1^N; X_1^M|E_1^N) = 0$) tells us $H(X_1^M|A_1^N) = H(X_1^M|E_1^N)$. But this statement is of no use –it just replaces one of the inequalities in the bound with an equality (as we already used the fact $H(X_1^M|A_1^N) \geq H(X_1^M|E_1^N)$). Nonetheless we conjecture the upper bound is tight in that possessing only statistical knowledge of E_1^N is no better than possessing no knowledge at all.

Conjecture 5.2: For the I.I.D. BSCs problem when Alice is denied access to E_1^N , the minimum achievable Δ -secrecy rate satisfies

$$R_S^*(\gamma) = K\mathcal{H}(\gamma) - (K-1)\Delta. \quad \square$$

This conjecture would imply that any approach to doing distributed source coding will behave just like binning in that even if it intends to target at a particular recipient it will end up benefitting all recipients.

REFERENCES

- [1] J. K. Wolf, "Source Coding for a Noiseless Broadcast Channel," *Proc. 2004 CISS*, pp. 666-71.
- [2] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inform. Theory*, IT-19: pp. 471-480, 1973.
- [3] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Syst. Tech. J.* vol.28-4, pp. 656-715, 1949.
- [4] A. D. Wyner, "The Wiretap Channel," *Bell Syst. Tech. J.* vol. 54, no. 8, pp. 1355-1387, 1975.
- [5] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 339-348, May 1978.
- [6] U. M. Maurer, "Secret key agreement based on common information," *IEEE Trans. Inform. Theory*, vol. 39, pp. 733-742, May 1993.
- [7] G. Caire, S. Shamai and S. Verdú, "Noiseless Data Compression with Low-Density Parity-Check Codes," *Advances in Network Information Theory*, P. Gupta, G. Kramer and A. J. van Wijngaarden, Eds., DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 66, pp. 263-284, American Mathematical Society, 2004.
- [8] R. W. Yeung, *A First Course in Information Theory*, Kluwer Academic, 2002.