State amplification under masking constraints

O. Ozan Koyluoglu, Rajiv Soundararajan, and Sriram Vishwanath
Department of Electrical and Computer Engineering
The University of Texas at Austin
Austin, TX 78712
Email: ozan@austin.utexas.edu, rajivs@utexas.edu, sriram@austin.utexas.edu

***Abstract*—This paper considers a state dependent channel with one transmitter, Alice, and two receivers, Bob and Eve. The problem at hand is to effectively "amplify" the channel state sequence at Bob while "masking" it from Eve. The extent to which the state sequence cannot be masked from Eve is referred to as leakage, and the paper is aimed at characterizing the tradeoff-region between amplification and leakage rates for such a system. An achievable coding scheme is presented, wherein the transmitter enumerates the state sequence using two indices, and transmits one of the indices over the channel to facilitate the amplification process. For the case when Bob observes a "stronger" channel than Eve, the achievable coding scheme is enhanced with secure refinement. The optimal amplification-leakage rate difference, called as differential amplification capacity, is characterized for the degraded binary and the degraded Gaussian channels. For the degraded Gaussian model, extremal corner points of the trade-off region are characterized. In addition, the gap between the outer bound and achievable rate-regions is determined, where it is shown that the gap is less than half a bit for a wide set of channel parameters.**

I. Introduction

In this paper, we consider a state dependent broadcast channel model with two users, and consider the question of to what extent the state of the channel can be amplified at the receiver (Bob) and masked from the other receiver (called as Eve). In the best case, the state(s) seen by Bob and Eve will be completely different (or, independent). However, we consider what might be a pessimistic model where there is a single channel state defining the channel for both Bob and Eve. Moreover, the entire channel state is presumed to be known non-causally to the transmitter (a Gel'fand-Pinsker-style assumption [1]). The only manner in which an asymmetry can be affected between Bob and Eve is by the encoding used at the transmitter. For such a system, we aim to characterize the tradeoff between the "amplification"-rate at which the legitimate pair can operate and the "leakage"-rate to the eavesdropper. In essence, as long as there is a non-trivial difference between the two, this can be used to develop shared keys and enable cryptographic algorithms. In general, we are interested in understanding the entire rate tradeoff region. Two applications are of definite interest with such a formulation. Firstly, the problem is intimately related to the analysis of key agreement using channel states. Once obtained, this key can be used, for example, in symmetric key cryptography [2], [3]. The second application is in cognitive radios [4]–[6], where the cognitive encoder facilitates the secure communication of the primary signal (the channel state sequence) while masking it from the eavesdropper.

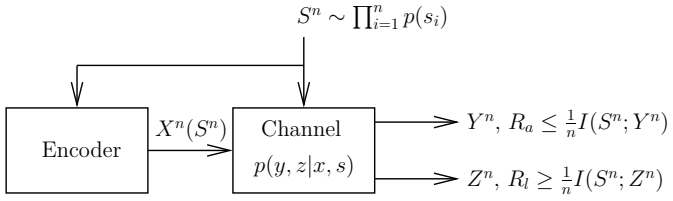

Fig. 1. The system model for amplification subject to masking problem.

A. Problem Statement

Consider a discrete memoryless channel given by $p(y,z|x,s)$, where $x \in \mathcal{X}$ is the channel input, $s \in \mathcal{S}$ is the channel state, and $(y,z) \in (\mathcal{Y} \times \mathcal{Z})$ is the channel output, with y corresponding to the legitimate receiver (Bob) and z the eavesdropper (Eve). The channel is memoryless in the sense that

$$p(Y^n = y^n, Z^n = z^n | X^n = x^n, S^n = s^n) = \prod_{i=1}^{n} p(y(i), z(i)|x(i), s(i)), \quad (1)$$

and the state sequence is independent and identically distributed (i.i.d.) according to a probability distribution indicated by $p(s)$. It is assumed that the channel state sequence is non-causally known at the transmitter. (The system model is depicted in Fig 1.)

The encoder is denoted by the mapping $X^n(S^n)$, which is allowed to "amplify" the state sequence at Bob (channel output Y^n) and to "mask" the state sequence from Eve (Z^n). Formally, we measure the former by the state amplification rate R_a and the latter with the state leakage rate R_l. We say (R_a, R_l) is achievable, if for any given $\epsilon > 0$,

$$\frac{1}{n} I(S^n; Y^n) \ge R_a - \epsilon \quad (2)$$

$$\frac{1}{n} I(S^n; Z^n) \le R_l + \epsilon \quad (3)$$

for sufficiently large n. The problem is to characterize all achievable (R_a,R_l) pairs, which we denote by the trade-off region $\mathcal{C}$. We also define *differential amplification capacity*, denoted by C_d, as

$$C_d \triangleq \sup_{(R_a,R_l)\in\mathcal{C}} R_a - R_l. \quad (4)$$

This difference measures the knowledge difference between the two receivers regarding the state of the channel.

A cost constraint may also be imposed on the channel input with

$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\{c(X(i))\} \leq C, \tag{5}$$

where $c : \mathcal{X} \to \mathbb{R}^+$ defines the cost per input letter and the expectation is over the distribution of the channel input. In this scenario, we say (R_a, R_l) is achievable under the cost function $c(.)$ and cost C, if (2), (3), and (5) are satisfied in the limit of large n. (We use this constraint for the Gaussian channel, where the cost is the average transmitted power.)

Remark: One can define equivocation rate as

$$\frac{1}{n}H(S^n|Z^n), \tag{6}$$

which satisfies $\frac{1}{n}\left(I(S^n;Z^n) + H(S^n|Z^n)\right) = \frac{1}{n}H(S^n)$. Hence, the problem can be re-stated in terms of equivocation rate, where we seek to characterize all achievable (R_a, Δ_l) pairs in the limit of large n, where Δ_l is achievable if $\frac{1}{n}H(S^n|Z^n) \geq \Delta_l - \epsilon$. Since both the equivocation and leakage rate notions characterize the same tradeoff, both notions can be used interchangeably.

B. Related work, summary of results, and organization

The problem of communication over state dependent channels is studied by Gel'fand and Pinsker [1], where a message has to be reliably transmitted over the channel with non-causal state knowledge at the transmitter. The Gaussian version of the problem is solved in [7] through the famous dirty paper coding scheme. While the wiretap channel is introduced and solved in [8], these results are extended to a broadcast setting in [9]. The problem of sending secure messages over state dependent wiretap channels is studied in [10], [11].

On the other hand, the problems of state amplification and state masking are individually solved in [12]–[14] for point-to-point channels. Both [12], [13] and [14] consider the problem of reliable transmission of messages in addition to state amplification and state masking respectively. In this paper, we consider the problem of amplifying the state to a desired receiver while trying to minimize the leakage (or mask the state) to the eavesdropper.

We note that, if we set $R_a = 0$ in our problem definition, it reduces to the state masking problem as studied in [14]. In other words,

$$R_a = 0 \tag{7}$$

$$R_l = \min_{p(x|s)} I(S;Z) \tag{8}$$

can be shown to be achievable [14]. Also, when $R_l \geq H(S)$, the problem reduces to a state amplification problem [13], and one can achieve the following rate pair.

$$R_a = \min\{H(S), \max_{p(x|s)} I(X,S;Y)\} \tag{9}$$

$$R_l \geq H(S) \tag{10}$$

These represent two extremes of the tradeoff-region between the amplification and masking rates. In this paper, we aim at developing an understanding of this tradeoff-region through achievable regions and outer bounds, and characterizing special cases when they match. Our achievability arguments are based on enumerating typical state sequences using two indices, and sending one of the indices over the channel. Towards this end, we construct a codebook corresponding to the codeword carrying this index (denoted by U^n) in such a way that reliable communication can be achieved over the state-dependent channel. Subsequently, we derive expressions for achievable amplification and leakage rates by determining single-letter bounds on $\frac{1}{n}I(S^n;Y^n)$ and $\frac{1}{n}I(S^n;Z^n)$ respectively. We also show that it is possible to extend the proposed region with secure refinement when Bob observes a "stronger" channel than Eve. In precise terms, this corresponds to instances of $p(u,x|s)$ satisfying $I(U;Y) \geq I(U;Z)$. We find that the utilization of the notion of secure refinement approach is critical to these less-noisy channels [15], [16]. In particular, we show that the proposed scheme achieves the differential amplification capacity over the set of achievable (R_a, R_l) pairs for the degraded binary channels and the degraded Gaussian channels. We also characterize the corner points of the region for the degraded Gaussian channel. In this scenario, we further bound the gap between achievable and converse regions, and show the following: Let us denote the message capacity of Bob's channel as $C = \frac{1}{2}\log(1+\text{SNR})$. Then, the gap between the upper and lower bounds on both the amplification rate (R_a) and the amplification-leakage rate difference $(R_a - R_l)$ is bounded by C for all achievable (R_a, R_l) pairs. In particular, both gaps are within half a bit when the SNR ≤ 1.

The rest of the paper is organized as follows. Section II presents our main results, where we provide our proposed coding schemes and outer bounding arguments. Section III provides optimality discussions and numerical results for special classes of DMCs including modulo additive binary channel model and the memory with defective cells model. The Gaussian channel model is considered in Section IV along with corresponding optimality results. Finally, we conclude the paper in Section V. The proofs are collected in Appendices to improve the flow of the paper. (Some of the proofs are provided in the extended version of the paper [17].)

II. Main Results

A. Achievable Regions

We have the following propositions for any given $p(s)$ and the channel $p(y,z|x,s)$.

1) State sequence covering: The scheme presented below is based on communication a covering of the state sequence while ensuring that the covering is decodable at Bob. We have the following result.

Proposition 1: Let $\mathcal{R}^1$ be the closure of the union of all

(R_a, R_l) pairs satisfying

$$\begin{aligned} R_a &\leq I(S;Y,U) \\ R_l &\geq \min\{I(S;Z,U), I(U,S;Z)\} \\ 0 &\leq I(U;Y) - I(U;S), \end{aligned}$$

over all distributions $p(u,x|s)$. Then, $\mathcal{R}^1 \subseteq \mathcal{C}$.

Proof: See Appendix A. ∎

We note that, provided $I(U;Y) - I(U;S) \geq 0$, the covering codeword can be decoded at Bob. Then, the state uncertainty can be reduced from $H(S)$ to $H(S|Y,U)$ by listing S^n sequences that are jointly typical with (U^n, Y^n). This will give rise to the expression $I(S;Y,U)$, as presented in the proposition. (Leakage expressions follow by a similar argument, where U^n sequence is added to the expression $\frac{1}{n}I(S^n;Z^n)$ to derive achievable leakage expressions.)

2) State enhanced messaging: In order to achieve a better rate region, the encoder can send a message over the state dependent channel, where the message carries partial information about the state sequence. The corresponding achievable region is given by the following result.

Proposition 2: Let $\mathcal{R}^2$ be the closure of the union of all (R_a, R_l) pairs satisfying

$$\begin{aligned} R_a &\leq \min\{H(S), I(U,S;Y)\} \\ R_l &\geq I(U,S;Z) \\ 0 &\leq I(U;Y) - I(U;S), \end{aligned}$$

over all distributions $p(u,x|s)$. Then, $\mathcal{R}^2 \subseteq \mathcal{C}$.

Proof: See Appendix B. ∎

The achievable rate region can be interpreted as follows: The rate $I(U;Y) - I(U;S)$ corresponds to the Gel'fand-Pinsker message rate that can be reliably communicated over the channel. As long as this rate is positive for a given input probability distribution, the codeword U^n can be reliably communicated over the channel. Bob can decode U^n from Y^n by employing a jointly-typical decoder. Subsequently, the state uncertainty can be reduced from $H(S)$ to $H(S|Y,U)$ by listing S^n sequences that are jointly typical with (U^n, Y^n). Further, the rate $I(U;Y) - I(U;S)$ provides an additional refinement to the uncertainty, which together with $I(S;Y,U)$ sums to $I(U,S;Y)$. (See also [13], where the authors show that it is possible to interpret this scheme as a source coding method with Wyner-Ziv coding [18].) The analysis of R_l follows by analyzing an upper-bound on the leakage rate by adding the codeword sequence to the expression, $\frac{1}{n}I(S^n;Z^n) \leq \frac{1}{n}I(U^n,S^n;Z^n)$, which can be single-letterized as given in Appendix B.

We observe that the leakage expression can be enhanced when $I(U;Z) \geq I(U;Y)$, and this is detailed in the following proposition.

Proposition 3: For all input distributions $p(u,x|s)$ that satisfy $I(U;Z) \geq I(U;Y)$. R_l is bounded as

$$R_l \geq I(S;Z,U) + R_u.$$

for some

$$R_u \leq \min\{I(U;Y) - I(U;S), H(S|U,Y)\}.$$

In particular,

$$\begin{aligned} R_l \geq \min\Big\{ & I(S;Z,U) + I(U;Y) - I(U;S) \\ & = I(U,S;Z) - [I(U;Z) - I(U;Y)], \\ & H(S) - [H(S|Z,U) - H(S|Y,U)] \Big\}. \end{aligned}$$

Thus Proposition 2 can be enhanced for those input distributions satisfying $I(U;Z) \geq I(U;Y)$.

Proof: (Sketch) The requirement of $I(U;Z) \geq I(U;Y)$ enables the decodability of U^n at Eve. Then, using arguments similar to those for the amplification bound in the proof of Proposition 2 (and upper bounding the corresponding terms), we obtain the R_l bound as

$$R_l \geq I(S;Z,U) + R_u. \tag{11}$$

Further, by choosing

$$R_u \leq \min\{I(U;Y) - I(U;S), H(S|U,Y)\}, \tag{12}$$

we have the desired result. ∎

We note that, in this case, increasing R_u will not only increase the amplification rate but will also increase the leakage rate.

3) Secure refinement: We now discuss how securing the refinement can help in the amplification and masking problem. (Please refer to [17] for details.) Consider all input distributions $p(u,x|s)$ satisfying $I(U;Y) \geq I(U;Z)$. For such inputs, it is possible to send the refinement information securely over the channel. It is known that the secure message rate of $[I(U;Y) - \max\{I(U;S), I(U;Z)\}]^+$ is achievable over the state dependent channels [10]. Thus, it is possible to set a refinement rate satisfying $R_u \leq \min\big\{[I(U;Y) - \max\{I(U;S), I(U;Z)\}]^+, H(S|Y,U)\big\}$, for the case of $I(U;Y) \geq I(U;Z)$, and secure the message at this rate. The resulting amplification rate is bounded as $R_a \leq I(S;Y,U) + R_u$, and the leakage rate is given by $R_l \geq \min\{I(U,S;Z), I(S;Z,U)\}$. (Follows from an analysis similar to the previous section.) Note that, the additive rate R_u in the leakage expression $R_l \geq I(S;Z,U) + R_u$ of the regions given in the previous section disappears here due to the security of the message. Hence, the leakage increase due to refinement index is decreased as the security of the index lowers the corresponding leakage rate achieved at Eve compared to the non-secured case.

B. Outer Bounds

We now derive upper bounds on R_a and lower (upper) bounds on R_l (respectively, on Δ_l).

Proposition 4: If (R_a, R_l) is achievable, then $(R_a, R_l) \in \mathcal{R}_o^1$, where

$$\mathcal{R}_o^1 = \bigcup_{p(u,x|s)} (R_a, R_l)$$

satisfying

$$\begin{aligned} R_a &\leq \min\{H(S), I(X,S;Y)\} \\ R_l &\geq I(S;Z,U) \\ 0 &\leq I(U;Z) - I(U;S), \end{aligned}$$

for any given $p(u,x|s)$.

Proof: Please refer to [17]. ∎

We now provide an outer bound for the degraded channel $p(y,z|x,s) = p(y|x,s)p(z|y)$ using the result above.

Proposition 5: If the channel satisfies $p(y,z|x,s) = p(y|x,s)p(z|y)$ and if (R_a, R_l) is achievable, then $(R_a, R_l) \in \mathcal{R}_o^2$, where

$$\mathcal{R}_o^2 = \bigcup_{p(u,x|s)} (R_a, R_l)$$

satisfying

$$\begin{aligned} R_a &\leq \min\{H(S), I(X,S;Y)\} \\ R_l &\geq I(S;Z,U) \\ R_a - R_l &\leq I(X,S;Y|Z) \\ 0 &\leq I(U;Y) - I(U;S), \end{aligned}$$

for any given $p(u,x|s)$.

Proof: Please refer to [17]. ∎

III. Special discrete memoryless channel models

A. Modulo additive binary model

Consider the channels given by

$$\begin{aligned} Y(i) &= X(i) \oplus S(i) \oplus N(i) \\ Z(i) &= X(i) \oplus S(i) \oplus N_z(i), \end{aligned} \tag{13}$$

where the state and noise distributions are generated i.i.d. as $S(i) \sim \text{Bern}(p_s)$, $N(i) \sim \text{Bern}(p_n)$, $N_z(i) \sim \text{Bern}(p_{n_z})$. (All p_ks satisfy $p_k \in [0, 0.5]$ for $k = \{s, n, n_z\}$.) In this section, we use the following notation for the binary convolution $p \otimes q \triangleq p(1-q) + q(1-p)$.

1) State cancelation scheme: To cancel the state from the channel, we send

$$X(i) = U(i) \oplus S(i),$$

where $U(i) \sim \text{Bern}(p_u)$ and the codewords U^n carry a description of the state sequence S^n. This way, we achieve the following inner-bound.

Corollary 6: The state cancelation scheme, which sends $\text{Bern}(p_u)$ distributed signal XORed with state sequence at each time instant, achieves the set of (R_a, R_l) pairs denoted by the region $\mathcal{R}^{\text{SC}} \subseteq \mathcal{C}$, where

$$\mathcal{R}^{\text{SC}} = \text{C.H.} \left\{ \bigcup_{p_u \in [0,0.5], p_u \otimes p_s \leq 0.5} (R_a(p_u), R_l(p_u)) \right\},$$

with[1]

$$\begin{aligned} R_a(p_u) &\leq \min\{H(p_s), H(p_u \otimes p_n) - H(p_n)\} \\ R_l(p_u) &\geq H(p_u \otimes p_{n_z}) - H(p_{n_z}). \end{aligned}$$

[1]C.H. denotes the closure of the convex hull operation.

Proof: Achievability follows from Proposition 2. ∎

2) Optimal rate difference ($R_a - R_l$):

Corollary 7: If $p_n \leq p_{n_z}$ and $H(p_s) \geq 1 - H(p_n)$ for a binary model the optimal amplification and leakage rate difference is given by

$$C_d = H(p_{n_z}) - H(p_n).$$

Proof: From Proposition 5, we obtain the following. If $p_n \leq p_{n_z}$, any given $(R_a, R_l) \in \mathcal{C}$ satisfies

$$\begin{aligned} R_a - R_l \leq\ & H(p_{n_z}) - H(p_n) + \max_{p(x|s)} \Big\{ H(X \oplus S \oplus N) \\ & - H(X \oplus S \oplus N_z) \Big\} \end{aligned}$$

Note that, this upper-bound can be evaluated by observing

$$\begin{aligned} &\max_{p(x|s)} \{H(X \oplus S \oplus N) - H(X \oplus S \oplus N_z)\} \\ &= \max_{p(x|s)} \{H(X \oplus S \oplus N) - H(X \oplus S \oplus N \oplus N_z^*)\} \\ &\leq \max_{p(x|s)} \{H(X \oplus S \oplus N) - H(X \oplus S \oplus N \oplus N_z^* | N_z^*)\} \\ &= 0, \end{aligned} \tag{14}$$

where the equality is due to the channel degradedness condition with appropriate noise term N_z^* independent of N such that $N \oplus N_z^* = N_z$, and the inequality is due to the fact that conditioning does not increase the entropy. Using this we observe that the outer-bound is maximized with a choice of $p(x) = 0.5$, which evaluates to

$$R_a - R_l \leq H(p_{n_z}) - H(p_n). \tag{15}$$

This expression is achieved by Theorem 6, when we choose $p(u) = 0.5$, if $H(p_s) \geq 1 - H(p_n)$.

∎

B. Memory with defective cells model

We consider the model of information transmission over write-once memory device with stuck-at defective cells [19], [20]. In this channel model, each memory cell corresponds to a channel state instant with cardinality $|\mathcal{S}| = 3$, where the binary channel output is determined from the binary channel input and the channel state as the following.

$$\begin{aligned} p(y=0|x, s=0) &= 1 \\ p(y=1|x, s=1) &= 1 \\ p(y=x|x, s=2) &= 1, \end{aligned}$$

where $\Pr\{S=0\} = p$ is the probability that the channel is stuck at 0, $\Pr\{S=1\} = q$ is the probability that the channel is stuck at 1, and $\Pr\{S=2\} = r$ is the probability of having a good channel where $y = x$. (Here, we have $p+q+r = 1$.) We consider a binary symmetric channel (BSC) from Y to Z, where

$$Z = Y \oplus N,$$

with $N \sim Bern(n)$ for some $n \in [0, 0.5]$. This corresponds to a degraded DMC model. (See Fig. 2.)

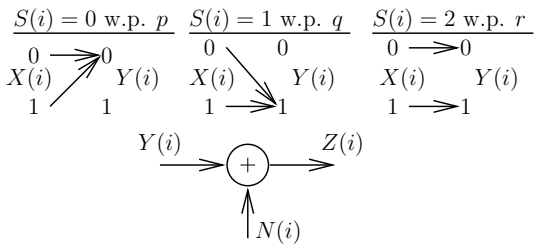

Fig. 2. Channel model of memory with defective cells. $p = \Pr\{S = 0\}$ (probability of being stuck at 0), $q = \Pr\{S = 1\} = q$ (probability of being stuck at 1), $r = \Pr\{S = 2\}$ (probability of being in a noiseless state), and $N \sim \text{Bern}(n)$, where $n \in [0, 0.5]$ is the cross over probability of the BSC from Y to Z.

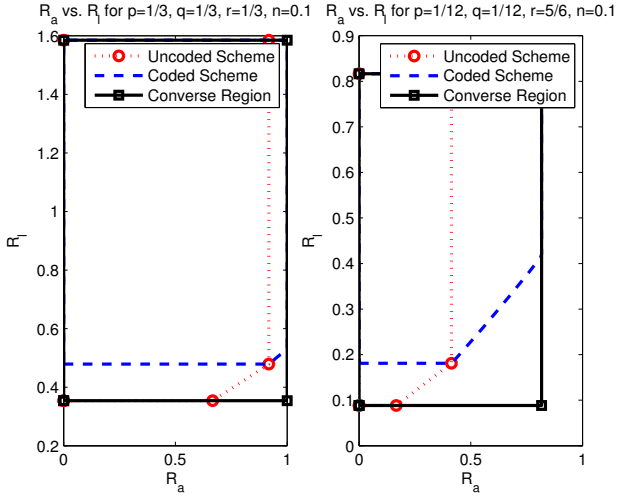

Fig. 3. Simulation results for memory with defective cells model.

We present numerical results for this channel model with three regions: Un-coded region, coded region, and an outer-bound region. The un-coded region is obtained by setting $U = \emptyset$ in Proposition 1, where we have the set of (R_a, R_l) pairs satisfying

$$\begin{aligned} R_a &\leq I(S;Y) \\ R_l &\geq I(S;Z) \end{aligned}$$

over all possible $p(x|s)$. For the coded region, we simulate a sub-region of the one given in Proposition 2, where we set $U = Y$ and achieve the set of (R_a, R_l) pairs satisfying

$$\begin{aligned} R_a &\leq \min\{H(S), H(Y)\} \\ R_l &\geq I(Y,S;Z) = H(Z) - H(N) \end{aligned}$$

over all possible $p(x|s)$. For converse arguments, we consider the outer-bound region given by the set of (R_a, R_l) pairs satisfying

$$\begin{aligned} R_a &\leq \min\{H(S), I(X,S;Y) = H(Y)\} \\ R_l &\geq I(S;Z) \end{aligned}$$

over all possible $p(x|s)$. (This outer-bound region follows from Proposition 4.) The numerical results are given in Fig. 3. (The regions are truncated with $R_l \leq H(S)$ as any $R_l > H(S)$ is trivially achievable.) We note that, the coded region can outperform the un-coded region (even when we plot a sub-region of the coded achievable region). This shows the enhancement provided by sending a refinement of the state sequence over the channel.

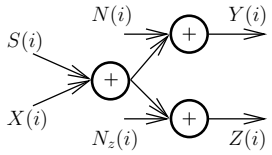

Fig. 4. The channel model for the Gaussian seeting. $S(i) \sim \mathcal{N}(0, \sigma_s^2)$, $N(i) \sim \mathcal{N}(0, \sigma_n^2)$, and $N_z(i) \sim \mathcal{N}(0, \sigma_{n_z}^2)$.

IV. Gaussian Scenario

Consider the channels given by

$$\begin{aligned} Y(i) &= X(i) + S(i) + N(i) \\ Z(i) &= X(i) + S(i) + N_z(i), \end{aligned} \tag{16}$$

where the state and noise distributions are generated i.i.d. as $S(i) \sim \mathcal{N}(0, \sigma_s^2)$, $N(i) \sim \mathcal{N}(0, \sigma_n^2)$, $N_z(i) \sim \mathcal{N}(0, \sigma_{n_z}^2)$, and the cost constraint on the channel input is given by $c(x) = x^2$ and $C = P$, i.e.,

$$\frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\{|X(i)|^2\} \leq P.$$

(See Fig. 4.)

A. Inner-bounding $\mathcal{C}$ with an un-coded scheme

The inner bound is based on sending an amplified version of S together with some additional Gaussian noise. This *un-coded* signal is constructed as follows.

$$X(i) = \rho\frac{\sigma_x}{\sigma_s}S(i) + \sqrt{(1-\rho^2)}\sigma_x V(i), \tag{17}$$

where $V(i) \sim \mathcal{N}(0,1)$ independent of S(i), $\rho \in [-1, 1]$, and $\sigma_x^2 \leq P$. Here, ρ^2 is the fraction of the power allocated to $S(i)$. This scheme achieves the following region.

Theorem 8: The un-coded scheme, which forwards $S(i)$ at each time step together with some i.i.d. Gaussian noise as given in (17), achieves the set of (R_a, R_l) pairs denoted by the region $\mathcal{R}^{\text{un-coded}} \subset \mathcal{C}$, where

$$\mathcal{R}^{\text{un-coded}} = \text{C.H.}\left\{\bigcup_{\rho\in[-1,1],\sigma_x^2\in[0,P]} (R_a(\rho,\sigma_x), R_l(\rho,\sigma_x))\right\},$$

with

$$R_a(\rho,\sigma_x) = \frac{1}{2}\log\left(1 + \frac{\sigma_s^2 + 2\rho\sigma_s\sigma_x + \rho^2\sigma_x^2}{\sigma_n^2 + (1-\rho^2)\sigma_x^2}\right) \tag{18}$$

$$R_l(\rho,\sigma_x) = \frac{1}{2}\log\left(1 + \frac{\sigma_s^2 + 2\rho\sigma_s\sigma_x + \rho^2\sigma_x^2}{\sigma_{n_z}^2 + (1-\rho^2)\sigma_x^2}\right). \tag{19}$$

The above expressions are obtained by evaluating $R_a = I(S;Y)$ and $R_l = I(S;Z)$ on account of uncoded transmission in (17).

Examples:

- If $P \geq \sigma_s^2$, one can set $X = -S$ and achieve the pair
$$(R_a = 0, R_l = 0).$$
- Another trivial point is obtained by setting $X = 0$, which achieves
$$\left(R_a = \frac{1}{2}\log\left(1 + \frac{\sigma_s^2}{\sigma_n^2}\right), R_l = \frac{1}{2}\log\left(1 + \frac{\sigma_s^2}{\sigma_{n_z}^2}\right)\right).$$

B. Outer-bounds on $\mathcal{C}$

Corollary 9: Let ρ denote the correlation coefficient between X and S. If $\sigma_n^2 \leq \sigma_{n_z}^2$, then the set of all achievable rate pairs (R_a, R_l) satisfy

$$\begin{aligned} R_a - R_l &\leq \frac{1}{2}\log\left(1 + \frac{\sigma_s^2 + 2\rho\sigma_s\sigma_x + \sigma_x^2}{\sigma_n^2}\right) \\ &\quad - \frac{1}{2}\log\left(1 + \frac{\sigma_s^2 + 2\rho\sigma_s\sigma_x + \sigma_x^2}{\sigma_{n_z}^2}\right) \quad (20) \\ R_a &\leq \frac{1}{2}\log\left(1 + \frac{\sigma_s^2 + 2\rho\sigma_s\sigma_x + \sigma_x^2}{\sigma_n^2}\right), \quad (21) \end{aligned}$$

for $-1 \leq \rho \leq 1$ and $\sigma_x^2 \leq P$.

Proof: By Proposition 5, we have

$$R_a - R_l \leq I(X, S; Y|Z).$$

Without loss of generality, we consider $N_z = N + N_z'$ with $\sigma_{n_z}^2 = \sigma_n^2 + \sigma_{n'}^2$ where N_z' is independent of N. Noting that,

$$I(X,S;Y|Z) = h(Y|Z) - h(Y|X,S,Z) = h(Y|Z) - h(N|N_z),$$

we upper bound $h(Y|Z)$ using the following. Consider two zero-mean correlated random variables A and B.

$$\begin{aligned} h(A|B) &\overset{(a)}{=} h(A - \hat{A}(B)|B) \\ &\leq h(A - \hat{A}(B)) \\ &\overset{(b)}{\leq} \frac{1}{2}\log(2\pi e\sigma_e^2), \end{aligned}$$

where in (a) we used $\hat{A}(B)$ as the estimate of A given B, and (b) follows by defining the estimation error variance $\sigma_e^2 \triangleq E\left[(A - \hat{A}(B))^2\right]$ and the fact that Gaussian distribution maximizes entropy given the variance. We then upper bound the optimal estimator error variance by the linear MMSE variance. Therefore,

$$h(A|B) \leq \frac{1}{2}\log\left(2\pi e\left(\text{var}(A) - \frac{E\left[(AB)^2\right]}{\text{var}(B)}\right)\right).$$

Using the above, we obtain

$$\begin{aligned} R_a - R_l &\leq \frac{1}{2}\log\left(2\pi e\Big(\sigma_s^2 + 2\rho\sigma_s\sigma_x + \sigma_x^2 + \sigma_n^2 \right. \\ &\qquad \left. - \frac{(\sigma_s^2 + 2\rho\sigma_s\sigma_x + \sigma_x^2 + \sigma_n^2)^2}{\sigma_s^2 + 2\rho\sigma_s\sigma_x + \sigma_x^2 + \sigma_n^2 + \sigma_{n'}^2}\Big)\right) \\ &\quad - \frac{1}{2}\log\left(2\pi e\left(\sigma_n^2 - \frac{(\sigma_n^2)^2}{\sigma_n^2 + \sigma_{n'}^2}\right)\right) \quad (22) \\ &= \frac{1}{2}\log\left(1 + \frac{\sigma_s^2 + 2\rho\sigma_s\sigma_x + \sigma_x^2}{\sigma_n^2}\right) \\ &\quad - \frac{1}{2}\log\left(1 + \frac{\sigma_s^2 + 2\rho\sigma_s\sigma_x + \sigma_x^2}{\sigma_n^2 + \sigma_{n'}^2}\right). \quad (23) \end{aligned}$$

Using Proposition 5, we also have

$$\begin{aligned} R_a &\leq I(X,S;Y) = h(Y) - h(Y|X,S) = h(Y) - h(N) \\ &\leq \frac{1}{2}\log\left(1 + \frac{\sigma_s^2 + 2\rho\sigma_s\sigma_x + \sigma_x^2}{\sigma_n^2}\right). \end{aligned}$$

■

C. Comparison of inner and outer bounds for the degraded Gaussian channel

We now compare the uncoded scheme and the outer bound presented above. In particular, we show that the uncoded transmission scheme achieves certain corner points of the amplification-masking region and that the gap between the inner and outer bounds on the region is within $1/2$ bit for certain channel parameters. We also show that the uncoded scheme achieves the optimal difference $R_a - R_l$.

1) Characterization of the gap between achievable and converse regions: We now bound the gap between uncoded transmission and the optimal region. Using (19), we see that uncoded transmission achieves a leakage of $I(S;Z)$ and an amplification of $I(S;Y)$. Given any point (R_a, R_l) in the outer bound region corresponding to a particular (ρ, σ_x), we fix X as in (17) to achieve the pair $(I(S;Y), I(S;Z))$. Therefore, the gap between the achievable R_a and the upper bound on R_a for every point corresponding to (ρ, σ_x) in the outer bound region is given by

$$I(X,S;Y) - I(S;Y) = \frac{1}{2}\log\left(1 + \frac{\sigma_x^2(1-\rho^2)}{\sigma_n^2}\right). \quad (24)$$

Similarly, the gap between the achievable $R_a - R_l$ and the upper bound on $R_a - R_l$ is given by

$$\begin{aligned} &I(X,S;Y|Z) - [I(S;Y) - I(S;Z)] = I(X;Y|Z,S) \\ &\quad = \frac{1}{2}\log\left(1 + \frac{\sigma_x^2(1-\rho^2)}{\sigma_n^2}\right) - \frac{1}{2}\log\left(1 + \frac{\sigma_x^2(1-\rho^2)}{\sigma_{n_z}^2}\right). \end{aligned} \quad (25)$$

Therefore, both the gap between the achievable R_a and optimum and the achievable $R_a - R_l$ and the optimum are upper bounded by the capacity of the channel between Alice and Bob, which is equal to $\frac{1}{2}\log(1 + \text{SNR})$, where

SNR $= \frac{P}{\sigma_n^2}$. Note that the gap is less than $1/2$ a bit when SNR < 1. This means that if the gap in R_a is exactly equal to $1/2$ a bit, then we achieve the optimal R_l. Similarly, if we achieve the optimal R_a, then the gap in R_l is within $1/2$ a bit.

2) Differential amplification capacity (C_d): Note that the un-coded transmission achieves the maximum $R_a - R_l$. The upper bound on $R_a - R_l$ in (20) is maximized for $\sigma_x^2 = P$ and $\rho = 1$. Thus, this maximum difference between R_a and R_l is achieved by un-coded transmission corresponding to $X = \frac{\sqrt{P}}{\sigma_s} S$ in Theorem 8.

3) Corner points of the trade-off region: Consider the corner points of the amplification-masking region. Inspecting (21), we observe that the point in the outer bound region corresponding to maximum amplification is given by $\rho = 1$. Clearly, from (24) and (25), we see that the gap is zero for $\rho = 1$. Similarly, consider the point corresponding to minimum leakage R_l in the *weak* and *moderate* interference regimes as in [14]. These points again correspond to $\rho = -1$ and we have $I(X, S; Y) = I(S; Y)$ and $I(X, S; Z) = I(S; Z)$, leading to the gap being zero. This is also verified by setting $\rho = -1$ in (24) and (25).

V. Conclusion

We studied the problem of state amplification under the masking constraints, where the encoder (with the knowledge of non-causal state S^n) facilitates the amplification rate ($\frac{1}{n} I(S^n; Y^n)$) at Bob (observing Y^n) while minimizing the leakage rate ($\frac{1}{n} I(S^n; Z^n)$) as much as possible at Eve (observing Z^n). The study of this trade-off region was the focus of the paper. Our coding schemes are based on indexing the state sequence and sending one of the indices over the channel to Bob. The achievable region corresponding to this strategy is derived by calculating bounds on amplification and masking rates. We also showed that for the input distributions enabling Bob to be a "stronger" receiver than Eve, the index of the state can be sent securely over the channel. (This secure refinement approach is further discussed in the extended version of the paper.) We also provided outer bounds, using which we characterized the differential amplification capacity for the degraded binary channels and degraded Gaussian channels. For the degraded Gaussian model, we also characterized the optimal corner points, and the gap between the outer bound and achievable regions.

Appendix A
Proof of Proposition 1

Proof: Fix $p(u, x|s)$, and consider s^n is the state sequence of the channel that is non-causally known at the encoder. We generate 2^{nR_u} codewords denoted by $u^n(w_u)$ with $w_u \in \{1, \cdots, 2^{nR_u}\}$, each distributed according to $\prod_{i=1}^{n} p(u_i)$.

The encoder chooses a $u^n(k)$ such that $(u^n(k), s^n) \in \mathcal{T}_\epsilon^n$. If no such codeword exists, an arbitrary sequence is picked. The encoder sends x^n generated by $\prod_{i=1}^{n} p(x_i|u_i(k), s_i)$.

We now derive an achievable amplification rate with this scheme. We consider the following.

$$
\begin{aligned}
&\tfrac{1}{n} I(S^n; Y^n) \\
&\overset{(a)}{=} \frac{1}{n} I(S^n; Y^n|\mathcal{E}_1)(1 - \Pr\{\mathcal{E}_1^c\}) + \frac{1}{n} I(S^n; Y^n|\mathcal{E}_1^c)\Pr\{\mathcal{E}_1^c\} \\
&\geq \frac{1}{n} I(S^n; Y^n|\mathcal{E}_1)(1 - \Pr\{\mathcal{E}_1^c\}) \\
&\overset{(b)}{\geq} \frac{1}{n} I(S^n; Y^n|\mathcal{E}_1) - \Pr\{\mathcal{E}_1^c\}(H(S) + \epsilon_1) \\
&\overset{(c)}{=} \frac{1}{n} I(S^n; Y^n|\mathcal{E}_1, \mathcal{E}_2)(1 - \Pr\{\mathcal{E}_2^c|\mathcal{E}_1\}) \\
&\quad + \frac{1}{n} I(S^n; Y^n|\mathcal{E}_1, \mathcal{E}_2^c)\Pr\{\mathcal{E}_2^c|\mathcal{E}_1\} - \Pr\{\mathcal{E}_1^c\}(H(S) + \epsilon_1) \\
&\overset{(d)}{\geq} \frac{1}{n} I(S^n; Y^n|\mathcal{E}_1, \mathcal{E}_2) \\
&\quad - (\Pr\{\mathcal{E}_1^c\} + \Pr\{\mathcal{E}_2^c|\mathcal{E}_1\})(H(S) + \epsilon_1) \\
&= \frac{1}{n} I(S^n; Y^n, U^n|\mathcal{E}_1, \mathcal{E}_2) \\
&\quad - (\Pr\{\mathcal{E}_1^c\} + \Pr\{\mathcal{E}_2^c|\mathcal{E}_1\})(H(S) + \epsilon_1) \\
&\overset{(e)}{\geq} (H(S) - \epsilon_1) - (H(S|Y, U) + \epsilon_2) \\
&\quad - (\Pr\{\mathcal{E}_1^c\} + \Pr\{\mathcal{E}_2^c|\mathcal{E}_1\})(H(S) + \epsilon_1) \\
&\overset{(f)}{=} I(S; Y, U) - \hat{\epsilon}_1
\end{aligned}
$$

where in (a) $\mathcal{E}_1$ is the event that S^n is a typical sequence, (b) follows as $\frac{1}{n} I(S^n; Y^n|\mathcal{E}_1) \leq \frac{1}{n} H(S^n|\mathcal{E}_1) \leq H(S) + \epsilon_1$ as the number of typical S^n sequences are bounded above by $2^{n(H(S)+\epsilon_1)}$ with $\epsilon_1 \to 0$ as $n \to \infty$, in (c) $\mathcal{E}_2$ is the event that U^n is decoded given Y^n, (d) is similar to (b), (e) follows as $H(S^n|\mathcal{E}_1)$ is lower bounded by $n(H(S) - \epsilon_1)$ and $H(S^n|Y^n, U^n, \mathcal{E}_1, \mathcal{E}_2)$ is upper bounded by $n(H(S|Y, U) + \epsilon_2)$ as U^n, S^n, Y^n are jointly typical, with $\epsilon_2 \to 0$ as $n \to \infty$, in (f) we define $\hat{\epsilon}_1 \triangleq (\Pr\{\mathcal{E}_1^c\} + \Pr\{\mathcal{E}_2^c|\mathcal{E}_1\})(H(S) + \epsilon_1) + \epsilon_1 + \epsilon_2$.

Here, as $n \to \infty$, $\Pr\{\mathcal{E}_1^c\} \to 0$, and $\Pr\{\mathcal{E}_2^c|\mathcal{E}_1\}) \to 0$ when we select

$$
\begin{aligned}
R_u &= I(U; S) + \epsilon_3 \qquad (26) \\
R_u &\leq I(U; Y), \qquad (27)
\end{aligned}
$$

where the first condition makes encoding error arbitrarily small (also known as mutual covering lemma), and the second one allows decoding U^n using joint typicality with Y^n given that there is no encoding error, i.e., U^n, S^n are jointly typical and generates Y^n. This shows that $\frac{1}{n} I(S^n; Y^n) \geq I(S; Y, U) - \hat{\epsilon}_1 \geq R_a - \hat{\epsilon}_1$, i.e., any $R_a \leq I(S; Y, U)$ is achievable.

We now derive the achievable leakage rate expression for this scheme.

$$
\begin{aligned}
&\tfrac{1}{n} I(S^n; Z^n) \\
&\overset{(a)}{\leq} \frac{1}{n} I(S^n; Z^n, U^n|\mathcal{E}_1) + H(S)\Pr\{\mathcal{E}_1^c\} \\
&\overset{(b)}{\leq} (H(S) + \epsilon_1) - (H(S|Z, U) - \epsilon_2) + H(S)\Pr\{\mathcal{E}_1^c\} \\
&\overset{(c)}{=} I(S; Z, U) + \hat{\epsilon}_2
\end{aligned}
$$

where in (a) we included the U^n chosen at the encoder, (b) follows as $H(S^n|\mathcal{E}_1)$ is upper bounded by $n(H(S)+\epsilon_1)$ and $H(S^n|Z^n,U^n,\mathcal{E}_1)$ is lower bounded by $n(H(S|Z,U)-\epsilon_2)$, which can be shown by using the event that U^n,S^n,Z^n are jointly typical w.h.p., and in (c) we define $\hat{\epsilon}_2 \triangleq \epsilon_1+\epsilon_2+H(S)\Pr\{\mathcal{E}_1^c\}$. Noting that $\hat{\epsilon}_2\to 0$ as $n\to\infty$ concludes the proof as $\frac{1}{n}I(S^n;Z^n)\le I(S;Z,U)+\hat{\epsilon}_2\le R_l+\hat{\epsilon}_2$, i.e., any $R_l\ge I(S;Z,U)$ is achievable. Along the same lines, one can similarly obtain that any $R_l\ge I(U,S;Z)$ is achievable. ■

Appendix B
Proof of Proposition 2

Proof: (The full analysis is provided in [17], the following provides a sketch.) Fix $p(u,x|s)$, and consider s^n is the state sequence of the channel that is non-causally known at the encoder. We generate $2^{n(R_u+R'_u)}$ codewords denoted by $U^n(w_u,w'_u)$ each distributed according to $\prod_{i=1}^{n}p(u_i)$, where $w_u\in\{1,\cdots,2^{nR_u}\}$ and $w'_u\in\{1,\cdots,2^{nR'_u}\}$. We also list all the typical S^n sequences with two indices $S^n(w_u,w_r)$.

For the given s^n sequence, if it is a typical sequence the encoder identify it as $s^n(k,l)$, otherwise arbitrary indices are chosen. Encoder then finds the index $m\in\{1,\cdots,2^{nR'_u}\}$, such that $u^n(k,m)$ and $s^n(k,l)$ are jointly typical. If no such codeword exists, an arbitrary sequence is picked. The encoder sends x^n generated by $\prod_{i=1}^{n}p(x_i|u_i(k,m),s_i(k,l))$. Denote $\mathcal{E}_1$ is the event that S^n is a typical sequence, and $\mathcal{E}_2$ is the event that U^n is decoded given Y^n using joint typicality decoder. Here, we select [1]

$$\begin{aligned} R'_u &= I(U;S)+\epsilon_1 \\ R_u &= \min\{I(U;Y)-I(U;S)-\epsilon_1, H(S|U,Y)-\epsilon_1\}, \end{aligned}$$

so that $\Pr\{\mathcal{E}_1^c\}\to 0$ and $\Pr\{\mathcal{E}_2^c|\mathcal{E}_1\}\to 0$, as $n\to\infty$. with some $\epsilon_1\to 0$ as $n\to\infty$. We derive the achievable amplification rate as follows.

$$\begin{aligned} &\tfrac{1}{n}I(S^n;Y^n) \\ &\overset{(a)}{\ge} \frac{1}{n}I(S^n;Y^n|\mathcal{E}_1,\mathcal{E}_2)-\epsilon \\ &= \frac{1}{n}I(S^n(K,L);Y^n,U^n(K,M)|\mathcal{E}_1,\mathcal{E}_2)-\epsilon \\ &= \frac{1}{n}H(S^n(K,L)|\mathcal{E}_1,\mathcal{E}_2) \\ &\quad -\frac{1}{n}H(S^n(K,L)|U^n(K,M),\mathcal{E}_1,\mathcal{E}_2) \\ &\quad +\frac{1}{n}H(Y^n|U^n(K,M),\mathcal{E}_1,\mathcal{E}_2) \\ &\quad -\frac{1}{n}H(Y^n|S^n(K,L),U^n(K,M),\mathcal{E}_1,\mathcal{E}_2)-\epsilon \\ &\overset{(b)}{\ge} R_u+R_r-R_r+I(U;S)-\epsilon_1 \\ &\quad +(H(Y|U)-\epsilon_2)-(H(Y|U,S)+\epsilon_3)-\epsilon \\ &= \min\{H(S),I(U,S;Y)\}-\hat{\epsilon}_1 \end{aligned}$$

where in (a) we used the event $\mathcal{E}_1$, and $\mathcal{E}_2$, (b) follows as $H(S^n(K,L)|\mathcal{E}_1,\mathcal{E}_2)=n(R_u+R_r)$

$H(S^n(K,L)|U^n(K,M),\mathcal{E}_1,\mathcal{E}_2)\le n(R_r-I(U;S)+\epsilon_1)$

$H(Y^n|U^n(K,M),\mathcal{E}_1,\mathcal{E}_2)\ge n(H(Y|U)-\epsilon_2)$

$H(Y^n|S^n(K,L),U^n(K,M),\mathcal{E}_1,\mathcal{E}_2)\le n(H(Y|S,U)+\epsilon_3)$, where $\epsilon_2,\epsilon_3\to 0$ as $n\to\infty$. (Please refer to [17].)

This shows that $\frac{1}{n}I(S^n;Y^n)\ge\min\{H(S),I(U,S;Y)\}-\hat{\epsilon}_1\ge R_a-\hat{\epsilon}_1$, i.e., any

$$R_a\le\min\{H(S),I(U,S;Y)\} \tag{28}$$

is achievable.

We bound $\frac{1}{n}I(S^n;Z^n)$ following the previous proof, but here we consider and single letterize $I(U^n(K,M),S^n(K,L);Z^n|\mathcal{E}_1)$ instead of $I(S^n;Z^n,U^n|\mathcal{E}_1)$. ■

References

[1] S. Gel'fand and M. Pinsker, "Coding for channels with random parameters," *Probl. Contr. and Inform. Theory*, vol. 9, no. 1, pp. 19–31, 1980.

[2] H. Delfs and H. Knebl, *Introduction to Cryptography: Principles and Applications*, 2nd ed. Springer, 2007.

[3] O. Goldreich, *Foundations of Cryptography: Volume II, Basic Applications*. Cambridge University Press, 2004.

[4] J. Mitola III and G. Q. Maguire Jr., "Cognitive radio: making software radios more personal," *IEEE Personal Commun. Mag.*, vol. 6, no. 4, pp. 13–18, Aug. 1999.

[5] J. Mitola III, "Cognitive radio: an integrated agent architecture for software defined radio," Ph.D. dissertation, Computer Communication System Laboratory, Department of Teleinformatics, Royal Institute of Technology (KTH), Stockholm, Sweden, May 2000.

[6] N. Devroye, P. Mitran, and V. Tarokh, "Achievable rates in cognitive radio channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 1813–1827, May 2006.

[7] M. H. M. Costa, "Writing on dirty paper," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 439–441, May 1983.

[8] A. Wyner, "The Wire-tap Channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[9] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[10] Y. Chen and A. J. H. Vinck, "Wiretap Channel With Side Information," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 395–402, Jan. 2008.

[11] C. Mitrpant, A. J. H. Vinck, and Y. Luo, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2181–2190, May 2006.

[12] A. Sutivong, M. Chiang, T. M. Cover, and Y.-H. Kim, "Channel capacity and state estimation for state-dependent Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1486–1495, 2005.

[13] Y.-H. Kim, A. Sutivong, and T. M. Cover, "State Amplification," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 1850–1859, 2008.

[14] N. Merhav and S. Shamai, "Information Rates Subject to State Masking," *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2254–2261, 2007.

[15] J. Körner and K. Marton, "A source network problem involving the comparison of two channels ii," *Trans. Colloquim Inform. Theory, Keszthely, Hungary, August*, 1975.

[16] ——, "Comparison of two noisy channels," *Topics in Information Theory (Second Colloq., Keszthely, 1975). Amsterdam: North-Holland*, pp. 411–423, 1977.

[17] O. O. Koyluoglu, R. Soundararajan, and S. Vishwanath, "State amplification under masking constraints," in submission.

[18] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 22, no. 1, 1976.

[19] C. Heegard and A. E. Gamal, "On the capacity of computer memory with defects," *IEEE Trans. Inf. Theory*, vol. 29, no. 5, pp. 731–739, 1983.

[20] A. V. Kuznetsov and B. S. Tsybakov, "Coding in a memory with defective cells," *Probl. Pered. Inform.*, vol. 10, no. 2, pp. 52–60, 1974.