Secret Communication on Interference Channels

Roy D. Yates
WINLAB
Rutgers University
email: *ryates@winlab.rutgers.edu*

David Tse
Wireless Foundations
UC Berkeley
email: *dtse@eecs.berkeley.edu*

Zang Li
WINLAB
Rutgers University
email: *zang@winlab.rutgers.edu*

***Abstract*—We examine secret communication over interference channels, starting with a model in which communication is *semi-secret* in that secrecy may depend on other transmitters to follow an agreed-upon signaling strategy. We compare this to *robustly-secret* communication, in which each user must allow for other users to deviate unilaterally from an agreed-upon strategy to enable better overhearing, as long as that alternate strategy impairs neither the secrecy rate of its own link nor the reliability of any other communicating links. For a particular two-user binary expansion deterministic interference channel, we find and compare the semi-secret and robustly-secret capacity regions.**

I. Introduction

In the traditional setting of information-theoretic secret communication, a transmitter wishes to communicate reliably but secretly to a receiver at a specified rate in the presence of an overhearing eavesdropper. Building on the fundamental contributions of Wyner [1] and Csiszár and Körner [2], there has been a burst of recent work on secret communication over wireless channels. Directly relevant to this work are those papers on multiuser channels, including multiple access [3], [4], relay [5], interference [6], and broadcast [7] channels.

In a wireless setting, the interference channel in which independent transmitter-receiver pairs wish to communicate reliably and secretly is of particular importance. Each transmitter i must encode its messages so that only the corresponding receiver i can decode the messages. The receiver of any link $j \neq i$ is not permitted to resolve more than arbitrarily little information regarding the communication on link i.

Because receiver j must also decode its own messages, the secrecy afforded to link i from an eavesdropping receiver j may depend on the signaling employed on link j as well as on other links. For example, in a 2-user Gaussian interference channel, if transmitter 2 is silent, then receiver 2 can act as a traditional eavesdropper of link 1. Similarly, over a DMC, user 2 may choose to transmit a particular symbol that best "opens" the channel for eavesdropping. On the other hand, if transmitter 2 sends at a nonzero rate, then this signal can interfere with the eavesdropping ability of receiver 2. That is, the rate at which user 1 can communicate secretly will depend on the signaling strategy of user 2.

In this case of multiple communication links, the enforcement of a secrecy requirement at a receiver suffers from an asymmetry of trust. Explicit in a receiver secrecy constraint is that the link i transmitter and receiver do not trust the link j receiver. Nevertheless, if secrecy on link i depends on the signaling employed on link j, then the link i user implictly trusts the link j user will not have its transmitter deviate to a signaling strategy that facilitates better overhearing.

Stronger secrecy definitions would ensure secrecy even if link j deviates from its signaling strategy. Thus this work examines secret communication over interference channels, starting with a model in which communication is *semi-secret* in that secrecy may depend on trusting other transmitters. In fact, semi-secret is the prevailing model for multiuser secret communication [4]–[8]. Here we compare semi-secrecy to *robustly-secret* communication in which user i must account for the possibility that user j will deviate from an agreed-upon strategy to enable better overhearing as long as that alternate strategy does not impair the secrecy rate of link j nor the reliability of any other communicating links.

While a complete characterization of semi-secret or robustly-secret rate regions for interference channels remains elusive, this work does find the robust-secrecy capacity for a binary expansion deterministic interference channel in the class of channels introduced in [9]. In the context of a converse result, an additional contribution of this work is the development of methods for evaluating robustly-secret strategies in the absence of a single-letter characterization.

II. System Model and Definitions

To formalize these ideas, we consider a discrete memoryless interference channel with two communication links. Each transmitter $i \in \{1,2\}$ produces input $x_i \in \mathcal{X}_i$ for each channel use and each receiver i observes the output $y_i \in \mathcal{Y}_i$ of a discrete memoryless channel $P_{Y_1,Y_2|X_1,X_2}(y_1,y_2|x_1,x_2)$. Each transmitter i communicates by coding over blocks of n_i symbols. Transmitter i communicates in block t a message $\mathbf{W}_i^{(t)} = [w_{i,1}^{(t)},\ldots,w_{i,l_i}^{(t)}]$, a sequence of l_i independent equiprobable bits, to receiver i by transmitting a codeword denoted by the vector $\mathbf{x}_i^{(t)} = [x_i^{(t)}(1),\ldots,x_i^{(t)}(n_i)]$ of n_i transmitted symbols. Given the observation vector $\mathbf{y}_i^{(t)} = [y_i^{(t)}(1),\ldots,y_i^{(t)}(n_i)]$, receiver i guesses the message bits $\hat{\mathbf{W}}_i^{(t)} = [\hat{w}_{i,1}^{(t)},\ldots,\hat{w}_{i,l_i}^{(t)}]$. Without loss of generality, we will assume receiver i employs maximum likelihood decoding on each bit $w_{i,l}^{(t)}$, i.e. chooses $\hat{w}_{i,l}^{(t)}$ that maximizes the *a posteriori probability* of the observed sequence $\mathbf{y}_i^{(1)},\mathbf{y}_i^{(2)},\ldots$ given the transmitted bit $w_{i,l}^{(t)}$.

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

Note that this communication scenario is more general than what is typical in multiuser information theory, as we allow the two users to code over different block lengths. However, such generality is necessary here, since even though the two users may agree *a priori* on a common block length, a self-interested user may unilaterally decide to choose a different block length during the actual communication process.

The encoding method on link i is represented by the signaling *strategy* s_i that defines

- the block length n_i,
- the code rate $R_i = l_i/n_i$,
- the codebook $\mathcal{C}_i$, the set of codewords $\mathbf{x}_i$ employed by transmitter i,
- the encoder $f_i : \{1, \ldots, M_i\} \times \Omega_i \rightarrow \mathcal{C}_i$ that maps the message $\mathbf{W}_i^{(t)}$ to a transmitted codeword $\mathbf{x}_i^{(t)} = f(\mathbf{W}_i^{(t)}, \omega_i^{(t)}) \in \mathcal{C}_i$,

We note that the encoder of transmitter i may employ a stochastic mapping from the block t message to the transmitted symbol sequence; $\omega_i^{(t)} \in \Omega_i$ representing the randomness in that mapping is assumed to be independent between transmitters and across different blocks and is only known at the respective transmitter and not at any receiver.

The communication strategy $\mathbf{s} = (s_1, s_2)$ defines a probability measure $P_{\mathbf{s}}(\cdot)$. As a function of the strategy $\mathbf{s}$, the bit error rate (BER) for block t of link i under strategy $\mathbf{s}$ is given by

$$\varepsilon_i^{(t)}(\mathbf{s}) = \frac{1}{l_i} \sum_{l=1}^{l_i} P_{\mathbf{s}}(\hat{w}_{i,l}^{(t)} \neq w_{i,l}^{(t)}). \tag{1}$$

Note that if the two users have different block lengths, the BER could vary from block to block even though each user employs the same encoding for all blocks. In this case, we measure the BER for user i by $\varepsilon_i(\mathbf{s}) = \max_t \varepsilon_i^{(t)}(\mathbf{s})$. We measure the reliability of a communication strategy $\mathbf{s}$ by the maximum BER $\varepsilon(\mathbf{s}) = \max_i \varepsilon_i(\mathbf{s})$. When $\varepsilon(\mathbf{s}) = \epsilon$, we say that $\mathbf{s}$ is a $(1-\epsilon)$ *reliable strategy*. When all users i agree on a common block length $n_i = n$, we say that $\mathbf{s} = (s_1, s_2)$ is a *block synchronous* strategy for the system. In this case, the error probability $\varepsilon_i^{(t)}(\mathbf{s}) = \varepsilon_i(\mathbf{s})$ for user i is the same across all blocks.

In the traditional setting, a receiver j is simply a passive eavesdropper on the communication of link i, and the secrecy-capacity requirement is that there exists a rate R_i encoding strategy s_i such that normalized information leakage $I(\mathbf{W}_i; \mathbf{Y}_j)/n$ can be made arbitrarily small. However, in the context of multiple transmitters, the leakage depends on the strategy $\mathbf{s}$. Thus we define the strategy-dependent information leakage

$$L_{i \rightarrow j}(\mathbf{s}) = I(\mathbf{W}_i; \mathbf{Y}_j)/n \tag{2}$$

associated with communication link i being overheard at receiver j. With more than two users, the secrecy of link i would then be measured by $L_i(\mathbf{s}) = \max_{j \neq i} L_{i \rightarrow j}(\mathbf{s})$. With only two users, $L_i(\mathbf{s}) = L_{i \rightarrow j}(\mathbf{s})$ for that user $j \neq i$; however, we preserve the (redundant) notation $L_{i \rightarrow j}(\mathbf{s})$ as a reminder of the direction of the information leakage. Given a strategy $\mathbf{s}$, the secrecy over all links is measured by

$$L(\mathbf{s}) = \max_i L_i(\mathbf{s}). \tag{3}$$

Definition 1: The rate vector $\mathbf{R}$ is *semi-secret* if given any $\epsilon > 0$ there exists a rate $\mathbf{R}$ strategy $\mathbf{s}$ such that $\varepsilon(\mathbf{s}) \leq \epsilon$ and $L(\mathbf{s}) \leq \epsilon$.

We note that Definition 1 is called semi-secret precisely because the link i transmitter and receiver trust the link j transmitter to stick to the nominal strategy. A stronger secrecy definition would ensure secrecy even if link j deviates to a strategy that facilitates better overhearing. However, we wish to distinguish between strategies of user j that compromise the secrecy of link i as opposed to jamming strategies that interfere with the reliability of link i.

Definition 2: The rate vector $\mathbf{R}$ is *robustly-secret* if given any $\epsilon > 0$ there exists a rate $\mathbf{R}$ strategy $\mathbf{s}$ such that $\varepsilon(\mathbf{s}) \leq \epsilon$ and $L(\mathbf{s}) \leq \epsilon$, and

(a) $L_{1 \rightarrow 2}(s_1, s_2') \leq \epsilon$ for all user 2 strategies s_2' such that (s_1, s_2') is a rate $\mathbf{R}$ strategy with $\varepsilon(s_1, s_2') \leq \epsilon$ and $L_{2 \rightarrow 1}(s_1, s_2') \leq \epsilon$,
(b) and vice-versa for user 1.

We note that this definition of robust secrecy incorporates the requirements of semi-secrecy but in addition allows unilateral strategy deviations by user j that injure the information leakage but *not* the reliability of link i nor cause any reduction in the rate, reliability, and secrecy of its own link. Such users have been called "nice but curious" in [10]. Consequently, a robust strategy for user $i \neq j$ must preserve its secrecy in the event that user j chooses such an alternative strategy.

With respect to both definitions of secrecy, we define the secrecy capacity region $\mathcal{R}$ to be the closure of the set of all rate pairs (R_1, R_2) such that for every $\epsilon > 0$, there exists a block length n and a $(1-\epsilon)$-reliable block-synchronous strategy pair (s_1, s_2) that achieves the rate pair (R_1, R_2).

The careful reader may note that while we allow users to code over different block-lengths, we restrict users to block-synchronous strategies in the definition of $\mathcal{R}$. We argue there is no loss in this assumption. First, we claim that if there is a $(1-\epsilon)$-reliable strategy pair (s_1, s_2) that achieves a rate pair (R_1, R_2) using block lengths n_1, n_2, then there exists a block-synchronous $(1-\epsilon)$ strategy pair that achieves the same rate pair. This follows by considering "super-blocks" of length n equal to the least common multiple of n_1 and n_2. Over these super-blocks, the users can be viewed as using two equal-length codes. The bit error rates, being the average bit error probabilities across the super-block, remain less than ϵ. Thus in computing the capacity region $\mathcal{R}$, we can consider only strategies in which both users employ the same block length.

We observe that the definitions imply for any channel that

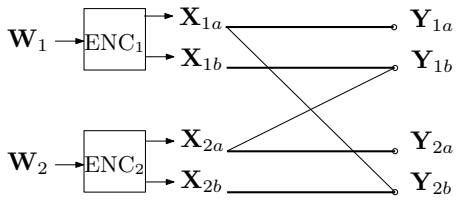

Fig. 1. A Two-Sided Deterministic Interference Channel

the robustly-secret rate region $\mathcal{R}_{\text{robust}}$ is contained in the semi-secret rate region $\mathcal{R}_{\text{semi}}$; however, to say more we must work with specific channel instances. For clarity, we focus now on a particular two-user deterministic interference channel (DIC). We look to identify secret communication strategies that combat opportunistic consequence-free eavesdropping by either user.

III. A Two-User Two-Sided DIC

Now we consider the two-user deterministic interference channel of Figure 1 in which user i controls inputs X_{ia} and X_{ib}. The users observe the corresponding outputs

$$Y_{1a} = X_{1a}, \qquad Y_{2a} = X_{2a}, \tag{4}$$

$$Y_{1b} = X_{1b} + X_{2a}, \qquad Y_{2b} = X_{2b} + X_{1a}, \tag{5}$$

under mod 2 addition. For non-secret capacity, this channel is a special case of the deterministic channels in [11] and the capacity region given by [11, equations (7)-(11)] reduces to

$$\mathcal{R}_{\text{DIC}} = \{(R_1, R_2) | R_1 \geq 0, R_2 \geq 0, R_1 + R_2 \leq 2\}. \tag{6}$$

The same rate region is also achievable under semi-secrecy using time-sharing and uncoded transmissions. In particular, in mode 1, user 1 transmits independent equiprobable binary data bits X_{1a} and X_{1b} while user 2 sends $X_{2a} = 0$, (silence on the a-level input) and equiprobable binary noise X_{2b} on the b-level input. Silence on X_{2a} allows user 1 to communicate 1 bit with the b-level input reliably and also secretly because user 2 has no observation of this input. In addition user 1 transmits 1 bit reliably with the a-level input because user 2 is self-deafening the Y_{2b} receiver through the transmission of noise on X_{2b}. Thus mode 1 enables reliable and secret communication at rate $(R_1, R_2) = (2, 0)$. In mode 2, the roles are reversed and we obtain the rate $(R_1, R_2) = (0, 2)$. Using mode i for a fraction of time r_i, we obtain the rates $(R_1, R_2) = 2(r_1, r_2)$ for all $r_1 + r_2 \leq 1$ and thus $\mathcal{R}_{\text{DIC}} \subseteq \mathcal{R}_{\text{semi}}$. Moreover, as any semi-secret achievable rate must be in the non-secret capacity region, $\mathcal{R}_{\text{semi}} = \mathcal{R}_{\text{DIC}}$.

To characterize the robustly-secret capacity region, we work with the n-symbol block inputs $\mathbf{X}_{1a} = [X_{1a}(1), \ldots, X_{1a}(n)]$ and $\mathbf{X}_{1b} = [X_{1b}(1), \ldots, X_{1b}(n)]$. Similarly, user 2 signals with the block inputs $\mathbf{X}_{2a}$ and $\mathbf{X}_{2b}$ as shown in Figure 1. Given a message $\mathbf{W}_i$ to communicate, the user i encoder generates $\mathbf{X}_{ia} = f_{ia}(\mathbf{W}_i, \omega_i)$ and $\mathbf{X}_{ib} = f_{ib}(\mathbf{W}_i, \omega_i)$, where ω_i denotes any randomness in the encoder mapping.

The interference channel of Figure 1 is a simple example of a binary expansion deterministic interference channel introduced in [9]. We note that labeling each user's inputs as a and b goes beyond mere convenience. For each sender, the a input causes interference at the corresponding eavesdropping receiver. In the parlance of [9], the signals X_{1a} and X_{2a} are *above* the noise floor at the corresponding eavesdropper while the signals X_{1b} and X_{2b} are *below* the noise floor. In the channel of Figure 1, each user exposes its a-level symbols to its corresponding eavesdropper. Thus each sender may well wish to employ a stochastic encoder for secrecy. We cannot conclude yet that there is no benefit to the b-level signal in that stochastic mapping. In addition, each user may wish to transmit correlated a-level and b-level inputs. As a result, even though this deterministic interference channel is simple, the evaluation of robustly-secret strategies is nontrivial.

A rate $\mathbf{R}$ strategy $\mathbf{s} = (s_1, s_2)$ is characterized by four parameters: the information rates $I(\mathbf{W}_1; \mathbf{Y}_{1a}, \mathbf{Y}_{1b})/n$ and $I(\mathbf{W}_2; \mathbf{Y}_{2a}, \mathbf{Y}_{2b})/n$, and the leakage rates $L_{1\to 2}(\mathbf{s}) = I(\mathbf{W}_1; \mathbf{Y}_{2a}\mathbf{Y}_{2b})/n$ and $L_{2\to 1}(\mathbf{s}) = I(\mathbf{W}_2; \mathbf{Y}_{1a}, \mathbf{Y}_{1b})/n$. For the semi-secret rate $\mathbf{R}$ strategy (s_1, s_2), the reliable decoding constraint $\varepsilon(s_1, s_2) \leq \epsilon$ implies each user i is subject to the Fano bound $H(\mathbf{W}_i | \mathbf{Y}_{ia}, \mathbf{Y}_{ib}) \leq 1 + n\epsilon R_i$. Since $H(\mathbf{W}_i) = nR_i$, it follows that

$$\frac{I(\mathbf{W}_i; \mathbf{Y}_{ia}, \mathbf{Y}_{ib})}{n} \geq R_i(1 - \epsilon) - \frac{1}{n}. \tag{7}$$

Given a semi-secret rate $\mathbf{R}$ strategy in which $\mathbf{X}_{2a}$ and $\mathbf{X}_{2b}$ may be dependent, our approach will be to show that user 2 can switch to a new policy s_2' in which inputs X_{2a} and X_{2b} are independent, without penalty to the rate and secrecy of user 2 but with improved eavesdropping on user 1. Of course, given the channel symmetry, user 1 can make the same switch and this will be reflected in the secrecy capacity region.

The idea of strategy s_2' is for user 2 to code over m uses of the n-symbol blocks with independent messages $\tilde{\mathbf{W}}_{2a}$ and $\tilde{\mathbf{W}}_{2b}$ communicated in nm channel uses. That is, under s_2', user 2 has switched to a blocklength $n_i = nm$ while user 1 continues to communicate with the agreed-upon blocklength $n_1 = n$. However, by the design of strategy s_2', this switch will be invisible to user 1 who will continue to see for each block t an error probability $\varepsilon_1^{(t)}(s_1, s_2') = \varepsilon_1(s_1, s_2)$.

The message $\tilde{\mathbf{W}}_{2a}$ is transmitted using a stochastic encoder that employs m uses of the stochastic encoder $\mathbf{X}_{2a} = f_{2a}(\mathbf{W}_2, \omega_2)$. On the other hand, the message $\tilde{\mathbf{W}}_{2b}$ is transmitted using a deterministic encoder that employs m uses of the block input $\mathbf{X}_{2b}$. For the m blocks of blocks signaling, inputs are denoted by $\mathbf{X}_{1a}^m, \mathbf{X}_{1b}^m$ and $\mathbf{X}_{2a}^m, \mathbf{X}_{2b}^m$ with the corresponding outputs $\mathbf{Y}_{1a}^m, \mathbf{Y}_{1b}^m$ and $\mathbf{Y}_{2a}^m, \mathbf{Y}_{2b}^m$.

We start by identifying an upper bound that shows how the information rate of user 2 can be partitioned into contributions $I(\mathbf{W}_2; \mathbf{Y}_{2a})$ and $I(\mathbf{X}_{2b}; \mathbf{Y}_{2b})$. For the functional dependency graph (FDG) of Figure 2(a), we use the d-separation method of [12, Definition 1] to verify the Markov

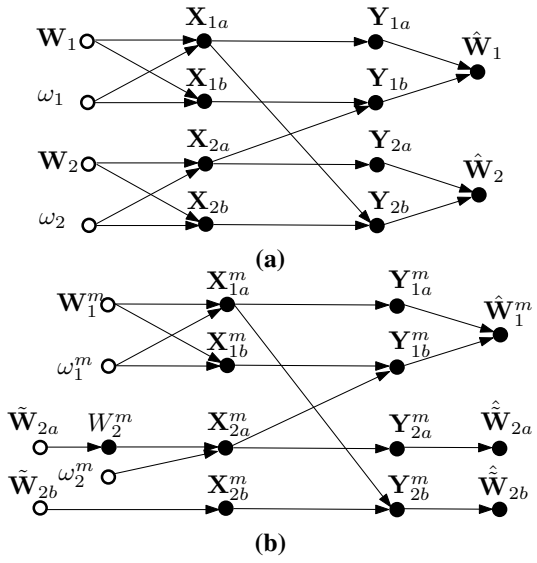

Fig. 2. Functional dependency graphs for (a) a general secret communication strategy (s_1, s_2) and (b) the block-of-blocks strategy (s_1, s_2') for the two-sided interference channel of Figure 1.

chain $\mathbf{W}_2\mathbf{Y}_{2a}$—$\mathbf{X}_{2b}$—$\mathbf{Y}_{2b}$, implying

$$I(\mathbf{X}_{2b};\mathbf{Y}_{2b}) \geq I(\mathbf{W}_2,\mathbf{Y}_{2a};\mathbf{Y}_{2b}) \quad (8)$$
$$= I(\mathbf{Y}_{2a};\mathbf{Y}_{2b}) + I(\mathbf{W}_2;\mathbf{Y}_{2b}|\mathbf{Y}_{2a}) \quad (9)$$
$$\geq I(\mathbf{W}_2;\mathbf{Y}_{2b}|\mathbf{Y}_{2a}). \quad (10)$$

It follows that

$$I(\mathbf{W}_2;\mathbf{Y}_{2a},\mathbf{Y}_{2b}) = I(\mathbf{W}_2;\mathbf{Y}_{2a}) + I(\mathbf{W}_2;\mathbf{Y}_{2b}|\mathbf{Y}_{2a}) \quad (11)$$
$$\leq I(\mathbf{W}_2;\mathbf{Y}_{2a}) + I(\mathbf{X}_{2b};\mathbf{Y}_{2b}). \quad (12)$$

We will show that user 2's information rate can achieve the upper bound (12) under a strategy s_2', that employs independent inputs X_{2a} and X_{2b} with codebooks $\mathcal{C}_{2a}$ and $\mathcal{C}_{2b}$. Codebook $\mathcal{C}_{2a}$ has $2^{mR_{2a}}$ codewords of the form $\mathbf{W}_2^m = [\mathbf{W}_2(1),\ldots,\mathbf{W}_2(m)]$, each consisting of m iid samples of $\mathbf{W}_2$. The message $\tilde{\mathbf{W}}_{2a}$, an iid sequence of mR_{2a} bits representing the binary expansion of an index $\tilde{w}_{2a}$, is communicated by selecting a codeword $\tilde{w}_{2a}$ from $\mathcal{C}_{2a}$. This results in the transmission of the block of blocks input signal $\mathbf{X}_{2a}^m = [\mathbf{X}_{2a}(1),\ldots,\mathbf{X}_{2a}(m)]$ where the kth block is given by the stochastic mapping $\mathbf{X}_{2a}[k] = f_{2a}(\mathbf{W}_2[k],\omega_2[k])$.

On the X_{2b} channel, we observe that the original strategy s_2 defines a PMF $P_{2b}(\mathbf{x}) = P\{\mathbf{X}_{2b} = \mathbf{x}\}$ on length n input vectors $\mathbf{X}_{2b}$. The $\mathcal{C}_{2b}$ codebook has $2^{mR_{2b}}$ codewords of the form $\mathbf{X}_{2b}^m = [\mathbf{X}_{2b}(1),\ldots,\mathbf{X}_{2b}(m)]$, each consisting of m iid samples of $\mathbf{X}_{2b}$ drawn from the PMF $P_{2b}(\mathbf{x})$. Now under strategy s_2', user 2 sends the message $\tilde{\mathbf{W}}_{2b}$, an iid sequence of mR_{2b} bits representing the binary expansion of an index $\tilde{w}_{2b}$, is communicated by sending a codeword $\tilde{w}_{2b}$ from $\mathcal{C}_{2b}$. The properties of the new strategy $\mathbf{s}' = (s_1, s_2')$ are summarized in the following lemma. The proof appears in the appendix.

Lemma 1: Under strategy $\mathbf{s}' = (s_1, s_2')$:

(a) User 1 communicates reliably: $\varepsilon_1(\mathbf{s}) = \varepsilon_1(\mathbf{s}')$.

(b) User 2 achieves reliable communication at rate $\tilde{R}_2 \geq R_2 - \epsilon$ for arbitrarily small ϵ.

(c) The leakage rate from user 2 to user 1 is unchanged: $L_{2\to1}(\mathbf{s}') = L_{2\to1}(\mathbf{s})$.

(d) For any $\delta > 0$, there exists block length n such that the leakage from user 1 to user 2 satisfies

$$L_{1\to2}(\mathbf{s}') \geq I(\mathbf{W}_1;\mathbf{X}_{1a})/n - \delta \quad (13)$$

The key in Lemma 1 is the lower bound (13). As robust secrecy requires user 1 adopt a policy s_1 such that $L_{1\to2}(\mathbf{s}') \leq \epsilon$ for all s_2', (13) implies for all $\epsilon, \delta > 0$ that

$$\frac{I(\mathbf{W}_1;\mathbf{X}_{1a})}{n} \leq \epsilon + \delta. \quad (14)$$

By using a deterministic encoder for the input X_{2b}, receiver 2 can decode the message $\tilde{\mathbf{W}}_{2b}$, and then learn and subtract the b-level input $\mathbf{X}_{2b}^m$ and thus get a clean look at $\mathbf{X}_{1a}^m$. Thus, the information communicated by user 1 through the X_{1a} input must be arbitrarily small. That is, under robust secrecy, the signal X_{1a} that is "above the noise floor" at the eavesdropper is rendered useless.

By the symmetry of the communication channels, we observe that a semi-secret strategy (s_1, s_2) also allows user 1 to switch to a strategy s_1' that matches the s_2' strategy of user 2. Under s_1', inputs X_{1a} and X_{1b} are independent with a deterministic encoder used for the b-level input. It follows receiver 1 gets a clean look at X_{2a} and that the input X_{2a} is similarly rendered useless for user 2 under robust secrecy.

It then follows straightforwardly that robustly-secret rates must satisfy $R_i \leq 1$ for $i = 1, 2$. Moreover, the strategy (s_1, s_2) in which each user i transmit zeroes on the a-level input and uncoded secret information bits on the b-level input is a robustly-secret strategy that achieves rates $R_1 = R_2 = 1$. These facts imply the following.

Theorem 1: The robustly-secret capacity region for the deterministic interference channel of Figure 1 is

$$\mathcal{R}_{\text{robust}} = \{(r_1, r_2) | 0 \leq r_1 \leq 1, 0 \leq r_2 \leq 1\}. \quad (15)$$

While the reader may view Theorem 1 as the "expected result," this example does suggest that semi-secret formulations of multiuser secret communication problems are perhaps overly optimistic. This work also demonstrates that it may well be possible to identify meaningful outer bounds to robustly-secret rate regions in the absence of a single-letter characterization of the semi-secret capacity region.

Acknowledgments: This work was supported by NSF grants ITR-0326503 and CNS-0721826. In addition, this work has benefited from convergence on a common game-theoretic

formulation for interference channels that also appears in [13], which studies strategic games on interference channels.

APPENDIX

Proof: Lemma 1

(a) The marginal joint distribution of the user 1 signals $\mathbf{X}_{1a}, \mathbf{X}_{1b}$ and $\mathbf{Y}_{1a}, \mathbf{Y}_{1b}$ remains unchanged by the switch to strategy $\mathbf{s}' = (s_1, s_2')$. As the error probability for user 1 depends only on this marginal joint distribution, $\varepsilon_1(\mathbf{s}) = \varepsilon_1(\mathbf{s}')$.

(b) The codebook construction implies that message $\tilde{\mathbf{W}}_{2a}$ can be transmitted reliably at rate $R_{2a} = I(\mathbf{W}_2; \mathbf{Y}_{2a}) - \epsilon$ for arbitrarily small $\epsilon > 0$. Similarly, the message $\tilde{\mathbf{W}}_{2b}$ can be transmitted reliably at rate $R_{2b} = I(\mathbf{X}_{2b}; \mathbf{Y}_{2b}) - \epsilon$. We note that rates R_{2a} and R_{2b} are in bits per n-symbol block. Hence the strategy $\mathbf{s}'$ can communicate reliably at a rate

$$\tilde{R}_2 = \frac{R_{2a} + R_{2b}}{n} \tag{16}$$

$$= \frac{I(\mathbf{W}_2; \mathbf{Y}_{2a}) + I(\mathbf{X}_{2b}; \mathbf{Y}_{2b}) - 2\epsilon}{n} \tag{17}$$

bits per channel use. It follows from (12) and (7) that under strategy $\mathbf{s}'$, user 2 achieves the rate

$$\tilde{R}_2 \geq \frac{I(\mathbf{W}_2; \mathbf{Y}_{2a}, \mathbf{Y}_{2b}) - 2\epsilon}{n} \tag{18}$$

$$\geq R_2(1-\epsilon) - \frac{1+2\epsilon}{n} \tag{19}$$

As $\epsilon \to 0$ with increasing block length n, $\mathbf{s}'$ is a rate $\mathbf{R} = (R_1, R_2 - \epsilon)$ reliable strategy.

(c) Under strategy $\mathbf{s}'$, we observe that independence of $\tilde{\mathbf{W}}_{2b}$ and the collection $(\tilde{\mathbf{W}}_{2a}, \mathbf{Y}_{1a}^m, \mathbf{Y}_{1b}^m)$ implies that $I(\tilde{\mathbf{W}}_{2b}; \mathbf{Y}_{1a}^m \mathbf{Y}_{1b}^m | \tilde{\mathbf{W}}_{2a}) = 0$ and thus by the chain rule,

$$L_{2\to1}(\mathbf{s}') = I(\tilde{\mathbf{W}}_{2a}, \tilde{\mathbf{W}}_{2b}; \mathbf{Y}_{1a}^m, \mathbf{Y}_{1b}^m)/(nm) \tag{20}$$

$$= I(\tilde{\mathbf{W}}_{2a}; \mathbf{Y}_{1a}^m, \mathbf{Y}_{1b}^m)/(nm) \tag{21}$$

$$= I(\mathbf{W}_2^m; \mathbf{Y}_{1a}^m, \mathbf{Y}_{1b}^m)/(nm) \tag{22}$$

$$= I(\mathbf{W}_2; \mathbf{Y}_{1a}, \mathbf{Y}_{1b})/n \tag{23}$$

$$= L_{2\to1}(s_1, s_2). \tag{24}$$

Note that (22) is an equality because of the deterministic bijective mapping from $\tilde{\mathbf{W}}_{2a}$ to the codeword in $\mathcal{C}_{2a}$.

(d) Lastly we consider the leakage from user 1 under m block channel uses. As user 1 has transmitted m messages $\mathbf{W}_1^m = [\mathbf{W}_1(1), \ldots, \mathbf{W}_1(m)]$, the leakage is

$$L_{1\to2}(\mathbf{s}') = \frac{I(\mathbf{W}_1^m; \mathbf{Y}_{2a}^m, \mathbf{Y}_{2b}^m)}{nm} \geq \frac{I(\mathbf{W}_1^m; \mathbf{Y}_{2b}^m)}{nm}. \tag{25}$$

Applying the chain rule both ways to $I(\mathbf{W}_1^m; \tilde{\mathbf{W}}_{2b} \mathbf{Y}_{2b}^m)$ and noting the independence of $\mathbf{W}_1^m$ and $\tilde{\mathbf{W}}_{2b}$ implies $I(\mathbf{W}_1^m; \tilde{\mathbf{W}}_{2b}) = 0$ yields

$$I(\mathbf{W}_1^m; \mathbf{Y}_{2b}^m) = I(\mathbf{W}_1^m; \mathbf{Y}_{2b}^m | \tilde{\mathbf{W}}_{2b}) - I(\mathbf{W}_1^m; \tilde{\mathbf{W}}_{2b} | \mathbf{Y}_{2b}^m). \tag{26}$$

The deterministic mapping from $\tilde{\mathbf{W}}_{2b}$ to $\mathbf{X}_{2b}^m$ implies

$$I(\mathbf{W}_1^m; \mathbf{Y}_{2b}^m | \tilde{\mathbf{W}}_{2b}) = I(\mathbf{W}_1^m; \mathbf{Y}_{2b}^m | \tilde{\mathbf{W}}_{2b} \mathbf{X}_{2b}^m) \tag{27}$$

$$= H(\mathbf{Y}_{2b}^m | \tilde{\mathbf{W}}_{2b} \mathbf{X}_{2b}^m) - H(\mathbf{Y}_{2b}^m | \mathbf{W}_1 \tilde{\mathbf{W}}_{2b} \mathbf{X}_{2b}^m). \tag{28}$$

Substituting $\mathbf{Y}_{2b}^m = \mathbf{X}_{1a}^m + \mathbf{X}_{2b}^m$ in (28), we obtain

$$I(\mathbf{W}_1^m; \mathbf{Y}_{2b}^m | \tilde{\mathbf{W}}_{2b}) = H(\mathbf{X}_{1a}^m | \tilde{\mathbf{W}}_{2b} \mathbf{X}_{2b}^m) - H(\mathbf{X}_{1a}^m | \mathbf{W}_1^m \tilde{\mathbf{W}}_{2b} \mathbf{X}_{2b}^m). \tag{29}$$

Note that $H(\mathbf{X}_{1a}^m | \tilde{\mathbf{W}}_{2b} \mathbf{X}_{2b}^m) = H(\mathbf{X}_{1a}^m)$ by independence of $\mathbf{X}_{1a}^m$ and $\tilde{\mathbf{W}}_{2b}, \mathbf{X}_{2b}^m$. Further, as conditioning reduces entropy, we can write

$$I(\mathbf{W}_1^m; \mathbf{Y}_{2b}^m | \tilde{\mathbf{W}}_{2b}) \geq H(\mathbf{X}_{1a}^m) - H(\mathbf{X}_{1a}^m | \mathbf{W}_1^m) \tag{30}$$

$$= I(\mathbf{W}_1^m; \mathbf{X}_{1a}^m) \tag{31}$$

$$= mI(\mathbf{W}_1; \mathbf{X}_{1a}). \tag{32}$$

Next we observe that reliable decoding of the message $\tilde{\mathbf{W}}_{2b}$ via $\mathbf{Y}_{2b}^m$ implies by the Fano bound that

$$I(\mathbf{W}_1^m; \tilde{\mathbf{W}}_{2b} | \mathbf{Y}_{2b}^m) \leq H(\tilde{\mathbf{W}}_{2b} | \mathbf{Y}_{2b}^m) \leq 1 + m\epsilon R_{2b}. \tag{33}$$

Combining (25), (26), (32) and (33), we obtain

$$L_{1\to2}(\mathbf{s}') \geq \frac{mI(\mathbf{W}_1; \mathbf{X}_{1a}) - (1 + m\epsilon R_{2b})}{nm}. \tag{34}$$

This completes the proof of the lemma. □

REFERENCES

[1] A. Wyner. The wire-tap channel. *Bell. Syst. Tech. J.*, 54(8):1355–1387, January 1975.

[2] I. Csiszár and J. Körner. Broadcast channels with confidental messages. *IEEE Trans. Info. Theory*, 24(3):339–348, May 1978.

[3] R. Liu, I. Maric, R. Yates, and P. Spasojevic. The discrete memoryless multiple access channel with confidential messages. In *IEEE Int. Symp. Info. Theory*, pages 957 – 961, July 2006.

[4] E. Tekin and A. Yener. The general gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming. *IEEE Trans. Info. Theory*, submitted 2007. arXiv:cs/0702112.

[5] L. Lai and H. El Gamal. The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Trans. Information Theory*. submitted 2006.

[6] R. Liu, I. Maric, P. Spasojevic, and R. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. Info. Theory*, June 2008.

[7] R. Liu and H. V. Poor. Secrecy capacity region of a multi-antenna gaussian broadcast channel with confidential messages. *IEEE Trans. Info. Theory*, Submitted 2007.

[8] Y. Liang and V.H. Poor. Generalized multiple access channels with confidential messages. *IEEE Transactions on Information Theory*, submitted 2006. arXiv:cs/0605084v1.

[9] A. S. Avestimehr, S. Diggavi, and D. Tse. A deterministic approach to wireless relay networks. In *Proceedings of Allerton Conference*, 2007.

[10] L. Lima, M. Medard, and J. Barros. Random linear network coding: A free cypher? In *IEEE Intl. Symp. Info. Theory ISIT*, 2007.

[11] A. A. El Gamal and M. H. M. Costa. The capacity region of a class of deterministic interference channels. *IEEE Trans. Info. Theory*, 28(2):343–346, March 1982.

[12] G. Kramer. Capacity results for the discrete memoryless network. *IEEE Trans. on Inf. Theory*, 49:4–21, January 2003.

[13] R. Berry and D. Tse. Information theoretic games on interference channels. In *IEEE Intl. Symp. Info. Theory ISIT*, 2008.