

Wiretap Channel With Causal State Information and Secure Rate-Limited Feedback

Alejandro Cohen and Asaf Cohen
 Department of Communication Systems Engineering
 Ben-Gurion University of the Negev,
 Beer-Sheva, 84105, Israel
 Email: {alejandr,coasaf}@bgu.ac.il

Abstract—In this paper, we consider the secrecy capacity of a wiretap channel in the presence of causal state information and secure rate-limited feedback. In this scenario, the causal state information from the channel is available to both the legitimate transmitter and the legitimate receiver. In addition, the legitimate receiver can send secure feedback to the transmitter at a limited rate R_f .

We derive upper and lower bounds on the secrecy capacity and show that, when the channel to the eavesdropper is *degraded*, the bounds are tight and the secrecy capacity is completely characterised.

The capacity achieving scheme is based on Wyner, Csiszár and Körner wiretap coding and two steps of shared-key generation: one from the state information and one via the noiseless feedback. The upper bound is more involved and requires a non-trivial recursive lemma extending previous results in the literature to include both state and feedback. We conclude the paper by showing that a few interesting known results can be seen as special cases of the above, especially the case where the state information is available only at the decoder, and the suggested scheme achieves the secrecy capacity without a source of randomness at the decoder.

I. INTRODUCTION

The increasing demand for network connectivity and high data rates dictate efficient utilization of resources, such as the sharing of a common medium for communication. However, in many practical applications, it is important to assure privacy is not compromised. In some systems, cryptographic schemes can be used to protect data from eavesdropping. Yet, these schemes usually involve a computational burden. *Information theoretic security*, on the other hand, offers privacy at the price of transmission rate.

A canonical model in the context of channel coding was given by Wyner in [1]. Therein, the wiretap channel, described in Figure 1, was introduced. In a wiretap channel, Bob receives the transmitted message of Alice via a channel C1, called the main channel. The eavesdropper Eve, however, observes the information transmitted by Alice through the wiretap channel, C2. The legitimate parties wish to communicate through C1 while concealing the information from Eve. Specifically, Alice wishes to encode its message M and transmit a codeword X^n on the channel C1. Bob receives Y^n , while Eve receives Z^n . The legitimate pair's objectives are

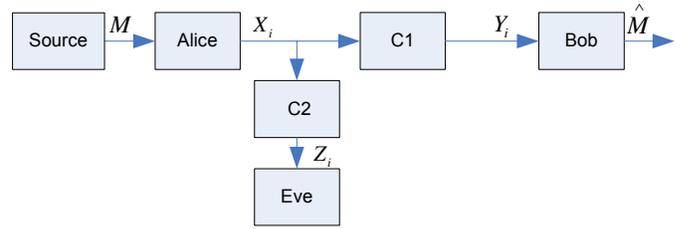


Fig. 1. Discrete Memoryless Wiretap Channel (DMWTC).

security, that is, Z^n should provide no information about M (more precisely, $\frac{1}{n}I(M; Z) \rightarrow 0$ as $n \rightarrow \infty$), and reliability, that is, M should be decoded from Y^n with a negligibly small probability of error. The maximal rate $\frac{1}{n} \log M$ at which both objectives can be fulfilled is called the *secrecy capacity*.

For a *physically degraded* wiretap channel, i.e., when $p(y, z|x) = p(y|x)p(z|y)$, Wyner showed that the secrecy capacity is

$$C_s = \max_{p(x)} \{I(X; Y) - I(X; Z)\}. \quad (1)$$

This result was later extended by Csiszár and Körner in [2], which considered *broadcast channels with confidential messages*. A special case of the results therein is the secrecy capacity of the *general wiretap channel* $p(y, z|x)$, namely,

$$C_s = \max_{p(u,x)} \{I(U; Y) - I(U; Z)\},$$

with an auxiliary U whose cardinality is bounded by that of X . Of course, this reduces to (1) when the wiretap channel is degraded. In fact, it suffices that the main channel is *more capable*, that is $I(X; Y) \geq I(X; Z)$ for any $p(x)$, for the Wyner result in (1) to hold. An important concept in the achievability of the above results is the *added randomness*, used to confuse the eavesdropper regarding the actual message sent. Such randomness will play a key role in this paper as well.

The current literature includes several generalizations of the canonical models given in [1] and [2]. We include here only the most relevant. A thorough discussion of related works is given in Section III. In [3], Ahlswede and Cai considered a discrete memoryless wiretap channel with secure

Parts of this work appeared at the 51st Annual Allerton Conference on Communication, Control, and Computing, 2013.

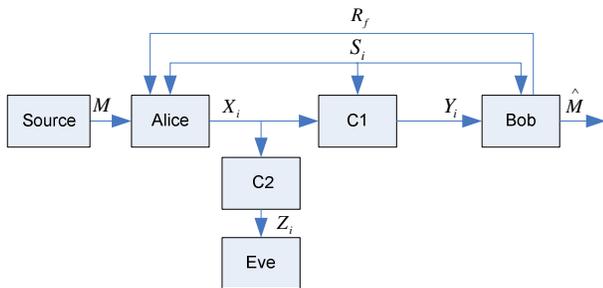


Fig. 2. The setting considered in this paper. On top of the Wyner wiretap model, a feedback link is available from the legitimate receiver to the transmitter. Moreover, the state information at the main channel is available causally to the legitimate parties. Both the main channel and the wiretap channel are DMCs.

output feedback. A general feedback link was considered by Ardestanizadeh *et al.* in [4]. Therein, since the feedback was not limited to merely pass the output symbols Y^n , the authors showed that it is beneficial to use the feedback to send *fresh randomness*, to be used as a shared key between Alice and Bob.

In [5], Liu and Chen considered a wiretap model where the main channel is a *state-dependent* DMC. While the eavesdropper remains ignorant of the state, the authors considered the cases where the transmitter and legitimate receiver may or may not have non-causal knowledge of the state. The closely related problem of *secret key agreement* in the wiretap channel with non-causal state information was considered in [6]. The work in [5] was later extended by Chia and El Gamal in [7] to the case where *causal* state information is available (i.e., only past and current state values are given). At the heart of Chia and El Gamal's methods stands a key generation scheme. Again, this key, shared by Alice and Bob, is used to increase the secrecy capacity. The works in [5]–[7], however, do not include a feedback link.

Main Contribution

In this work, we consider the system depicted in Figure 2. In this setting, both channel state information (CSI) denoted as S_i and a rate limited feedback denoted as R_f are available. We derive upper and lower bounds on the secrecy capacity, and show that when the eavesdropper's channel is degraded, namely, $p(y, z|x, s) = p(y|x, s)p(z|y)$, the bounds are tight and describe the secrecy capacity exactly. In the lower bound, we show that a combined scheme of both types of key generation is required to achieve the results: on top of the Wyner scheme, one has to create a shared key from the state information and send an additional key through the feedback. The main contribution is in the upper bound, which is more involved, and requires showing that indeed such a use of the feedback link is optimal. We prove the upper bound via a non-trivial recursive lemma, which enables us to include *both state and feedback*. The resulting region reduces to previously known results in the literature when the feedback or state information are not available, and thus extends them. When the state information is available only at the legitimate decoder, the state information can be viewed as part of the

channel output, hence the framework of [4] applies. However, a comparison of achievable schemes suggests that, unlike what [4] suggests, one should not use the feedback to send fresh randomness, but might as well *losslessly describe the state to the transmitter*, avoiding the need for randomness at the decoder.

Applications of the above results include, but are not limited to, cases where the eavesdropper channel is *not weaker than the main channel*, yet, one can achieve secure communication via channel state and feedback, extending the range of scenarios where information theoretic security can be used. Moreover, a deep understanding of the capacity of the wiretap channel under diverse conditions such as state information and feedback will facilitate the application of such physical layer security concepts to modern, real world networks, where state information and feedback are available (through estimation or two way communication), but to date, are not used at their full potential.

The structure of this work is as follows. In Section II, the problem is formally described. In Section III, we summarize the related work. Section IV includes our main results, with the lower bound proved in Section V and the upper bound in Section VI. Section VII includes a description of a few important special cases. Section VIII concludes the paper.

II. PROBLEM FORMULATION

We consider the Discrete Memoryless Wiretap Channel (DMWTC) with secure rate limited feedback and causal state information given in Figure 2. Both Alice, the encoder, and Bob, the decoder, have access to the state information S_i . In general, the state information can be available non-causally or causally. In this paper, we focus on the causal case. Alice desire is keeping Eve ignorant of the confidential message, denoted as $M \in \{1, \dots, 2^{nR}\}$, sent to Bob.

Throughout the paper, capital letters denote random variables, lower case letters denote their realizations, and calligraphic letters denote the alphabet. Thus, the sent message is $(X_1, \dots, X_n) = X^n$, $X \in \mathcal{X}$, the output at the legitimate receiver is Y^n , $Y \in \mathcal{Y}$, and the output at the eavesdropper is Z^n , $Z \in \mathcal{Z}$. The main channel is affected by a *memoryless* state sequence S^n , $S \in \mathcal{S}$, known causally to both the encoder and the legitimate decoder. We assume a memoryless channel, that is,

$$p(y_i, z_i|x^i, y^{i-1}, z^{i-1}, s_i) = p(y_i, z_i|x_i, s_i).$$

In the case where just the main channel is affected by the state information, the cross-over probabilities at the wiretap channel is $p(z_i|x^i, z^{i-1}) = p(z_i|x_i)$.

We assume a rate-limited feedback at rate R_f is available from the decoder to the encoder. That is, symbols K_i^f , $i \in \{1, \dots, n\}$ are sent over a feedback link, secretly from the eavesdropper. The feedback alphabets are denoted as $\{\mathcal{K}_1^f, \dots, \mathcal{K}_n^f\}$. Thus, their cardinalities must satisfy

$$\frac{1}{n} \sum_{i=1}^n \log(|\mathcal{K}_i^f|) \leq R_f. \quad (2)$$

The symbol K_i^f at instant i may depend on prior outputs up to instant $i - 1$ of the channel, $Y^{i-1} = (Y_1, \dots, Y_{i-1})$ and the prior symbols $(K_1^f, \dots, K_{i-1}^f) = K_f^{i-1}$. Note that, with a slight misuse of notation, a single instant of the feedback value at time i is denoted K_i^f while the *vector* (K_1^f, \dots, K_i^f) is denoted K_f^i . This will remain throughout the paper. We allow a random feedback, that is, its actual values can depend on some conditional probability distributions

$$p(k_i^f | y^{i-1}, k_f^{i-1}).$$

Consequently, a code with parameters $(2^{nR}, 2^{nR_f}, n)$ for the wiretap channel in the presence of causal state information and rate-limited feedback is defined by a message set $\{1, \dots, 2^{nR}\}$; The conditional probability distributions of the stochastic coding for the legitimate encoder

$$p(x_i | m, x^{i-1}, s^i, k_f^i),$$

where m denotes the message to be sent; The feedback at rate R_f defined above and, finally, a decoding map

$$\hat{m}: \mathcal{Y}^n \times \mathcal{S}^n \times \mathcal{K}_f^n \mapsto \{1, \dots, 2^{nR}\}.$$

Hence, the decoded message is $\hat{M} = \hat{m}(Y^n, S^n, K_f^n)$. The message M at the legitimate encoder is distributed uniformly on $\{1, \dots, 2^{nR}\}$, thus $H(M) = nR$.

The normalized equivocation at the eavesdropper is the ratio $H(M|Z^n)/H(M)$. Denote the error probability $p(\hat{M} \neq M)$ as $P_e^{(n)}$. We say that the rate/normalized equivocation tuple (R, R_f, d) is achievable if for any $\varepsilon > 0$ there exists an $(2^{nR}, 2^{nR_f}, n)$ code such that

$$\frac{H(M|Z^n)}{H(M)} \geq d - \varepsilon \quad \text{and} \quad P_e^{(n)} \leq \varepsilon. \quad (3)$$

Furthermore, we say the secrecy capacity is C_s if C_s is the supremum of R in the tuples $(R, R_f, 1)$ satisfying the inequalities in (3). Namely, tuples where asymptotically, the eavesdropper is ignorant of the message sent. In this paper, we focus *only on the above case where $d = 1$* , that is, we are interested in the secrecy capacity C_s .

III. RELATED WORK

The first information theoretic study on the problem of securely transmitting a message over a public channel was done in [8]. Therein, Shannon considered the problem of transmitting a message M from the legitimate sender to the legitimate receiver via an open channel. Perfect secrecy was defined by $I(M; X) = 0$, where X is the transmitted word. The result was that the legitimate parties must share a key of the same length as the message itself in order to achieve such a strong secrecy requirement. However, as was shown later, slightly relaxing the perfect secrecy constraint is beneficial.

The wiretap channel in Fig. 1 was presented in [1], under only an *asymptotic* independence constraint, requiring $\frac{1}{n}I(M; Z^n)$ to vanish. For this channel, one would expect that when the capacity of the main channel is larger than that of the wiretap channel, the secrecy capacity will be positive. Indeed, in [1] Wyner proved that when the wiretap channel is a degraded version of the main channel, the secrecy

capacity is positive. [2] extended this and concluded that a positive secrecy capacity is possible whenever the main channel is *less noisy* than the wiretap, that is, less noisy than Z , namely, $I(U; Y) \geq I(U; Z)$ for any auxiliary U such that $U \leftrightarrow X \leftrightarrow (Y, Z)$. Moreover, as was later discussed in [4], [5], [7], even if the wiretap channel is not degraded, or less noisy, the secrecy capacity can be positive using *state information*. We elaborate on this now.

A. Channel State Information

In [5], a DMWTC with CSI at both ends was discussed. Specifically, the CSI S_1^N was given non-causally at the encoder while S_2^N was given non-causally at the decoder. The main channel was specified through $p(y|x, s_1, s_2)$. The following information rates were defined.

$$\begin{aligned} R_{U1} &= I(U; Y, S_2) - \max\{I(U; Z), I(U; S_1)\}, \\ R_{U2} &= I(U; Y, S_2) - I(U; S_1). \end{aligned}$$

U was an auxiliary random variable and, in addition, a Markov condition $U \leftrightarrow (X, S_1, S_2) \leftrightarrow (Y, Z)$ must hold. It was shown that the set

$$R_s = \bigcup_{U \leftrightarrow (X, S_1, S_2) \leftrightarrow (Y, Z)} (R, d), \quad (4)$$

is achievable, under the constraints $Rd \leq R_{U1}$ ($0 \leq d \leq 1$) and $0 \leq R \leq R_{U2}$. Of special interest to us is the case where $d = 1$ and we have

$$R \leq \max_{U \leftrightarrow (X, S_1, S_2) \leftrightarrow (Y, Z)} \min\{R_{U1}, R_{U2}\}.$$

This is an achievable rate for the wiretap channel with two-sided non-causal state information. Moreover, when the state information is available only at the receiver, that is $S_1 = \emptyset$ and $S_2 = S$, we have

$$\begin{aligned} R_{U1} &= I(U; Y, S) - I(U; Z), \\ R_{U2} &= I(U; Y, S). \end{aligned}$$

In a recent paper [7], Chia and El-Gamal considered a similar setting, yet with causal state information. As mentioned, at the heart of the scheme is a key generation step. In particular, random binning of the state sequence known to both the encoder and decoder gives rise to a *shared key*. This key is used to encrypt part of the message. The achievable scheme results in higher rates compared to [5]. In particular, they established that

$$\begin{aligned} C_S &\geq \max\left\{ \max_{p(u|s)p(x|u,s)} \min\{I(U; Y|S) - I(U; Z|S) \right. \\ &\quad \left. + H(S|Z), I(U; Y|S)\}, \right. \\ &\quad \left. \max_{p(u)p(x|u,s)} \min\{H(S|Z, U), I(U; Y|S)\} \right\}. \quad (5) \end{aligned}$$

When Y is less noisy than Z , namely, $I(U; Y|S) \geq I(U; Z|S)$ for any auxiliary U such that $(U, S) \leftrightarrow (X, S) \leftrightarrow (Y, Z)$, this results in

$$C_S = \max_{p(x|s)} \min\{I(X; Y|S) - I(X; Z|S) + H(S|Z), I(X; Y|S)\}.$$

Specific results for the Gaussian channel were given in [9] and in [10] for a Gaussian channel with state. Secret agreement schemes for channels with state known at the transmitter were given in [6]. Of course, CSI plays a key role in MIMO-Wiretap channels as well. Secrecy capacity (and in particular, outage) was discussed in [11], where it was shown that one can take the advantage of having perfect knowledge of the channel state to the legitimate receiver by adding artificial noise to the null space of the main channel. Later results regarding the optimal beamforming vectors can be found in [12]. The advantage of perfect knowledge of the channel state to the legitimate receiver was also used in [13] under a Rician fading setting. Fading channels in the context of OFDM were considered in [14]. Finally, the current literature also includes work on *active eavesdropping* in the presence of channel state [15].

B. Feedback

In this work, besides state information, we are interested in the availability of noiseless feedback as well. Interactions in secure duplex communication can benefit from the insights of such models. Indeed, we will establish that in the case of wiretap channels with CSI, feedback can increase the secrecy capacity significantly.

In [3], the authors characterized the capacity of a wiretap channel with *noiseless feedback of the channel output*, and showed that in this case,

$$C_s = \max_{p(x)} \min\{I(X; Y|Z) + H(Y|X, Z), I(X; Y)\}. \quad (6)$$

This is exactly the capacity when one extracts a key from the feedback (as feedback does not increase capacity otherwise).

In [4], the authors investigated the secrecy capacity $C_s(R_f)$ of a wiretap channel where the legitimate parties have a secure link (feedback) from the decoder to the encoder at rate R_f . Note that the feedback was not limited to carry output symbols. The upper bound in [4] was

$$C_s(R_f) \leq \max_{p(x)} \min\{I(X; Y|Z) + R_f, I(X; Y)\}. \quad (7)$$

Again, when the wiretap channel is physically degraded, the upper bound is tight, establishing (7) as the secrecy capacity.

C. Secret Key Agreement, Networks and Practical Schemes

A closely related set of problems fall under *secret key agreement* schemes [16]–[18]. In these problems, one is interested in the *number of secret bits* which can be distilled in a system. In fact, it is not hard to see that any wiretap coding scheme is also a secret key agreement scheme, hence the secret key capacity is an upper bound on the secrecy rate. However, it is tight only in specific cases (e.g., [19, Example 4.7]). The difference stems from the fact that the underlying metric is different (number of secret bits distilled versus number of bits transmitted securely). Moreover, many secret key agreement schemes allow public information exchanges between Alice and Bob (on top of the main channel or the correlated sources available to them). To the best of our

knowledge, there are no concrete results from the literature on secret key capacity which, for the problem at hand, give tighter bounds than the ones we give in the paper.

The theory and practice of wiretap channel coding has been found useful in a variety of networking scenarios as well. E.g., in [20], the authors suggested a client-server setting where the binary erasure wiretap channel approach was found constructive. A multitude of network coding scenarios exist in [21], [22].

Finally, we mention that the current literature includes practical coding schemes as well, rendering them as desirable solutions for physical layer security. LDPC for the Gaussian wiretap channel was suggested in [23], as well as in [24] to suggest secret sharing schemes. LDPCs were also used to allow strong secrecy over a binary erasure channel in [25].

IV. MAIN RESULTS

We list the main results of the paper, and conclude with an illustrative example. The proofs are deferred to Sections V and VI.

A. Lower Bound

The achievability part is given by the following theorem.

Theorem 1. *Assume a DMWTC, with causal CSI given at the encoder and the legitimate decoder and in the presence of rate limited feedback. Then, the secrecy capacity is lower bounded by*

$$C_s \geq \max_{p(u|s)p(x|u,s)} \left\{ \min\{I(U; Y|S) - I(U; Z|S) + H(S|Z) + R_f, I(U; Y|S)\}, \right. \\ \left. \max_{p(u|s)p(x|u,s)} \min\{H(S|Z, U) + R_f, I(U; Y|S)\} \right\},$$

where U is an auxiliary random variable and the distributions $p(u|s)$ and $p(x|u, s)$ can be optimized.

Theorem 1 proves that the secrecy capacity is dictated by the following three rates:

$$\begin{aligned} \hat{R}_1 &= I(U; Y|S) - I(U; Z|S) + H(S|Z) + R_f, \\ \hat{R}_2 &= I(U; Y, S) - I(U; S) = I(U; Y|S), \\ \hat{R}_3 &= H(S|Z, U) + R_f. \end{aligned}$$

Note that \hat{R}_3 is the maximal rate at which a key can be extracted and used to secure the communication. Clearly, up to this rate, there is no need in Wyner-like wiretap coding, and the message can be protected solely by the key. On the other hand, \hat{R}_2 is the capacity of the main channel. This bound certainly cannot be exceeded. Between these two bounds, Wyner-like coding is beneficial, and the resulting secrecy rate will be \hat{R}_1 , which is the most interesting constraint.

The achievability, while based on extracting a key from the side information sequence similar to [7], involves both Wyner-like wiretap coding and *two levels of protection* using secret keys: one extracted from the CSI and one transmitted through the feedback. Hence, a message is divided into *three sub-messages*, which should not leak to the eavesdropper. However, *as feedback introduces memory, a key challenge is in proving a corresponding upper bound.*

B. Upper Bound

The upper bound is the following.

Theorem 2. *Assume a DMWTC, with causal CSI given at the encoder and the legitimate decoder and in the presence of rate limited feedback. Then, the secrecy capacity is upper bounded by*

$$C_S \leq \max_{p(x|s)} \min\{I(X;Y|Z,S) + H(S|Z) + R_f, I(X;Y|S)\}.$$

The availability of a rate-limited feedback complicates the converse as it renders many of the tools used for memoryless channels impractical. Specifically, in the presence of feedback, $p(y^n, z^n|x^n, s^n)$ no longer has a simple product form. Thus, the proof of the converse involves a non-trivial generalization of a recursive lemma from [4], which incorporates both state information and feedback.

C. Complete Characterization of the Secrecy Capacity

It is interesting to investigate the cases where the lower and upper bounds match. As for the lower bound, when $\hat{R}_1 \geq \hat{R}_3$ and the main channel is less noisy than the eavesdropper channel, with the data processing inequality $I(U;Y|S) \leq I(X;Y|S)$ the bound sums up to

$$C_S \geq \max_{p(x|s)} \{I(X;Y|S) - I(X;Z|S) + H(S|Z) + R_f\}.$$

Note that the less noisy assumption is weaker than the degraded assumption, hence the result holds in this case as well. Now, when the eavesdropper channel is degraded such that $p(y, z|x, s) = p(y|x, s)p(z|y)$ and $(X, S) \leftrightarrow Y \leftrightarrow Z$ from a Markov chain, the upper bound on the secrecy capacity reduces to

$$C_S \leq \max_{p(x|s)} \{I(X;Y|S) - I(X;Z|S) + H(S|Z) + R_f\}$$

and the bounds match.

Corollary 1. *Assume a DMWTC, with causal CSI given at the encoder and the legitimate decoder and in the presence of rate limited feedback. If the eavesdropper channel is degraded, then the secrecy capacity is*

$$C_S = \max_{p(x|s)} \min\{I(X;Y|S) - I(X;Z|S) + H(S|Z) + R_f, I(X;Y|S)\}.$$

D. Example

We compare several scenarios for a degraded binary symmetric wiretap channel, where the scenarios differ by the availability of channel state and noiseless feedback.

A degraded DMWTC with noiseless feedback and without CSI is given in Figure 3 A. The main channel between Alice and Bob is a binary symmetric channel with a transition probability p_y . That is,

$$\begin{aligned} p_{y|x}(0|0) &= 1 - p_y, & p_{y|x}(0|1) &= p_y \\ p_{y|x}(1|1) &= 1 - p_y, & p_{y|x}(1|0) &= p_y. \end{aligned}$$

We denote this channel model by $BSC(p_y)$. The wiretap channel is realized by cascading the main binary symmetric channel, $BSC(p_y)$, and the eavesdropper's binary symmetric channel, $BSC(p_z)$.

A degraded wiretap channel with noiseless feedback and CSI is shown in Figure 3 B. Now, the main BSC is state-dependent, that is, it is $BSC(p_{s_i})$ if the state at time i is s_i . The wiretap channel is a cascade of this channel and $BSC(p_z)$. The maximum of $C_s^{NS}(R_f)$ (over the input distribution), i.e., the capacity of the degraded DMWTC without CSI yet with feedback, and the maximum of $C_s^S(R_f)$, i.e., the capacity of the degraded DMWTC with CSI and feedback, are both achieved using a symmetric input probability distribution, namely, $P(X=0) = P(X=1) = 0.5$. Thus, X , Y and Z are uniformly distributed over $\{0, 1\}$. The binary entropy function and the binary convolution are denoted by $h(p) = -p \log p - (1-p) \log(1-p)$ and by $p_y * p_z = p_y(1-p_z) + (1-p_y)p_z$, respectively. With these distributions, without state information (case A) the mutual information is

$$I(X;Y) = 1 - h(p_y),$$

hence the relevant capacity is

$$I(X;Y) - I(X;Z) = h(p_y * p_z) - h(p_y).$$

Now, assume the main channel has state (Case B). We assume only two states are possible, and each state corresponds to a different cross over probability in the main channel. That is, assume $P(S=s_0) = 1-q$ and $P(S=s_1) = q$. When $S=s_0$, $p_{y|x,s}(y|x, 0) = 1-p_{s_0}$ if $x=y$ and p_{s_0} otherwise. When $S=s_1$, $p_{y|x,s}(y|x, 1) = 1-p_{s_1}$ if $x=y$ and p_{s_1} otherwise. Hence, for the case with state information, we have

$$I(X;Y|S) = 1 - (1-q)h(p_{s_0}) - qh(p_{s_1}).$$

Furthermore, with the symmetric input distribution as in this example, it is not hard to verify that $I(Z;S) = 0$. Thus,

$$H(S|Z) = H(S) = h(q).$$

As for the wiretap channel, we have

$$I(X;Z|S) = 1 - (1-q)h(p_{s_0} * p_z) - qh(p_{s_1} * p_z).$$

Hence,

$$\begin{aligned} I(X;Y|S) - I(X;Z|S) + H(S|Z) &= 1 - (1-q)h(p_{s_0}) - qh(p_{s_1}) \\ &\quad - \{1 - qh(p_{s_1} * p_z) - (1-q)h(p_{s_0} * p_z)\} \\ &\quad + h(q) \\ &= (1-q)h(p_{s_0} * p_z) + qh(p_{s_1} * p_z) \\ &\quad - (1-q)h(p_{s_0}) - qh(p_{s_1}) + h(q). \end{aligned}$$

As a result, the capacities to compare are

$$C_s^{NS}(R_f) = \min\{1 - h(p_y), h(p_y * p_z) - h(p_y) + R_f\}$$

and

$$\begin{aligned} C_s^S(R_f) &= \min\{1 - (1-q)h(p_{s_0}) - qh(p_{s_1}), \\ &\quad (1-q)h(p_{s_0} * p_z) + qh(p_{s_1} * p_z) \\ &\quad - (1-q)h(p_{s_0}) - qh(p_{s_1}) + h(q) + R_f\}. \end{aligned}$$

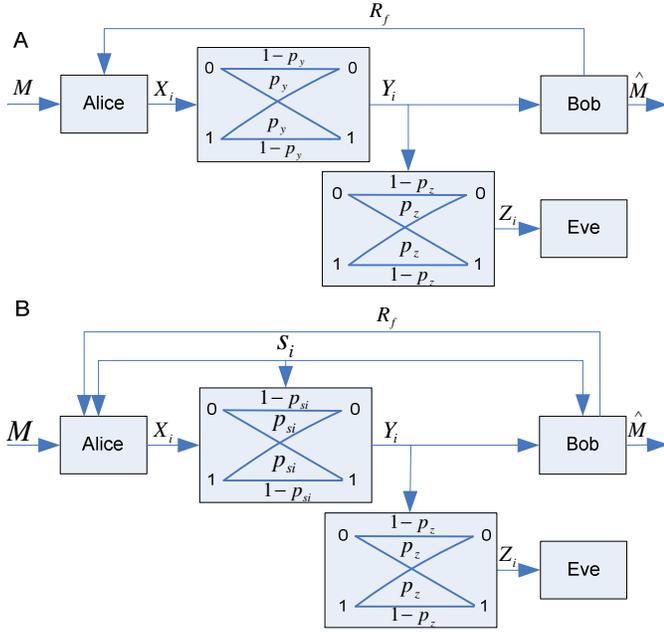


Fig. 3. (A) Degraded wiretap channel without causal CSI, (B) Degraded wiretap channel with causal CSI.

Numerical results for the capacities above are given in Figures 4 and 5. The cross-over probabilities are fixed on $p_z = p_y = 0.1$, $p_{s_0} = 0.05$ and $p_{s_1} = 0.15$. 4 gives the capacities $C_s^{NS}(R_f)$ and $C_s^S(R_f)$ versus R_f . The same saturation phenomenon observed with no state is visible with state as well (with linear increase until the saturation point), however, it is clear that the probabilities for each state affect the capacity. This effect is, in fact, twofold. First, the value of the state affects the capacity of the direct channel. Yet, besides this effect, the fact that *there is a state sequence* affects the secrecy capacity. The more entropy the state sequence has, the higher the key rate, hence the faster the capacity saturates at its maximal value (which is the main channel capacity). 5 gives another perspective, plotting the secrecy capacities as a function of q . It is clear that once the capacities saturate, the value is independent of R_f . It decreases with q , though the higher q is the lower is the capacity of the direct channel. This is only due to the specific choices of p_{s_0} and p_{s_1} .

V. LOWER BOUND

A. Achievability of \hat{R}_1

Consider \hat{R}_1 , with the maximization on the input distribution:

$$\hat{R}_1 = \max_{p(u|s)p(x|u,s)} \{I(U; Y|S) - I(U; Z|S) + H(S|Z) + R_f\}.$$

Similar to [7], we perform the maximization in \hat{R}_1 through distributions $p(u')$, $p(x|u',s)$ and functions of the form $u(u',s)$, using the functional representation lemma [26]. This way, the achievability can be proved for an equivalent

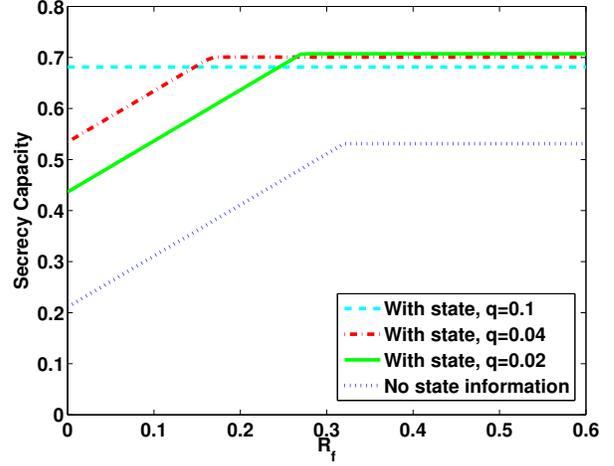


Fig. 4. The secrecy capacities $C_s^{NS}(R_f)$ and $C_s^S(R_f)$ versus R_f , with and without a state sequence. $(q, 1 - q)$ is the (memoryless) probability distribution for the state sequence. Note that for $q = 0.1$, in this case, the amount of randomness in the key suffices to saturate the secrecy capacity regardless of the value of R_f . For lower q , however, there is not enough randomness in the key generated from the state, and the capacity saturates only for non-zero values of R_f .

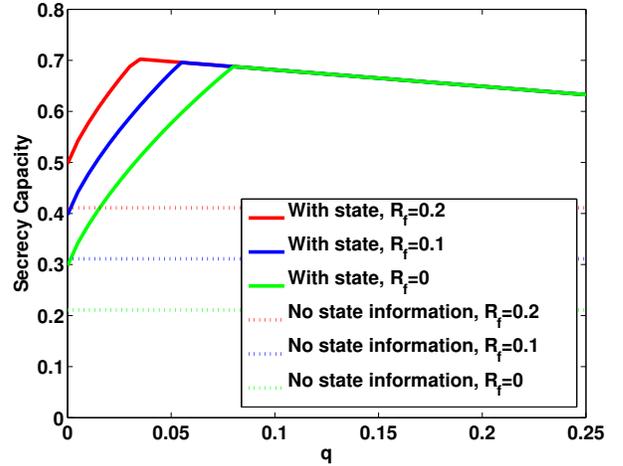


Fig. 5. The secrecy capacities, this time as a function of the state probabilities, that is, $C_s^{NS}(q)$ and $C_s^S(q)$. For low values of q , the key factor in the secrecy capacity is the amount of randomness in the state sequence. Hence, in this range, the higher q is, the higher the secrecy capacity. However, when the secrecy capacity saturates, due to the specific choices of probabilities p_{s_0} and p_{s_1} , the higher q is, lower the main channel capacity, hence the secrecy capacity decreases.

characterization of \hat{R}_1 ,

$$\max_{p(u'), u(u',s), p(x|u,s)} \{I(U'; Y, S) - I(U'; Z, S) + H(S|Z) + R_f\}.$$

We split the proof to two cases, the first is when $I(U'; Y, S) \geq I(U'; Z, S)$, where for this case $(U', S) \leftrightarrow (X, S) \leftrightarrow (Y, Z)$ from a Markov chain, and the second case is when $I(U'; Y, S) \leq I(U'; Z, S)$.

1) *First Case* - $I(U'; Y, S) \geq I(U'; Z, S)$:

a) *Encoding of Legitimate Sender (Alice)*: The encoding scheme in this case requires the transmission of $B - 1$ protected blocks during the transmission of B blocks, each of length n . The message in the first block is not fully protected.

Given a distribution $P_{U'}$ and a function $u(u', s)$, we set the following three rates:

$$\begin{aligned} R_0 &= I(U'; Y, S) - I(U'; Z, S) - 2\epsilon, \\ R_1 &= H(S|Z) - \epsilon, \\ R_2 &= R_f. \end{aligned}$$

The coding scheme corresponds to a transmission rate

$$R = R_0 + R_1 + R_2 = \hat{R}_1 - 3\epsilon,$$

secretly from the eavesdropper. We assume $R \leq I(U'; Y, S)$. Of course, this is not an actual restriction as $I(U'; Y, S) \leq I(U'; Y|S)$, which is, in turn, an upper bound on the secrecy capacity 1 claims is achievable. Hence, cases where $R_0 + R_1 + R_2 > I(U'; Y, S)$ are of no interest.

We split the message $M_j, j \in \{2, \dots, B\}$, into three independent messages $M^0 \in \{1, \dots, 2^{nR_0}\}$, $M^1 \in \{1, \dots, 2^{nR_1}\}$ and $M^2 \in \{1, \dots, 2^{nR_2}\}$. The message at rate R_0 will be protected by the Wyner wiretap coding scheme, while the messages at rate $R_1 + R_2$ will be protected by the keys: a message at rate R_1 protected by the key generated from the CSI and a message at rate R_2 protected by the key received from the feedback.

The first step is the generation of the message codebook. We randomly generate $2^{n[I(U'; Y, S) - \epsilon]}$ i.i.d. sequences $u^n(l)$, using the distribution $P(U^n = u_i) = \prod_{i=1}^n P_{U'}(u'_i)$. Then, these sequences are distributed randomly into 2^{nR_0} equal size bins. The index of each bin is denoted as $j \in \{1, 2, \dots, J = 2^{nR_0}\}$. Next, these sequences are distributed randomly into 2^{nR_1} sub-bins, and we further partition each sub-bin to 2^{nR_2} equal size sub-bins. Denote the resulting bin indices by $C(m^0, m^1, m^2)$.

Next we create the keys from the CSI. We bin the channel state sequences s^n at random into 2^{nR_1} bins $\{B(k_s)\}_{k_s=1}^{2^{nR_1}}$. The key K_{j-1}^s used to protect M^1 in block j is the bin index of the state sequence $S^n(j-1)$ in block $j-1$.

The third step is the generation of the feedback codebook. Similar to [4], it is used solely to give the encoder random bits. Herein, however, such random bits are sent for each block. The key is of rate R_2 , i.e., Bob sends k_j^f drawn uniformly from 2^{nR_2} indices to be used in the j th block. This key is the one used to encrypt M^2 of the given block.

To encode the first block of the message M_1 , given M_1^0 , M_1^1 and M_1^2 , the encoder selects a random codeword $u^n(L)$ from $C(M_1^0, M_1^1, M_1^2)$. Then it computes $u_i = u(u'_i(L), s_i)$ and the symbol transmitted is a random one, according to $X_i \sim p(x_i|s_i, u_i)$ for $i \in \{1 \dots n\}$. Note that the first block is not protected by the keys. However, during the transmission of the $j-1$ block, the encoder (Alice) gathers two keys, k_{j-1}^s from the state sequence and k_{j-1}^f from the feedback. To encode the j -th block of the message $M_j, j \in \{2, \dots, B\}$, given M_j^0, M_j^1 and M_j^2 , the encoder selects a random codeword $u^n(L)$ from $C(M_j^0, M_j^1 \oplus k_{j-1}^s, M_j^2 \oplus k_{j-1}^f)$. \oplus denotes

modulo- $[2^{R_1}]$ and $[2^{R_2}]$ additions. It then computes $u_i = u(u'_i(L), s_{1i})$ and the symbol transmitted is, again, random, according to $X_i \sim p(x_i|s_i, u_i)$ for $i \in \{(j-1)n + 1 \dots jn\}$.

Note that M^0 , similar to [7], is protected using the Wyner coding scheme, therefore the eavesdropper cannot comprehend this part from the message when $I(U'; Y, S_1) - I(U'; Z, S_2) > 0$. The second part, M^1 , is encrypted with the key k_{j-1}^s and the third part, M^2 , is encrypted with the key k_{j-1}^f .

b) *Decoding at legitimate receiver (Bob)*: The decoding involves standard joint typicality arguments. We list here only the most important steps.

In the first block the legitimate receiver searches for a word $u^n(L)$ in the codebook, such that $(u^n(l), y^n(j), s^n(j))$ is jointly typical, then the legitimate receiver (Bob) declares the index of the bin containing this $u^n(l)$ as the message received.

As the number of originally drawn sequences, $2^{n[I(U'; Y, S) - \epsilon]}$, is similar to that in [7], the analysis of the error probability is similar, and the jointly typical $u^n(l)$ is identified with high probability. The probability that a different sequence is identified is arbitrarily close to zero. Thus, the message indices m_j^0, m_j^1 and m_j^2 are decoded correctly with high probability.

As for the decoding at the j -th block $j \in \{2, \dots, B\}$, the decoder uses a similar procedure to retrieve $m_j^0, m_j^1 \oplus k_{j-1}^s$ and $m_j^2 \oplus k_{j-1}^f$. It then uses k_{j-1}^s to retrieve m_j^1 and k_{j-1}^f to retrieve m_j^2 . It is easy to verify that a rate $\hat{R}_1 = \min\{I(U'; Y|S) - I(U'; Z|S) + H(S|Z) + R(f) - \delta_n, I(U'; Y|S)\}$ can be achieved.

c) *Information Leakage at the Eavesdropper (Eve)*: For $j \in \{1, \dots, B\}$ we let Z_j^n denote the eavesdropper's observation in block j . The information leaked $L(\tilde{C}_{nB})$, given the codebook and coding procedure \tilde{C}_{nB} is then

$$\begin{aligned} \frac{1}{nB} L(\tilde{C}_{nB}) &= \frac{1}{nB} I(M_1^0 \dots M_B^0 M_1^1 \dots M_B^1 \\ &\quad M_1^2 \dots M_B^2; Z_1^n \dots Z_B^n | \tilde{C}_{nB}) \\ &= \frac{1}{nB} I(M_1^0 \dots M_B^0 M_1^1 \dots M_B^1; Z_1^n \dots Z_B^n | \tilde{C}_{nB}) \\ &\quad + \frac{1}{nB} I(M_1^2 \dots M_B^2; Z_1^n \dots Z_B^n \\ &\quad | M_1^0 \dots M_B^0 M_1^1 \dots M_B^1, \tilde{C}_{nB}) \end{aligned} \quad (8)$$

where the equality is due to the chain rule for mutual information. We now consider the two summands. As for the first, this is exactly the information leakage on the messages protected by the Wyner wiretap scheme and the messages protected by the key *drawn from the state sequence*. Hence, by the results of Chia and El Gamal [7], specifically, Proposition 1 therein and the discussion which follows, as long as the key extracted from the *state* is at rate smaller than $H(S|Z)$, Eve's knowledge on the key is negligible, hence the first summand is negligible.

Consider the second summand. $\{M_j^2\}$ are the portions of the messages *protected by the keys received from the feedback*.

The keys sent through the feedback are random, independent of all other variables in our problem. Remember that the encoder selects a random codeword from $C(M_j^0, M_j^1 \oplus k_{j-1}^s, M_j^2 \oplus k_{j-1}^f)$. Thus, the actually transmitted codewords (at all blocks), and, of course, the received ones at Eve's side may depend on M_j^2 only through $M_j^2 \oplus k_{j-1}^f$, that is, they are completely independent of M_j^2 unless the key is given. Due to the above, the second summand is zero. In other words, if one considers $M_1^2 \dots M_B^2$ as a single message at rate BR_2 and $Z_1^n \dots Z_B^n$ as an output block of size Bn , the second summand is equivalent to the expression $I(M_2; Z^n | \mathcal{C}, M_1)$ that appears in [4, equation (45)], which is shown to be zero therein. We conclude that \hat{R}_1 is achievable.

2) *Second Case* - $I(U'; Y, S) \leq I(U'; Z, S)$: Herein, the main channel capacity is too low, and the encoder cannot use the Wyner wiretap scheme to secretly send message to the legitimate receiver. Therefore, only the two keys, the one resulting from the CSI and the one resulting from the feedback can be used to protect the message. We only consider the scenario where $(I(U'; Y|S) - I(U'; Z|S)) + (H(S|Z) + R_f) > 0$. Otherwise the secrecy capacity is zero.

The same key splitting as in [7] is used. In short, in the block $j \in \{2 \dots B\}$, we split the message to three parts as before, yet protect the first two with the state key. The state information key k_{j-1}^s is split to two independent parts, $k_{(j-1,0)}^s$ and $k_{(j-1,1)}^s$ at rates which coincides with case 2 of $R_{S-CSI-1}$ in [7]. Thus, compared with the first case of \hat{R}_1 , to send message $M_j, j \in \{2 \dots B\}$, transmit $X^n(k_{(j-1,0)}^s, M_j^1 \oplus k_{(j-1,1)}^s, M_j^2 \oplus k_{j-1}^f) \in C_n$. The reminder of the proof is very similar to [7].

B. Achievability of \hat{R}_3

In this case, to encode the message we use purely the key K_s in the block, which coincides with $R_{S-CSI-2}$ in Chia and El Gamal [7, Theorem 1]. We split the message $M_j, j \in \{2, \dots, B\}$, into two independent messages $M^1 \in \{1, \dots, 2^{nR_1}\}$ and $M^2 \in \{1, \dots, 2^{nR_2}\}$, where $R \geq R_1 + R_2$ and $I(U'; Y, S) - 3\epsilon > R$, such that to send message $M_j, j \in \{2 \dots B\}$ given M_j^1 and M_j^2 transmit $X^n(M_j^1 \oplus k_{j-1}^s, M_j^2 \oplus k_{j-1}^f) \in C_n$ using Shannon's strategy [8] (one-time pad). The decoder uses joint typicality decoding together with the knowledge of the keys and the state information to decode message \hat{M}_j .

VI. UPPER BOUND

Assume $\epsilon_n, \delta_n \rightarrow 0$ when $n \rightarrow \infty$. Consider first the two upper bounds, when the CSI is available at both transmitter and legitimate receiver, and a feedback at rate R_f is present,

$$R \leq \frac{1}{n} \sum_{i=1}^n I(X_i; Y_i | S_i) + \epsilon_n \quad (9)$$

and

$$R \leq \frac{1}{n} \sum_{i=1}^n I(X_i; Y_i | Z_i, S_i) + \frac{1}{n} \sum_{i=1}^n H(S_i | Z_i) + R_f + \delta_n. \quad (10)$$

The upper bound in (9) is since the secrecy capacity cannot be greater than the channel capacity. Thus, 2 follows by combining (9) and (10), then introducing a time sharing random variable [27] to show that the secrecy capacity must satisfy

$$R \leq \max_{p(x|s)} \min \{I(X; Y|S), I(X; Y|Z, S) + H(S|Z) + R_f\}. \quad (11)$$

We now continue similar to [4] using Fano's inequality, the fact that $L^n \rightarrow 0$ (the constraint on the secrecy) and the fact that $\frac{1}{n} \sum_{i=1}^n \log(|K_i^f|) \leq R_f$. Together with 1 below, a non-trivial extension of [4, Lemma 1] for a wiretap with state information, the upper bound in (10) will follow.

By Fano's inequality, for $\hat{M} = \hat{m}(Y^n, K_f^n, S^n)$,

$$H(M | \hat{M}) \leq 1 + P_e^{(n)} nR = n\epsilon_n,$$

where $\epsilon_n \rightarrow 0$ as $n \rightarrow \infty$ if $P_e^{(n)} \rightarrow 0$. Since \hat{M} is a function of Y^n, K_f^n, S^n ,

$$\begin{aligned} H(M | Y^n, K_f^n, S^n) &\leq H(M | \hat{M}) \\ &\leq n\epsilon_n. \end{aligned}$$

Using the secrecy constraint,

$$I(M; Z^n) = n\gamma_n, \quad (12)$$

where $\gamma_n \rightarrow 0$ as $n \rightarrow \infty$. Consequently,

$$\begin{aligned} nR &= H(M) \\ &= H(M | Z^n) + I(M; Z^n) \\ &\stackrel{(a)}{=} H(M | Z^n) + n\gamma_n \\ &= I(M; Y^n, K_f^n, S^n | Z^n) + H(M | Y^n, Z^n, S^n, K_f^n) \\ &\quad + n\gamma_n \\ &= I(M; Y^n, K_f^n | Z^n, S^n) + I(M; S^n | Z^n) \\ &\quad + H(M | Y^n, Z^n, S^n, K_f^n) + n\gamma_n \\ &\stackrel{(b)}{\leq} I(M; Y^n, K_f^n | Z^n, S^n) + I(M; S^n | Z^n) \\ &\quad + n\epsilon_n + n\gamma_n \\ &\stackrel{(c)}{=} I(M; K_f^n | Z^n, S^n) + I(M; Y^n | K_f^n, Z^n, S^n) \\ &\quad + I(M; S^n | Z^n) + n\delta_n \\ &\stackrel{(d)}{\leq} H(K_f^n | Z^n, S^n) + I(M, X^n; Y^n | K_f^n, Z^n, S^n) \\ &\quad + H(S^n | Z^n) + n\delta_n \end{aligned}$$

where (a) follows from (12), (b) follows from Fano's inequality, and (c) follows by defining $\delta_n = \epsilon_n + \gamma_n$. The following recursive lemma is now required.

Lemma 1. For each $j \in \{1, \dots, n\}$,

$$\begin{aligned} &H(K_f^j | Z^j, S^j) + I(M, X^j; Y^j | K_f^j, Z^j, S^j) + H(S^j | Z^j) \\ &\leq H(K_f^{j-1} | Z^{j-1}, S^{j-1}) + I(M, X^{j-1}; Y^{j-1} | K_f^{j-1}, Z^{j-1}, S^{j-1}) \\ &\quad + H(S^{j-1} | Z^{j-1}) + H(K_f^j | M, X^{j-1}, K_f^{j-1}, Z^{j-1}, S^{j-1}) \\ &\quad + I(X_j; Y_j | Z_j, S_j) + H(S_j | Z_j). \end{aligned}$$

Proof: We start with the left hand side in the lemma, and show that one can indeed decrease j to $j - 1$ at the price of the added terms:

$$\begin{aligned}
& H(K_f^j|Z^j, S^j) + I(M, X^j; Y^j|K_f^j, Z^j, S^j) + H(S^j|Z^j) \\
&= H(K_f^j|Z^j, S^j) + I(M, X^j; Y^j|K_f^j, Z^j, S^j) \\
&\quad + H(S^{j-1}|Z^j) + H(S_j|Z^j, S^{j-1}) \\
&\leq H(K_f^j|Z^j, S^j) + I(M, X^j; Y^j|K_f^j, Z^j, S^j) \\
&\quad + H(S^{j-1}|Z^{j-1}) + H(S_j|Z_j) \\
&= H(K_f^j|Z^j, S^j) + I(M, X^j; Y^{j-1}|K_f^j, Z^j, S^j) \\
&\quad + I(M, X^j; Y_j|Y^{j-1}, K_f^j, Z^j, S^j) \\
&\quad + H(S^{j-1}|Z^{j-1}) + H(S_j|Z_j) \\
&\leq H(K_f^j|Z^j, S^j) + I(M, X^j; Y^{j-1}|K_f^j, Z^j, S^j) \\
&\quad + I(M, Y^{j-1}, K_f^j, Z^{j-1}, S^{j-1}, X^j; Y_j|Z_j, S_j) \\
&\quad + H(S^{j-1}|Z^{j-1}) + H(S_j|Z_j) \\
&\stackrel{(e)}{\leq} H(K_f^j|Z^j, S^j) + I(M, X^j; Y^{j-1}|K_f^j, Z^j, S^j) \\
&\quad + H(S^{j-1}|Z^{j-1}) + I(X_j; Y_j|Z_j, S_j) + H(S_j|Z_j) \\
&\leq H(K_f^j|Z^j, S^j) \\
&\quad + I(M, X^j, Z_j, S_j; Y^{j-1}|K_f^j, Z^{j-1}, S^{j-1}) \\
&\quad + H(S^{j-1}|Z^{j-1}) + I(X_j; Y_j|Z_j, S_j) + H(S_j|Z_j) \\
&\stackrel{(f)}{\leq} H(K_f^j|Z^j, S^j) + I(M, X^j; Y^{j-1}|K_f^j, Z^{j-1}, S^{j-1}) \\
&\quad + H(S^{j-1}|Z^{j-1}) + I(X_j; Y_j|Z_j, S_j) + H(S_j|Z_j) \\
&= H(K_f^j|Z^j, S^j) + I(M, X^{j-1}; Y^{j-1}|K_f^j, Z^{j-1}, S^{j-1}) \\
&\quad + I(X_j; Y^{j-1}|M, X^{j-1}, K_f^j, Z^{j-1}, S^{j-1}) \\
&\quad + H(S^{j-1}|Z^{j-1}) + I(X_j; Y_j|Z_j, S_j) + H(S_j|Z_j) \\
&\stackrel{(g)}{\leq} H(K_f^j|Z^j, S^j) + I(M, X^{j-1}; Y^{j-1}|K_f^j, Z^{j-1}, S^{j-1}) \\
&\quad + H(S^{j-1}|Z^{j-1}) + I(X_j; Y_j|Z_j, S_j) + H(S_j|Z_j) \\
&= H(K_f^j|Z^j, S^j) \\
&\quad + I(M, X^{j-1}, K_f^j; Y^{j-1}|K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad - I(K_f^j; Y^{j-1}|K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad + H(S^{j-1}|Z^{j-1}) + I(X_j; Y_j|Z_j, S_j) + H(S_j|Z_j) \\
&= H(K_f^j|Z^j, S^j) \\
&\quad + I(M, X^{j-1}; Y^{j-1}|K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad + I(K_f^j; Y^{j-1}|M, X^{j-1}, K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad - I(K_f^j; Y^{j-1}|K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad + H(S^{j-1}|Z^{j-1}) + I(X_j; Y_j|Z_j, S_j) + H(S_j|Z_j) \\
&= H(K_f^{j-1}|Z^j, S^j) + H(K_f^j|K_f^{j-1}, Z^j, S^j) \\
&\quad + I(M, X^{j-1}; Y^{j-1}|K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad + I(K_f^j; Y^{j-1}|M, X^{j-1}, K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad + H(K_f^j|Y^{j-1}, K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad - H(K_f^j|K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad + H(S^{j-1}|Z^{j-1}) + I(X_j; Y_j|Z_j, S_j) + H(S_j|Z_j) \\
&\stackrel{(h)}{\leq} H(K_f^{j-1}|Z^j, S^j) \\
&\quad + I(M, X^{j-1}; Y^{j-1}|K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad + I(K_f^j; Y^{j-1}|M, X^{j-1}, K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad + H(K_f^j|Y^{j-1}, K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad + H(S^{j-1}|Z^{j-1}) + I(X_j; Y_j|Z_j, S_j) + H(S_j|Z_j)
\end{aligned}$$

$$\begin{aligned}
&= H(K_f^{j-1}|Z^j, S^j) \\
&\quad + I(M, X^{j-1}; Y^{j-1}|K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad + H(K_f^j|M, X^{j-1}, K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad - H(K_f^j|Y^{j-1}, M, X^{j-1}, K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad + H(K_f^j|Y^{j-1}, K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad + H(S^{j-1}|Z^{j-1}) + I(X_j; Y_j|Z_j, S_j) + H(S_j|Z_j) \\
&\stackrel{(i)}{=} H(K_f^{j-1}|Z^j, S^j) \\
&\quad + I(M, X^{j-1}; Y^{j-1}|K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad + H(K_f^j|M, X^{j-1}, K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad + H(S^{j-1}|Z^{j-1}) + I(X_j; Y_j|Z_j, S_j) + H(S_j|Z_j) \\
&\stackrel{(j)}{\leq} H(K_f^{j-1}|Z^{j-1}, S^{j-1}) \\
&\quad + I(M, X^{j-1}; Y^{j-1}|K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad + H(K_f^j|M, X^{j-1}, K_f^{j-1}, Z^{j-1}, S^{j-1}) \\
&\quad + H(S^{j-1}|Z^{j-1}) + I(X_j; Y_j|Z_j, S_j) + H(S_j|Z_j)
\end{aligned}$$

where (e) is due to the Markov chain $Y_j \leftrightarrow (X_j, Z_j, S_j) \leftrightarrow (M, X^{j-1}, K_f^j, Y^{j-1}, Z^{j-1}, S^{j-1})$; (f) follows from $(S_j, Z_j) \leftrightarrow (M, X^j, K_f^j, Z^{j-1}, S^{j-1}) \leftrightarrow Y^{j-1}$. (g) is because $Y^{j-1} \leftrightarrow (M, X^{j-1}, K_f^j, Z^{j-1}, S^{j-1}) \leftrightarrow X_j$ form a Markov chain. (h) and (j) follow since conditioning reduces the entropy and (i) is due to the Markov chain $(M, X^{j-1}) \leftrightarrow (Z^{j-1}, Y^{j-1}, K_f^{j-1}, S^{j-1}) \leftrightarrow K_f^j$. ■

To continue, we use Lemma 1 recursively starting from (d):

$$\begin{aligned}
nR &\leq H(K_f^n|Z^n, S^n) + I(M, X^n; Y^n|K_f^n, Z^n, S^n) \\
&\quad + H(S^n|Z^n) + n\delta_n \\
&\leq H(K_f^{n-1}|Z^{n-1}, S^{n-1}) \\
&\quad + I(M, X^{n-1}; Y^{n-1}|K_f^{n-1}, Z^{n-1}, S^{n-1}) \\
&\quad + H(S^{n-1}|Z^{n-1}) \\
&\quad + I(X_n; Y_n|Z_n, S_n) \\
&\quad + H(S_n|Z_n) + H(K_n^f) + n\delta_n \\
&\leq H(K_f^{n-2}|Z^{n-2}, S^{n-2}) \\
&\quad + I(M, X^{n-2}; Y^{n-2}|K_f^{n-2}, Z^{n-2}, S^{n-2}) \\
&\quad + H(S^{n-2}|Z^{n-2}) \\
&\quad + I(X_{n-1}; Y_{n-1}|Z_{n-1}, S_{n-1}) \\
&\quad + I(S_{n-1}|Z_{n-1}) + H(K_{n-1}^f) \\
&\quad + I(X_n; Y_n|Z_n, S_n) \\
&\quad + H(S_n|Z_n) + H(K_n^f) + n\delta_n \\
&\leq \dots \\
&\leq \sum_{i=1}^n I(X_i; Y_i|Z_i, S_i) + \sum_{i=1}^n H(S_i|Z_i) \\
&\quad + \sum_{i=1}^n H(K_i^f) + n\delta_n.
\end{aligned}$$

Thus,

$$\begin{aligned}
nR &\leq \sum_{i=1}^n I(X_i; Y_i|Z_i, S_i) + \sum_{i=1}^n H(S_i|Z_i) \\
&\quad + \sum_{i=1}^n H(K_i^f) + n\delta_n.
\end{aligned}$$

We now normalize by n , and use the constraint $\frac{1}{n} \sum_{i=1}^n \log(|K_i^f|) \leq R_f$. We have,

$$R \leq \frac{1}{n} \sum_{i=1}^n I(X_i; Y_i | Z_i, S_i) + \frac{1}{n} \sum_{i=1}^n H(S_i | Z_i) + R_f + \delta_n.$$

To conclude, the well-known technique of introducing a time sharing random variable is used. Assume Q is independent of X^n, Y^n, Z^n, S^n and uniform on $\{1, \dots, n\}$, this results in

$$\begin{aligned} R &\leq R_f + \frac{1}{n} \sum_{i=1}^n (I(X_i; Y_i | Z_i, S_i) + H(S_i | Z_i)) + \delta_n \\ &= R_f + \frac{1}{n} \sum_{i=1}^n (I(X_i; Y_i | Z_i, S_i, Q = i) \\ &\quad + H(S_i | Z_i, Q = i)) + \delta_n \\ &= R_f + I(X_Q; Y_Q | Z_Q, S_Q, Q) + H(S_Q | Z_Q, Q) + \delta_n \\ &= R_f + I(X; Y | Z, S, Q) + H(S | Z, Q) + \delta_n \end{aligned}$$

where $X := X_Q, Y := Y_Q, Z := Z_Q, S := S_Q$.

Now, letting $n \rightarrow \infty$, we get $\delta_n \rightarrow 0$ and $\epsilon_n \rightarrow 0$, we have

$$\begin{aligned} R &\leq R_f + I(X; Y | Z, S, Q) + H(S | Z, Q) \\ &\leq R_f + I(X, Q; Y | Z, S) + H(S, Q | Z) \\ &\leq R_f + I(X; Y | Z, S) + H(S | Z). \end{aligned}$$

Similarly, it is also easy to see that $R \leq I(X; Y | S)$.

From the two above bounds,

$$R \leq \min\{I(X; Y | S), I(X; Y | Z, S) + H(S | Z) + R_f\},$$

and the theorem easily follows.

VII. SPECIAL CASES

We start with the simple reductions, which show that our result generalizes known results in the literature, and conclude with an interesting observation on the case where the CSI is given only to the legitimate receiver.

A. Degraded Channel with no Dependence on the State

When Z is a degraded¹ version of Y and $p(y, z | x, s) = p(y, z | x)$, we have

$$C_S = \max_{p(x)} \min\{I(X; Y) - I(X; Z) + H(S) + R_f, I(X; Y)\}.$$

That is, both S and R_f come into play as keys to increase the secrecy capacity of the *canonical* DMWTC. Of course, in the case there is no state information at all (yet the feedback is still present), the results coincide with those of [4] (Figure 6). That is, equation (7) and the cases where it is tight.

¹Note that [7] lists a few interesting cases for which its bounds are tight. We do not include this list here, and only referred to the degraded version.

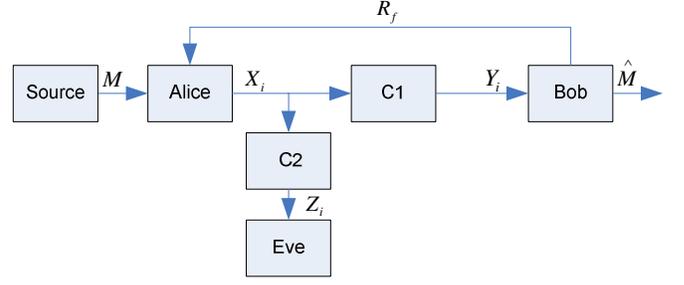


Fig. 6. DMWTC in the presence of feedback.

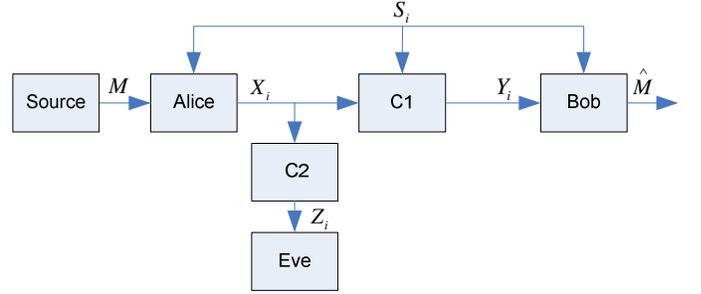


Fig. 7. DMWTC with causal CSI.

B. Less Noisy Eavesdropper

Consider the case where the output of the main channel is more noisy than the output of the eavesdropper channel and $p(y, z | x, s) = p(y, z | x)$. That is, $I(U; Z) \geq I(U; Y)$ for every U such that $U \leftrightarrow X \leftrightarrow (Y, Z)$ from a Markov chain. We have

$$I(U; Y | S) - I(U; Z | S) + H(S | Z) \leq H(S | Z) \leq H(S).$$

Consequently, the secrecy capacity of this special class of channels is

$$C_S = \max_{p(x)} \min\{H(S) + R_f, I(X; Y)\}.$$

In this case, there is no benefit in a regular (Wyner-type) wiretap coding, and secrecy can be achieved *only via the shared keys* (up to the main channel capacity).

C. No Feedback

When the causal CSI is provide to the legitimate sender and legitimate receiver, yet the rate limited feedback is absent, the results easily reduce to those of Chia and El Gamal [7]. describes this case. The secrecy capacity is lower bounded by

$$\begin{aligned} C_S &\geq \max_{p(u|s)} \min_{p(x|u,s)} \{I(U; Y | S) - I(U; Z | S) \\ &\quad + H(S | Z), I(U; Y | S)\}, \\ &\quad \max_{p(u)p(x|u,s)} \min\{H(S | Z, U), I(U; Y | S)\}. \end{aligned} \quad (13)$$

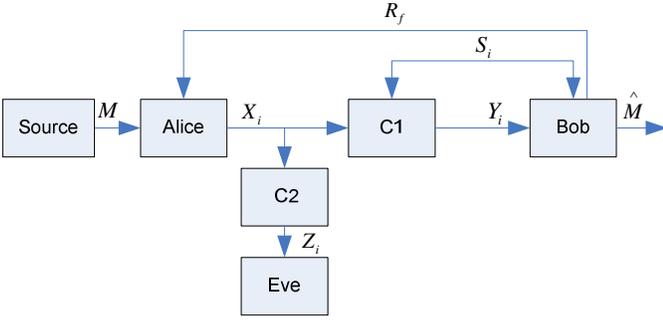


Fig. 8. DMWTC with CSI only at the decoder and in the presence of rate limited feedback.

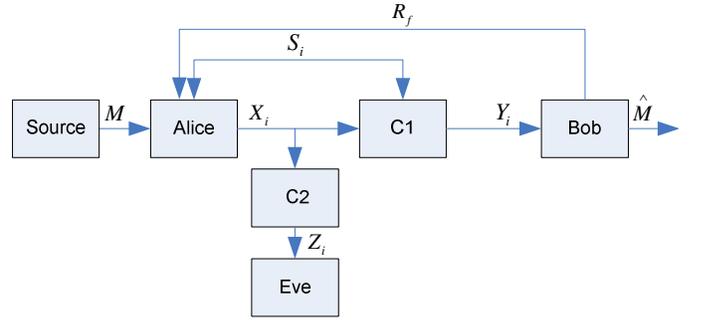


Fig. 9. Wiretap Channel With State Information In The Encoder And Rate Limited Feedback.

D. Causal State Information Only at the Legitimate Decoder

Finally, we consider the following case where the rate limited feedback is available but the causal CSI is given only to the legitimate decoder. Figure 8 depicts this scenario. Note that *without the feedback*, this case coincides with case 3 in [5]. However, even with feedback, when the side information is available only at the decoder, it can be viewed as part of the output, hence the results of [4] essentially apply with $Y' = (Y, S)$. Nevertheless, it is interesting to see that the same results can be achieved without sending keys from an outside source, and, rather, by feeding the state to the encoder. In particular, consider two possible achievable schemes. The first is similar to [4], that is, use the feedback solely in order to send a key to the transmitter, and use this key to encrypt part of the message. The resulting lower bound is

$$\begin{aligned} C_S &\geq I(U; Y, S) - I(U; Z) + R_f \\ &= I(U; S) + I(U; Y|S) - I(U; Z) + R_f \\ &= I(U; Y|S) - I(U; Z) + R_f, \end{aligned}$$

where, S and U are independent and the joint distribution is defined as $p(s)p(u)p(x|u)p(yz|x, s)$.

In the second, *instead of sending fresh randomness through the feedback, the decoder sends the state sequence* (if the rate limit permits). Assume for now that $R_f = H(S)$. The encoder uses this information to *both generate a key and optimize the main channel capacity*, as in the proof of the lower bound \hat{R}_1 when $R_f = H(S)$. In this case, we have

$$C_S \geq \max_{p(u|S)} \min \{ I(U; Y|S) - I(U; Z|S) + H(S|Z), I(U; Y|S) \}. \quad (14)$$

We now show that the achievable scheme which results in (13) is at least as good. We have

$$\begin{aligned} &I(U; Y|S) - I(U; Z) + H(S) \\ &= I(U; Y|S) - H(Z) + H(Z|U) + H(S) \\ &\stackrel{(a)}{=} I(U; Y|S) - H(Z) + H(Z|U, S) + H(S) \\ &= I(U; Y|S) - H(Z) + H(Z|U, S) + H(S, Z) - H(Z|S) \\ &= I(U; Y|S) - H(Z|S) + H(Z|U, S) + H(S|Z) \\ &= I(U; Y|S) - I(U; Z|S) + H(S|Z), \end{aligned}$$

where (a) follows from the Markov chain $S \leftrightarrow U \leftrightarrow Z$. While the two expressions are equal, it is clear that the later achievability scheme is at least as good as the optimization is over all possible $p(u|s)$ and not simply $p(u)$. Of course, since [4] applies here, the benefit can only be in avoiding the need for an outside source of randomness.

When $R_f > H(S)$, the same scheme can be used, yet, in addition to sending the state information from the decoder to the encoder through the secure rate limited feedback, one can send also a key K_f , with $H(K_f) < R_f - H(S)$. The encoding procedure is as in the proof of the lower bound \hat{R}_1 . For this case, the resulting secrecy capacity is bounded by

$$C_S \geq \max_{p(u|s)} \min \{ I(U; Y|S) - I(U; Z|S) + H(S|Z) + H(K_f), I(U; Y|S) \}.$$

Note that, as inferred from [3] and re-assured in [4], the best use of the feedback is in sending a random key, hence, there is no need to send Y or a compressed version of it in the extra rate above $H(S)$.

When $R_f < H(S)$, we conjecture that the preferred scheme is to feedback the *compressed state information* S' , and use it to extract *common randomness*, though, of course, at rate smaller than $H(S)$.

Finally, note that in the case where there is state information only at the encoder and, in addition, a secure feedback is available (Figure 8), similar arguments to the one used above can be used. Thus, we conjecture that by case 4 in [5], [7], and when adding the secure rate limited feedback, the resulting bound is

$$C_S \geq \max_{p(u, x|s)} \min \{ I(U; Y) - I(U; Z|S) + H(S|Z) + R_f, I(U; Y) - I(U; S) \}.$$

VIII. CONCLUSIONS

Physical layer security promises to achieve secret transmission at the expense of transmission rate. While several models in this area, such as the wiretap channel, are well understood, with both capacity results and practical codes, more complex scenarios are still unsolved. For example, in order to apply the concepts of physical layer security to networks with

state information and two way communication, the canonical model of a wiretap channel with state and feedback should be understood.

In this paper, the wiretap channel with causal state information and secure rate limited feedback at the encoder and legitimate decoder is studied. We established upper and lower bounds on the secrecy capacity, and proved their tightness in the case of a less capable eavesdropper. The suggested coding scheme is based on two steps of key generation, one from the causal state information and one from fresh randomness through the rate limited feedback. It was shown that in several special cases, the results reduce to known expressions in the literature.

ACKNOWLEDGMENT

This research was partially supported by DSP Group inc.

REFERENCES

- [1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.
- [2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *Information Theory, IEEE Transactions on*, vol. 24, no. 3, pp. 339–348, 1978.
- [3] R. Ahlswede and N. Cai, "Transmission, identification and common randomness capacities for wire-tape channels with secure feedback from the decoder," in *General Theory of Information Transfer and Combinatorics*. Springer, 2006, pp. 258–275.
- [4] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap channel with secure rate-limited feedback," *Information Theory, IEEE Transactions on*, vol. 55, no. 12, pp. 5353–5361, 2009.
- [5] W. Liu and B. Chen, "Wiretap channel with two-sided channel state information," in *Signals, Systems and Computers, 2007. ACSSC 2007. Conference Record of the Forty-First Asilomar Conference on*. IEEE, 2007, pp. 893–897.
- [6] A. Khisti, S. N. Diggavi, and G. W. Wornell, "Secret-key agreement with channel state information at the transmitter," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, pp. 672–681, 2011.
- [7] Y.-K. Chia and A. El Gamal, "Wiretap channel with causal state information," *Information Theory, IEEE Transactions on*, vol. 58, no. 5, pp. 2838–2849, 2012.
- [8] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.
- [9] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *Information Theory, IEEE Transactions on*, vol. 24, no. 4, pp. 451–456, 1978.
- [10] Y. Chen and A. Han Vinck, "Wiretap channel with side information," *Information Theory, IEEE Transactions on*, vol. 54, no. 1, pp. 395–402, 2008.
- [11] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 2, pp. 704–716, 2012.
- [12] J. Li and A. P. Petropulu, "Optimality of beamforming for secrecy capacity of MIMO wiretap channels," in *Information Forensics and Security (WIFS), 2012 IEEE International Workshop on*. IEEE, 2012, pp. 276–281.
- [13] —, "Ergodic secrecy rate for multiple-antenna wiretap channels with Rician fading," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, pp. 861–867, 2011.
- [14] F. Renna, N. Laurenti, and H. V. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 4, pp. 1354–1367, 2012.
- [15] H. Boche and R. F. Wyrembelski, "Comparison of different attack classes in arbitrarily varying wiretap channels," in *Information Forensics and Security (WIFS), 2012 IEEE International Workshop on*. IEEE, 2012, pp. 270–275.
- [16] U. M. Maurer, "Secret key agreement by public discussion from common information," *Information Theory, IEEE Transactions on*, vol. 39, no. 3, pp. 733–742, 1993.
- [17] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. part i: secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, 1993.
- [18] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. ii. cr capacity," *Information Theory, IEEE Transactions on*, vol. 44, no. 1, pp. 225–240, 1998.
- [19] M. Bloch and J. Barros, *Physical-layer security*. Cambridge University Press, 2011.
- [20] M. Bloch, R. Narasimha, and S. W. McLaughlin, "Network security for client-server architecture using wiretap codes," *Information Forensics and Security, IEEE Transactions on*, vol. 3, no. 3, pp. 404–413, 2008.
- [21] N. Cai and R. W. Yeung, "Secure network coding on a wiretap network," *Information Theory, IEEE Transactions on*, vol. 57, no. 1, pp. 424–435, 2011.
- [22] S. El Rouayheb, E. Soljanin, and A. Sprintson, "Secure network coding for wiretap networks of type II," *Information Theory, IEEE Transactions on*, vol. 58, no. 3, pp. 1361–1371, 2012.
- [23] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the gaussian wiretap channel," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, pp. 532–540, 2011.
- [24] C. W. Wong, T. F. Wong, and J. M. Shea, "Secret-sharing LDPC codes for the BPSK-constrained gaussian wiretap channel," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, pp. 551–564, 2011.
- [25] A. Subramanian, A. Thangaraj, M. Bloch, and S. W. McLaughlin, "Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, pp. 585–594, 2011.
- [26] A. El Gamal and Y.-H. Kim, *Network information theory*. Cambridge University Press, 2011.
- [27] T. M. Cover and M. Chiang, "Duality between channel capacity and rate distortion with two-sided state information," *Information Theory, IEEE Transactions on*, vol. 48, no. 6, pp. 1629–1638, 2002.