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 legitimate receiver. In addition, the legitimate receiver can send secure feedback to the transmitter at a limited rate $R_f$. We shown that the secrecy capacity is bounded by

$$CS \geq \max \{ \max_{p(u|v)p(x|u)} \min \{ I(U;Y|V) - I(U;Z|V) \\ + H(V|Z) + R_f, I(U;Y|V) \}, \max_{p(v)p(x|u)} \min \{ H(V|Z,U) + R_f, I(U;Y|V) \} \}.$$ 

Moreover, when the channel to the legitimate receiver is less noisy than the channel to the eavesdropper, the bound is shown to be tight. The capacity achieving scheme is based on both the Wyner wiretap coding and two steps of shared-key generation: one from the state information and one via the noiseless feedback. Finally, we consider several special cases. When state information is available only at the legitimate receiver, the analysis suggests that unlike previous results involving feedback, it is better to use the feedback to send the state information to the transmitter (when possible), rather than send a random key.

I. INTRODUCTION

The increasing demand for network connectivity and high data rates dictate efficient utilization of resources, such as sharing of a common medium for communication. However, in many practical applications, it is important to assure privacy is not compromised. Privacy, however, has its price. On the one hand, one may use cryptographic schemes to protect data from eavesdropping. Such schemes usually involve a computational burden. Information theoretic security, however, offers privacy at the price of transmission rate. Indeed, in recent years, information theoretic security was found useful from physical layer [1] schemes to networking applications [2].

A canonical model for information theoretic security was given by Wyner in [3]. Therein, the wiretap channel, described in Figure 1 was introduced. In a wiretap channel, Bob receives the transmitted message of Alice via a channel $C_1$, called the main channel. The eavesdropper Eve, however, observes information transmitted by Alice through the wiretap channel, $C_2$. The legitimate parties wish to communicate through $C_1$ while concealing the information from Eve. Hence, Alice wishes to encodes its message $M$ and transmit a codeword $X^n$ on the channel $C_1$. Bob receives $Y^n$, while Eve receives $Z^n$. The legitimate pair’s objectives are security, that is, $Z^n$ should provide no information about $M$ (more precisely, $\frac{1}{n} I(M;Z) \to 0$ as $n \to \infty$), and reliability, that is, $M$ should be decoded from $Y^n$ with a negligibly small probability of error. The rate at which both objectives can be fulfilled is called the secrecy capacity. For discrete memoryless wiretap and eavesdropper channels (DMCs), Wyner showed that the secrecy capacity is

$$C_s = \max_{U \leftrightarrow X \\ Y,Z} \{ I(U;Y) - I(U;Z) \}.$$ 

When the main channel is “less noisy” than the wiretap channel, this reduces to

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

An important concept in the achieveability of the above result is the added randomness, used to confuse the eavesdropper regarding the actual message sent.

The current literature includes several generalizations of the canonical model given in [3]. We include here only the most relevant. A thorough discussion of related works is given in Section III in [4]. Ahlswede and Cai considered a discrete memoryless wiretap channel with secure output feedback. A general feedback link was considered by Ardestanizadeh et al. in [5]. 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 [6], 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 [7]. The work in [6] was later extended in [8] when causal state information is available by Chia and El Gamal. At the heart of Chia and El Gamal’s methods stands a key generation scheme. Again, this key, shared by Alice and Bob, was used to increase the secrecy capacity. The works in [6]–[8] do not include a feedback link.

A. Main Contribution

In this work, we consider the system depicted in Figure 2 in [6]. In this setting, both channel state information (CSI) and feedback are available. We derive upper and lower bounds on the secrecy capacity, and show that when the main channel is less noisy than the eavesdropper’s, the bounds are tight and describe the secrecy capacity exactly. In the direct, 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 link. The converse is more involved, and requires showing that indeed such a use of the feedback link is optimal. We prove the converse 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. Moreover, when state information is available only at the legitimate decoder, a comparison of achievable schemes suggests that, unlike previously known results [5], one should not use the feedback to send fresh randomness (to be used as a shared key), but rather losslessly describe the state to the transmitter.

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 in practice. 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 (available through estimation or two way communication) are available, 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. Section V includes a description of a few important special cases. As for the proofs, Section VII includes the direct, while Section VIII includes the converse. Section IX concludes the paper.

II. PROBLEM FORMULATION

In this section, we formally define the problem at hand. A discrete memoryless wiretap channel (DMWTC) in the presence of secure rate limited feedback and causal state information is given in Figure 2. In this case, both Alice the encoder and Bob the decoder have access to the state information $V_i$. In general, the state information can be available non-causally as in [6] or causally as in [8]. In this paper, we focus on the causal case. Alice desire is keeping Eve ignorant as possible from the confidential message, denoted as $M \in \{1, \ldots, 2^{nR}\}$, 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 $(X_1, \ldots, X_n) = X^n$, $X \in X$, the output at the legitimate receiver is $Y^n$, $Y \in Y$, and the output at the eavesdropper is $Z^n$, $Z \in Z$. The main channel is affected by a memoryless state sequence $V^n$, $V \in V$, known causally to both the encoder and the legitimate decoder. We assume a memoryless channel, that is,

$$p(Y^n|X^n, V^n) = \prod_{i=1}^{n} p(y_i|x_i, v_i),$$

$$p(Z^n|X^n, V^n) = \prod_{i=1}^{n} p(z_i|x_i, v_i).$$

In the case where just the main channel is affected by the state information, the cross-over probabilities at the wiretap channel are

$$p(Z^n|X^n, V^n) = \prod_{i=1}^{n} p(z_i|x_i).$$

We assume a rate-limited feedback at rate $R_f$ is available from the decoder to the encoder. That is, symbols $K_i \in \{K_1, \ldots, K_n\}$ are sent over a feedback link, secretly from the eavesdropper. The feedback alphabets are denoted as $\{K_i, \ldots, K_n\}$. Thus, their cardinalities must satisfy

$$\frac{1}{n} \sum_{i=1}^{n} \log(|K_i|) \leq R_f. \quad (1)$$

The causal dependency of the symbol $K_i$ at instant $i$ comes from the fact that it only depends on prior outputs up to instant...
i − 1 of the channel $Y_{i−1} = (Y_1, \ldots, Y_{i−1})$ and the prior symbols $(K_f^0, \ldots, K_f^0) = K_f^{i−1}$. Note that, with a slight misuse of notation, a single instant of the feedback value at time $i$ is denoted $K_f^i$ while the vector $(K_f^0, \ldots, K_f^i)$ 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

$$p(k_f^i | y_i, k_f^{i−1}).$$

Thus, the 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 $\{1, \ldots, 2^{nR}\}$; The conditional probability distributions of the stochastic coding for the legitimate encoder

$$p(x|m, x_{i−1}, v_i, k_f^i),$$

where $m$ denotes the message to be sent; The conditional probability distributions of the (possibly) random feedback

$$p(k_f^i | y_i, k_f^{i−1})$$

and a decoding map

$$\tilde{m} : Y^n \times V^n \times K_f^n \rightarrow \{1, \ldots, 2^{nR}\}.$$

The decoded message is thus

$$\tilde{M} = \tilde{m}(Y^n, V^n, K_f^n).$$

The message $M$ at the legitimate encoder is distributed uniformly over $\{1, \ldots, 2^{nR}\}$, thus $R = \frac{1}{n} H(M)$. The normalized equivocation $d$ at the eavesdropper is defined as

$$d = \frac{H(M|Z^n)}{H(M)}.$$

Denote the error probability $p(\tilde{M} \neq M)$ as $P_e(n)$. If for any $\epsilon > 0$, there exists an $(2^{nR}, 2^{nR_f}, n)$ code satisfying

$$R \geq R^* - \epsilon, \quad R_f \geq R_f^* + \epsilon, \quad d \geq d^* - \epsilon,$$

we say that the rate/normalized equivocation tuple $(R^*, R_f^*, d^*)$ is achievable. 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 (2). Namely, tuples where asymptotically, the eavesdropper is ignorant of the message sent.

### III. Related Work

The first information theoretic study on the problem of securely transmitting a message over a public channel was done in [9]. 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 discussed in Section [4] (Figure [4]) was presented in [3], 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. In [3], indeed Wyner proved that when the wiretap channel is a degraded version of the main channel, the secrecy capacity is positive. [10] extended this and concluded that a positive secrecy capacity is possible whenever the main channel is less noisy than the wiretap. Moreover, as was later discussed in [5], [6], [8], 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 [6], a DMWTC with CSI at both ends was discussed. The conditional probability of the main channel was specified through $P(y|x, v_1, v_2)$, were the CSI $V^n$ was given non-causally at the encoder while $V^n_2$ was given non-causally at the decoder. The CSI $V^n_1$ at the encoder and $V^n_2$ at the decoder have some joint probability distribution. The conditional probability of Eve’s channel was $p(z|x, v_1, v_2)$.

Therein, the following information rates were defined.

$$R_{U1} = I(U; Y, V_2) - \max\{I(U; Z), I(U; V_1)\},$$

$$R_{U2} = I(U; Y, V_2) - I(U; V_1).$$

$U$ was an auxiliary random variable and, in addition, a Markov condition $U \leftrightarrow (X, V_1, V_2) \leftrightarrow (Y, Z)$ must hold. It was shown that the set

$$R_s = \bigcup_{U \leftrightarrow (X, V_1, V_2) \leftrightarrow (Y, Z)} (R, d),$$

is achievable, where $Rd = R_{U1}$ for $0 \leq d \leq 1$ and $0 \leq R \leq R_{U2}$. The formulation above is based on the definitions in [11], [12]. For example, in the Gaussian case, the complete rate equivocation region $R_L$ given by $Rd \leq C_s^*$ and $R \leq C_M$, where the main channel capacity is $C_M$ and the secrecy capacity is $C_s^*$. Under these definitions, the achievability of the entire region was established by considering the two extreme points, $(C_s^*, 1)$ and $(C_M; C_s^*/C_M)$, and applying a time sharing argument. The point $(R, 1)$ is defined as perfect secrecy. Indeed, note that the result of Liu and Chen gives rise to the special case of

$$R \leq \max_{U \leftrightarrow (X, V_1, V_2) \leftrightarrow (Y, Z)} \min\{R_{U1}, R_{U2}\}$$

when $d = 1$. This is an achievable rate for the wiretap channel with two-sided non-causal state information. We will be interested in a special case, where the state information is available only at the receiver, that is $V_1 = 0, V_2 = V$. In this case, we have

$$R_{U1} = I(U; Y, V) - I(U; Z)$$

$$R_{U2} = I(U; Y, V) - I(U; V).$$
In a recent paper [8], 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 [6]. In particular, when the wiretap channel is physically degraded $p(y,z|x) = p(y|x)p(z|y)$, the upper bound is tight, establishing (5) as the secrecy capacity.

C. Practical Coding Schemes

Finally, we mention that the current literature includes several practical coding schemes for wiretap channels, rendering them as desirable solutions for physical layer security. Practical schemes for the Gaussian wiretap channel using LDPC codes were suggested in [18], as well as in [19] to suggest secret sharing schemes. LDPCs were also used to allow strong secrecy over a binary erasure channel in [20]. Practical schemes under OFDM signaling were discussed in [1]. The theory and practice of wiretap channel coding has been found useful in a variety of networking scenarios as well. In [2], 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].

IV. MAIN RESULTS

In this section, we list the main results of the paper. Direct and converse proofs are given in Section VI and Section VII respectively.

A. Lower Bound

The achievability part presented in this paper, proves that the rate equivocation region for a DMWTC in presence of rate-limited feedback and causal SCI at the encoder and decoder is dictated by the following three rates:

$$R_{U1} = I(U;Y|V) - I(U;Z|V) + H(V|Z) + R_f,$$

$$R_{U2} = I(U;Y,V) - I(U;V) = I(U;Y|V),$$

$$R_{U3} = H(V|Z,U) + R_f.$$  

For a given $R_f$, let $R_d$ denote the pairs $(R,d)$ such that

$$0 \leq R \leq R_{U2},$$

$$0 \leq d \leq 1,$$

$$R \cdot d \leq \max\{R_{U1}, R_{U3}\}.$$

The achievability of the entire rate region can be proved by proving the achievability of the rate equivocation pairs

$$\max\{(R_{U1},1), (R_{U3},1)\},$$

$$\max\{(R_{U2}, d_{U2} = \frac{R_{U1}}{R_{U2}}), (R_{U2}, d_{U2} = \frac{R_{U3}}{R_{U2}})\}.$$  

In this paper, we focus on (6), and thus prove the following secrecy capacity lower bound.

Theorem 1. Assume a DMWTC, when causal CSI is given at the legitimate encoder and at the legitimate decoder and output symbols (we allow general feedback in this work as well). The upper bound in [5] was

$$C_s(R_f) \leq \max_{p(x)} \min\{I(X;Y|Z) + R_f, I(X;Y)\}. \quad (5)$$

Again, when the wiretap channel is physically degraded $p(y,z|x) = p(y|x)p(z|y)$, the upper bound is tight, establishing (5) as the secrecy capacity.
in the presence of rate limited feedback. Then, the secrecy capacity is lower bounded as
\[
C_S \geq \max_{p(x|v)} \min \{ I(U; Y|V) - I(U; Z|V) + H(V|Z) + R_f, I(U; Y|V) \},
\]
max \{ I(U; Y|Z, U) + R_f, I(U; Y|V) \}.

B. Upper Bound

Our converse result is the following.

**Theorem 2.** Assume a DMWTC, when the causal CSI is given at the legitimate encoder and at the legitimate decoder and in the presence of rate limited feedback. Then, the secrecy capacity is upper bounded as
\[
C_S \leq \max_{p(x|v)} \min \{ I(X; Y|V) - I(X; Z|V) + H(V|Z) + R_f, I(X; Y|V) \}.
\]

C. Complete Characterization of the Secrecy Capacity

It is interesting to investigate the cases where the lower and upper bound match. Indeed, if, in addition to the original Markov condition, we also have \( I(U; Z|V) \leq I(U; Y|V) \), i.e., if the output of the eavesdropper channel is more noisy (or degraded) than the output of the main channel, by a simple application of the data processing inequality and the above assumption we have the following.

**Corollary 1.** Assume a DMWTC, when the causal CSI is given at the legitimate encoder and at the legitimate decoder and in the presence of rate limited feedback. If the main channel is less noisy than the wiretap channel, then the secrecy capacity is
\[
C_S = \max_{p(x|v)} \min \{ I(X; Y|V) - I(X; Z|V) + H(V|Z) + R_f, I(X; Y|V) \}.
\]

**Example 1.** In this 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 clean 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,
\[
\begin{align*}
p_{y|x}(0|0) &= 1 - p_y, \quad p_{y|x}(0|1) = p_y \\
p_{y|x}(1|1) &= 1 - p_y, \quad p_{y|x}(1|0) = p_y.
\end{align*}
\]
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 clean feedback and CSI is shown in Figure 3 B. Now, the main \( BSC(p_{v_0}) \) if the state at time \( i \) is \( v_i \). The wiretap channel is a cascade of this channel and \( BSC(p_z) \).

The maximum of \( C^N_{SV}(R_f) \) (over the input distribution), i.e., the capacity of the degraded DMWTC without CSI yet with feedback, and the maximum of \( C^V_{SV}(R_f) \), 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 \( p_y \cdot p_z = p_{y_0}(1 - p_{z_0}) + (1 - p_{y_0})p_z \), 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
\[
I(X; Y) - I(X; Z) = h(p_y) - h(p_y \cdot p_z).
\]

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 \( P(V = v_0) = 1 - q \) and \( P(V = v_1) = q \). When \( V = v_0 \), \( p_{y|x,v}(y|x,0) = 1 - p_{v_0} \) if \( x = y \) and \( p_{v_0} \) otherwise.

When \( V = v_1 \), \( p_{y|x,v}(y|x,1) = 1 - p_{v_1} \) if \( x = y \) and \( p_{v_1} \) otherwise. Hence, for the case with state information, we have
\[
I(X; Y|V) = 1 - (1 - q) h(p_{v_0}) - q h(p_{v_1}).
\]
Furthermore, with the symmetric input distribution as in this example, it is not hard to verify that \( I(Z; V) = 0 \). Thus,
\[
H(V|Z) = H(V) = h(q).
\]

As for the wiretap channel, we have
\[
I(X; Z|V) = 1 - (1 - q) h(p_{v_0} \cdot p_z) - q h(p_{v_1} \cdot p_z).
\]

Hence,
\[
I(X; Y|V) - I(X; Z|V) + H(V|Z) \\
= 1 - (1 - q) h(p_{v_0}) - q h(p_{v_1}) \\
- \{1 - q h(p_{v_1} \cdot p_z) - (1 - q) h(p_{v_0} \cdot p_z)\} \\
+ h(q) \\
= (1 - q) h(p_{v_0} \cdot p_z) + q h(p_{v_1} \cdot p_z) \\
- (1 - q) h(p_{v_0}) - q h(p_{v_1}) + h(q).
\]

As a result, the capacities to compare are
\[
C^V_{SV}(R_f) = \min \{1 - (1 - q) h(p_{v_0}) - h(p_y) \cdot p_z - h(p_y) \cdot p_z + R_f\}
\]
and
\[
C^N_{SV}(R_f) = \min \{1 - (1 - q) h(p_{v_0}) - q h(p_{v_1}), \\
(1 - q) h(p_{v_0} \cdot p_z) + q h(p_{v_1} \cdot p_z) \\
- (1 - q) h(p_{v_0}) - q h(p_{v_1}) + h(q) + R_f\}.
\]

Numerical results for the capacities above are given in Figures 5 and 6. The cross-over probabilities are fixed on \( p_z = p_y = 0.1, p_{v_0} = 0.05 \) and \( p_{v_1} = 0.15 \). Figure 6 gives the capacities \( C^N_{SV}(R_f) \) and \( C^V_{SV}(R_f) \) 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 possible probabilities for each state
A. Degraded Channel with no Dependence on the State

When $Z$ is a degraded\footnote{Note that [8] 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.} version of $Y$ and $p(y, z|x, v) = p(y|x)\cdot p(z|v)$, we have

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

That is, both $V$ 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 [5] (Figure 6). That is, equation (5) and the cases where it is tight.

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 $p(y, z|x, v) = p(y, z|x)$. 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

$$I(U; Y|V) - I(U; Z|V) + H(V|Z) \leq H(V|Z) \leq H(V).$$
Consider two possible achievable schemes for this scenario. The first is as follows. Using a scheme similar to the one used in the achievability herein, 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

\[ C_S \geq I(U;Y|V) - I(U;Z) + R_f \]

\[ = I(U;V) + I(U;Y|V) - I(U;Z) + R_f \]

\[ = I(U;Y|V) - I(U;Z) + R_f, \]

(9)

where, \( V \) and \( U \) are independent and the joint distribution is defined as \( p(v)p(u)p(x|u)p(yz|x,v) \).

However, in this case, it is interesting to discuss a different achievable scheme, where instead of sending fresh randomness through the feedback, the decoder sends the state sequence (if the rate limit permits). The question that then arises is, of course, which scheme is more capable: sending a random key or sending the state sequence?

Assume for now that \( R_f = H(V) \). By (9), when a secret key is sent through the feedback channel, we have the following bound on the secrecy capacity:

\[ C_S \geq \max_{p(u)} \min \{ I(U;Y|V) - I(U;Z) + H(V), I(U;Y|V) \}. \]

If instead of sending a key through the secure rate-limited feedback, one sends the state information, and the encoder uses this information to both generate a key and optimize the main channel capacity, as in the proof of the lower bound \( R_{U1} \) when \( R_f = H(V) \), by (8), we have

\[ C_S \geq \max_{p(u|v)} \min \{ I(U;Y|V) - I(U;Z) + H(V|Z), I(U;Y|V) \}. \]

(10)

We now show that the achievable scheme which results in

---

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

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

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

In case where 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 [8]. Figure 7 describes this case. The secrecy capacity is lower bounded by

\[ C_S \geq \max \{ \max_{p(u|v)p(x|u,v)} \min \{ I(U;Y|V) - I(U;Z|V) + H(V|Z), I(U;Y|V) \}, \max_{p(u)p(x|u,v)} \min \{ H(V|Z,U), I(U;Y|V) \} \}. \]

(8)

\[ = \max \{ \max_{p(u|v)p(x|u,v)} \min \{ I(U;Y|V) - I(U;Z|V) + H(V|Z), I(U;Y|V) \} \}. \]

(10)

We now show that the achievable scheme which results in

---

**Fig. 6.** DMWTC in the presence of feedback.

**Fig. 7.** DMWTC with causal CSI.

**Fig. 8.** DMWTC with CSI only at the decoder and in the presence of rate limited feedback.
(10) is indeed favorable. We have
\[
I(U; Y | V) - I(U; Z) + H(V)
\]
where (a) follows from the Markov chain \( V \leftrightarrow U \leftrightarrow Z \). While the two expressions are equal, it is clear that the later achievability scheme is favorable as the optimization is over all possible \( p(u | v) \) and not simply \( p(u) \). This is similar to the difference between channel coding with state at both encoder and decoder compared to state only at the decoder.

When \( R_f > H(V) \), 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 \( H(K_f) < R_f - H(V) \). The encoding procedure is as in the proof of the lower bound \( R_{U1} \). For this case, the resulting secrecy capacity is bounded by

\[
C_S \geq \max_{p(u | v)} \min\{I(U; Y | V) - I(U; Z | V) + H(V | Z) + H(K_f), I(U; Y | V)\}.
\]

When \( R_f < H(V) \), we conjecture that the preferred scheme is to send through the secure rate limited feedback the compressed state information \( V' \), and use it to extract common randomness, though, of course, at rate smaller than \( H(V) \).

Remark 1. Note that in the case where there is state information only at the encoder and, in addition, a secure feedback is available (Figure 9), similar arguments to the one used above can be used. Thus, we conjecture that by case 4 in [6], [8], and when adding the secure rate limited feedback, the resulting bound is

\[
C_S \geq \max_{p(u, x | v)} \min\{I(U; Y) - I(U; Z | V) + H(V | Z) + R_f, I(U; Y) - I(U; V)\}.
\]

VI. LOWER BOUND (DIRECT)

A. Achievability of \( R_{U1} \)

Consider the rate equivocation pair \((R_{U1}, 1)\), where

\[
R_{U1} = \max_{p(u | v)p(x | u, v)} \{I(U; Y | V) - I(U; Z | V) + H(V | Z) + R_f\}.
\]

Similar to [8], we perform the maximization in \( R_{U1} \), through distributions \( p(u'), p(x'u, v) \) and functions of the form \( u'(u', v) \), using the functional representation lemma [23]. This way, the achievability can be proved for an equivalent characterization of \( R_{U1} \),

\[
\max_{p(u'), u(x'u, v), p(x | u, v)} \{I(U'; Y, V) - I(U'; Z, V) + H(V | Z) + R_f\}.
\]

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

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

a) Encoding of Legitimate Sender (Alice): The encoding scheme in this case requires the transmission of only \( B-1 \) independent (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 \( u(u', v) \), we set the following three rates:

\[
\begin{align*}
R_0 &= I(U'; Y, V) - I(U'; Z, V) - 2\epsilon, \\
R_1 &= H(V | Z) - \epsilon, \\
R_2 &= R_f.
\end{align*}
\]

The coding scheme we suggest will correspond to a transmission rate

\[
R = R_0 + R_1 + R_2 = R_{U1} - 3\epsilon,
\]

secretly from the eavesdropper. We encode the message in three steps. In particular, we split the message \( M_i, j \in \{2, \ldots, B\} \), into three independent messages \( M^0_i \in \{1, \ldots, 2^{nR_0}\} \), \( M^1_i \in \{1, \ldots, 2^{nR_1}\} \) and \( M^2_i \in \{1, \ldots, 2^{nR_2}\} \). The message at rate \( R_0 \) will be the one protected by the Wyner wiretap coding scheme, while the messages at rate \( R_1 \) and \( R_2 \) will be the ones protected by the keys: a message at rate \( R_1 \) protected by the key generated from the state information and a message at rate \( R_2 \) protected by the key received in the feedback link.

The first step is the generation of the message codebook. We randomly generate \( 2^{nI(U'; Y, V) - \epsilon} \) i.i.d sequences \( u'(u', v) \), using the distribution of the auxiliary, that is, \( P(U' = u'_i) = \prod_{i=1}^{n} P_{U'}(u'_i) \). Then, these sequences are distributed...
randomly into $2^{nR_0}$ equal size bins. The index of each bin is denoted as $j \in \{1, 2, \ldots, J = 2^{nR_0}\}$. 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 $C(n^0, m^1, m^2)$.

In the next step we create the keys from the given channel state information. We bin the channel state sequences $v^n$ at random into $2^{nR_1}$ bins $\{B(k_v)\}_{k_v=1}^{2^{nR_1}}$. The key $K_{V,j}^1$ used in block $j$ is the bin index of the state sequence $V^n(j-1)$ in block $j-1$. Thus, the message $M^1$ in block $j$ is encrypted with the key $K_{V,j}^1$.

The third step is the generation of the feedback codebook. As mentioned before, similar to the technique in [3], 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 $k_{j}^1$ 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.

Finally, to encode the first block of the message $M_1$, given $M_0^0$, $M_1^0$ and $M_2^0$, the encoder selects a random codeword $u^n(L)$ from $C(M_0^0, M_1^0, M_2^0)$. Then it computes $u_i = u(u_i(L), v_i)$ and the symbol transmitted is a random one, according to $X_i \sim p(x_i|v_i, u_i)$ for $i \in \{1 \ldots n\}$. 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, $k_{j-1}^0$ from the state sequence and $k_{j-1}^1$ from the feedback. Thus, to encode the $j$-th block of the message $M_j, j \in \{2, \ldots, B\}$, given $M_0^j, M_1^j$ and $M_2^j$, the encoder selects a random codeword $u^n(L)$ from $C(M_0^j, M_1^j, \oplus k_{j-1}^0, M_2^j \oplus k_{j-1}^1)$. $\oplus$ denotes modulo-$2^{R_1}$ and $2^{R_2}$ additions. It then computes $u_i = u(u_i(L), v_i)$ and the symbol transmitted is, again, random, according to $X_i \sim p(x_i|v_i, u_i)$ for $i \in \{(j-1)n + 1 \ldots jn\}$.

Note that $M_0^0$, similar to [3], is protected using the regular Wyner coding scheme, therefore the eavesdropper cannot comprehend this part from the message when $I(U^j; Y, V_j) - I(U^j; Z, V_j) > 0$. The second part of message $M^1$ is encrypted with the key $k_{j-1}^0$ and the third part of the message $M^2$ is encrypted with the key $k_{j-1}^1$.

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 $(u^n(L), y^n(j), v^n(j))$ 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, $2^{n[I(U^n; Y; V^n) - \epsilon]}$, is similar to that in [3], 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 $m_0^0, m_1^j$ and $m_2^j$ are decoded correctly with high probability.

As for the decoding at the j-th block $j \in \{2, \ldots, B\}$, the decoder uses a similar procedure to retrieve $m_0^0, m_1^j \oplus k_{j-1}^0$ and $m_2^j \oplus k_{j-1}^1$. It then uses $k_{j-1}^1$ to retrieve $m_1^j$ and $k_{j-1}^0$ to retrieve $m_2^j$. It is thus easy to verify that a rate $R_{U1} = \min[I(U^n); Y | V] - I(U^n; Z | V) + H(V | Z) + R(f) - \delta_n, I(U^n; Y | V)]$ can be achieved.

c) Information Leakage at the Eavesdropper (Eve):
For $j \in \{1, \ldots, B\}$ we let $Z^0_j$ denote the eavesdropper’s observation in block $j$. The information leaked $L(C_{n,B})$, given the codebook and coding procedure $C_{n,B}$ is then

$$\frac{1}{nB} L(C_{n,B}) = \frac{1}{nB} I(M_0^1 \ldots M_B^1 \ldots M_B^1 \ldots M_B^1 | M_B^2 \ldots M_B^2; Z^n \ldots Z^n | \tilde{C}_{n,B})$$

$$= \frac{1}{nB} I(M_0^1 \ldots M_B^1 \ldots M_B^1 \ldots M_B^1; Z^n \ldots Z^n | \tilde{C}_{n,B})$$

$$+ \frac{1}{nB} \sum_{j=1}^{B} I(M_j^0; Z_j^n | M_0^1 \ldots M_B^1 \ldots M_B^1 \ldots M_B^1 | \tilde{C}_{n,B})$$

$$= \frac{1}{nB} I(M_0^0 \ldots M_B^0 \ldots M_B^0 \ldots M_B^0 | Z^n \ldots Z^n | \tilde{C}_{n,B})$$

$$= \frac{1}{nB} I(M_0^0 \ldots M_B^0 \ldots M_B^0 \ldots M_B^0; Z^n \ldots Z^n | \tilde{C}_{n,B})$$

In the above (a) results from the chain rule for mutual information, (b) results since $M_0^j$ depend only on $Z_0^j$, and (c) is since for each $M_0^j$, the message is xored with random bits before the generation of the sent sequence $X^n(j)$, hence is independent of the channel output. As for the remaining term, 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 [8], this leakage is negligible. Hence, we conclude that $(R_{U1}, 1)$ is achievable with

$$R_{U1} = I(U^n; Y | V) - I(U^n; Z | V) + H(V | Z) + R_f.$$  

2) Second Case - $I(U^n; Y, V) \leq I(U^n; Z, V)$: 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 $(I(U^n; Y | V) - I(U^n; Z | V)) + (H(V | Z) + R_f) > 0$. Otherwise for this case the secrecy capacity is zero. The same key splitting as in [8] is used.

In short, in the block $j \in \{2 \ldots B\}$, we split the message to three parts as before, yet protect the first two with the state key. The state information key $k_{j-1}^0$ is split to two independent parts, $k_{j-1}^{0,0}$ and $k_{j-1}^{0,1}$ at rates which coincides with case 2 of $R_{S-CS1-1}$ in [8]. Thus, compared with the first case of $R_{U1}$, to send message $M_j, j \in \{2 \ldots B\}$, transmit $X^n(k_{j-1}^{0,0}, M_0^1 \oplus k_{j-1}^{0,0}, M_0^2 \oplus k_{j-1}^{0,1}) \in C_a$. Again, joint typicality decoding is used, together with the knowledge of the keys and the state information to decode message $M_j$.

The reminder of the proof is very similar to [8].
B. Achievability of $R_{U^3}$

For $R_{U^3}$, we have $R_{U^3} = H(V|Z,U) + R_f$. In this case, to encode the message we use purely the key $K_e$ in the block, which coincides with $R_{S-CSI-2}$ in Chia and El Gamal [8]. Thus, we split the message $M_j, j \in \{2,\ldots,B\}$, into two independent messages $M^1 \in \{1,\ldots,2^{nR_1}\}$ and $M^2 \in \{1,\ldots,2^{nR_2}\}$, where $R \geq R_0 + R_2$ and $I(U';Y,V) - 3\epsilon > R$, such that to send message $M_j, j \in \{2\ldots B\}$ given $M^1_j$ and $M^2_j$, transmit $X^n(M^1_j \oplus k^{v_n}_j, M^2_j \oplus k^{f_{j-1}}_n) \in C_n$ using Shannon’s strategy. The decoder uses join typicality decoding together with the knowledge of the keys and the state information to decode message $M_j$.

C. Achievability When the Causal State Information is not Available at the encoder yet Available at the Decoder

For the case where the state information is not available at the encoder yet available at the decoder, compared with the $R_{U^1}$ case, we split the message $M_j, j \in \{2,\ldots,B\}$, into two independent messages $M^0 \in \{1,\ldots,2^{nR_1}\}$ and $M^2 \in \{1,\ldots,2^{nR_2}\}$, where $R \geq R_0 + R_2 - 3\epsilon$. To send message $M_j, j \in \{2,\ldots b\}$ given $M^0_j$ and $M^2_j$, transmit $X^n(M^0_j \oplus k^{v_n}_j, M^2_j \oplus k^{f_{j-1}}_n) \in C_n$ using Fano’s inequality, for $\hat{M} = \hat{m}(X^n, K^n_j, V^n)$, $H(M|\hat{M}) \leq 1 + P_{e}^{(n)}nR = n\epsilon_n$, where $\epsilon_n \to 0$ as $n \to \infty$ if $P_{e}^{(n)} \to 0$. Since $\hat{M}$ is a function of $V^n, K^n_j, V^n$, $H(M|\hat{M}) \leq n\epsilon_n$.

Using the secrecy constraint, $I(M;Z^n) = n\gamma_n$, (17)

where $\gamma_n \to 0$ as $n \to \infty$. Consequently, $nR = H(M) = H(M|Z^n) + I(M;Z^n)$

(a) $H(M|Z^n) + n\gamma_n = I(M;Y^n, K^n_j, V^n|Z^n) + H(M|Y^n, Z^n, V^n, K^n_j) + n\gamma_n$

(b) $I(M;Y^n, K^n_j, V^n|Z^n) + I(M;V^n|Z^n) + n\epsilon_n + n\gamma_n$

(c) $I(M;K^n_j|Z^n, V^n) + I(M;Y^n|K^n_j, Z^n, V^n) + I(M;V^n|Z^n) + n\delta_n$

(d) $H(K^n_j|Z^n, V^n) + I(M;X^n;Y^n|K^n_j, Z^n, V^n) + I(M;V^n|Z^n) + n\delta_n$.

where (a) follows from (17), (b) follows from Fano’s inequality, and (c) follows by defining $\delta_n = \epsilon_n + \gamma_n$.

As mentioned, the following lemma extends [5] to wiretap channels with state.

**Lemma 1.** Assume a memoryless channel for which $p(Z^n, Y^n|X^n, V^n) = \prod_{i=1}^n p(z_i, y_i|x_i, v_i)$ and a conditional pmf $p(x_i|m, v^i, k^i_j, x^{i-1})$. For each $j \in \{1,\ldots,n\}$,

$$H(K^n_j|Z^n, V^n) + I(M;X^n;Y^n|K^n_j, Z^n, V^n) + I(M;V^n|Z^n)$$

$$\leq H(K^n_j|Z^n-1, V^{j-1}) + I(M;X^n-1;Y^n-1|K^n_j-1, Z^{j-1}, V^{j-1})$$

$$+ I(M;V^{j-1}|Z^{j-1}) + I(K^n_j|M, X^{j-1}, K^{j-1}, Z^{j-1}, V^{j-1}) + I(X_j;Y_j|Z_j, V_j) + I(X_j;V_j|Z_j).$$

**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:

\[ H(K'_j|Z^j', V^j) + I(M; X^j; Y^j|K'_j, Z^j, V^j) + I(M; V^j|Z^j') \]

\[ = H(K'_j|Z^j', V^j) + I(M; X^j; Y^j|K'_j, Z^j, V^j) + I(M; V^j|Z^j') + I(M; V^j|Z^j, V^j') - I(M; V^j|Z^j', V^j') \]

\[ \leq H(K'_j|Z^j, V^j) + I(M; X^j; Y^j|K'_j, Z^j, V^j) + I(M; V^j|Z^j'| Z^j, V^j) + I(M; V^j|Z^j) \]

\[ = H(K'_j|Z^j', V^j) + I(M; X^j; Y^j|K'_j, Z^j, V^j) + I(M; V^j|Z^j') + I(M; V^j|Z^j, V^j') - I(M; V^j|Z^j', V^j') \]

\[ \leq H(K'_j|Z^j, V^j) + I(M; X^j; Y^j|K'_j, Z^j, V^j) + I(M; V^j|Z^j') \]

where (e) is since \( Y_j \leftrightarrow (X_j, Z_j, V_j) \leftrightarrow (M, X^{j-1}, Y^{j-1}, Z^{j-1}, V^{j-1}) \) and \((M, Z^{j-1}, V^{j-1}, X^{j-1}) \leftrightarrow (X_j, Z_j) \leftrightarrow V_j \) form Markov chains. (f) is due to the chain \( Z_j \leftrightarrow (M, Z^{j-1}) \leftrightarrow V^{j-1} \), (g) follows from \((V_j, Z_j) \leftrightarrow (M, X^j, K'_j, Z^{j-1}, V^{j-1}) \leftrightarrow Y^{j-1} \). (h) is because \( Y^{j-1} \leftrightarrow (M, X^{j-1}, K'_j, Z^{j-1}, V^{j-1}) \leftrightarrow X_j \) form a Markov chain. (i) and (k) follow since conditioning reduces the entropy and (j) is from Markov chain \((M, X^{j-1}) \leftrightarrow (Z^{j-1}, Y^{j-1}, K'_j, V^{j-1}) \leftrightarrow K'_j \).

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

\[ nR \leq H(K'_j|Z^n, V^n) + I(M; X^n; Y^n|K'_j, Z^n, V^n) + I(M; V^n|Z^n) + n\delta_n \]

\[ \leq H(K'_j|Z^n, V^n) + I(M; V^n|Z^n) + I(X_n; V_n|Z_n) + I(X_{n-1}; Y_{n-1}|Z_{n-1}) + I(X_{n-1}; V_{n-1}|Z_{n-1}) \]

\[ \leq \cdots \]

\[ \leq \sum_{i=1}^n I(X_i; Y_i|Z_i, V_i) + \sum_{i=1}^n I(X_i; V_i|Z_i) \]

\[ + \sum_{i=1}^n H(K'_j) + n\delta_n. \]
Thus,
\[
R \leq \sum_{i=1}^{n} I(X_i; Y_i|V_i) - \sum_{i=1}^{n} I(X_i; Z_i|V_i) \\
+ \sum_{i=1}^{n} I(X_i; V_i|Z_i) + \sum_{i=1}^{n} H(K'_i) + n\delta_n \\
\leq \sum_{i=1}^{n} I(X_i; Y_i|V_i) - \sum_{i=1}^{n} I(X_i; Z_i|V_i) \\
+ \sum_{i=1}^{n} H(V_i|Z_i) + \sum_{i=1}^{n} H(K'_i) + n\delta_n. \tag{18}
\]

We now normalize by \( n \), and use the constraint \( \frac{1}{n} \sum_{i=1}^{n} \log(|K'_i|) \leq R_f \). We have,
\[
R \leq \frac{1}{n} \sum_{i=1}^{n} I(X_i; Y_i|V_i) - \frac{1}{n} \sum_{i=1}^{n} I(X_i; Z_i|V_i) \\
+ \frac{1}{n} \sum_{i=1}^{n} H(V_i|Z_i) + R_f + \delta_n. \tag{19}
\]

Now, the well-known technique of introducing a time-sharing random variable is used. Assume \( Q \) is independent of \( X^n, Y^n, Z^n, V^n \) and uniform on \( \{1, \ldots, n\} \), this results in
\[
R \leq R_f + \frac{1}{n} \sum_{i=1}^{n} (I(X_i; Y_i|V_i) - I(X_i; Z_i|V_i)) \\
+ H(V_i|Z_i) + \delta_n
\]
\[
= R_f + \frac{1}{n} \sum_{i=1}^{n} (I(X_i; Y_i|V_i, Q = i) - I(X_i; Z_i|V_i, Q = i)) \\
+ H(V_i|Z_i, Q = i) + \delta_n
\]
\[
= R_f + I(X; Y|V, Q) - I(X; Z|V, Q) \\
+ H(V_Q|Z_Q, Q) + \delta_n
\]
\[
= R_f + I(X; Y|V, Q) - I(X; Z|V, Q) \\
+ H(V|Z, Q) + \delta_n. \tag{20}
\]

where \( X := X_Q, Y := Y_Q, Z := Z_Q, V := V_Q \).

Now, letting \( n \to \infty \), we get \( \delta_n \to 0 \) and \( \epsilon_n \to 0 \), hence, using the Markov chain \( Q \leftrightarrow (X, V) \leftrightarrow (Y, V) \leftrightarrow Z \), we have
\[
R \leq R_f + I(X; Y|V, Q) - I(X; Z|V, Q) + H(V|Z, Q)
\]
\[
\leq R_f + I(X; Q; Y|V) - I(X; Q; Z|V) + H(V|Q|Z)
\]
\[
\leq R_f + I(X; Y|V) - I(X; Z|V) + H(V|Z). \tag{21}
\]

Similarly, it is also easy to see that \( R \leq I(X|Y|V) \). From the two above bounds,
\[
R \leq \min \{ I(X; Y|V), \\
I(X; Y|V) - I(X; Z|V) + H(V|Z) + R_f \}, \tag{22}
\]
and the theorem easily follows.

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. Moreover, when the channel state is known only at the receiver, the results suggest that sending the channel state to the transmitter through the feedback channel results in higher secrecy capacity compared to sending fresh randomness as a key.

ACKNOWLEDGMENT

This research was partially supported by DSP Group inc.

REFERENCES

[1] 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.
[2] 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.
[3] A. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol. 54, pp. 1355–1387, 1975.
[4] 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.
[5] 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.
[6] 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.
[7] 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.
[8] Y.-K. Chia and A. ElGamal, “Wiretap channel with causal state information,” Information Theory, IEEE Transactions on, vol. 58, no. 5, pp. 2838–2849, 2012.
[9] C. E. Shannon, “Communication theory of secrecy systems,” Bell system technical journal, vol. 28, no. 4, pp. 656–715, 1949.
[10] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” Information Theory, IEEE Transactions on, vol. 24, no. 3, pp. 339–348, 1978.
[11] 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.
[12] Y. Chen and A. Han Vinck, “Wiretap channel with side information,” Information Theory, IEEE Transactions on, vol. 54, no. 1, pp. 395–402, 2008.
[13] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, “Secrecy outage in MIMO systems with partial channel information,” Information Forensics and Security, IEEE Transactions on, vol. 7, no. 2, pp. 704–716, 2012.
[14] 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.
[15] ——, “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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[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] A. El Gamal and Y.-H. Kim, *Network information theory*. Cambridge University Press, 2011.