Digital Communications and Networks 6 (2020) 129–135

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/dcan

Enhancing secrecy rates in a wiretap channel☆

Shahid M. Shah *, Vinod Sharma

Department of ECE, Indian Institute of Science, Bangalore, 560012, India

ARTICLE INFO

Keywords:
Physical layer security
Rate loss
Secret key
Wiretap channel
Secrecy capacity

ABSTRACT

Reliable communication imposes an upper limit on the achievable rate, namely the Shannon capacity. Wyner's wiretap coding ensures a security constraint and reliability, but results in a decrease of achievable rate. To mitigate the loss in secrecy rate, we propose a coding scheme in which we use sufficiently old messages as key and prove that multiple messages are secure with respect to all the information possessed by the eavesdropper. We also show that we can achieve security in the strong sense. Next, we study a fading wiretap channel with full channel state information of the eavesdropper's channel and use our coding/decoding scheme to achieve a secrecy capacity close to the Shannon capacity of the main channel (in the ergodic sense). Finally, we study a case where the transmitter does not have instantaneous information of the channel state of the eavesdropper, but only its distribution.

1. Introduction

With the advent of wireless communication, the issue of security has gained more importance due to the broadcasting nature of the wireless channel. To implement security at the physical layer for a degraded wiretap channel, Wyner [1] proposed a coding scheme which is independent of the computational capacity of the adversary. The result of Wyner's scheme was generalized into a more general broadcast channel [2]. More recently, the growth of wireless communication systems has intensified the interest in implementing security at the physical layer [3-5].

There is a trade-off between the achievable rate and the level of secrecy to be achieved. In particular, in the coding scheme which achieves a secrecy capacity in a discrete memoryless wiretap channel, the eavesdropper (Eve) is confused with random messages at a rate close to its channel capacity, thus resulting in a loss of transmission rate [1,2].

Recently, considerable progress has been made to improve the achievable secrecy rate of a wiretap channel. In Ref. [6] a wiretap channel with rate-distortion has been studied, wherein the transmitter and the receiver have access to some shared secret key before the communication starts. Secret key agreement between the transmitter (Alice) and the legitimate receiver (Bob) has been studied extensively in Refs. [7,8]. Condisdering the situation in which Alice and Bob have access to a public channel, the authors in Refs. [7,9] propose a scheme to agree on a secret key about which the adversary has less information (leakage rate goes to zero asymptotically).

In Ref. [10] the authors study a wiretap channel with secure rate limited feedback. The feedback is used to agree on a secret key, and the overall secrecy rate is enhanced. Under some conditions, it even equals the main channel capacity. In Ref. [11] the authors study a modulo-additive discrete memoryless wiretap channel with feedback. The feedback is transmitted by using a feed-forward channel only, and its signal can be used as a secret key. The authors propose a coding scheme which achieves a secrecy rate equal to the main channel capacity. A wiretap channel with a shared key has been studied in Ref. [12].

The fading wiretap channel has been studied in Refs. [13-15]. In Ref. [16], previously transmitted confidential messages are stored in a secret key buffer and used in future slots to overcome the secrecy outage in a fading wiretap channel. In this model, the data to be securely transmitted is delay sensitive. In Ref. [17] the authors use previously transmitted bits stored in a secret key buffer to leverage the secrecy capacity against deep fades in the main channel. They prove that all messages are secure w.r.t. (with regard to) all the outputs of the eavesdropper. The secrecy rate is not enhanced but prevented from decreasing when the main channel is worse than the eavesdropper's channel. A multiplex coding technique has been proposed in Ref. [18] to enhance the secrecy capacity to ordinary channel capacity. The mutual information rate between Eve's received symbols and the (single)

☆ Part of the paper was presented in 2013 IEEE International Conference on Communications Workshop on Physical Layer Security (ICC), Budapest, Hungary.

* Corresponding author.
E-mail address: shahid.nit@gmail.com (S.M. Shah).

https://doi.org/10.1016/j.dcan.2018.03.006
Received 13 July 2017; Received in revised form 22 January 2018; Accepted 27 March 2018
Available online 29 March 2018

message transmitted is shown to decrease to zero as codeword length increases.

In most of the works cited above, the security constraint used is *weak secrecy,* where if the message to be confidentially transmitted is W, and the information that eavesdropper gets in n channel used is Z^n, then $I(W;Z^n) \leq n\epsilon$. From the perspective of stringent security, this notion is proved to be vulnerable for leaking some useful information to the eavesdropper [4]. Maurer in Ref. [9] provides a coding scheme combined with privacy amplification and information reconciliation, which achieves a secrecy capacity (same as in the weak secrecy case) with a strong secrecy constraint, i.e., $I(W;Z^n) \leq \epsilon$. There are also other ways to achieve strong secrecy (see chapter 21 in Refs. [19-21]).

In this paper, we propose a time slotted wiretap channel, in which the messages transmitted in a slot are used as a key to encrypt the message in the next slot of communication. Simultaneously, we use a wiretap encoder for another message in the same slot, which enhances the secrecy rate. We ensure that in each slot the currently transmitted message is secure w.r.t. all the output that Eve receives.

In the next part of this paper, we extend this work to a wiretap channel with a secret key buffer, which is used to store previously transmitted secret messages. In this scheme, we use the oldest messages stored in the key buffer as a key in a slot and then remove those messages from the key buffer (a previous message is used as a key only once). In each slot this key is used along with a wiretap encoder to enhance the secrecy rate. In this way, not only the current message but all the messages sent in recent past are jointly secure w.r.t. all the data received by Eve till now. We also study a slow fading wiretap channel with the proposed coding scheme. We show that the water-filling power control and our coding scheme provide a secrecy capacity close to the Shannon capacity.

We also show that if a *resolvability*-based coding scheme [21] is used in a slot instead of a *wiretap* coding, a secrecy capacity equal to the main channel capacity in the strong sense can be achieved.

The rest of the paper is organised as follows: Section 2 presents the channel model and the problem statement; Section 3 provides our coding and decoding scheme and shows that it can achieve the Shannon capacity for an AWGN wiretap channel; Section 4 extends the scheme to a fading wiretap channel with Eavesdropper's channel information at the transmitter; Section 5 provides the results when this information is not available at the transmitter; Section 6 provides the numerical results of the AWGN wiretap channel; Section 7 concludes the paper.

A note about the notation: capital letters, e.g., W, will denote a random variable and the corresponding small letter w denotes its realization; an n-length vector $(A_1, A_2, \ldots, A_n)$ will be denoted as $\overline{A}$; information theoretic notation will be same as in Ref. [22].

2. Channel model and problem statement

We consider a discrete time, memoryless, degraded wiretap channel in which Alice wants to transmit messages to Bob. We want to keep Eve (who is passively "listening") ignorant of the messages (Fig. 1).

Formally, Alice wants to communicate messages $W \in \mathscr{W} = \{1, 2, \ldots, 2^{nR_s}\}$ reliably via the wiretap channel to Bob while ensuring that Eve is not able to decode them, where R_s (the secrecy capacity) is defined

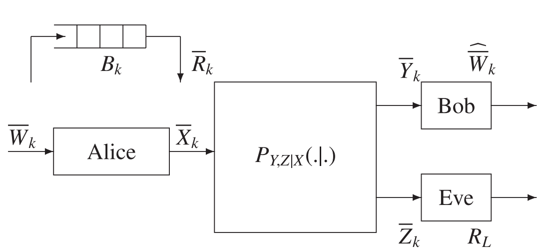

Fig. 1. Wiretap channel with secret key buffer.

below. W is distributed uniformly over $\mathscr{W}$. At time i, X_i is the channel input, and Bob and Eve receive the channel outputs Y_i and Z_i respectively, where $X_i \in \mathscr{X}, Y_i \in \mathscr{Y}, Z_i \in \mathscr{Z}$. The transition probability matrix of the channel is $p(y, z|x)$. The secrecy capacity ([1])

$$R_s = \max_{p(x)}[I(X;Y) - I(X;Z)] \tag{1}$$

is assumed > 0.

We consider the system as a time slotted system, in which each slot consists of $M+1$ minislots and one minislot consists of n channel uses, M being a positive large integer. We are interested in transmitting a sequence $\{W_m, m \geq 1\}$ of *iid* messages uniformly distributed over $\mathscr{W}$. Let C be the capacity of Alice-Bob channel and $[x]$ denote the integer part of x. For simplicity, we take $\frac{C}{R_s}$ as an integer. The message $\overline{W}_k$ to be transmitted in slot k consists of one or more messages W_m. The codeword for message $\overline{W}_k$ is denoted by $\overline{X}_k$. The corresponding received bits by Eve are $\overline{Z}_k$. To increase the secrecy rate, the transmitter uses previous messages as keys for transmitting the messages in a later slot.

We will denote by $P_e^{(n)}$ the probability that any of the messages transmitted in a slot is not properly received by Bob: $P_e^{(n)} = Pr(\overline{W}_k \neq \widehat{W}_k)$, where $\widehat{W}_k$ is the decoded message by Bob in slot k.

For secrecy we consider the leakage rate

$$\frac{1}{n} I\left(\overline{W}_k, \overline{W}_{k-1}, \ldots, \overline{W}_{k-N_1}; \overline{Z}_1, \ldots, \overline{Z}_k\right) \tag{2}$$

in slot k, where N_1 is an arbitrarily positive large integer which can be chosen as a design parameter to take into account the secrecy requirement of the application at hand.[2] Then of course we should consider $k > N_1$, which means that Eve at time k is not interested in very old messages transmitted before slot $k - N_1$.

Definition 2.1. Rate R is achievable if there are coding-decoding schemes for each n such that $P_e^{(n)} \to 0$ and $\frac{1}{n} I(\overline{W}_k, \ldots, \overline{W}_{k-N_1}; \overline{Z}_1, \ldots, \overline{Z}_k) \to 0$ as $n \to \infty$, where N_1 is an arbitrarily large fixed constant.

Our coding scheme is as following: the message $\overline{W}_k$ transmitted in slot k is stored in a key buffer (of infinite length) for later use as a key. After certain bits from the key buffer are used as a key for data transmission, they are discarded from the key buffer, not to be used again. Let B_k be the number of bits in the key buffer at the beginning of slot k. Let $\overline{R}_k$ be the number of key bits used in slot k from the key buffer. Then,

$$B_{k+1} = B_k + \left|\overline{W}_k\right| - \overline{R}_k \tag{3}$$

where $\left|\overline{W}_k\right|$ denotes the number of bits in $\overline{W}_k$. Now we explain the coding-decoding scheme used in this paper.

2.1. Encoder

To transmit message $\overline{W}_k$ in slot k, the encoder has two parts

$$f_s : \mathscr{W} \to \mathscr{X}^n, \quad f_d : \mathscr{W}^M \times \mathscr{K} \to \mathscr{X}^{nM} \tag{4}$$

where $\mathscr{K}$ is the set of secret keys generated and f_s is the wiretap encoder, as in Ref. [1]. We use the following encoder for f_d: take binary version of the message and *XOR* with the binary version of the key. Encode the resulting encrypted message with an optimal usual channel encoder (e.g., an efficient LDPC code).

Assume $B_0 = 0$. The case of $B_0 > 0$ can be easily handled in the same way. In the first slot, message $\overline{W}_1 = W_1$, encoded by using the wiretap coding only, is transmitted (we use only the first minislot, see Fig. 2). At

[2] One motivation for this is the law in various countries where old secret documents are declassified after a certain number of years.

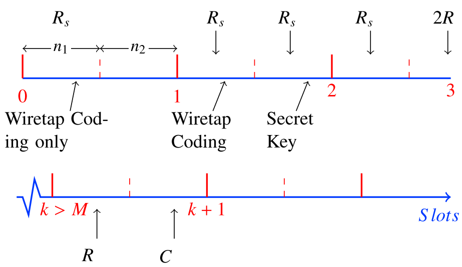

Fig. 2. Coding Scheme to achieve Shannon Capacity in Wiretap Channel.

the end of slot 1, nR_s bits of this message are stored in the key buffer. Thus, $B_1 = R_s n$. In slot 2, message $\overline{W}_2$ consisting of two messages $(\overline{W}_{21}, \overline{W}_{22}) = (W_2, W_3)$ are transmitted. W_2 is transmitted via wiretap coding, W_3 uses $\overline{W}_1$ as a key, and the encrypted message $\overline{W}_1 \oplus W_3$ is transmitted via a usual capacity achieving channel code. At the end of slot 2, $R_s n$ bits of $\overline{W}_1$ are removed from the key buffer and $2R_s n$ bits of $\overline{W}_2$ are stored in the key buffer. Since Bob is able to decode $\overline{W}_1$ with a large probability, but not Eve, $\overline{W}_1$ can be an effective key in slot 2. In slot 3, message $\overline{W}_3$ consisting of 3 messages from the source message sequence is transmitted: one message in the first mini slot denoted as $W_{3,1}$ via wiretap coding, and two messages denoted together as $\overline{W}_{3,2}$ via encryption with message $\overline{W}_2$ as key bits. In any mini-slot we can transmit up to C/R_s messages via encryption with a key. This is because we cannot transmit reliably at a rate higher than Bob's capacity C. Thus, the maximum number of messages that can be transmitted in a slot is $1 + \frac{C}{R_s} M \triangleq M_1$. Once we reach this limit, from then onwards M_1 messages will be transmitted in a slot providing the achievable rate $\frac{R_s + CM}{M+1}$, which can be made as close to C as we wish by making M arbitrarily large.

Consequently, in slot $k \le M_1$, k messages from the source message stream are transmitted, $(k-1)R_s n$ bits from the key buffer are removed in the beginning of slot k, and $kR_s n$ bits are added to the key buffer at the end of slot k. The overall message is denoted by $\overline{W}_k = (\overline{W}_{k,1}, \overline{W}_{k,2})$, with $\overline{W}_{k,1}$ consisting of one source message transmitted via wiretap coding and $\overline{W}_{k,2}$ consisting of $k-1$ messages transmitted via the secret key. From slot M_1 onwards, M_1 messages are transmitted in the above mentioned fashion.

We use the key buffer as a First In First Out (FIFO) queue, i.e., at any time the oldest key bits in the buffer are used first. Also, $B_k \to \infty$ as $k \to \infty$.

2.2. Decoder

We also have a secret key buffer at Bob's decoder , and it is used in the same way as at the transmitter. The confidential messages decoded by the decoder are stored in this buffer. For decoding at Bob, the usual wiretap decoder (say, a joint-typicality decoder) is used in slot 1. From slot 2 onwards, we use the wiretap decoder for the first mini slot, while for the rest of the mini-slots, we use the channel decoder (corresponding to the channel encoder used) and then *XOR* the decoded message with the key used.

The above coding-decoding schemes ensure that $P_e^{(n)} \to 0$ as $n \to \infty$. There is a small issue of error propagation due to using the previous message as key. Let ε_n be the message error probability for the wiretap encoder and let δ_n be the message error probability due to the channel encoder for $\overline{W}_k$. Then, $\varepsilon_n \to 0$ and $\delta_n \to 0$ as $n \to \infty$. For the k^{th} slot, we have $P(\overline{W}_k \ne \widehat{W}_k) \le Pr$(Error in decoding $\overline{W}_{k1}$)Error in decoding $\overline{W}_{k2}$)Error in decoding $\overline{W}_{k-1}$). Thus, the error increases with k. But restarting (as in slot 1) after some large k slots as in slot 1 (i.e., again start with one message in the first minislot and no message in the rest of the slot) will ensure that $P(\overline{W}_k \ne \widehat{W}_k) \to 0$ as $n \to \infty$.

In the rest of the paper, we will show that our coding scheme provides an achievable rate with the above secrecy criterion as close to C as needed, for all k large enough. We also note that the following proof is valid for $N_1 > 1$. The proof for $N_1 = 1$ is different from the proposed proof and one can refer to [23] for details of the proof. We will denote the codeword $\overline{X}_k = (\overline{X}_{k,1}, \overline{X}_{k,2})$ and $\overline{Z}_k = (\overline{Z}_{k,1}, \overline{Z}_{k,2})$ for data received by Eve in the first and second part of slot k.

3. Capacity of wiretap channel

Theorem 3.1. *The secrecy capacity of our coding-decoding scheme is C and it satisfies (2) for any $N_1 \ge 0$, for all k large enough.*

Proof: As mentioned in the last section, by using our coding-decoding scheme, using wiretap coding and secure key, in any slot k, Bob is able to decode the message $\overline{W}_k$ with probability $P_e^{(n)} \to 0$ as $n \to \infty$.

Fix $N_1 \ge 0$ and a small $\varepsilon > 0$. Due to wiretap coding, we can choose n such that $I(\overline{W}_{k,1}; \overline{Z}_{k,1}) \le n\varepsilon$ for all $k \ge 1$. Since key buffer $B_k \to \infty$, we use the oldest key bits in the buffer first and do not use more than MC key bits in any slot. After sometime (say N_2 slots), for all $k \ge N_2$ we use key bits only from messages $\overline{W}_1, \overline{W}_2, \ldots, \overline{W}_{k-N_1-1}$ for messages $\overline{W}_k$, $\overline{W}_{k-1}$, …, $\overline{W}_{k-N_1}$. Furthermore,

$$I(\overline{W}_k, \overline{W}_{k-1}, \ldots, \overline{W}_{k-N_1}; \overline{Z}_1, \ldots, \overline{Z}_k) = I(\overline{W}_{k,1}, \overline{W}_{k-1,1}, \ldots, \overline{W}_{k-N_1,1}; \overline{Z}_1, \ldots, \overline{Z}_k) + I(\overline{W}_{k,2}, \ldots, \overline{W}_{k-N_1,2}; \overline{Z}_1, \ldots, \overline{Z}_k | \overline{W}_{k,1}, \ldots, \overline{W}_{k-N_1,1}) \quad (5)$$

We show in Lemma 1 that

$$I(\overline{W}_{k,1}, \overline{W}_{k-1,1}, \ldots, \overline{W}_{k-N_1,1}; \overline{Z}_1, \ldots, \overline{Z}_k) \le (N_1 + 1)n\varepsilon \quad (6)$$

and in Lemma 2 that

$$I(\overline{W}_{k,2}, \ldots, \overline{W}_{k-N_1,2}; \overline{Z}_1, \ldots, \overline{Z}_k | \overline{W}_{k,1}, \ldots, \overline{W}_{k-N_1,1}) = N_1\varepsilon \quad (7)$$

From (5), (6) and (7)

$$\frac{1}{n} I(\overline{W}_k, \overline{W}_{k-1}, \ldots, \overline{W}_{k-N_1}; \overline{Z}_1, \ldots, \overline{Z}_k) \le (2N_1 + 1)\varepsilon \quad (8)$$

By fixing N_1, we can take ε small enough such that $(N_1 + 1)\varepsilon$ is less than any desired value.

So far, we have been considering an infinite buffer system. Neverthless, an actual system will have a finite buffer. Now we compute the key buffer length needed for our system.

If we fix the probability of error for Bob and the upper bound on equivocation, then we can get the code length n needed. Also, from the secrecy requirement, we can fix N_1. Once n and N_1 are fixed, to ensure that eventually, in slot k we will use a key from messages before time $k - N_1$. The key buffer size should be $\ge CMN_1 n$ bits. Also, since the key buffer length increases by nR_s bits in each slot, the key buffer will have at least $CMN_1 n$ bits after slot $\frac{CMN_1}{R_s}$. In the finite buffer case, eventually the key buffer will overflow. We shall loose only the latest bits arriving at any slot (not the bits already stored).

We can obtain the Shannon capacity even with strong secrecy. For this aim, instead of using the usual wiretap coding of Wyner in the first minislot of each slot, we use the *resolvability*-based coding scheme [21].

Then, $I(\overline{W}_{k,1};\overline{Z}_{k,1}) \le \varepsilon$, instead of $I(\overline{W}_{k,1};\overline{Z}_{k,1}) \le n\varepsilon$, for n large enough. Then from proof of Theorem 1, our coding-decoding scheme provides

$$I\left(\overline{W}_k, \ldots, \overline{W}_{k-N_1}; \overline{Z}_1, \ldots, \overline{Z}_k\right) \le \varepsilon \tag{9}$$

4. AWGN slow fading channel

Now we consider a slow flat fading AWGN channel (Fig. 1), where the channel gains in a slot are constant. The channel outputs are,

$$Y_i = \tilde{H}X_i + N_{1i} \tag{10}$$

$$Z_i = \tilde{G}X_i + N_{2i} \tag{11}$$

where X_i is the channel input, $\{N_{1i}\}$ and $\{N_{2i}\}$ are independent, identically distributed ($i.i.d.$) sequences independent of each other, and $\{X_i\}$ with distributions $\mathcal{N}(0,\sigma_1^2)$ and $\mathcal{N}(0,\sigma_2^2)$ respectively. $\mathcal{N}(a,b)$ denotes Gaussian distribution with mean a and variance b. $\tilde{H}$ and $\tilde{G}$ are the channel gains to Bob and Eve respectively in the given slot. Let $H = |\tilde{H}|^2$ and $G = |\tilde{G}|^2$.

The channel gains H_k and G_k in slot k are constant, and sequences $\{H_k, k \ge 0\}$ and $\{G_k, k \ge 0\}$ are *iid* and independent of each other. We assume that (H_k, G_k) is known to the transmitter and Bob at the beginning of slot k. The notation and assumptions are same as in Section 3. Power $P(H_k, G_k)$ is used in slot k for transmission. There is an average power constraint,

$$\limsup_{k\to\infty} \frac{1}{k}\sum_{m=1}^{k} \mathsf{E}\left[P(H_k, G_k)\right] \le \overline{P} \tag{12}$$

Given H_k, G_k, and B_k at the beginning of slot k, Alice needs to decide on $P(H_k, G_k)$ and $\overline{R}_k$ such that the resulting average transmission rate $\limsup_{k\to\infty}\frac{1}{k}\sum_{l=1}^{k} r_l$ is maximized subject to (12), (2) and $P_e^n \to 0$, where r_k is the transmission rate in slot k. We compute this capacity for $P(H_k > G_k) > 0$; otherwise, the capacity is zero. At the end of slot k, $n(M+1)r_k \triangleq \overline{r}_k$ bits are stored in the key buffer for later use as a key while $\overline{R}_k$ bits have been removed. Thus, the buffer size evolves as,

$$B_{k+1} = B_k + \overline{r}_k - \overline{R}_k \tag{13}$$

For convenience, we define

$$C(P(H,G)) = \frac{1}{2}\log\left(1 + \frac{HP(H,G)}{\sigma_1^2}\right) \tag{14}$$

and

$$C_e(P(H,G)) = \frac{1}{2}\log\left(1 + \frac{GP(H,G)}{\sigma_2^2}\right) \tag{15}$$

where $P(H,G)$ is the power used when the channel gains are H and G. Unlike in Sections II and III where initial messages W are with cardinality 2^{nR_s}, we use adaptive coding and power control. Then, we have the following theorem.

Theorem 4.1. *The secrecy rate*

$$C_s = \mathsf{E}_H[C(P(H))] \tag{16}$$

is achievable if $Pr(H_k > G_k) > 0$, where $P(H) = P(H,G)$ is the water-filling power policy for Alice → Bob channel.

Proof. We follow the coding-decoding scheme of Section 3 with the following change to account for the fading.

Each slot has $M+1$ mini-slots. We fix a power control policy $P(H,G)$ to satisfy average power constraint. We transmit for the first time when $H_k > G_k$, use wiretap coding in all the $(M+1)$ minislots, and also store all the transmitted bits in the key buffer.

From next slot onwards, we use the first mini-slot for wiretap coding (if $H_k > G_k$) and the rest of the mini-slots for transmission via secret key (if $H_k \le G_k$, use only M minislots for transmission with secret key in slot k and do not use the first minislot, with $\overline{R}_k = \min(B_k, MC(P(H_k,G_k))n)$. In every slot we remove R_k bits and add $\overline{r}_k \ge R_k$ bits to the key buffer. Since $Pr(H_k > G_k) > 0$, $Pr(\overline{r}_k > \overline{R}_k) > 0$. Thus $B_k \uparrow \infty$ $a.s.$ and eventually, in every slot we will transmit in the first mini-slot at rate

$$[C(P(H_k,G_k)) - C_e(P(H_k,G_k))]^+ \tag{17}$$

and in the rest of the mini-slots at rate $C(P(H_k,G_k))$ with arbitrarily large probability. The average rate in a slot can be made as close to $C(P(H_k,G_k))$ as we wish by making M large enough. Thus, the rate for this coding scheme is maximized by *water filling*.

Now we want to ensure that for k large enough, for messages $(\overline{W}_k, \overline{W}_{k-1}, \ldots, \overline{W}_{k-N_1})$ we use only keys from $(\overline{W}_1, \ldots, \overline{W}_{k-N_1-1})$. It can be ensured that if we do not use more than $\overline{M}$ key bits in a slot and from $k - N_1$ onward the key queue length $\ge \overline{M}N_1$ bits, where the constant $\overline{M}$ can be chosen arbitrarily large. Thus we modify the above scheme such that we use $\min(B_k, \overline{M}, nMC(P(H_k)))$ key bits in a slot instead of $\min(B_k, nMC(P(H_k)))$ bits. By making $\overline{M}$ as large as needed, we can get arbitrarily close to the water filling rate.

Strong secrecy can be achieved as the non-fading case in Section 3. Also, to attain the required reliability and secrecy, the key buffer length required can be obtained as in Section 3 by using $\overline{M}$ (defined in the proof of Theorem 2).

5. Fading wire-tap with no CSI of eavesdropper

In this section, we assume that the transmitter knows only the channel state of Bob at time k but not G_k, the channel state of Eve. This is more realistic because Eve is a passive listener. Now we modify our fading model. Instead of (H_k, G_k) being constant during a slot (slow fading), the coherence time of (H_k, G_k) is much smaller than the duration n of a minislot. Then we can use the coding-decoding scheme of [13] in the first minislot with secrecy rate R_s and $I(\overline{W}_{k,1}; \overline{Z}_1, \ldots, \overline{Z}_k) \le n\varepsilon$, where

$$R_s = \frac{1}{2}\mathsf{E}_{H,G}\left\{\left[\log\left(1 + \frac{HP(H)}{\sigma_1^2}\right) - \log\left(1 + \frac{GP(H)}{\sigma_2^2}\right)\right]^+\right\} \tag{18}$$

Now we have the following proposition.

Proposition 5.1. *Secrecy capacity equals to the main channel capacity without CSI of Eve at the transmitter*

$$C = \frac{1}{2}\mathsf{E}_H\left[\log\left(1 + \frac{HP(H)}{\sigma_1^2}\right)\right] \tag{19}$$

is achievable subject to power constraint $\mathsf{E}_H[P(H)] \le \overline{P}$, where $P(H)$ is the waterfilling policy.

Proof. Since each mini-slot is of long duration compared to the coherence time of the fading process (H_k, G_k), the coding scheme of [13] can be used without CSI of Eve in the first minislot of each slot. This can achieve secrecy capacity

$$C_s = \mathsf{E}_{H,G}\left[\frac{1}{2}\log\left(\frac{1 + HP(H)/\sigma_1^2}{1 + GP(H)/\sigma_2^2}\right)^+\right] \tag{20}$$

subject to the power constraint $\mathsf{E}_{H,G}[P(H)] \le \overline{P}$, with $I(\overline{W}_k; \overline{Z}_k) \le n\varepsilon$. Now we can use the coding-decoding scheme of Section 3 to achieve a secrecy capacity equal to the main channel capacity

$$C = \frac{1}{2}\mathsf{E}_H\left[\log\left(1 + \frac{HP(H)}{\sigma_1^2}\right)\right] \tag{21}$$

6. Numerical results

6.1. AWGN wiretap channel

In this section we take an example of Additive White Gaussian Noise (AWGN) wiretap channel. The input/output relation becomes a special case of (10) and (11), by taking $H = G = 1$, i.e.,

$$Y_i = X_i + N_{1i} \tag{22}$$

$$Z_i = X_i + N_{2i} \tag{23}$$

In this case we know that the channel capacity from Alice to Bob (Main channel) is given by

$$C = \frac{1}{2}\log\left(1 + \frac{P}{\sigma_1^2}\right) \tag{24}$$

and secrecy capacity is given by (assuming degraded wiretap channel, i.e., $\sigma_1^2 < \sigma_2^2$)

$$C_s = \frac{1}{2}\log\left(1 + \frac{P}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1 + \frac{P}{\sigma_2^2}\right) \tag{25}$$

To perform numerical evaluation, we take $\sigma_1^2 = 1$ and $\sigma_2^2 = 1.7213$. Using only Wyner's wiretap coding, we can achieve a secrecy rate equal to the secrecy capacity of channel given by (25). Now if we use the coding/decoding scheme proposed in this paper, we can achieve a secrecy rate close to the Shannon capacity of Alice-to-Bob channel, i.e., (24). See Fig. 3.

Next we evaluate the number of slots it takes for our proposed coding/decoding scheme to achieve the secrecy rate equal to the Shannon capacity. We note that the slot number at which the secrecy rate becomes equal to Shannon capacity, k is

$$k = \frac{\frac{1}{2}\log(1 + P/\sigma_1^2)}{\frac{1}{2}\log(1 + P/\sigma_1^2) - \frac{1}{2}\log(1 + P/\sigma_2^2)} = 5 \tag{26}$$

Hence after the fifth time slot, we can always transmit messages at a rate equal to the Shannon capacity, but the security metric will now be (2). See Fig. 4.

7. Conclusions

In this paper we achieve a secrecy rate equal to the main channel capacity of a wiretap channel by using the previous secret messages as a key for transmitting the current message. We show that not only the current message is securely transmitted, but all messages transmitted in last N_1 slots are secure w.r.t. all the outputs of the eavesdropper till now,

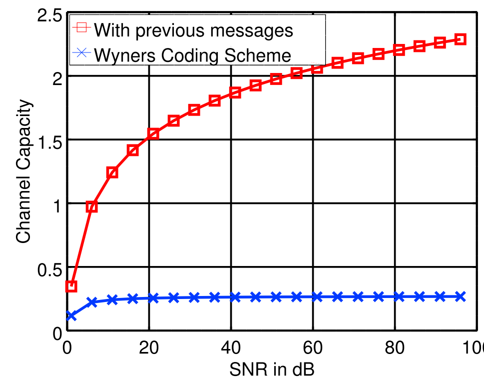

Fig. 3. Comparision of proposed coding scheme with usual wiretap coding for AWGN channel.

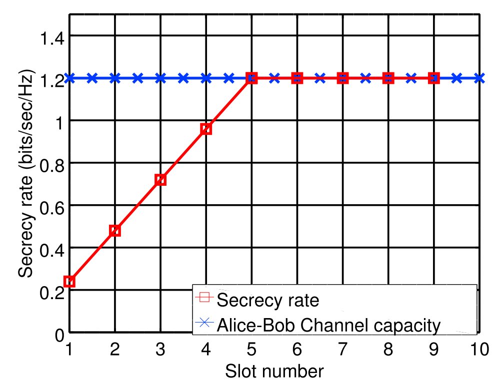

Fig. 4. Secrecy rate enhancement with time.

where N_1 can be taken arbitrarily large. We extend this result to fading wiretap channels when CSI of Eve may or may not be available to the transmitter. The optimal power control is water filling itself. Finally, we provide a numerical example of AWGN wiretap channel, where we demonstrate the effect of rate loss and how the proposed coding/decoding scheme mitigates the rate loss.

Acknowledgments

The first author would like to thank Deekshit PK for useful discussions.

Appendices

Proofs of lemmas

Lemma 1. *The following holds*

$$I\left(\overline{W}_{k,1}, \overline{W}_{k-1,1}, \ldots, \overline{W}_{k-N_1,1}; \overline{Z}_1, \overline{Z}_2, \ldots, \overline{Z}_k\right) \le (N_1 + 1)n\varepsilon \tag{27}$$

Proof: We have,

$$I\left(\overline{W}_{k,1}, \overline{W}_{k-1,1}, \ldots, \overline{W}_{k-N_1,1}; \overline{Z}_1, \overline{Z}_2, \ldots, \overline{Z}_k\right) = I\left(\overline{W}_{k,1}; \overline{Z}_1, \overline{Z}_2, \ldots, \overline{Z}_k\right) + I\left(\overline{W}_{k-1,1}; \overline{Z}_1, \overline{Z}_2, \ldots, \overline{Z}_k \middle| \overline{W}_{k,1}\right) + \ldots + +I\left(\overline{W}_{k-N_1,1}; \overline{Z}_1, \overline{Z}_2, \ldots, \overline{Z}_k \middle| \overline{W}_{k,1}, \ldots, \overline{W}_{k-N_1+1,1}\right) \tag{28}$$

But

$$I\left(\overline{W}_{k,1}; \overline{Z}_1, \overline{Z}_2, \ldots, \overline{Z}_k\right) = I\left(\overline{W}_{k,1}; \overline{Z}_{k,1}\right) + I\left(\overline{W}_{k,1}; \overline{Z}_1, \ldots, \overline{Z}_{k-1}, \overline{Z}_{k,2} \middle| \overline{Z}_{k,1}\right) \le n\varepsilon + 0 \tag{29}$$

because $(\overline{Z}_1, \ldots, \overline{Z}_{k-1}, \overline{Z}_{k,2}) \perp (\overline{Z}_{k,1}, \overline{W}_{k,1})$, where $X \perp Y$ denotes that random variable X is independent of Y.

Next consider

$$I(\overline{W}_{k-1,1}; \overline{Z}_1, \overline{Z}_2, \ldots, \overline{Z}_k | \overline{W}_{k,1}) = I(\overline{W}_{k-1,1}; \overline{Z}_{k-1,1} | \overline{W}_{k,1}) + I(\overline{W}_{k-1,1}; (\overline{Z}_1, \ldots, \overline{Z}_k) - \overline{Z}_{k-1,1} | \overline{W}_{k,1}, \overline{Z}_{k-1,1}) \tag{30}$$

where $(\overline{Z}_1, \ldots, \overline{Z}_k) - \overline{Z}_{k-1,1}$ denotes the sequence $(\overline{Z}_1, \ldots, \overline{Z}_k)$ without $\overline{Z}_{k-1,1}$. However,

$$I(\overline{W}_{k-1,1}; \overline{Z}_{k-1,1} | \overline{W}_{k,1}) = I(\overline{W}_{k-1,1}; \overline{Z}_{k-1,1}) \leq n\varepsilon \tag{31}$$

Also, because $(\overline{Z}_1, \ldots, \overline{Z}_{k-2})$ is independent of $(\overline{W}_{k-1,1}, \overline{W}_{k,1}, \overline{Z}_{k-1,1})$

$$I(\overline{W}_{k-1,1}; (\overline{Z}_1, \ldots, \overline{Z}_k) - \overline{Z}_{k-1,1} | \overline{W}_{k,1}, \overline{Z}_{k-1,1}) = I(\overline{W}_{k-1,1}; \overline{Z}_1, \ldots, \overline{Z}_{k-2} | \overline{W}_{k,1}, \overline{Z}_{k-1,1}) + I(\overline{W}_{k-1,1}; \overline{Z}_k, \overline{Z}_{k-1,2} | \overline{W}_{k,1}, \overline{Z}_{k-1,1}, \overline{Z}_1, \ldots, \overline{Z}_{k-2}) \tag{32}$$

$$\overset{(a)}{=} 0 + I(\overline{W}_{k-1,1}; \overline{Z}_{k,1} | \overline{W}_{k,1}, \overline{Z}_{k-1,1}, \overline{Z}_1, \ldots \overline{Z}_{k-2}) + I(\overline{W}_{k-1,1}; \overline{Z}_{k,2}, \overline{Z}_{k-1,2} | \overline{W}_{k,1}, \overline{Z}_{k-1,1}, \overline{Z}_1, \ldots \overline{Z}_{k-2}, \overline{Z}_{k,1}) \tag{33}$$

Furthermore, since $(\overline{W}_{k-1,1}, \overline{W}_{k,1}, \overline{Z}_{k,1}, \overline{Z}_{k-1,1}) \perp (\overline{Z}_1, \ldots, \overline{Z}_{k-2})$ we have

$$I(\overline{W}_{k-1,1}; Z_{k,1} | \overline{W}_{k,1}, \overline{Z}_{k-1,1}, \overline{Z}_1, \ldots, \overline{Z}_{k-2}) = I(\overline{W}_{k-1}; Z_{k,1} | \overline{W}_{k,1}, \overline{Z}_{k-1,1}) \tag{34}$$

Using the fact that $(\overline{W}_{k-1}, \overline{Z}_{k-1,1}) \perp (\overline{W}_{k,1}, \overline{Z}_{k,1})$ we can directly show that the right side equals zero.

Let A denote the indices of the slots in which messages are transmitted which are used as keys for transmitting $\overline{W}_{k,2}$ and $\overline{W}_{k-1,2}$. Since

$$(\overline{Z}_{k,2}, \overline{Z}_{k-1,2}) \leftrightarrow (\overline{W}_{k-1,1}, \overline{W}_A) \leftrightarrow (\overline{W}_{k,1}, \overline{Z}_{k-1,1}, \overline{Z}_{k,1}, \overline{Z}_1, \ldots, \overline{Z}_{k-2}) \tag{35}$$

where $X \leftrightarrow Y \leftrightarrow Z$ denotes that $\{X, Y, Z\}$ forms a Markov chain, we have

$$\begin{aligned} & I(\overline{W}_{k-1,1}; \overline{Z}_{k,2}, \overline{Z}_{k-1,2} | \overline{W}_{k,1}, \overline{Z}_{k-1,1}, \overline{Z}_1, \ldots, \overline{Z}_{k-2}, \overline{Z}_{k,1}) \\ & \leq I(\overline{W}_{k-1,1}, \overline{W}_A; \overline{Z}_{k,2}, \overline{Z}_{k-1,2} | \overline{W}_{k,1}, \overline{Z}_{k-1,1}, \overline{Z}_1, \ldots, \overline{Z}_{k-2}, \overline{Z}_{k,1}) \\ & \overset{(a)}{\leq} I(\overline{W}_{k-1,1}, \overline{W}_A; \overline{Z}_{k,2}, \overline{Z}_{k-1,2}) \end{aligned} \tag{36}$$

$$\leq I(\overline{W}_{k-1,1}; \overline{Z}_{k,2}, \overline{Z}_{k-1,2}) + I(\overline{W}_A; \overline{Z}_{k,2}, \overline{Z}_{k-1,2} | \overline{W}_{k-1,1}) \overset{(b)}{=} 0 + I(\overline{W}_A; \overline{Z}_{k,2}, \overline{Z}_{k-1,2}) \overset{(c)}{=} 0 \tag{37}$$

where (a) follows from (35), (b) follows since $(\overline{W}_{k-1,1}, \overline{Z}_{k-1,1}) \perp (\overline{W}_A, \overline{Z}_{k,2}, \overline{Z}_{k-1,2})$ and (c) follows since $\overline{W}_A \perp Z_{k,2}, Z_{k-1,2}$.

From (30), (31), (34), (37),

$$I(\overline{W}_{k-1,1}; \overline{Z}_1, \overline{Z}_2, \ldots, \overline{Z}_k | \overline{W}_{k,1}) \leq n\varepsilon \tag{38}$$

We can similarly show that the other terms on the right side of (5) are also upper bounded by $n\varepsilon$. This proves the lemma.

Lemma 2. *The following holds*

$$I(\overline{W}_{k,2}, \overline{W}_{k-1,2}, \ldots \overline{W}_{k-N_1,2}; \overline{Z}_1, \ldots, \overline{Z}_k | \overline{W}_{k,1}, \ldots, \overline{W}_{k-N_1,1}) \leq N_1 n\varepsilon \tag{39}$$

Proof: We have

$$\begin{aligned} I(\overline{W}_{k,2}, \ldots, \overline{W}_{k-N_1,2}; \quad \overline{Z}_1, \ldots, \overline{Z}_k | \overline{W}_{k,1}, \ldots, \overline{W}_{k-N_1,1}) &= I(\overline{W}_{k,2}, \ldots, \overline{W}_{k-N_1,2}; \quad \overline{Z}_1, \ldots, \overline{Z}_{k-N_1-1} | \overline{W}_{k,1}, \ldots, \overline{W}_{k-N_1,1}) \\ &+ I(\overline{W}_{k,2}, \ldots, \overline{W}_{k-N_1,2}; \quad \overline{Z}_{k-N_1}, \ldots, \overline{Z}_k | \overline{W}_{k,1}, \ldots, \overline{W}_{k-N_1,1}, \overline{Z}_1, \ldots, \overline{Z}_{k-N_1-1}) \end{aligned} \tag{40}$$

Since $\overline{W}_{k,1}, \ldots, \overline{W}_{k-N_1,1}$ is independent of $\overline{W}_{k,2}, \ldots, \overline{W}_{k-N_1,2}, \overline{Z}_1, \ldots, \overline{Z}_{k-N_1-1}$, the first term on the right equals

$$I(\overline{W}_{k,2}, \overline{W}_{k-1,2}, \ldots, \overline{W}_{k-N_1,2}; \overline{Z}_1, \ldots, \overline{Z}_{k-N_1-1}) = 0 \tag{41}$$

The second term in the RHS of (40).

$$\begin{aligned} &= I(\overline{W}_{k,2}, \ldots, \overline{W}_{k-N_1,2}; \overline{Z}_{k-N_1}, \ldots, \overline{Z}_k | \\ &\quad \overline{W}_{k,1}, \ldots, \overline{W}_{k-N_1,1}, \overline{Z}_1, \ldots, \overline{Z}_{k-N_1-1}) \\ &= I(\overline{W}_{k,2}, \ldots, \overline{W}_{k-N_1,2}; \overline{Z}_{k-N_1,1}, \ldots \overline{Z}_{k,1} | \\ &\quad \overline{W}_{k,1}, \ldots, \overline{W}_{k-N_1,1}, \overline{Z}_1, \ldots, \overline{Z}_{k-N_1-1}) \\ &+ I(\overline{W}_{k,2}, \overline{W}_{k-1,2}, \ldots, \overline{W}_{k-N_1,2}; \overline{Z}_{k-N_1,2}, \ldots, \overline{Z}_{k,2} | \\ &\overline{W}_{k,1}, \ldots, \overline{W}_{k-N_1,1}, \overline{Z}_1, \ldots, \overline{Z}_{k-N_1-1}, \overline{Z}_{k-N_1,1}, \ldots, \overline{Z}_{k,1}) \end{aligned} \tag{42}$$

The first term on the right is zero because $(\overline{W}_{k,2}, \overline{W}_{k-1,2}, \ldots, \overline{W}_{k-N_1,2})$ is independent of $(\overline{Z}_{k,1}, \ldots, \overline{Z}_{k-N_1,1})$, $(\overline{W}_{k,1}, \ldots, \overline{W}_{k-N_1})$ and $\overline{Z}_1, \ldots \overline{Z}_{k-N_1-1}$. Also since $(\overline{W}_{k,1}, \ldots, \overline{W}_{k-N_1,1})$ and $(\overline{Z}_{k,1}, \ldots, \overline{Z}_{k-N_1,1})$ are independent of the other random variables in the second term on the right side, this term equals

$$I\left(\overline{W}_{k,2}, \overline{W}_{k-1,2}, \ldots, \overline{W}_{k-N_1,2}; \overline{Z}_{k,2}, \ldots, \overline{Z}_{k-N_1,2} \middle| \overline{Z}_1, \ldots, \overline{Z}_{k-N_1-1}\right) \tag{43}$$

For convenience we denote it as $I(\widehat{W}_2; \widehat{Z}_2 | \widehat{Z}_1)$ with $\widehat{W}_2$, $\widehat{Z}_2$, $\widehat{Z}_1$ denoting the respective sequences of random variables. Since

$$I(\widehat{W}_2;\widehat{Z}_1,\widehat{Z}_2) = I(\widehat{W}_2;\widehat{Z}_1) + I(\widehat{W}_2;\widehat{Z}_2|\widehat{Z}_1) = I(\widehat{W}_2;\widehat{Z}_2) + I(\widehat{W}_2;\widehat{Z}_1|\widehat{Z}_2) \tag{44}$$

and we have

$$I(\widehat{W}_2,\widehat{Z}_1) = 0 = I(\widehat{W}_2;\widehat{Z}_2) \tag{45}$$

and

$$\widehat{Z}_1 \leftrightarrow (\widehat{W}_1,\widehat{W}_A,\widehat{W}_2) \leftrightarrow \widehat{Z}_2 \tag{46}$$

where $\widehat{W}_1 = (\overline{W}_{k,1},\ldots,\overline{W}_{k-N_1,1})$, we get

$$\begin{aligned}
& I(\widehat{W}_2;\widehat{Z}_2|\widehat{Z}_1) \overset{(a)}{=} I(\widehat{W}_2;\widehat{Z}_1|\widehat{Z}_2) \\
& \leq I(\widehat{W}_1,\widehat{W}_2,\widehat{W}_A;\widehat{Z}_1|\widehat{Z}_2) \\
& \overset{(b)}{\leq} I(\widehat{W}_1,\widehat{W}_2,\widehat{W}_A;\widehat{Z}_1) \\
& = I(\widehat{W}_1;\widehat{Z}_1) + I(\widehat{W}_2,\widehat{W}_A;\widehat{Z}_1|\widehat{W}_1) \\
& \overset{(c)}{=} 0 + I(\widehat{W}_2,\widehat{W}_A;\widehat{Z}_1) \\
& = I(\widehat{W}_A;\widehat{Z}_1) + I(\widehat{W}_2;\widehat{Z}_1|\widehat{W}_A) \\
& \overset{(d)}{\leq} N_1 n\varepsilon + 0 = N_1 n\varepsilon
\end{aligned} \tag{47}$$

where (a) follow from (45), (b) follows from (46) (c) follows from $\widehat{W}_1 \perp (\widehat{W}_2,\widehat{W}_A,\widehat{Z}_1)$, (d) follows from wiretap coding and the fact that the set A will not have larger cardinality than N_1, and $\widehat{W}_2 \perp (\widehat{Z}_1,\widehat{W}_A)$.

Therefore

$$I(\widehat{W}_2;\widehat{Z}_2|\widehat{Z}_1) \leq N_1 n\varepsilon \tag{48}$$

From (41), (42) and (48), we get the lemma.

References

[1] A.D. Wyner, The wire-tap channel, Bell Syst. Tech. J. 54 (8) (1975) 1355–1387.
[2] I. Csiszar, J. Korner, Broadcast channels with confidential messages, Inf. Theor. IEEE Trans. 24 (3) (1978) 339–348, https://doi.org/10.1109/TIT.1978.1055892.
[3] Y. Liang, H.V. Poor, et al., Information theoretic security, Found. Trends Commun. Inf. Theor. 5 (4–5) (2009) 355–580.
[4] M. Bloch, J. Barros, Physical-Layer Security: from Information Theory to Security Engineering, Cambridge University Press, 2011.
[5] R. Liu, W. Trappe, Securing Wireless Communications at the Physical Layer, Springer, 2010.
[6] H. Yamamoto, Rate-distortion theory for the shannon cipher system, Inf. Theor. IEEE Trans. 43 (3) (1997) 827–835.
[7] R. Ahlswede, I. Csiszar, Common randomness in information theory and cryptography. part i: secret sharing, IEEE Trans. Inf. Theor. 39(4).
[8] V.M. Prabhakaran, K. Eswaran, K. Ramchandran, Secrecy via sources and channels, Inf. Theor. IEEE Trans. 58 (11) (2012) 6747–6765.
[9] U.M. Maurer, Secret key agreement by public discussion from common information, Inf. Theor. IEEE Trans. 39 (3) (1993) 733–742.
[10] E. Ardestanizadeh, M. Franceschetti, T. Javidi, Y.-H. Kim, Wiretap channel with secure rate-limited feedback, Inf. Theor. IEEE Trans. 55 (12) (2009) 5353–5361.
[11] L. Lai, H. El Gamal, H.V. Poor, The wiretap channel with feedback: encryption over the channel, Inf. Theor. IEEE Trans. 54 (11) (2008) 5059–5067.
[12] W. Kang, N. Liu, Wiretap channel with shared key, in: 2010 Information Theory Workshop, 2010. Dublin.
[13] P.K. Gopala, L. Lai, H. El Gamal, On the secrecy capacity of fading channels, Inf. Theor. IEEE Trans. 54 (10) (2008) 4687–4698.
[14] Y. Liang, H.V. Poor, S. Shamai, Secure communication over fading channels, Inf. Theor. IEEE Trans. 54 (6) (2008) 2470–2492.
[15] M. Bloch, J. Barros, M.R. Rodrigues, S.W. McLaughlin, Wireless information-theoretic security, Inf. Theor. IEEE Trans. 54 (6) (2008) 2515–2534.
[16] K. Khalil, O.O. Koyluoglu, H.E. Gamal, M. Youssef, Opportunistic secrecy with a strict delay constraint, Commun. IEEE Trans. 61 (11) (2013) 4700–4709.
[17] O. Gungor, J. Tan, C.E. Koksal, H. El-Gamal, N.B. Shroff, Secrecy outage capacity of fading channels, Inf. Theor. IEEE Trans. 59 (9) (2013) 5379–5397.
[18] D. Kobayashi, H. Yamamoto, T. Ogawa, Secure multiplex coding attaining channel capacity in wiretap channels, Inf. Theor. IEEE Trans. 59 (12) (2013) 8131–8143, https://doi.org/10.1109/TIT.2013.2282673.
[19] I. Csiszar, J. Körner, Information Theory: Coding Theorems for Discrete Memoryless Systems, Cambridge University Press, 2011.
[20] I. Devetak, The private classical capacity and quantum capacity of a quantum channel, Inf. Theor. IEEE Trans. 51 (1) (2005) 44–55.
[21] M. Bloch, N. Laneman, Strong secrecy from channel resolvability, Inf. Theor. IEEE Trans. 51 (1) (2011) 44–55.
[22] A. El Gamal, Y.-H. Kim, Network Information Theory, Cambridge University Press, 2011.
[23] S.M. Shah, S. Parameswaran, V. Sharma, Previous messages provide the key to achieve shannon capacity in a wiretap channel, in: Communications Workshops (ICC), 2013 IEEE International Conference on, IEEE, 2013, pp. 697–701.