

Secrecy Rate Region Enhancement in Multiple Access Wiretap Channel

Shahid Mehraj Shah

Department of Electronics and Communication Engineering, National Institute of Technology, Srinagar, Jammu and Kashmir, India

<https://doi.org/10.26636/jtit.2022.152021>

Abstract—It is commonly known that physical layer security is achieved with a trade-off in terms of the achievable rate. Hence, security constraints generate rate losses in wiretap channels. To mitigate such rate losses in multi-user channels, we propose a coding/decoding scheme for multi-user multiple access wiretap channel (MAC-WT), where previously transmitted messages are used as a secret key to enhance the secrecy rates of the transmitting users, until the usual Shannon capacity region of a multiple access channel (MAC) is achieved without the secrecy constraint. With this coding scheme, all messages transmitted in the recent past are secure with respect to all the information of the eavesdropper till now. To achieve this goal, we introduce secret key buffers at both the users and the legitimate receiver. Finally, we consider a fading MAC-WT and show that with this coding/decoding scheme, we can achieve the capacity region of a fading MAC channel (in the ergodic sense).

Keywords—multiple access channel, physical layer security, strong secrecy, wiretap channel.

1. Introduction

In [1], Wyner proved, degraded wiretap channel, that by assigning multiple codewords to a single message, we can achieve reliability as well as security in a point-to-point channel communication and characterized secrecy capacity for this channel. After decades of work commenced after the wireless revolution had begun, researchers started extending Wyner's coding scheme (wiretap coding) in different directions. A single user fading wiretap channel was studied in [2], [3]. A secret key buffer was used in [4] to mitigate the fluctuations in the secrecy capacity due to the variations in the channel's gain over time.

A multiple access channel (MAC) with security constraints was studied in [5] and [6]. In [5], the transmitting users treat each other as eavesdroppers (Eve) and an achievable secrecy rate region is characterized. In some special cases the secrecy capacity region is also found. In [6], the authors consider the eavesdropper to be listening at the receiving end. The authors provide an achievable secrecy-rate region. The secrecy-capacity region is not known for such

a MAC. The same authors also studied a fading MAC with full channel state information (CSI) of Eve known at the transmitters. Paper [7] is a research extension of a scenario in which the CSI of Eve is not known at the transmitters. For a detailed review of theoretical information theoretic security see [8], [9], and [10].

In all of the above mentioned papers, a notion of weak secrecy was used, i.e. if M is the message transmitted and the eavesdropper receives Z^n for a codeword of length n channel uses, then $I(M; Z^n)/n \rightarrow 0$, as $n \rightarrow \infty$. This notion of secrecy is not stringent enough in various cases [9]. In [11], Maurer proposed a notion of *strong secrecy*: $I(W; Z^n) \rightarrow 0$ as $n \rightarrow \infty$. For a point-to-point channel, he showed that it can be achieved without any change in secrecy capacity. Since then, other methods have been proposed for achieving strong secrecy [12], [13] and [14]. The methods shown in [12] and [14] have been used to obtain strong secrecy for a MAC-WT in [15] and [16], respectively.

In all these works one may notice that security is achieved at the cost of transmission rate. For a single user AWGN wiretap channel, if C_b is the capacity of the legitimate receiver (Bob) and C_e is the capacity of Eve's channel, then the secrecy capacity of this channel is $C_s = (C_b - C_e)^+$, where $(x)^+ = \max(0, x)$ [17]. In recent years, some work has been devoted to mitigating the secrecy rate loss. A feedback channel is used in [18] and [19] to enhance the secrecy rate, and under certain conditions the authors prove that the secrecy capacity can approach the main channel capacity. In [20], the authors assume that the transmitter (Alice) and Bob have access to a secret key, and then they propose a coding scheme which utilizes that key to enhance the secrecy rate. A secure multiplex scheme has been proposed in [21] which achieves Shannon channel capacity for a point-to-point wiretap channel. In this model, multiple messages are transmitted. The authors show that the mutual information of the currently transmitted message with respect to (w.r.t.) all the information received by Eve goes to zero as the codeword length $n \rightarrow \infty$. In [22], Shah *et al.* propose a simple coding scheme, without any feedback channels or access to a specific key, and enhance

the secrecy capacity of a wiretap channel to the Shannon capacity of the main channel. In this work, only the message currently being transmitted is secure with respect to all information possessed by Eve.

In [23], the coding scheme of [22] was extended to a multiple access wiretap channel and it was shown that the Ahleswede-Liao region of the MAC can be achieved as the secrecy rate region, while keeping the currently transmitted message secure with respect to all information of Eve. In this paper, we extend the coding/decoding schemes of [22] and [23] to a multiple access wiretap channel and prove that we can achieve the Ahleswede-Liao region [24], [25] of the MAC as the secrecy-rate region, while keeping all recent messages secure with respect to the information possessed by Eve until the present. Finally, we achieve the same for a fading MAC-WT.

The remaining part of the paper is organized as follows. In Section 2, we define the channel model and recall some previous results which will be used in this paper. We extend the coding/decoding scheme from [22] to two user discrete memoryless MAC-WT (DM-MAC-WT) in Section 3, and prove the achievability of the Ahleswede-Liao region, under the security constraint that only the currently transmitted message is secured with respect to all data received by Eve. In Section 4, we consider a two-user DM-MAC-WT where each user, i.e. the receiver as well as Eve, has infinite length buffers to store previous messages. We propose a coding scheme to enhance the secrecy rate region to the Ahleswede-Liao region of the usual MAC, this time with the security constraint that *all recent* messages are secure with respect to all information possessed by Eve. In Section 5, we consider a two-user fading MAC-WT and extend the coding scheme from the previous sections to enhance the secrecy-rate region of the fading MAC-WT to the Ahleswede-Liao region of the MAC in the ergodic sense. Section 6 concludes the paper. The Appendix contains several lemmas used in the proofs of the main theorems.

In this paper, random variables will be denoted by capital letters X, Y, Z , vectors will be denoted with upper-bar letters, e.g. $\bar{X} = (X_1, \dots, X_n)$, and scalar constants will be denoted by lower case letters a, b , etc.

2. Multiple Access Wiretap Channel

A discrete memoryless multiple access channel with a wiretapper and two users is considered (Fig. 1). The channel is represented by a transition probability matrix $p(y, z|x_1, x_2)$, where $x_i \in \mathcal{X}_i$ is the channel input from user i , $i = 1, 2$, $y \in \mathcal{Y}$ is the channel output to Bob and $z \in \mathcal{Z}$ is the channel output to Eve. Sets $\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}, \mathcal{Z}$ are finite. The two transmitting users want to securely and reliably send messages $M^{(1)}$ and $M^{(2)}$ to Bob (legitimate receiver), while ensuring that eavesdropper (Eve) cannot decode the messages.

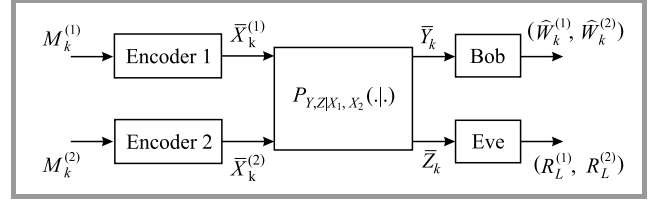


Fig. 1. Discrete memoryless multiple access wiretap channel.

Definition 2.1. For a MAC-WT, a $(2^{nR_1^{(s)}}, 2^{nR_2^{(s)}}, n)$ codebook comprises of (1) two sets of messages $\mathcal{M}^{(i)}$, $i = 1, 2$, where cardinality of each message set is 2^{nR_i} , (2) uniformly distributed messages $M^{(1)}$ and $M^{(2)}$ over corresponding message sets (messages are assumed to be independent of each other), (3) two stochastic encoders:

$$f_i: \mathcal{M}^{(i)} \rightarrow \mathcal{X}_i^n, \quad i = 1, 2, \quad (1)$$

and (4) a decoder at Bob:

$$g: \mathcal{Y}^n \rightarrow \mathcal{M}^{(1)} \times \mathcal{M}^{(2)}. \quad (2)$$

The decoded (estimated) messages are denoted by $(\hat{M}^{(1)}, \hat{M}^{(2)})$.

The average error probability at the receiver (Bob) is:

$$P_e^{(n)} \triangleq P \left\{ (\hat{M}^{(1)}, \hat{M}^{(2)}) \neq (M^{(1)}, M^{(2)}) \right\}, \quad (3)$$

and leakage rate at Eve is:

$$R_L^{(n)} = \frac{1}{n} I(M^{(1)}, M^{(2)}; Z^n). \quad (4)$$

In [6], the authors have defined two types of security requirements depending upon the mutual trust of the transmitting users. If each user is conservative, such that when the other user is transmitting, then it may compromise with Eve and provide Eve with its codeword, then *individual leakage* constraints:

$$R_{L,1}^{(n)} = \frac{1}{n} I(M^{(1)}; Z^n | \bar{X}^{(2)}), \quad (5)$$

$$R_{L,2}^{(n)} = \frac{1}{n} I(M^{(2)}; Z^n | \bar{X}^{(1)}), \quad (6)$$

are relevant, where $\bar{X}^{(i)}$ denotes the codeword for user i .

In a scenario where the users trust each other, *collective leakage*:

$$R_L^{(n)} = \frac{1}{n} I(M^{(1)}, M^{(2)}; Z^n). \quad (7)$$

is relevant. Since, $M^{(1)} \perp M^{(2)}$ and, hence, also $\bar{X}^{(1)} \perp \bar{X}^{(2)}$, where $X \perp Y$ denotes that random variable X is independent of Y :

$$\begin{aligned}
 nR_L^{(n)} &= I(M^{(1)}, M^{(2)}; Z^n) \\
 &= I(M^{(1)}; Z^n) + I(M^{(2)}; Z^n | M^{(1)}) \\
 &= H(M^{(1)}) - H(M^{(1)} | Z^n) + H(M^{(2)}) \\
 &\quad - H(M^{(2)} | Z^n, M^{(1)}) \\
 &\leq H(M^{(1)} | X_2^n) - H(M^{(1)} | Z^n, X_2^n) \\
 &\quad + H(M^{(2)} | X_1^n) - H(M^{(2)} | Z^n, X_1^n) \\
 &= I(M^{(1)}; Z^n | X_2^n) + I(M^{(2)}; Z^n | X_1^n) \\
 &= nR_{L,1}^{(n)} + nR_{L,2}^{(n)} \tag{8}
 \end{aligned}$$

and hence, if individual leakage rates are small, then so is the collective leakage rate. In this paper, we consider the secrecy notion (7).

Definition 2.2. The secrecy-rates $(R_1^{(s)}, R_2^{(s)})$ are achievable if there exists a sequence of codes $(2^{nR_1^{(s)}}, 2^{nR_2^{(s)}}, n)$ with $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$ and

$$\limsup_{n \rightarrow \infty} R_{L,i}^{(n)} = 0, \quad \text{for } i = 1, 2. \tag{9}$$

By taking closure of convex-hull of the achievable secrecy-rate tuple $(R_1^{(s)}, R_2^{(s)})$, we obtain secrecy-capacity region for MAC-WT.

In [6], the authors propose a superposition coding-based scheme to obtain the following secrecy-rate region.

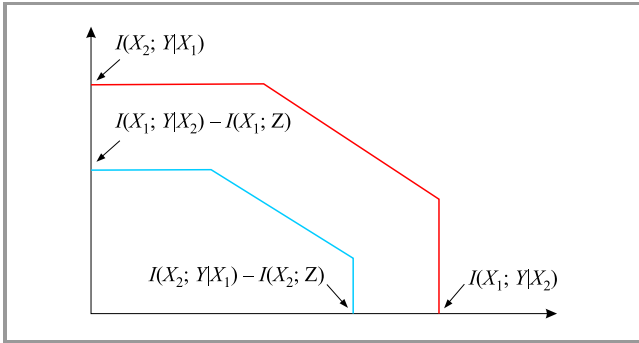


Fig. 2. Capacity region and secrecy rate region of MAC.

Theorem 2.1. Rates $(R_1^{(s)}, R_2^{(s)})$ are achievable with a $\limsup_{n \rightarrow \infty} R_{L,i}^{(n)} = 0$, $i = 1, 2$, if there exist independent random variables (X_1, X_2) as channel inputs satisfying:

$$R_1^{(s)} < I(X_1; Y | X_2) - I(X_1; Z),$$

$$R_2^{(s)} < I(X_2; Y | X_1) - I(X_2; Z),$$

$$R_1^{(s)} + R_2^{(s)} < I(X_1, X_2; Y) - I(X_1; Z) - I(X_2; Z), \tag{10}$$

where Y and Z are the corresponding symbols received by Bob and Eve. \square

The capacity region for a multiple access wiretap channel with the secrecy constraint is not known. Without the secrecy constraint, the capacity region for a multiple access

channel is obtained by taking a convex closure of the regions in Theorem 2.1, excluding the terms $I(X_i; Z)$, $i = 1, 2$ on the RHS of (10) (Fig. 2) [24]. In the following section, we show that we can achieve the Ahleswede-Liao capacity region of a MAC even when some modified metric of security metrics is satisfied. First, we restate the result of [24] and [25] which defines the capacity region for MAC without a security constraint, which we call as the Ahleswede-Liao capacity region.

Theorem 2.2. The capacity region of MAC is given by convex hull of rate pairs (R_1, R_2) satisfying:

$$\begin{aligned}
 R_1 &< I(X_1; Y | X_2), \\
 R_2 &< I(X_2; Y | X_1), \\
 R_1 + R_2 &< I(X_1, X_2; Y). \tag{11}
 \end{aligned}$$

3. Mitigating Rate Loss in MAC-WT to Achieve Ahleswede-Liao Capacity

In this section, the coding scheme proposed in [22] for a single-user point-to-point wiretap channel is extended to the multiple transmitters case in order to enhance the achievable secrecy rates of discrete time MAC-WT. As in [22], we assume that the system is time slotted (i.e. each user transmits one message in one time slot), where each slot consists of n channel uses. In slot 1, the first message is encoded via point-to-point wiretap coding, as in [1]. In slot 2, the message transmitted in slot 1 is used as a secret key along with the usual wiretap code, and then the two messages are transmitted in that slot (the number of channels uses remains the same). Hence, the secrecy-rate is twice as high as in slot 1. We use the same coding scheme in the respective time slots *mutatis mutandis*, until the secrecy rate becomes saturated with the Shannon capacity of the main channel. After this time slot, the previously transmitted secure message is used as a key and no wiretap coding is used. We show that the proposed scheme ensures that the message currently being transmitted is secure with respect to all of Eve's outputs, i.e. if message M_k is securely transmitted in slot k then:

$$\frac{1}{n} I(M_k; \bar{Z}_1, \dots, \bar{Z}_k) \rightarrow 0, \tag{12}$$

as the length of codeword $n \rightarrow \infty$, where \bar{Z}_i is the information received by Eve in slot i .

Next, we not only extend this coding/decoding scheme to a multiple access wiretap channel, but also modify the scheme, so that it can be used to improve its secrecy criterion (12) and can be used for fading multiple access wiretap channels as well. The following secrecy criterion is used. In slot k , if user i transmits message $\bar{M}_k^{(i)}$, we need:

$$I(\bar{M}_l^{(1)}, \bar{M}_l^{(2)}; \bar{Z}_1, \dots, \bar{Z}_k) \leq n\epsilon, \quad \text{for } l = 1, \dots, k. \tag{13}$$

for any given $\epsilon > 0$. This will be strengthened so that it satisfies strong secrecy requirement also, $I(\bar{M}_l^{(1)}, \bar{M}_l^{(2)};$

$\bar{Z}_1, \dots, \bar{Z}_k) \rightarrow 0$ as $n \rightarrow \infty$ at the end of the section. To achieve this goal, we modify the message sets and encoders/decoders with respect to Section 2 in the following manner.

Each slot has n channel uses and is divided into two parts. The first part has n_1 channel uses and the second n_2 , $n_1 + n_2 = n$. The message sets are $\mathcal{M}^{(i)} = \{1, \dots, 2^{nR_i^s}\}$ for users $i = 1, 2$, where (R_1^s, R_2^s) satisfy (10) for some (X_1, X_2) . Here, there are two parts of the each encoder:

$$f_1^s : \mathcal{M}^{(1)} \rightarrow \mathcal{X}_1^{n_1}, \quad f_1^d : \mathcal{M}^{(1)} \times \mathcal{K}_1 \rightarrow \mathcal{X}_1^{n_2}, \quad (14)$$

$$f_2^s : \mathcal{M}^{(2)} \rightarrow \mathcal{X}_2^{n_1}, \quad f_2^d : \mathcal{M}^{(2)} \times \mathcal{K}_2 \rightarrow \mathcal{X}_2^{n_2}, \quad (15)$$

where $X_i \in \mathcal{X}_i$, $i = 1, 2$, and \mathcal{K}_i is the set of secret keys generated for the respective user $i = 1, 2$, f_i^s , $i = 1, 2$ are the usual wiretap encoders corresponding to each transmitting user, as in [6], and f_i^d , $i = 1, 2$ are the deterministic encoders (used for channel models without security constraint) corresponding to each user in the usual MAC. User i may transmit multiple messages from $\mathcal{M}^{(i)}$ in a slot. In the first part of each slot of n_1 length, one message from $\mathcal{M}^{(i)}$ may be transmitted using wiretap coding via f_i^s (denoted by $\bar{M}_{k,1}^{(i)}$ in slot k) and in the second part multiple messages from $\mathcal{M}^{(i)}$ may be transmitted (denoted by $\bar{M}_{k,2}^{(i)}$) using messages transmitted in previous slots as keys. The overall message transmitted in slot k by user i is $\bar{M}_k^{(i)} = (\bar{M}_{k,1}^{(i)}, \bar{M}_{k,2}^{(i)})$.

Theorem 3.1. The secrecy rate region achieved while satisfying (13) is the Ahleswede-Liao capacity region for MAC, i.e. it is the closure of convex hull of all rate pairs $(R_1^{(s)}, R_2^{(s)})$ satisfying:

$$\begin{aligned} R_1^{(s)} &< I(X_1; Y|X_2), \\ R_2^{(s)} &< I(X_2; Y|X_1), \\ R_1^{(s)} + R_2^{(s)} &< I(X_1, X_2; Y), \end{aligned} \quad (16)$$

for some independent random variables X_1, X_2 .

Proof. We fix distributions p_{X_1}, p_{X_2} . Initially we take $n_1 = n_2 = n/2$. In the first slot, i -th user selects message $\mathcal{M}_1^{(i)} \in \mathcal{M}^{(i)}$ to be securely transmitted in the first part of the slot, while the second part is not used. Both users use the multiple access wiretap coding scheme of [6]. Hence, the achievable rate pair $(R_1^{(s)}, R_2^{(s)})$ satisfies (10) and $R_{L,i}^{(n)} \leq n_1 \epsilon$, $i = 1, 2$. In slot 2, the two users select two messages each, $(\bar{M}_{2,1}^{(1)}, \bar{M}_{2,2}^{(1)})$ and $(\bar{M}_{2,1}^{(2)}, \bar{M}_{2,2}^{(2)})$ to be transmitted. Both transmitting users use the multiple access wiretap coding scheme (as in [6]) for the first part of the message, i.e. $(\bar{M}_{2,1}^{(1)}, \bar{M}_{2,1}^{(2)})$, and for the second part, transmitter i first takes XOR of $\bar{M}_{2,2}^{(i)}$ with the previous message, i.e. $\bar{M}_{2,2}^{(i)} \oplus \bar{M}_1^{(i)}$. This message (i.e. XOR of the second part and the previous message) is transmitted over the multiple access wiretap channel using a usual MAC coding scheme, i.e. without security [24], [25]. Therefore, the achievable secrecy rate in both sub-slots satisfies (10) for both the

transmitting users. This achievable secrecy rate is also the overall rate of slot two.

In the third slot, the rate satisfies (10) in the first part (via wiretap coding). Since in the second part we XOR with message $\bar{M}_2^{(i)}$ and are able to send two messages, hence the rate of (10), assuming $2(R_1^{(s)}, R_2^{(s)})$ via (10), is within the range of (16).

Define:

$$\lambda_1 \triangleq \left\lceil \frac{I(X_1; Y|X_2)}{I(X_1; Y|X_2) - I(X_1; Z)} \right\rceil, \quad (17)$$

where $\lceil x \rceil$ is the ceiling of x , i.e. the smallest integer greater than or equal to x . In slot $\lambda_1 + 1$ the rate of user 1 in the second part of the slot satisfies:

$$\begin{aligned} R_1^{(s)} &\leq \min(\lambda_1 (I(X_1; Y|X_2) - I(X_1; Z)), I(X_1; Y|X_2)) \\ &= I(X_1; Y|X_2). \end{aligned} \quad (18)$$

Similarly, we define λ_2 as:

$$\lambda_2 \triangleq \left\lceil \frac{I(X_2; Y|X_1)}{I(X_2; Y|X_1) - I(X_2; Z)} \right\rceil. \quad (19)$$

In slot $\lambda_2 + 1$, the rate $R_2^{(s)}$ satisfies:

$$R_2^{(s)} \leq I(X_2; Y|X_1). \quad (20)$$

In slot $\lambda = \max\{\lambda_1, \lambda_2\} + 1$, the sum-rate will satisfy:

$$\begin{aligned} R_1^{(s)} + R_2^{(s)} &\leq \min \left\{ \lambda \left[I(X_1, X_2; Y) - \sum_{i=1}^2 I(X_i; Z) \right], \right. \\ &\quad \left. I(X_1, X_2; Y) \right\}. \end{aligned} \quad (21)$$

After some particular slot, say, λ^* which is greater than λ , the achievable secrecy sum-rate will get saturated by the Shannon sum-rate (i.e. sum-capacity of the usual MAC), i.e. $I(X_1, X_2; Y)$, and, hence, thereafter the rate pair $(R_1^{(s)}, R_2^{(s)}) \triangleq (R_1^{(s)*}, R_2^{(s)*})$ in the second part of the slot will be at a boundary point of (16) and the overall rate for the whole slot is the average of the rates in the first mini-slot and the second mini-slot.

In k -th slot, ($k > \lambda^*$) to securely transmit a pair of messages $(\bar{M}_k^{(1)}, \bar{M}_k^{(2)})$, where $\bar{M}_k^{(i)} = (\bar{M}_{k,1}^{(i)}, \bar{M}_{k,2}^{(i)})$, $i = 1, 2$, we

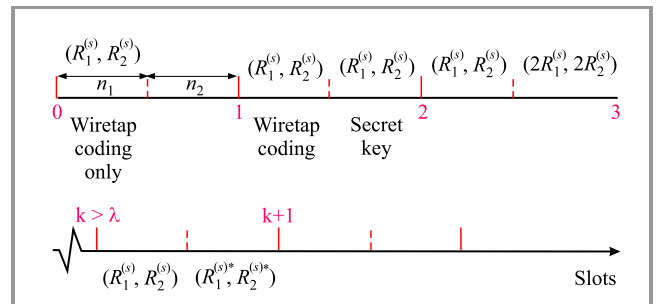


Fig. 3. Coding scheme to achieve Ahleswede-Liao region in MAC.

use the usual wiretap coding for $(\overline{M}_{k,1}^{(1)}, \overline{M}_{k,1}^{(2)})$ and for the second part of the message, we XOR it with the previously transmitted message, i.e. $\overline{M}_{k,2}^{(i)} \oplus \overline{M}_{k-1,2}^{(i)}$, $i = 1, 2$, and transmit the overall codeword over the MAC-WT (Fig. 3). We let $n_2 = ln_1$ such that the overall rate of a slot is close to that in (16). Hence, by taking a sufficiently large l , one can achieve rates arbitrarily close to the boundary of (16). For the above-mentioned coding scheme, $P_e^n \rightarrow 0$. A convex combination of the achievable rates in (16) can be achieved by time sharing. Now, we show that our coding/decoding scheme also satisfies (13).

Leakage rate analysis. Before we compute the leakage rate, we set up the notation which will be used in the subsequent part of the proof. For transmitting user i , we represent the codeword sent in slot k by $\overline{X}_k^{(i)}$. Similarly, $\overline{X}_{k,1}^{(i)}$ and $\overline{X}_{k,2}^{(i)}$ will represent n_1 -length and n_2 -length codewords of i -th user i in slot number k . We define a notation here, when $i = 1$ then $\bar{i} = 2$ and when $i = 2$ then $\bar{i} = 1$. In k -th slot, the noisy version of the codeword received by Eve is $\overline{Z}_k \equiv (\overline{Z}_{k,1}, \overline{Z}_{k,2})$, where $\overline{Z}_{k,1}$ is the sequence corresponding to the wiretap coding part and $\overline{Z}_{k,2}$ is corresponding to the XOR part in which the previous message is used as a key.

Since wiretap coding of [6] is employed in slot 1, the leakage rate will satisfy:

$$I(\overline{M}_1^{(1)}; \overline{Z}_1 | \overline{X}_1^{(2)}) \leq n_1 \varepsilon, \quad I(\overline{M}_1^{(2)}; \overline{Z}_1 | \overline{X}_1^{(1)}) \leq n_1 \varepsilon. \quad (22)$$

For user 1 in slot 2, we show:

$$\begin{aligned} I(\overline{M}_1^{(1)}; \overline{Z}_1, \overline{Z}_2 | \overline{X}_2^{(2)}) &\leq n_1 \varepsilon, \\ I(\overline{M}_2^{(1)}; \overline{Z}_1, \overline{Z}_2 | \overline{X}_2^{(1)}) &\leq n_1 \varepsilon. \end{aligned} \quad (23)$$

A similar calculation can be made for user 2.

First, we note that:

$$\begin{aligned} I(\overline{M}_1^{(1)}; \overline{Z}_1, \overline{Z}_2 | \overline{X}_2^{(2)}) &= I(\overline{M}_1^{(1)}; \overline{Z}_1) + I(\overline{M}_1^{(1)}; \overline{Z}_2 | \overline{Z}_1, \overline{X}_2^{(2)}) \\ &\stackrel{(a)}{\leq} n_1 \varepsilon + H(\overline{M}_1^{(1)} | \overline{Z}_1, \overline{X}_2^{(2)}) - H(\overline{M}_1^{(1)} | \overline{Z}_1, \overline{X}_2^{(2)}, \overline{Z}_2) \\ &\stackrel{(b)}{=} n_1 \varepsilon + H(\overline{M}_1^{(1)} | \overline{Z}_1) - H(\overline{M}_1^{(1)} | \overline{Z}_1) = n_1 \varepsilon. \end{aligned} \quad (24)$$

where (a) follows from the usual wiretap coding and (b) follows from the fact that $\overline{X}_2^{(2)} \perp (\overline{M}_1^{(1)}, \overline{Z}_1)$, and $(\overline{X}_2^{(2)}, \overline{Z}_2) \perp (\overline{M}_1^{(1)}, \overline{Z}_1)$.

Next, we consider:

$$\begin{aligned} I(\overline{M}_2^{(1)}; \overline{Z}_1, \overline{Z}_2 | \overline{X}_2^{(2)}) &= I(\overline{M}_{2,1}^{(1)}, \overline{M}_{2,2}^{(1)}; \overline{Z}_1, \overline{Z}_2 | \overline{X}_2^{(2)}) \\ &= I(\overline{M}_{2,1}^{(1)}; \overline{Z}_1, \overline{Z}_2 | \overline{X}_2^{(2)}) + I(\overline{M}_{2,2}^{(1)}; \overline{Z}_1, \overline{Z}_2 | \overline{X}_2^{(2)}, \overline{M}_{2,1}^{(1)}) \\ &\triangleq I_1 + I_2. \end{aligned} \quad (25)$$

We get the upper bounds on I_1 and I_2 . The first term:

$$\begin{aligned} I_1 &= I(\overline{M}_{2,1}^{(1)}; \overline{Z}_1, \overline{Z}_2 | \overline{X}_2^{(2)}) \\ &= I(\overline{M}_{2,1}^{(1)}; \overline{Z}_1, \overline{Z}_{2,1}, \overline{Z}_{2,2} | \overline{X}_2^{(2)}) \\ &= I(\overline{M}_{2,1}^{(1)}; \overline{Z}_1 | \overline{X}_2^{(2)}) + I(\overline{M}_{2,1}^{(1)}; \overline{Z}_{2,1} | \overline{X}_2^{(2)}, \overline{Z}_1) \\ &\quad + I(\overline{M}_{2,1}^{(1)}; \overline{Z}_{2,2} | \overline{X}_2^{(2)}, \overline{Z}_1, \overline{Z}_{2,1}) \\ &\stackrel{(a)}{=} 0 + I(\overline{M}_{2,1}^{(1)}; \overline{Z}_{2,1} | \overline{X}_2^{(2)}, \overline{X}_{2,2}^{(2)}, \overline{Z}_1) \\ &\quad + I(\overline{M}_{2,1}^{(1)}; \overline{Z}_{2,2} | \overline{X}_2^{(2)}, \overline{Z}_1, \overline{Z}_{2,1}) \\ &\triangleq I_{11} + I_{12}, \end{aligned} \quad (26)$$

where (a) follows because \overline{Z}_1 is independent of $(\overline{M}_{2,1}^{(1)}, \overline{X}_2^{(2)})$. Furthermore:

$$\begin{aligned} I_{11} &= I(\overline{M}_{2,1}^{(1)}; \overline{Z}_{2,1} | \overline{X}_{2,1}^{(2)}, \overline{X}_{2,2}^{(2)}, \overline{Z}_1) \\ &= H(\overline{M}_{2,1}^{(1)}; | \overline{X}_{2,1}^{(2)}, \overline{X}_{2,2}^{(2)}, \overline{Z}_1) \\ &\quad - H(\overline{M}_{2,1}^{(1)}; | \overline{Z}_{2,1}, \overline{X}_{2,1}^{(2)}, \overline{X}_{2,2}^{(2)}, \overline{Z}_1) \\ &\stackrel{(a)}{=} H(\overline{M}_{2,1}^{(1)}; | \overline{X}_{2,1}^{(2)}) - H(\overline{M}_{2,1}^{(1)}; | \overline{Z}_{2,1}, \overline{X}_{2,1}^{(2)}) \\ &= I(\overline{M}_{2,1}^{(1)}; \overline{Z}_{2,1} | \overline{X}_{2,1}^{(2)}) \stackrel{(b)}{\leq} n_1 \varepsilon, \end{aligned} \quad (27)$$

where (a) follows, since $(\overline{X}_{2,2}^{(2)}, \overline{Z}_1) \perp (\overline{M}_{2,1}^{(1)}, \overline{Z}_{2,1}, \overline{X}_{2,1}^{(2)})$ and (b) follows because the first part of the message is encoded via the usual wiretap coding scheme for the multiple access wiretap channel. Also:

$$\begin{aligned} I_{12} &= I(\overline{M}_{2,1}^{(1)}; \overline{Z}_{2,2} | \overline{X}_2^{(2)}, \overline{Z}_1, \overline{Z}_{2,1}) \\ &= H(\overline{M}_{2,1}^{(1)}; | \overline{X}_{2,1}^{(2)}, \overline{X}_{2,2}^{(2)}, \overline{Z}_1, \overline{Z}_{2,1}) \\ &\quad - H(\overline{M}_{2,1}^{(1)}; | \overline{X}_{2,1}^{(2)}, \overline{X}_{2,2}^{(2)}, \overline{Z}_1, \overline{Z}_{2,1}, \overline{Z}_{2,2}) \\ &\stackrel{(a)}{=} H(\overline{M}_{2,1}^{(1)}; | \overline{X}_{2,1}^{(2)}, \overline{Z}_{2,1}) - H(\overline{M}_{2,1}^{(1)}; | \overline{X}_{2,1}^{(2)}, \overline{Z}_{2,1}) = 0, \end{aligned}$$

where (a) follows, since $(\overline{X}_{2,2}^{(2)}, \overline{Z}_1, \overline{Z}_{2,2}) \perp (\overline{M}_{2,1}^{(1)}, \overline{X}_{2,1}^{(2)}, \overline{Z}_{2,1})$.

From Eqs. (25), (26) and (27), we have $I_1 = I_{11} + I_{12} \leq n_1 \varepsilon$. Next, we consider:

$$\begin{aligned} I_2 &= I(\overline{M}_{2,2}^{(1)}; \overline{Z}_1, \overline{Z}_2 | \overline{X}_2^{(2)}, \overline{M}_{2,1}^{(1)}) \\ &= I(\overline{M}_{2,2}^{(1)}; \overline{Z}_2 | \overline{X}_2^{(2)}, \overline{M}_{2,1}^{(1)}) \\ &\quad + I(\overline{M}_{2,2}^{(1)}; \overline{Z}_1 | \overline{X}_2^{(2)}, \overline{M}_{2,1}^{(1)}, \overline{Z}_2). \end{aligned} \quad (28)$$

We have:

$$\begin{aligned} I(\overline{M}_{2,2}^{(1)}; \overline{Z}_2 | \overline{X}_2^{(2)}, \overline{M}_{2,1}^{(1)}) &= I(\overline{M}_{2,2}^{(1)}; \overline{Z}_{2,1} | \overline{X}_2^{(2)}, \overline{M}_{2,1}^{(1)}) \\ &\quad + I(\overline{M}_{2,2}^{(1)}; \overline{Z}_{2,2} | \overline{X}_2^{(2)}, \overline{M}_{2,1}^{(1)}, \overline{Z}_{2,1}) \\ &\stackrel{(a_1)}{=} 0 + I(\overline{M}_{2,2}^{(1)}; \overline{Z}_{2,2} | \overline{X}_2^{(2)}, \overline{M}_{2,1}^{(1)}, \overline{Z}_{2,1}) \\ &\stackrel{(a_2)}{=} I(\overline{M}_{2,2}^{(1)}; \overline{Z}_{2,2} | \overline{X}_{2,2}^{(2)}) \stackrel{(a_3)}{=} 0, \end{aligned}$$

and (a_1) follows, since $\overline{M}_{2,2}^{(1)} \perp (\overline{Z}_{2,1}, \overline{X}_2^{(2)}, \overline{M}_{2,1}^{(1)})$; (a_2) holds because $(\overline{X}_{2,1}^{(2)}, \overline{M}_{2,1}^{(1)}) \perp (\overline{M}_{2,2}^{(1)}, \overline{Z}_{2,2}, \overline{X}_{2,2}^{(2)})$; and (a_3) is true, since $\overline{M}_{2,2}^{(1)} \perp (\overline{X}_{2,2}^{(2)}, \overline{Z}_{2,2})$. In addition:

$$\begin{aligned} & I(\overline{M}_{2,2}^{(1)}; \overline{Z}_1 | \overline{X}_2^{(2)}, \overline{M}_{2,1}^{(1)}, \overline{Z}_2) \\ &= I(\overline{M}_{2,2}^{(1)}; \overline{Z}_1 | \overline{X}_{2,1}^{(2)}, \overline{X}_{2,2}^{(2)}, \overline{M}_{2,1}^{(1)}, \overline{Z}_{2,1}, \overline{Z}_{2,2}) \\ &\stackrel{(b_1)}{=} I(\overline{M}_{2,2}^{(1)}; \overline{Z}_1 | \overline{X}_{2,2}^{(2)}, \overline{Z}_{2,2}) \stackrel{(b_2)}{=} 0, \end{aligned}$$

where (b_1) follows, since $(\overline{M}_{2,1}^{(1)}, \overline{Z}_{2,1}, \overline{X}_{2,1}^{(2)}) \perp (\overline{Z}_{2,2}, \overline{X}_{2,2}^{(2)}, \overline{M}_{2,2}^{(1)}, \overline{Z}_1)$ and (b_2) follows because $\overline{Z}_1 \perp (\overline{M}_{2,2}^{(1)}, \overline{X}_{2,2}^{(2)}, \overline{Z}_{2,2})$. Hence, from (28) we have $I_2 = 0$. From (25), we have:

$$I(\overline{M}_2^{(1)}; \overline{Z}_1, \overline{Z}_2 | \overline{X}_2^{(2)}) \leq n_1 \varepsilon. \quad (29)$$

Similarly, one can show that:

$$I(\overline{M}_2^{(2)}; \overline{Z}_1, \overline{Z}_2 | \overline{X}_2^{(1)}) \leq n_1 \varepsilon. \quad (30)$$

Therefore, from (8):

$$\begin{aligned} & I(\overline{M}_2^{(1)}, \overline{M}_2^{(2)}; \overline{Z}_1, \overline{Z}_2) \\ &\leq I(\overline{M}_2^{(1)}; \overline{Z}_1, \overline{Z}_2 | \overline{X}_2^{(2)}) + I(\overline{M}_2^{(2)}; \overline{Z}_1, \overline{Z}_2 | \overline{X}_2^{(1)}). \end{aligned}$$

To prove that (13) holds for any slot, we use the principle of mathematical induction in the lemma below. For a proof, please see [23].

Lemma 3.2. Let (13) hold for k , then it also holds for $k+1$. \square

Remark 1 (extension to strong secrecy notion). We have used the notion of *weak secrecy* in the above proof, i.e. if message W is transmitted via wiretap coding and Eve receives sequence Z^n , then $I(W; Z^n) \leq n_1 \varepsilon$. The criteria of *strong secrecy* provide not only for the information leakage rate, but also require that the absolute information vanishes, i.e. $I(W; Z^n) \leq \varepsilon$. In a single-user point-to-point wiretap channel, if the weak secrecy notion is replaced by the strong secrecy notion, the secrecy capacity of the channel does not change [26]. A similar result has been proved for a MAC-WT in [16], using the channel resolvability-based coding scheme. If we use, in the coding scheme proposed in this paper (Theorem 2), a coding scheme based on the resolvability technique in slot 1, and in other slots use both coding schemes together (i.e. resolvability-based coding in the first part of the slot) and the previously transmitted message (which is now secure in the strong sense with respect to Eve) as a secret key in the second part of the slot, we can achieve the same secrecy-rate region, i.e. the capacity region of the usual multiple access channel without Eve, satisfying the following leakage rate:

$$\limsup_{n \rightarrow \infty} I(\overline{M}_k^{(1)}, \overline{M}_k^{(2)}; \overline{Z}_1, \overline{Z}_2, \dots, \overline{Z}_k) = 0, \quad (31)$$

as $n \rightarrow \infty$, because in the RHS of (13), we can get ε instead of $2n_1 \varepsilon$.

4. Discrete Memoryless MAC-WT with Buffer

In this section we improve the result from Theorem 3.1 by obtaining rates (16) while enhancing the secrecy requirement from (13) to:

$$\begin{aligned} & I(\overline{M}_k^{(1)}, \overline{M}_{k-1}^{(1)}, \dots, \overline{M}_{k-N_1}^{(1)}; \overline{Z}_1, \dots, \overline{Z}_k | \overline{X}_k^{(2)}) \leq n_1 \varepsilon, \\ & I(\overline{M}_k^{(2)}, \overline{M}_{k-1}^{(2)}, \dots, \overline{M}_{k-N_1}^{(2)}; \overline{Z}_1, \dots, \overline{Z}_k | \overline{X}_k^{(1)}) \leq n_1 \varepsilon, \\ & I(\overline{M}_k^{(1)}, \overline{M}_k^{(2)}, \dots, \overline{M}_{k-N_1}^{(1)}, \overline{M}_{k-N_1}^{(2)}; \overline{Z}_1, \dots, \overline{Z}_k) \leq 2n_1 \varepsilon, \end{aligned} \quad (32)$$

where N_1 can be arbitrarily large. This will satisfy the requirements of any practical system. Therefore, we use a key buffer at each of the users and instead of using the messages transmitted in slot $k-1$ as the key in slot k , we use the messages transmitted in slots before $k-N_1-1$.

Let each user have an infinite key buffer to store the key bits. The message $\overline{M}_k^{(i)}$ after transmission in slot k from user i is stored in its key buffer at the end of the slot. However, now in slot $k+1$ we use the *oldest* bits stored in its key buffer as a key in the second part of its slot. Once certain bits from the key buffer have been used as a key, these are discarded from the key buffer.

Let $B_k^{(i)}$ be the number of key bits in the key buffer of the i -th user at the beginning of the k -th slot. Then, out of this, for $k \geq \lambda^*$, the number of key bits used in a slot by user 1 is $C_1 n_2$, since these are used only in the second part of the slot where $C_1 \leq I(X_1; Y | X_2)$, while the total number of secret bits transmitted in the slot is $C_1 n_2 + R_s^{(1)} n_1$. These transmitted bits also get stored in its key buffer at time $k+1$. Similarly, the same holds for user 2. Thus, $B_k^{(i)} \rightarrow \infty$ as $k \rightarrow \infty$ for $i = 1, 2$.

After some time (say N_2 slots) has elapsed since using the oldest bits in the key buffer, for $k \geq N_2$, we will be using the secret key bits only from messages $(\overline{M}_1^{(i)}, \overline{M}_2^{(i)}, \dots, \overline{M}_{k-N_1-1}^{(i)})$ for securing messages $(\overline{M}_k^{(i)}, \overline{M}_{k-1}^{(i)}, \dots, \overline{M}_{k-N_1}^{(i)})$, for user $i = 1, 2$, respectively. The following proof works for $N_1 > 0$. Theorem 2.1 for $N_1 = 0$.

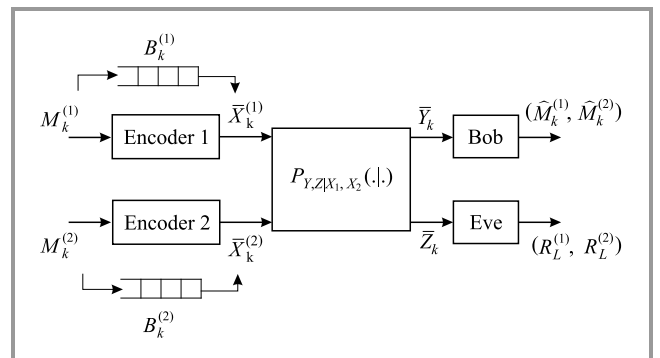


Fig. 4. Discrete memoryless multiple access wiretap channel with secret key buffers.

Theorem 4.1. The secrecy-rate region with the leakage rate constraints (32) of a DM-MAC-WT is equal to the usual Ahleswede-Liao region (16) of MAC.

Proof. With the proposed modification of the coding-decoding scheme presented in Section 3, in any slot k , the legitimate receiver is able to decode the message pair $(\bar{M}_k^{(1)}, \bar{M}_k^{(2)})$ with the error probability of $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$. Also (13) along with $R_{L,i}^{(n)} \leq n_1 \epsilon_1, i = 1, 2$ continue to be satisfied, where $\epsilon_1 > 0$ will be fixed later on. Now we consider the leakage rate. We have:

$$\begin{aligned} & I(\bar{M}_k^{(1)}, \bar{M}_{k-1}^{(1)}, \dots, \bar{M}_{k-N_1}^{(1)}; \bar{Z}_1, \dots, \bar{Z}_k | \bar{X}_k^{(2)}) \\ &= I(\bar{M}_{k,1}^{(1)}, \bar{M}_{k-1,1}^{(1)}, \dots, \bar{M}_{k-N_1,1}^{(1)}; \bar{Z}_1, \dots, \bar{Z}_k | \bar{X}_k^{(2)}) \\ &+ I(\bar{M}_{k,2}^{(1)}, \bar{M}_{k-1,2}^{(1)}, \dots, \bar{M}_{k-N_1,2}^{(1)}; \bar{Z}_1, \dots, \bar{Z}_k \\ &| \bar{X}_k^{(2)}, \bar{M}_{k,1}^{(1)}, \dots, \bar{M}_{k-N_1,1}^{(1)}) . \end{aligned}$$

From Lemma 7.1 and Lemma 7.2 in the Appendix:

$$I(\bar{M}_{k,1}^{(1)}, \bar{M}_{k-1,1}^{(1)}, \dots, \bar{M}_{k-N_1,1}^{(1)}; \bar{Z}_1, \dots, \bar{Z}_k | \bar{X}_k^{(2)}) \leq n_1 \epsilon \quad (33)$$

and

$$\begin{aligned} & I(\bar{M}_{k,2}^{(1)}, \bar{M}_{k-1,2}^{(1)}, \dots, \bar{M}_{k-N_1,2}^{(1)}; \bar{Z}_1, \dots, \bar{Z}_k | \bar{X}_k^{(2)}, \bar{M}_{k,1}^{(1)}, \dots, \\ & \bar{M}_{k-N_1,1}^{(1)}) \leq 6n_1 \epsilon . \end{aligned} \quad (34)$$

Thus, taking $\epsilon = \epsilon/7$, we obtain the first inequality in (32). Similarly, we can show the second inequality.

To prove the third inequality, we define $\tilde{M}^{(1)} \triangleq (\bar{M}_k^{(1)}, \bar{M}_{k-1}^{(1)}, \dots, \bar{M}_{k-N_1}^{(1)})$, $\tilde{M}^{(2)} \triangleq (\bar{M}_k^{(2)}, \bar{M}_{k-1}^{(2)}, \dots, \bar{M}_{k-N_1}^{(2)})$ and $\tilde{Z} \triangleq (\bar{Z}_1, \dots, \bar{Z}_k)$, and we have:

$$\begin{aligned} & I(\tilde{M}^{(1)}, \tilde{M}^{(2)}; \tilde{Z}) \\ &= I(\tilde{M}^{(1)}; \tilde{Z}) + I(\tilde{M}^{(2)}; \tilde{Z} | \tilde{M}^{(1)}) \\ &= H(\tilde{M}^{(1)}) - H(\tilde{M}^{(1)} | \tilde{Z}) + H(\tilde{M}^{(2)}) - H(\tilde{M}^{(2)} | \tilde{Z}, \tilde{M}^{(1)}) \\ &\stackrel{(a)}{\leq} H(\tilde{M}^{(1)} | \bar{X}_k^{(2)}) - H(\tilde{M}^{(1)} | \tilde{Z}, \bar{X}_k^{(2)}) + H(\tilde{M}^{(2)} | \bar{X}_k^{(1)}) \\ &\quad - H(\tilde{M}^{(2)} | \tilde{Z}, \bar{X}_k^{(1)}) \\ &= I(\tilde{M}^{(1)}; \tilde{Z} | \bar{X}_k^{(2)}) + I(\tilde{M}^{(2)}; \tilde{Z} | \bar{X}_k^{(1)}), \end{aligned} \quad (35)$$

where (a) follows because: conditioning decreases the entropy, all transmitted messages are independent of each other and the codeword is a one-to-one function of the message to be transmitted. Hence, from (33) and (34):

$$I(\bar{M}_k^{(1)}, \bar{M}_k^{(2)}, \dots, \bar{M}_{k-N_1}^{(1)}, \bar{M}_{k-N_1}^{(2)}; \bar{Z}_1, \dots, \bar{Z}_k^n) \leq n_1 \epsilon . \quad (36)$$

5. Fading MAC-WT

In this section, we consider a two-user discrete time additive white Gaussian fading channel. If X_1, X_2 are the channel inputs, then Bob receives:

$$Y = \tilde{H}_1 X_1 + \tilde{H}_2 X_2 + N_1 \quad (37)$$

and Eve receives:

$$Z = \tilde{G}_1 X_1 + \tilde{G}_2 X_2 + N_2, \quad (38)$$

where \tilde{H}_i is the channel gain to Bob, \tilde{G}_i is the channel gain to Eve, and N_i has Gaussian distribution with a mean 0 and variance $\sigma_i^2, i = 1, 2$. We assume that the random variables $\tilde{H}_1, \tilde{H}_2, \tilde{G}_1, \tilde{G}_2, N_1, N_2$ are independent of each other. The channel is experiencing slow fading, i.e. the channel gains remain the same during the transmission of the entire codeword. Let $H_i = |\tilde{H}_i|^2$ and $G_i = |\tilde{G}_i|^2, i = 1, 2$. The average power constraint for user i is \bar{P}_i .

We define some notation for convenience. For $H = (H_1, H_2), G = (G_1, G_2)$:

$$\begin{aligned} C_1(P_1(H, G)) &\triangleq \frac{1}{2} \log \left(1 + \frac{H_1 P_1(H, G)}{\sigma_1^2} \right), \\ C_2(P_2(H, G)) &\triangleq \frac{1}{2} \log \left(1 + \frac{H_2 P_2(H, G)}{\sigma_1^2} \right), \\ C_1^e(P_1(H, G)) &\triangleq \frac{1}{2} \log \left(1 + \frac{G_1 P_1(H, G)}{\sigma_2^2 + G_2 P_2(H, G)} \right), \\ C_2^e(P_2(H, G)) &\triangleq \frac{1}{2} \log \left(1 + \frac{G_2 P_2(H, G)}{\sigma_2^2 + G_1 P_1(H, G)} \right), \\ C(P_1(H, G), P_2(H, G)) &\triangleq \frac{1}{2} \log \left(1 + \right. \\ & \left. \frac{H_1 P_1(H, G) + H_2 P_2(H, G)}{\sigma_1^2} \right). \end{aligned} \quad (39)$$

The achievable secrecy rate region for this channel is:

$$\begin{aligned} & \mathcal{R}_g^s(\bar{P}) = \\ & \left\{ \begin{array}{l} (R_1^{(s)}, R_2^{(s)}) : \\ R_1^{(s)} \leq \mathbb{E}_{H,G} [(C_1(P_1) - C_1^e(P_1))^+] \\ R_2^{(s)} \leq \mathbb{E}_{H,G} [(C_2(P_2) - C_2^e(P_2))^+] \\ R_1^{(s)} + R_2^{(s)} \leq \mathbb{E}_{H,G} [(C(P_1, P_2) - \sum_{i=1}^2 C_i^e(P_i))^+] \end{array} \right\} \end{aligned} \quad (40)$$

where $\bar{P} = (\bar{P}_1, \bar{P}_2)$. To achieve these rates (with $P_i(H, G) \equiv \bar{P}_i$), the transmitters need not know the channel states, but Bob's receiver needs to know all H_i, G_i . We assume this in this section.

If the channel states (H, G) are known to each of the users, as well as at the receiver of Bob, then we can improve over the rate region in (40) by making the transmit power as functions of (H, G) :

$$\mathcal{P} : H \times G \rightarrow \mathbb{R}_+^2, \quad (41)$$

where $\mathcal{P} = (P_1, P_2)$. Now we note the rate region as $\mathcal{C}_f^s(\mathcal{P})$. Therefore, the secrecy capacity region of MAC-WT ($\mathcal{C}_f^s(\mathcal{P})$) is not known, but $\mathcal{R}_f^s(\mathcal{P}) \subseteq \mathcal{C}_f^s(\mathcal{P})$ [27].

Now, we apply the coding scheme of Section 3 to the two-user fading MAC-WT in order to enlarge the secrecy rate region to the usual capacity region of the fading channel. The message pair $(\overline{M}_k^{(1)}, \overline{M}_k^{(2)})$ is to be transmitted confidentially by the two users over the fading MAC in slot k , and will be stored in their respective secret key buffers at the end of the k -th slot. Let $B_k^{(1)}, B_k^{(2)}$ be the number of bits in the key buffers of users 1 and 2, respectively, at the beginning of the slot k .

Let $\overline{R}_k^{(i)}$ bits be taken from the key buffer of user i to act as a secret key for the transmission of message $\overline{M}_k^{(i)}$. The two users satisfy the long-term average power constraint:

$$\limsup_{k \rightarrow \infty} \frac{1}{k} \sum_{m=1}^k \mathbb{E}[P_i(H_k, G_k)] \leq \overline{P}_i, \quad i = 1, 2, \quad (42)$$

where H_k, G_k are the channel gains in slot k and $P_i(H_k, G_k)$ is the average power used by user i in slot k . We need to compute $P_i(H, G)$ and $\overline{R}_k^{(i)}$, $i = 1, 2$, such that the resulting average rate region $(\overline{r}^{(1)}, \overline{r}^{(2)})$ is maximized, where:

$$\overline{r}^{(i)} = \limsup_{k \rightarrow \infty} \frac{1}{k} \sum_{l=1}^k r_l^{(i)}, \quad (43)$$

$r_k^{(i)}$ is the transmission rate of user i in slot k , subject to the long-term respective power constraints (42). The secrecy-rate region is computed when:

$$\Pr(\{H_{1k} > G_{1k}\} \cup \{H_{2k} > G_{2k}\}) > 0, \quad (44)$$

where $\Pr(A)$ represents the probability of event A . Otherwise, the secrecy-rate region is zero. Actually, we state the following theorem for $\Pr(H_{ik} > G_{ik}) > 0$, $i = 1, 2$. If it is not true for any one i , then the secrecy rate for that user is zero. For both transmitting users, at the end of slot k , $\hat{r}_k^{(i)} = n(l+1)r_k^{(i)}$ bits are stored in the secret key buffer for future use as a key, where $n_2 = ln_1$. Hence, $B_k^{(i)}$ evolves as:

$$B_{k+1}^{(i)} = B_k^{(i)} + \hat{r}_k^{(i)} - \overline{R}_k^{(i)}, \quad (45)$$

where $\hat{r}_k^{(i)} \geq \overline{R}_k^{(i)}$ and $\hat{r}_k^{(i)} > \overline{R}_k^{(i)}$ with positive probability $\Pr(H_{ik} > G_{ik})$. Therefore, $B_k^{(i)} \rightarrow \infty$ a.s. for $i = 1, 2$.

Theorem 5.1. If $\Pr(H_{ik} > G_{ik}) > 0$, $i = 1, 2$, and all the channel gains are available at all the transmitters, then the following long-term average rates that maintain the leakage rates (32), are achievable:

$$\begin{aligned} R_1^{(s)} &\leq \frac{1}{2} \mathbb{E}_{H,G} [C_1(P_1(H))] , \\ R_2^{(s)} &\leq \frac{1}{2} \mathbb{E}_{H,G} [C_2(P_2(H))] , \\ R_1^{(s)} + R_2^{(s)} &\leq \frac{1}{2} \mathbb{E}_{H,G} [C(P_1(H), P_2(H))] . \end{aligned} \quad (46)$$

where P is any policy that satisfies the average power constraint. If Bob is the only party knowing all channel states (not the transmitters), then $(R_1^{(s)}, R_2^{(s)})$ satisfies (46) with $P_i(H, G) \equiv \overline{P}_i$, $i = 1, 2$.

Achievability scheme outline. We use the coding-decoding scheme proposed in Section 3 with appropriate changes to account for the fading process. Assuming that $B_0^{(i)} = 0$, $i = 1, 2$, user i transmits the first time when $H_{ik} > G_{ik}$. Then, it uses the usual MAC wiretap coding as proposed in [6] in all its $l+1$ mini-slots.

In the next slot (say k -th), user i uses the first mini-slot for wiretap coding (if $H_{ik} > G_{ik}$ for user i) and the rest of the m mini-slots for transmission via the secret key (if $H_{ik} < G_{ik}$ the first mini-slot is not used). It uses $\overline{R}_k^{(i)} = \min[B_k^{(i)}, IC_i(P_i(H, G)n_1)]$ key bits which are removed from the key buffer at the end of the slot. The total number of bits transmitted by user i in slot k is:

$$\hat{r}_k^{(i)} = \overline{R}_k^{(i)} + n_1 [C_i(P_i(H_k, G_k)) - C_i^e [P_i(H_k, G_k)]^+ . \quad (47)$$

These bits are stored in the key buffer at the end of the slot. Thus, $\hat{r}_k^{(i)} \geq \overline{R}_k^{(i)}$ and since $\Pr(H_{ik} > G_{ik}) > 0$, $i = 1, 2$, $\Pr(\hat{r}_k^{(i)} > \overline{R}_k^{(i)}) > 0$. Finally, $B_k^{(i)} \rightarrow \infty$ a.s. for $i = 1, 2$.

Also, as before, we can show that after some slot $k \geq N_2$, with an arbitrarily large probability, the messages transmitted in slots $k, k-1, \dots, k-N_1$ will use the messages transmitted before $k-N_1-1$, and the rate used in the first mini-slot will satisfy (40), but the rate used in the second mini-slot will satisfy (46). The overall rate of the slot can be made as close to (46) as we wish, by taking a large value of l . Thus, the rest of the proof demonstrating $P_e^n \rightarrow 0$ and that (32) is satisfied follows from Theorem 3.1.

All the above results extend in *strong* secrecy sense, as in Section 3, by using the *resolvability*-based coding scheme of [16] instead of the usual wiretap coding for MAC-WT of [6].

6. Conclusions

In this paper, we obtain the secrecy-rate region for a time-slotted MAC-WT. By using the previously transmitted message as a secret key in the next slot, we show that we can mitigate the rate loss and achieve the secrecy-rate region equal to the Ahleswede-Liao region of a multiple access channel (without wiretapper), if we consider the secrecy rate of the individual messages. We then extend the results to a scenario in which an arbitrarily large number of recently transmitted multiple messages is now secure with respect to the information of Eve, by using the secret key buffer for both transmitters. Finally, we further extend our coding scheme to a fading Gaussian channel and show that the usual Ahleswede-Liao region can be obtained while retaining the secrecy of the multiple messages.

Appendix

DM-MAC-WT with Secret Key Buffer

Lemma 7.1. The following inequality is satisfied

$$I(\overline{M}_{k,1}^{(1)}, \overline{M}_{k-1,1}^{(1)}, \dots, \overline{M}_{k-N_1,1}^{(1)}; \overline{Z}_1, \dots, \overline{Z}_k | \overline{X}_k^{(2)}) \leq n_1 \varepsilon. \quad (48)$$

Proof. We have:

$$\begin{aligned} & I(\overline{M}_{k,1}^{(1)}, \overline{M}_{k-1,1}^{(1)}, \dots, \overline{M}_{k-N_1,1}^{(1)}; \overline{Z}_1, \dots, \overline{Z}_k | \overline{X}_k^{(2)}) \\ &= I(\overline{M}_{k,1}^{(1)}; \overline{Z}_1, \dots, \overline{Z}_k | \overline{X}_k^{(2)}) \\ &+ I(\overline{M}_{k-1,1}^{(1)}; \overline{Z}_1, \dots, \overline{Z}_k | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}) \\ &+ \dots + I(\overline{M}_{k-N_1,1}^{(1)}; \overline{Z}_1, \dots, \overline{Z}_k | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{M}_{k-1,1}^{(1)}, \dots, \\ &\overline{M}_{k-N_1+1,1}^{(1)}) \triangleq I_1 + I_2 + \dots + I_{N_1}. \end{aligned} \quad (49)$$

Now let us evaluate each term. Denoting the two parts of \overline{Z}_k by $\overline{Z}_{k,1}, \overline{Z}_{k,2}$, and choosing the wiretap coding with leakage rate $\leq n_1 \varepsilon_1$, where $\varepsilon_1 = \varepsilon/N_1$:

$$\begin{aligned} I_1 &= I(\overline{M}_{k,1}^{(1)}; \overline{Z}_{1,1}, \overline{Z}_{1,2}, \dots, \overline{Z}_{k,1}, \overline{Z}_{k,2} | \overline{X}_k^{(2)}) \\ &= I(\overline{M}_{k,1}^{(1)}; \overline{Z}_{k,1} | \overline{X}_k^{(2)}) + I(\overline{M}_{k,1}^{(1)}; \overline{Z}_1, \dots, \overline{Z}_{k-1}, \overline{Z}_{k,2} | \overline{X}_k^{(2)}) \\ &\stackrel{(a)}{\leq} n_1 \varepsilon_1 + I(\overline{M}_{k,1}^{(1)}; \overline{Z}_1, \dots, \overline{Z}_{k-1}, \overline{Z}_{k,2} | \overline{X}_k^{(2)}) \\ &= n_1 \varepsilon_1 + H(\overline{M}_{k,1}^{(1)} | \overline{X}_k^{(2)}) - H(\overline{M}_{k,1}^{(1)} | \overline{X}_k^{(2)}, \overline{Z}_1, \dots, \overline{Z}_{k-1}, \overline{Z}_{k,2}) \\ &\stackrel{(b)}{=} n_1 \varepsilon_1 + H(\overline{M}_{k,1}^{(1)} | \overline{X}_k^{(2)}) - H(\overline{M}_{k,1}^{(1)} | \overline{X}_k^{(2)}) = n_1 \varepsilon_1, \end{aligned} \quad (50)$$

where (a) follows from wiretap coding and (b) follows, since $(\overline{Z}_1, \dots, \overline{Z}_{k-1}, \overline{Z}_{k,2}) \perp (\overline{W}_{k,1}^{(1)}, \overline{X}_k^{(2)})$.

Next consider I_2 . We have:

$$\begin{aligned} I_2 &= I(\overline{M}_{k-1,1}^{(1)}; \overline{Z}_1, \dots, \overline{Z}_{k-1,1}, \overline{Z}_{k-1,2}, \overline{Z}_k | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}) \\ &= I(\overline{M}_{k-1,1}^{(1)}; \overline{Z}_{k-1,1} | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}) + I(\overline{M}_{k-1,1}^{(1)}; \\ &(\overline{Z}_1, \dots, \overline{Z}_k) \setminus \overline{Z}_{k-1,1} | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_{k-1}) \\ &= H(\overline{M}_{k-1,1}^{(1)} | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}) - H(\overline{M}_{k-1,1}^{(1)} | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_{k-1,1}) \\ &+ I(\overline{M}_{k-1,1}^{(1)}; (\overline{Z}_1, \dots, \overline{Z}_k) \setminus \overline{Z}_{k-1,1} | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_{k-1}) \quad (51) \\ &\stackrel{(a)}{=} H(\overline{M}_{k-1,1}^{(1)}) - H(\overline{M}_{k-1,1}^{(1)} | \overline{Z}_{k-1,1}) \\ &+ I(\overline{M}_{k-1,1}^{(1)}; (\overline{Z}_1, \dots, \overline{Z}_k) \setminus \overline{Z}_{k-1,1} | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_{k-1}) \\ &= I(\overline{M}_{k-1,1}^{(1)}; \overline{Z}_{k-1,1}) I(\overline{M}_{k-1,1}^{(1)}; (\overline{Z}_1, \dots, \overline{Z}_k) \setminus \overline{Z}_{k-1,1} | \overline{X}_k^{(2)}, \\ &\overline{M}_{k,1}^{(1)}, \overline{Z}_{k-1}) \\ &\stackrel{(b)}{\leq} n_1 \varepsilon_1 + I(\overline{M}_{k-1,1}^{(1)}; (\overline{Z}_1, \dots, \overline{Z}_k) \setminus \overline{Z}_{k-1,1} | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_{k-1}) \\ &= n_1 \varepsilon_1 + I(\overline{M}_{k-1,1}^{(1)}; \overline{Z}_1, \dots, \overline{Z}_{k-1,2}, \overline{Z}_k | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_{k-1}) \\ &= n_1 \varepsilon_1 + I(\overline{M}_{k-1,1}^{(1)}; \overline{Z}_1, \dots, \overline{Z}_{k-2}, \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_{k-1}) \\ &+ I(\overline{M}_{k-1,1}^{(1)}; \overline{Z}_k, \overline{Z}_{k-1,2} | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_{k-1}, \overline{Z}_1, \dots, \overline{Z}_{k-2}) \end{aligned}$$

$$\begin{aligned} &\stackrel{(c)}{=} n_1 \varepsilon_1 + 0 + I(\overline{M}_{k-1,1}^{(1)}; \overline{Z}_k, \overline{Z}_{k-1,2} | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_{k-1}, \overline{Z}_1, \dots, \\ &\overline{Z}_{k-2}) \\ &= n_1 \varepsilon_1 + I(\overline{M}_{k-1,1}^{(1)}; \overline{Z}_{k,1} | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_{k-1}, \overline{Z}_1, \dots, \overline{Z}_{k-2}) \\ &+ I(\overline{M}_{k-1,1}^{(1)}; \overline{Z}_{k,2}, \overline{Z}_{k-1,2} | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_{k-1}, \overline{Z}_1, \dots, \overline{Z}_{k-2}, \\ &\overline{Z}_{k,1}) \\ &= n_1 \varepsilon_1 + H(\overline{M}_{k-1,1}^{(1)}; | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_{k-1}, \overline{Z}_1, \dots, \overline{Z}_{k-2}) \\ &- H(\overline{M}_{k-1,1}^{(1)}; | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_{k-1}, \overline{Z}_1, \dots, \overline{Z}_{k-2}, \overline{Z}_{k,1}) \\ &+ I(\overline{M}_{k-1,1}^{(1)}; \overline{Z}_{k,2}, \overline{Z}_{k-1,2} | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_{k-1}, \overline{Z}_1, \dots, \overline{Z}_{k-2}, \\ &\overline{Z}_{k,1}) \\ &\stackrel{(d)}{=} n_1 \varepsilon_1 + H(\overline{M}_{k-1,1}^{(1)}; | \overline{Z}_{k-1,1}) - H(\overline{M}_{k-1,1}^{(1)}; | \overline{Z}_{k-1,1}) \\ &+ I(\overline{M}_{k-1,1}^{(1)}; \overline{Z}_{k,2}, \overline{Z}_{k-1,2} | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_{k-1}, \overline{Z}_1, \dots, \\ &\overline{Z}_{k-2}, \overline{Z}_{k,1}), \end{aligned} \quad (52)$$

where (a) follows since $\overline{M}_{k-1,1}^{(1)} \perp (\overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)})$ and $(\overline{M}_{k-1,1}^{(1)}, \overline{Z}_{k-1}) \perp (\overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)})$, (b) follows from wiretap coding, (c) follows since $(\overline{M}_{k-1,1}^{(1)}, \overline{Z}_{k-1}) \perp (\overline{Z}_1, \dots, \overline{Z}_{k-2}, \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)})$, $(\overline{Z}_1, \dots, \overline{Z}_{k-2}) \perp (\overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)})$ and $(\overline{Z}_1, \dots, \overline{Z}_{k-1}) \perp (\overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)})$ and (d) follows since $(\overline{M}_{k-1,1}^{(1)}, \overline{Z}_{k-1,1}) \perp (\overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_1, \dots, \overline{Z}_{k-2})$.

But:

$$\begin{aligned} & I(\overline{M}_{k-1,1}^{(1)}; \overline{Z}_{k,2}, \overline{Z}_{k-1,2} | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_{k-1,1}, \\ &\overline{Z}_1, \dots, \overline{Z}_{k-2}, \overline{Z}_{k,1}) \\ &= H(\overline{M}_{k-1,1}^{(1)} | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_{k-1,1}, \overline{Z}_1, \dots, \overline{Z}_{k-2}, \overline{Z}_{k,1}) \\ &- H(\overline{M}_{k-1,1}^{(1)} | \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_{k-1,1}, \overline{Z}_1, \dots, \overline{Z}_{k-2}, \overline{Z}_{k,1}, \\ &\overline{Z}_{k,2}, \overline{Z}_{k-1,2}) \\ &\stackrel{(a)}{=} H(\overline{M}_{k-1,1}^{(1)} | \overline{Z}_{k-1,1}) - H(\overline{M}_{k-1,1}^{(1)} | \overline{Z}_{k-1,1}) \\ &= 0, \end{aligned} \quad (53)$$

where (a) follows, since $(\overline{M}_{k-1,1}^{(1)}, \overline{Z}_{k-1,1}) \perp (\overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_1, \dots, \overline{Z}_{k-2}, \overline{Z}_{k,1})$ and $(\overline{M}_{k-1,1}^{(1)}, \overline{Z}_{k-1,1}) \perp (\overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \overline{Z}_1, \dots, \overline{Z}_{k-2}, \overline{Z}_{k,1}, \overline{Z}_{k,2}, \overline{Z}_{k-1,2})$.

Hence we have:

$$I_2 \leq n_1 \varepsilon_1. \quad (54)$$

One can similarly prove that $I_i \leq n_1 \varepsilon_1$ for $i = 3, 4, \dots, N_1$. Therefore:

$$\begin{aligned} & I(\overline{M}_{k,1}^{(1)}, \overline{M}_{k-1,1}^{(1)}, \dots, \overline{M}_{k-N_1,1}^{(1)}; \overline{Z}_1, \dots, \overline{Z}_k | \overline{X}_k^{(2)}) \\ &\leq N_1 n_1 \varepsilon_1 = n_1 \varepsilon. \end{aligned} \quad (55)$$

□

Lemma 7.2. The following inequality is satisfied

$$\begin{aligned} & I(\overline{M}_{k,2}^{(1)}, \overline{M}_{k-1,2}^{(1)}, \dots, \overline{M}_{k-N_1,2}^{(1)}; \overline{Z}_1, \dots, \overline{Z}_k \\ &| \overline{X}_k^{(2)}, \overline{M}_{k,1}^{(1)}, \dots, \overline{M}_{k-N_1,1}^{(1)}) \leq 6n_1 \varepsilon. \end{aligned} \quad (56)$$

Proof.

$$\begin{aligned}
 & I(\overline{M}_{k,2}^{(1)}, \overline{M}_{k-1,2}^{(1)}, \dots, \overline{M}_{k-N_1,2}^{(1)}; \overline{Z}_1, \dots, \overline{Z}_k | \overline{X}_k^{(2)}, \\
 & \quad \overline{M}_{k,1}^{(1)}, \overline{M}_{k-1,1}^{(1)}, \dots, \overline{M}_{k-N_1,1}^{(1)}) \\
 &= I(\overline{M}_{k,2}^{(1)}, \overline{M}_{k-1,2}^{(1)}, \dots, \overline{M}_{k-N_1,2}^{(1)}; \overline{Z}_1, \dots, \overline{Z}_{k-N_1-1} | \overline{X}_k^{(2)}, \\
 & \quad \overline{M}_{k,1}^{(1)}, \overline{M}_{k-1,1}^{(1)}, \dots, \overline{M}_{k-N_1,1}^{(1)}) \\
 &+ I(\overline{M}_{k,2}^{(1)}, \overline{M}_{k-1,2}^{(1)}, \dots, \overline{M}_{k-N_1,2}^{(1)}; \overline{Z}_{k-N_1}, \dots, \overline{Z}_k | \overline{X}_k^{(2)}, \\
 & \quad \overline{M}_{k,1}^{(1)}, \overline{M}_{k-1,1}^{(1)}, \dots, \overline{M}_{k-N_1,1}^{(1)}, \overline{Z}_1, \dots, \overline{Z}_{k-N_1-1}) \\
 &\stackrel{(a)}{=} 0 + I(\overline{M}_{k,2}^{(1)}, \overline{M}_{k-1,2}^{(1)}, \dots, \overline{M}_{k-N_1,2}^{(1)}; \overline{Z}_{k-N_1}, \dots, \overline{Z}_k | \overline{X}_k^{(2)}, \\
 & \quad \overline{M}_{k,1}^{(1)}, \overline{M}_{k-1,1}^{(1)}, \dots, \overline{M}_{k-N_1,1}^{(1)}, \overline{Z}_1, \dots, \overline{Z}_{k-N_1-1}) \\
 &= I(\overline{M}_{k,2}^{(1)}, \overline{M}_{k-1,2}^{(1)}, \dots, \overline{M}_{k-N_1,2}^{(1)}; \overline{Z}_{k-N_1,1}, \dots, \overline{Z}_{k,1} | \overline{X}_k^{(2)}, \\
 & \quad \overline{M}_{k,1}^{(1)}, \overline{M}_{k-1,1}^{(1)}, \dots, \overline{M}_{k-N_1,1}^{(1)}, \overline{Z}_1, \dots, \overline{Z}_{k-N_1-1}) \\
 &+ I(\overline{M}_{k,2}^{(1)}, \overline{M}_{k-1,2}^{(1)}, \dots, \overline{M}_{k-N_1,1}^{(1)}; \overline{Z}_{k-N_1,2}, \dots, \overline{Z}_{k,2} | \overline{X}_k^{(2)}, \\
 & \quad \overline{M}_{k,1}^{(1)}, \overline{M}_{k-1,1}^{(1)}, \dots, \overline{M}_{k-N_1,1}^{(1)}, \overline{Z}_1, \dots, \overline{Z}_{k-N_1-1}, \\
 & \quad \overline{Z}_{k,1}, \overline{Z}_{k-1,1}, \dots, \overline{Z}_{k-N_1,1}) \\
 &\stackrel{(b)}{=} 0 + I(\overline{M}_{k,2}^{(1)}, \dots, \overline{M}_{k-N_1,2}^{(1)}; \overline{Z}_{k-N_1,2}, \dots, \overline{Z}_{k,2} | \overline{M}_{k,1}^{(1)}, \dots, \\
 & \quad \overline{M}_{k-N_1,1}^{(1)}, \overline{Z}_1, \dots, \overline{Z}_{k-N_1}, \overline{Z}_{k-N_1,1}, \dots, \overline{Z}_{k-1}, \overline{X}_k^{(2)}) \\
 &\stackrel{(c)}{=} I(\overline{M}_{k,2}^{(1)}, \dots, \overline{M}_{k-N_1,2}^{(1)}; \overline{Z}_{k-N_1,2}, \dots, \overline{Z}_{k,2} | \overline{Z}_1, \dots, \\
 & \quad \overline{Z}_{k-N_1}, \overline{X}_k^{(2)}) \\
 &\stackrel{\triangleq}{=} I(\hat{M}_2^{(1)}; \hat{Z}_2 | \hat{Z}_1, \overline{X}_k^{(2)}),
 \end{aligned}$$

where (a) follows, since $(\overline{M}_{k,2}^{(1)}, \dots, \overline{M}_{k-N_1,2}^{(1)}) \perp (\overline{Z}_1, \dots, \overline{Z}_{k-N_1-1}, \overline{M}_{k,1}^{(1)}, \dots, \overline{M}_{k-N_1,1}^{(1)}, \overline{X}_k^{(2)})$, (b) follows, since $(\overline{M}_{k,2}^{(1)}, \overline{M}_{k-1,2}^{(1)}, \dots, \overline{M}_{k-N_1,2}^{(1)})$ is independent of the other random variables (RVs) in the first expression, (c) follows, since $(\overline{M}_{k,1}^{(1)}, \dots, \overline{M}_{k-N_1,1}^{(1)}, \overline{Z}_{k-N_1,1}, \dots, \overline{Z}_{k-1,1})$ is independent of all other RVs in the expression, and in the last inequality we denote the respective random sequences with their respective widehat symbols.

Now we observe that:

$$\begin{aligned}
 & I(\hat{M}_2^{(1)}; \hat{Z}_1, \hat{Z}_2 | \overline{X}_k^{(2)}) \\
 &= I(\hat{M}_2^{(1)}; \hat{Z}_1 | \overline{X}_k^{(2)}) + I(\hat{M}_2^{(1)}; \hat{Z}_2 | \hat{Z}_1, \overline{X}_k^{(2)}) \\
 &\stackrel{(a)}{=} 0 + I(\hat{M}_2^{(1)}; \hat{Z}_2 | \hat{Z}_1, \overline{X}_k^{(2)}) \\
 &\leq I(\hat{M}_2^{(1)}; \hat{Z}_1, \hat{Z}_2 | \overline{X}_k^{(2)}) \\
 &= I(\hat{M}_2^{(1)}; \hat{Z}_2 | \overline{X}_k^{(2)}) + I(\hat{M}_2^{(1)}; \hat{Z}_1 | \hat{Z}_2, \overline{X}_k^{(2)}) \\
 &\stackrel{(b)}{=} 0 + I(\hat{M}_2^{(1)}; \hat{Z}_1 | \hat{Z}_2, \overline{X}_k^{(2)}), \tag{57}
 \end{aligned}$$

where (a) follows, since $\hat{M}_2^{(1)} \perp (\hat{Z}_1, \overline{X}_k^{(2)})$, and (b) follows, since $\hat{M}_2^{(1)} \perp (\hat{Z}_2, \overline{X}_k^{(2)})$.

We will also use the following notation: $\hat{M}_1^{(1)} \triangleq (\overline{M}_{k,1}^{(1)}, \dots, \overline{M}_{k-N_1,1}^{(1)})$, A_i are the indices of messages transmitted in slots $1, \dots, k-N_1-1$ that are used as secret keys by user i for transmitting messages in slots $k-N_1, \dots, k$, $\overline{M}_{A_i}^{(i)} = (\overline{M}_k^{(i)}, k \in A_i)$, $\overline{M}_{A_i^c}^{(i)} = (\overline{M}_k^{(i)}, k \in \{1, \dots, k-N_1-1\})$, similarly we define $\overline{Z}_{A_i}, \overline{Z}_{A_i^c}$. Then we have:

$$\begin{aligned}
 & I(\hat{M}_2^{(1)}; \hat{Z}_1 | \hat{Z}_2, \overline{X}_k^{(2)}) \\
 &\leq I(\hat{M}_2^{(1)}, \overline{M}_{A_1}^{(1)}, \overline{M}_{A_2}^{(2)}; \hat{Z}_1, | \hat{Z}_2, \overline{X}_k^{(2)}) \\
 &= I(\overline{M}_{A_1}^{(1)}, \overline{M}_{A_2}^{(2)}; \hat{Z}_1, | \overline{X}_k^{(2)}, \hat{Z}_2) \\
 &+ I(\hat{M}_2^{(1)}; \hat{Z}_1 | \overline{X}_k^{(2)}, \hat{Z}_2, \overline{M}_{A_1}^{(1)}, \overline{M}_{A_2}^{(2)}) \\
 &\stackrel{(a)}{\leq} I(\overline{M}_{A_1}^{(1)}, \overline{M}_{A_2}^{(2)}; \hat{Z}_1) + I(\hat{M}_2^{(1)}; \hat{Z}_1 | \overline{X}_k^{(2)}, \hat{Z}_2, \overline{M}_{A_1}^{(1)}, \overline{M}_{A_2}^{(2)}) \\
 &\stackrel{(b)}{=} I(\overline{M}_{A_1}^{(1)}, \overline{M}_{A_2}^{(2)}; \hat{Z}_1) + 0 \\
 &= I(\overline{M}_{A_{1,1}}^{(1)}, \overline{M}_{A_{1,2}}^{(1)}, \overline{M}_{A_{2,1}}^{(2)}, \overline{M}_{A_{2,2}}^{(2)}; \hat{Z}_1) \\
 &= I(\overline{M}_{A_{1,1}}^{(1)}, \overline{M}_{A_{2,1}}^{(2)}; \hat{Z}_1) \\
 &+ I(\overline{M}_{A_{1,2}}^{(1)}, \overline{M}_{A_{2,2}}^{(2)}; \hat{Z}_1 | \overline{M}_{A_{1,1}}^{(1)}, \overline{M}_{A_{2,1}}^{(2)}) \\
 &\stackrel{(c)}{=} I(\overline{M}_{A_{1,1}}^{(1)}, \overline{M}_{A_{2,1}}^{(2)}; \hat{Z}_1) + 0 \\
 &= I(\overline{M}_{A_{1,1}}^{(1)}; \hat{Z}_1) + I(\overline{M}_{A_{2,1}}^{(2)}; \hat{Z}_1 | \overline{M}_{A_{1,1}}^{(1)}) \\
 &\leq I(\overline{M}_{A_{1,1}}^{(1)}, \overline{M}_{A_{1,1}}^{(2)}; \hat{Z}_1) + I(\overline{M}_{A_{2,1}}^{(2)}; \hat{Z}_1 | \overline{M}_{A_{1,1}}^{(1)}) \\
 &\stackrel{(d)}{\leq} 2n_1 \varepsilon + I(\overline{M}_{A_{2,1}}^{(2)}; \hat{Z}_1 | \overline{M}_{A_{1,1}}^{(1)}) \\
 &\stackrel{(e)}{=} 2n_1 \varepsilon + I(\overline{M}_{A_{2,1}}^{(2)}; \overline{Z}_{A_2}, \overline{Z}_{A_2^c} | \overline{M}_{A_{1,1}}^{(1)}) \\
 &= 2n_1 \varepsilon + I(\overline{M}_{A_{2,1}}^{(2)}; \overline{Z}_{A_2} | \overline{M}_{A_{1,1}}^{(1)}) \\
 &+ I(\overline{M}_{A_{2,1}}^{(2)}; \overline{Z}_{A_2^c} | \overline{M}_{A_{1,1}}^{(1)}, \overline{Z}_{A_2}) \\
 &\stackrel{\triangleq}{=} 2n_1 \varepsilon + I_1 + I_2, \tag{58}
 \end{aligned}$$

where:

- (a) follows, because $\hat{Z}_1 \leftrightarrow (\overline{M}_{A_1}^{(1)}, \overline{M}_{A_2}^{(2)}) \leftrightarrow (\hat{Z}_2, \overline{X}_k^{(2)})$,
- (b) follows, since $\hat{M}_2^{(1)} \leftrightarrow (\overline{M}_{A_1}^{(1)}, \overline{M}_{A_2}^{(2)}, \hat{Z}_2, \overline{X}_k^{(2)}) \leftrightarrow \hat{Z}_1$,
- (c) follows, since $(\overline{M}_{A_{1,2}}^{(1)}, \overline{M}_{A_{2,2}}^{(2)}) \perp (\hat{Z}_1, \overline{M}_{A_{1,1}}^{(1)}, \overline{M}_{A_{2,1}}^{(2)})$,
- (d), (j) and (m) follows by wiretap coding,
- (e) follows, since $\hat{Z}_1 = (\overline{Z}_1, \dots, \overline{Z}_{k-N_1}) = (\overline{Z}_{A_2}, \overline{Z}_{A_2^c})$.

Now, we evaluate I_2 :

$$\begin{aligned}
 I_2 &= I(\overline{M}_{A_2,1}^{(2)}; \overline{Z}_{A_2} \overline{M}_{A_1,1}^{(1)}, \overline{Z}_{A_2}) \\
 &= H(\overline{M}_{A_2,1}^{(2)} | \overline{M}_{A_1,1}^{(1)}, \overline{Z}_{A_2}) \\
 &\quad - H(\overline{M}_{A_2,1}^{(2)} | \overline{M}_{A_1,1}^{(1)}, \overline{Z}_{A_2}, \overline{Z}_{A_2}^c) \\
 &\stackrel{(a)}{=} H(\overline{M}_{A_2,1}^{(2)} | \overline{M}_{A_1,1}^{(1)}, \overline{Z}_{A_2,1}, \overline{Z}_{A_2,2}) \\
 &\quad - H(\overline{M}_{A_2,1}^{(2)} | \overline{M}_{A_1 \cap A_2,1}^{(1)}, \overline{Z}_{A_2,1}) \\
 &\stackrel{(b)}{=} H(\overline{M}_{A_2,1}^{(2)} | \overline{M}_{A_1 \cap A_2,1}^{(1)}, \overline{Z}_{A_2,1}) \\
 &\quad - H(\overline{M}_{A_2,1}^{(2)} | \overline{M}_{A_1 \cap A_2,1}^{(1)}, \overline{Z}_{A_2,1}) = 0, \quad (59)
 \end{aligned}$$

where (a) and (b) follow because $\overline{M}_{A_1,1}^{(1)}$ and $\overline{M}_{A_1,1}^{(1)}$ are used as keys only in slots $k - N_1, \dots, k$.

Next, we evaluate I_1 :

$$\begin{aligned}
 I_1 &= I(\overline{M}_{A_2,1}^{(2)}; \overline{Z}_{A_2} \overline{M}_{A_1,1}^{(1)}) \\
 &= I(\overline{M}_{A_2 \cap A_1,1}^{(2)}, \overline{M}_{A_2 \cap A_1^c,1}^{(2)}; \overline{Z}_{A_2} | \overline{M}_{A_1,1}^{(1)}) \\
 &= I(\overline{M}_{A_2 \cap A_1^c,1}^{(2)}; \overline{Z}_{A_2} | \overline{M}_{A_1,1}^{(1)}) \\
 &\quad + I(\overline{M}_{A_2 \cap A_1,1}^{(2)}; \overline{Z}_{A_2} | \overline{M}_{A_1,1}^{(1)}, \overline{M}_{A_2 \cap A_1^c,1}^{(2)}) \\
 &\stackrel{\triangle}{=} I_3 + I_4. \quad (60)
 \end{aligned}$$

Now:

$$\begin{aligned}
 I_3 &= I(\overline{M}_{A_2 \cap A_1^c,1}^{(2)}; \overline{Z}_{A_2} | \overline{M}_{A_1,1}^{(1)}) \\
 &= I(\overline{M}_{A_2 \cap A_1^c,1}^{(2)}; \overline{Z}_{A_2 \cap A_1}, \overline{Z}_{A_2 \cap A_1^c} | \overline{M}_{A_1,1}^{(1)}) \\
 &= I(\overline{M}_{A_2 \cap A_1^c,1}^{(2)}; \overline{Z}_{A_2 \cap A_1^c} | \overline{M}_{A_1,1}^{(1)}) \\
 &\quad + I(\overline{M}_{A_2 \cap A_1^c,1}^{(2)}; \overline{Z}_{A_2 \cap A_1} | \overline{M}_{A_1,1}^{(1)}, \overline{Z}_{A_2 \cap A_1^c}) \\
 &\stackrel{\triangle}{=} I_{31} + I_{32}. \quad (61)
 \end{aligned}$$

Consider:

$$\begin{aligned}
 I_{31} &= I(\overline{M}_{A_2 \cap A_1^c,1}^{(2)}; \overline{Z}_{A_2 \cap A_1^c} | \overline{M}_{A_1,1}^{(1)}) \\
 &= I(\overline{M}_{A_2 \cap A_1^c,1}^{(2)}; \overline{Z}_{A_2 \cap A_1^c,1}, \overline{Z}_{A_2 \cap A_1^c,2} | \overline{M}_{A_1,1}^{(1)}) \\
 &= I(\overline{M}_{A_2 \cap A_1^c,1}^{(2)}; \overline{Z}_{A_2 \cap A_1^c,1} | \overline{M}_{A_1,1}^{(1)}) \\
 &\quad + I(\overline{M}_{A_2 \cap A_1^c,1}^{(2)}; \overline{Z}_{A_2 \cap A_1^c,2} | \overline{M}_{A_1,1}^{(1)}, \overline{Z}_{A_2 \cap A_1^c,1}) \\
 &\stackrel{(a)}{\leq} I(\overline{M}_{A_2 \cap A_1^c,1}^{(1)}; \overline{M}_{A_2 \cap A_1^c,1}^{(2)}; \overline{Z}_{A_2 \cap A_1^c,1}) + 0 \\
 &\stackrel{(b)}{\leq} 2n_1 \varepsilon, \quad (62)
 \end{aligned}$$

where (a) follows, since $\overline{Z}_{A_2 \cap A_1^c,2} \perp (\overline{M}_{A_2 \cap A_1^c,1}^{(2)}, \overline{M}_{A_1,1}^{(1)}, \overline{Z}_{A_2 \cap A_1^c,1})$, (b) follows from wiretap coding and that $\overline{M}_{A_1,1}^{(1)} \perp$

$(\overline{M}_{A_2 \cap A_1^c,1}^{(2)}, \overline{Z}_{A_2 \cap A_1^c,1})$. Next consider the second term of (61). We get:

$$\begin{aligned}
 I_{32} &= I(\overline{M}_{A_2 \cap A_1^c,1}^{(2)}; \overline{Z}_{A_2 \cap A_1} | \overline{M}_{A_1,1}^{(1)}, \overline{Z}_{A_2 \cap A_1^c}) \\
 &= I(\overline{M}_{A_2 \cap A_1^c,1}^{(2)}; \overline{Z}_{A_2 \cap A_1,1}, \overline{Z}_{A_2 \cap A_1,2} | \overline{M}_{A_1,1}^{(1)}, \overline{Z}_{A_2 \cap A_1^c}) \\
 &= I(\overline{M}_{A_2 \cap A_1^c,1}^{(2)}; \overline{Z}_{A_2 \cap A_1,1} | \overline{M}_{A_1,1}^{(1)}, \overline{Z}_{A_2 \cap A_1^c}) \\
 &\quad + I(\overline{M}_{A_2 \cap A_1^c,1}^{(2)}; \overline{Z}_{A_2 \cap A_1,2} | \overline{M}_{A_1,1}^{(1)}, \overline{Z}_{A_2 \cap A_1^c}, \overline{Z}_{A_2 \cap A_1,1}) \\
 &\stackrel{(a)}{=} I(\overline{M}_{A_2 \cap A_1^c,1}^{(2)}; \overline{Z}_{A_2 \cap A_1,1} | \overline{M}_{A_1,1}^{(1)}, \overline{Z}_{A_2 \cap A_1^c}) + 0 \\
 &= H(\overline{M}_{A_2 \cap A_1^c,1}^{(2)} | \overline{M}_{A_1,1}^{(1)}, \overline{Z}_{A_2 \cap A_1^c}) \\
 &\quad - H(\overline{M}_{A_2 \cap A_1^c,1}^{(2)} | \overline{M}_{A_1,1}^{(1)}, \overline{Z}_{A_2 \cap A_1^c}, \overline{Z}_{A_2 \cap A_1,1}) \\
 &\stackrel{(b)}{=} H(\overline{M}_{A_2 \cap A_1^c,1}^{(2)} | \overline{Z}_{A_2 \cap A_1^c}) - H(\overline{M}_{A_2 \cap A_1^c,1}^{(2)} | \overline{Z}_{A_2 \cap A_1^c}) \\
 &= 0, \quad (63)
 \end{aligned}$$

where (a) follows, since $\overline{Z}_{A_2 \cap A_1,2} \perp (\overline{M}_{A_2 \cap A_1^c,1}^{(2)}, \overline{M}_{A_1,1}^{(1)}, \overline{Z}_{A_2 \cap A_1^c}, \overline{Z}_{A_2 \cap A_1,1})$, (b) follows, since $\overline{M}_{A_1,1}^{(1)} \perp (\overline{M}_{A_2 \cap A_1^c,1}^{(2)}, \overline{Z}_{A_2 \cap A_1^c})$ and $(\overline{M}_{A_1,1}^{(1)}, \overline{Z}_{A_2 \cap A_1,1}) \perp (\overline{M}_{A_2 \cap A_1^c,1}^{(2)}, \overline{Z}_{A_2 \cap A_1^c})$.

Finally, we consider:

$$\begin{aligned}
 I_4 &= I(\overline{M}_{A_2 \cap A_1,1}^{(2)}; \overline{Z}_{A_2} | \overline{M}_{A_1,1}^{(1)}, \overline{M}_{A_2 \cap A_1^c,1}^{(2)}) \\
 &= I(\overline{M}_{A_2 \cap A_1,1}^{(2)}; \overline{Z}_{A_2,1}, \overline{Z}_{A_2,2} | \overline{M}_{A_1,1}^{(1)}, \overline{M}_{A_2 \cap A_1^c,1}^{(2)}) \\
 &= I(\overline{M}_{A_2 \cap A_1,1}^{(2)}; \overline{Z}_{A_2,1} | \overline{M}_{A_1,1}^{(1)}, \overline{M}_{A_2 \cap A_1^c,1}^{(2)}) \\
 &\quad + I(\overline{M}_{A_2 \cap A_1,1}^{(2)}; \overline{Z}_{A_2,2} | \overline{M}_{A_1,1}^{(1)}, \overline{M}_{A_2 \cap A_1^c,1}^{(2)}, \overline{Z}_{A_2,1}) \\
 &\stackrel{(a)}{=} I(\overline{M}_{A_2 \cap A_1,1}^{(2)}; \overline{Z}_{A_2,1} | \overline{M}_{A_1,1}^{(1)}, \overline{M}_{A_2 \cap A_1^c,1}^{(2)}) + 0 \\
 &= I(\overline{M}_{A_2 \cap A_1,1}^{(2)}; \overline{Z}_{A_2 \cap A_1,1}, \overline{Z}_{A_2 \cap A_1^c,1} | \overline{M}_{A_1,1}^{(1)}, \overline{M}_{A_2 \cap A_1^c,1}^{(2)}) \\
 &= I(\overline{M}_{A_2 \cap A_1,1}^{(2)}; \overline{Z}_{A_2 \cap A_1,1} | \overline{M}_{A_1,1}^{(1)}, \overline{M}_{A_2 \cap A_1^c,1}^{(2)}) \\
 &\quad + I(\overline{M}_{A_2 \cap A_1,1}^{(2)}; \overline{Z}_{A_2 \cap A_1^c,1} | \overline{M}_{A_1,1}^{(1)}, \overline{M}_{A_2 \cap A_1^c,1}^{(2)}, \overline{Z}_{A_2 \cap A_1,1}) \\
 &\leq I(\overline{M}_{A_2 \cap A_1,1}^{(2)}, \overline{M}_{A_2 \cap A_1,1}^{(2)}; \overline{Z}_{A_2 \cap A_1,1} | \overline{M}_{A_1,1}^{(1)}) \\
 &\quad + H(\overline{Z}_{A_2 \cap A_1^c,1} | \overline{M}_{A_1,1}^{(1)}, \overline{M}_{A_2 \cap A_1^c,1}^{(2)}, \overline{Z}_{A_2 \cap A_1,1}) \\
 &\quad - H(\overline{Z}_{A_2 \cap A_1^c,1} | \overline{M}_{A_1,1}^{(1)}, \overline{M}_{A_2 \cap A_1^c,1}^{(2)}, \overline{Z}_{A_2 \cap A_1,1}, \overline{M}_{A_2 \cap A_1,1}^{(2)}) \\
 &\stackrel{(b)}{\leq} 2n_1 \varepsilon + H(\overline{Z}_{A_2 \cap A_1^c,1} | \overline{M}_{A_2 \cap A_1^c,1}^{(2)}) \\
 &\quad - H(\overline{Z}_{A_2 \cap A_1^c,1} | \overline{M}_{A_2 \cap A_1^c,1}^{(2)}) \\
 &= 2n_1 \varepsilon, \quad (64)
 \end{aligned}$$

where (a) follows, since $\overline{Z}_{A_2,2}$ is independent of the rest of the terms in the expression, (b) follows, because $(\overline{Z}_{A_2 \cap A_1^c,1}, \overline{M}_{A_2 \cap A_1^c,1}^{(2)}) \perp (\overline{M}_{A_1,1}^{(1)}, \overline{Z}_{A_2 \cap A_1,1})$ and $(\overline{Z}_{A_2 \cap A_1^c,1}, \overline{M}_{A_2 \cap A_1^c,1}^{(2)}) \perp (\overline{M}_{A_1,1}^{(1)}, \overline{Z}_{A_2 \cap A_1,1}, \overline{M}_{A_2 \cap A_1,1}^{(2)})$.

Hence, we have from (60) that $I \leq 6n_1 \varepsilon$. Thus, we get:

$$I(\hat{M}_2^{(1)}; \hat{Z}_2 | \hat{Z}_1, \overline{X}_k^{(2)}) \leq 6n_1 \varepsilon, \quad (65)$$

and the lemma is established. \square


References

- [1] A. D. Wyner, "The wire-tap channel", *Bell Syst. Techn. J.*, vol. 54, no. 8, pp. 1355–1387, 1975 (DOI: 10.1002/j.1538-7305.1975.tb02040.x).
- [2] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels", *IEEE Trans. on Inform. Theory*, vol. 54, no. 10, pp. 4687–4698, 2008 (DOI: 10.1109/TIT.2008.928990).
- [3] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security", *IEEE Trans. on Inform. Theory*, vol. 54, no. 6, pp. 2515–2534, 2008 (DOI: 10.1109/TIT.2008.921908).
- [4] O. Gungor, J. Tan, C. E. Koksall, H. El-Gamal, and N. B. Shroff, "Secrecy outage capacity of fading channels", *IEEE Trans. on Inform. Theory*, vol. 59, no. 9, pp. 5379–5397, 2013 (DOI: 10.1109/TIT.2013.2265691).
- [5] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages", *IEEE Trans. on Inform. Theory*, vol. 54, no. 3, pp. 976–1002, 2008 (DOI: 10.1109/TIT.2007.915978).
- [6] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel", *IEEE Trans. on Inform. Theory*, vol. 54, no. 12, pp. 5747–5755, 2008 (DOI: 10.1109/TIT.2008.2006422).
- [7] S. M. Shah, V. Kumar, and V. Sharma, "Achievable secrecy sum-rate in a fading MAC-WT with power control and without CSI of eavesdropper", in *Proc. of Int. Conf. on Sig. Process. and Commun. SPCOM 2012*, Bangalore, India, 2012 (DOI: 10.1109/SPCOM.2012.6290033).
- [8] Y. Liang *et al.*, "Information theoretic security", *Foundations and Trends in Commun. and Inform. Theory*, vol. 5, no. 4–5, pp. 355–580, 2009 (DOI: 10.1561/0100000036).
- [9] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011 (ISBN: 9780511977985).
- [10] R. Liu and W. Trappe (Eds.), *Securing Wireless Communications at the Physical Layer*. Boston, MA: Springer, 2010 (ISBN: 9781441913852).
- [11] U. M. Maurer, "Secret key agreement by public discussion from common information", *IEEE Trans. on Inform. Theory*, vol. 39, no. 3, pp. 733–742, 1993 (DOI: 10.1109/18.256484).
- [12] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel", *IEEE Trans. on Inform. Theory*, vol. 51, no. 1, pp. 44–55, 2005 (DOI: 10.1109/TIT.2004.839515).
- [13] I. Csiszar and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press, 2011 (ISBN: 9780511921889).
- [14] M. Bloch and N. Laneman, "Strong secrecy from channel resolvability", *IEEE Trans. on Inform. Theory*, vol. 51, no. 1, pp. 44–55, 2011 (DOI: 10.1109/TIT.2013.2283722).
- [15] M. Wiese and H. Boche, "Strong secrecy for multiple access channels", in *Information Theory, Combinatorics, and Search Theory*, H. Aydinian, F. Cicalese, and C. Deppe, Eds. LNCS, vol. 7777, pp. 71–122. Berlin, Heidelberg: Springer, 2013 (DOI: 10.1007/978-3-642-36899-8_4).
- [16] M. H. Yassaee and M. R. Aref, "Multiple access wiretap channels with strong secrecy", in *Proc. Inform. Theory Worksh. ITW 2010*. Dublin, Ireland, 2010 (DOI: 10.1109/CIG.2010.5592953).
- [17] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel", *IEEE Trans. on Inform. Theory*, vol. 24, no. 4, pp. 451–456, 1978 (DOI: 10.1109/TIT.1978.1055917).
- [18] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap channel with secure rate-limited feedback", *IEEE Trans. on Inform. Theory*, vol. 55, no. 12, pp. 5353–5361, 2009 (DOI: 10.1109/TIT.2009.2032814).
- [19] L. Lai, H. El Gamal, and H. V. Poor, "The wiretap channel with feedback: Encryption over the channel", *IEEE Trans. on Inform. Theory*, vol. 54, no. 11, pp. 5059–5067, 2008 (DOI: 10.1109/TIT.2008.929914).
- [20] W. Kang and N. Liu, "Wiretap channel with shared key", in *Proc. 2010 IEEE Inform. Theory Worksh.*, Dublin, Ireland, 2010 (DOI: 10.1109/CIG.2010.5592665).
- [21] D. Kobayashi, H. Yamamoto, and T. Ogawa, "Secure multiplex coding attaining channel capacity in wiretap channels", *IEEE Trans. on Inform. Theory*, vol. 59, no. 12, pp. 8131–8143 (DOI: 10.1109/TIT.2013.2282673).
- [22] S. M. Shah, S. Parameswaran, and V. Sharma, "Previous messages provide the key to achieve Shannon capacity in a wiretap channel", in *Proc. IEEE Int. Conf. on Commun. Workshops ICC 2013*, Budapest, Hungary, 2013, pp. 697–701 (DOI: 10.1109/ICCW.2013.6649323).
- [23] S. M. Shah and V. Sharma, "Achieving Shannon capacity region as secrecy rate region in a multiple access wiretap channel", in *Proc. IEEE Wireless Commun. and Network. Conf. WCNC 2015*, New Orleans, LA, USA, 2015 (DOI: 10.1109/WCNC.2015.7127565).
- [24] R. Ahlswede, "Multi-way communication channels", in *Second International Symposium on Information Theory: Tsahkadsor, Armenia, U. S. S. R., September 2-8, 1971*, F. Csáki, B. N. Petrov, Eds. Budapest: Akademiai Kiado, 1973 [Online]. Available: https://pub.uni-bielefeld.de/download/1780371/2312888/Ahlswede_12.pdf
- [25] H. H.-J. Liao, "Multiple access channels", DTIC Document, Defense Tech. Inform. Center, Fort Belvoir, VA, Tech. Rep., 1972 [Online]. Available: <http://www.dtic.mil/docs/citations/AD0753127>
- [26] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free", in *Advances in Cryptology – EUROCRYPT 2000. International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, 2000, Proceedings*, B. Preneel, Ed. LNCS, vol. 1807, pp. 351–368. Springer, 2000 (DOI: 10.1007/3-540-45539-6_24).
- [27] E. Tekin and A. Yener, "Secrecy sum-rates for the multiple-access wire-tap channel with ergodic block fading", in *Proc. of 45th Ann. Allerton Conf. on Commun., Control and Comput.*, Monticello, IL, USA, 2007, vol. 2, pp. 856–863 (ISBN: 9781605600864).



Shahid Mehraj Shah received his B.Tech. in ECE from the National Institute of Technology, Srinagar, and Ph.D. from the Indian Institute of Science Bangalore, in 2008 and 2017, respectively. Since 2018, he has been working as an Assistant Professor at the Department of ECE at NIT Srinagar, where he leads the communication control and learning lab. His research interests include information theory, wireless communication, cyber-physical systems, machine learning.

His research interests include information theory, wireless communication, cyber-physical systems, machine learning.

 <https://orcid.org/0000-0002-8583-7904>

E-mail: shahid.nit@gmail.com

Communication Control & Learning Lab
 Department of Electronics and Communication Engineering
 National Institute of Technology
 Srinagar, Jammu and Kashmir, India